Célzott kibertámadások

Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2018

BODÓ ATTILA PÁL – CSER ORSOLYA ANIKÓ – GYARAKI RÉKA ESZTER – KACZUR GÁBOR – LATTMANN TAMÁS – SOLYMOS ÁKOS – SZABÓ ZSOLT MIHÁLY – TIKOS ANITA – VÁCZI DÁNIEL – ZÁMBÓ NÓRA

Nemzeti Közszolgálati Egyetem, Budapest

A hatályosított kiadvány
a **KÖFOP-2.1.1-VEKOP-15-2016-00001**
„A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése” című projekt
keretében jelent meg.

Szerkesztő:
Deák Veronika

Szerzők:
Dr. Bodó Attila Pál
Cser Orsolya Anikó
Dr. Gyaraki Réka Eszter
Kaczur Gábor
Dr. Lattmann Tamás
Solymos Ákos
Szabó Zsolt Mihály
Tikos Anita
Váczi Dániel
Dr. Zámbó Nóra

Szakmai lektor:
Dr. Muha Lajos

Olvasószerkesztő:
Császár-Biró Anna
Kiss Eszter

A kézirat lezárásának dátuma:
2019. március 6.

Kiadja:

Felelős kiadó:
Prof. Dr. Kis Norbert
Dékán

TARTALOM

1. BODÓ ATTILA PÁL – ZÁMBÓ NÓRA: ÚJDONSÁGOK A KIBERVÉDELMI SZABÁLYOZÁSBAN[1]

1.1. Bevezető gondolatok

Az elmúlt években világszerte egyre erősödnek a globális kibertérből[2] érkező fenyegetések, amelynek hatására fokozatosan növekszik a biztonsági események száma. Ezen események következtében Európában mind a nemzetállamoknak, mind az Európai Uniónak (a továbbiakban: EU) és intézményeinek megfelelő válaszlépéseket kell találnia az eseménykezelésre és a fenntartható biztonság megteremtését célzó intézkedések kiválasztására. A hatékony válaszlépések megjelenhetnek szabályozási, szervezeti, technológiai, gazdasági és társadalmi folyamatok mentén. Jelen jegyzetben az előzőekben említett folyamatok közül a szabályozási oldalt vizsgáljuk, amely alapvetően két szinten közelíthető meg. Az egyik az EU stratégia- és jogalkotása és az abból eredő, nemzetállami szinten megjelenő kötelezettségek köre, a másik az önálló, szuverén államok által végzett jogalkotási tevékenység. Utóbbi Magyarországon nem csak a fentiekben említett események hatása miatt aktuális, hanem amiatt is, hogy a 2013. július 1-jén hatályba lépett, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) idén ünnepli 5. születésnapját. Ezen okok alapján egyértelmű, hogy időszerű a jogszabály novelláris felülvizsgálata.

Jelen tananyag célja, hogy rövid áttekintést nyújtson a fent vázolt események hatására bekövetkezett – az uniós szabályozás változásain is alapuló – nemzeti jogalkotásra. Az áttekintés azonban nem lehet teljes körű néhány stratégiai alapvetés és a kibervédelem[3] főáramának számbavétele nélkül.

1.2. Stratégiai alapok

Jean-Claude Juncker az Európai Bizottság elnöke 2017. szeptember 13-i, az EU helyzetéről szóló évértékelő beszédében (a továbbiakban: Juncker beszéd) átfogó kiberbiztonsági csomag megvalósítását jelentette be, amely stratégiai szintű változásokat eredményez az unión belül. A évértékelésből érzékelhető, hogy az ezredfordulótól tapasztalt, egy-egy részterületre fókuszáló, elsősorban büntetőjogi szempontú megközelítést alkalmazó gondolkodásmódtól hosszú út vezetett az uniós és tagállami szintű együttműködést sürgető komplex megközelítésig. Jelen tananyagnak nem célja a részletes

---

1 A fejezet az *Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2018 – Célzott kibertámadások* című közszolgálati továbbképzési program szakanyagához készült (Bodó Attila Pál – Marsi Tamás – Sebők Viktória – Zámbó Nóra: *Célzott kibertámadások*. Budapest, Dialóg Campus Kiadó, 2018).

2 Globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese - az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 1. § (1) bekezdés 22. pontja.

3 Kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését – Ibtv. 1. § (1) bekezdés 27. pont.

történeti áttekintés, azonban a változások és az aktuális helyzet megismerése érdekében néhány mérföldkövet rögzíteni szükséges mind nemzetközi, mind nemzeti színtéren, mivel a stratégiai irányok kihatnak a nemzeti szintű jogi szabályozásra.

1.2.1 Európai Uniós irányok

Az Európai Tanács által 2003 decemberében elfogadott *Európai biztonsági stratégia – Biztonságos Európa egy jobb világban* című dokumentum elsőként rögzítette az EU biztonsági érdekeinek védelmét szolgáló alapelveket és célokat, a biztonsági kihívások között a kiberfenyegetés nevesítése azonban még elmaradt. A felülvizsgálatáról szóló 2008. évi jelentés már kiemelte a létfontosságú infrastruktúrák jelentőségét és a számítógépes biztonságot, valamint a tagállamok IT-rendszerei ellen elkövetett támadásokat mint esetleges új gazdasági, politikai és katonai fegyverként jelentkező fenyegetéseket.[4] A felülvizsgálat után egy évvel, 2009-ben adta ki az Európai Bizottság az *Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása*[5] ***című, a kritikus informatikai infrastruktúrák védelméről szóló közleményét (a továbbiakban: közlemény), amely uniós szintű politikai elképzelésként vázolja fel az információs társadalom védelmét és a társadalmi bizalom fokozását.***

A közlemény kritikai éllel kiemelte, hogy bár valamennyi tagállam közös célja az európai kritikus infrastruktúrák biztonságának garantálása, az egyes országok felkészültségi szintje és módszerei nagyon eltérőek, ezért a határon átnyúló, összehangolt együttműködés hiánya nem eredményez hatékony reagálást. Megoldási lehetőségként az európai szintű partnerség létrehozására tett javaslatot az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (a továbbiakban: ENISA) hatáskörének kiterjesztésével, amelyben az állami szereplők mellett a magánszektor képviselői is véleményformálók lehetnek. Emellett Európa korai figyelmeztető és reagáló képességének erősítéséhez jól működő számítástechnikai katasztrófaelhárító csoportok kialakítását és e területen már tapasztalattal és gyakorlattal rendelkező nemzetközi szervezetekkel való együttműködés fontosságát hangsúlyozta.

A 2008-as pénzügyi és gazdasági válság következményeire reagált a 2010-es *Europa 2020 foglalkoztatási és növekedési stratégia* (a továbbiakban: Europa 2020 stratégia),[6] amely rögzíti az EU intézményei, a tagállamok és a szociális partnerek intézkedéseit a következő tíz éves időszakra. Az Europa 2020 stratégia hét kiemelt kezdeményezése közül változást generáló célkitűzés az *Európai digitális menetrend* (a továbbiakban: EDM), amely a digitális technológia előnyeinek megismertetését és elérhetővé tételét célozza az európai polgárok és vállalkozások számára. Az EDM keretében tervezett szabályozási területet érintő intézkedések között szerepel az uniós adatvédelmi szabályozási keret felülvizsgálata, a fokozott interoperabilitás, illetve a bizalom és az internetes biztonság megerősítése. Utóbbi intézkedési területen az alábbi célok rendelkeznek – figyelemmel a Juncker beszédre – jelentőséggel:

a) javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra;

b) a számítógépes támadások elleni gyors reagálású európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok hálózatának létrehozása, az ENISA szerepének megerősítése.

Az Europa 2020 stratégia megjelenése hozzájárult ahhoz, hogy a kibervédelem témaköre egyre nagyobb érdeklődést váltott ki tagállami és az uniós döntéshozó szervek szintjén egyaránt. 2012-ben az Európai Parlament állásfoglalást adott ki *A kritikus informatikai infrastruktúrák védelme. Ered-*

4 Lásd: http://www.consilium.europa.eu/media/30811/qc7809568huc.pdf

5 Lásd: http://ec.europa.eu/transparency/regdoc/rep/1/2009/HU/1-2009-149-HU-F1-1.Pdf

6 Lásd: http://ec.europa.eu/eu2020/pdf/1_HU_ACT_part1_v1.pdf

mények és következő lépések: a globális kiberbiztonság felé című dokumentummal.[7] Ezen állásfoglalás hangsúlyozta az uniós intézmények és tagállamok együttműködésének, az információbiztonsági szabványok, protokollok és uniós szintű jogi normák megalkotásának, a tagállami kiberbiztonsági vészhelyzeti tervek elkészítésének és a nemzeti CERT-ek[8] közötti koordinációnak a szükségességét.

Látható, hogy az EU számos dokumentumot fogadott el az ezredfordulót követően, mégis a kiberbiztonság[9] átfogó megközelítését az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága által készített, *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* című uniós stratégiáról szóló, 2013-ban közzétett közös közleménye[10] rögzítette elsőként. Célként fogalmazta meg:

a) az információs rendszerek kibertámadásokkal szembeni ellenálló képességének megteremtését;
b) a kiberbűnözés drasztikus visszaszorítását;
c) a kibervédelmi politika kidolgozását és a közös biztonság- és védelempolitikát érintő képességek fejlesztését;
d) a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtését;
e) az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozását, valamint az alapvető uniós értékek terjesztését.

A felsorolt mérföldkövek eredményei és azok elmaradása vezetett oda, hogy az EU az együttműködést sürgető, komplex megközelítést tekintse stratégiai alapvetésnek. A bevezetőben említett Juncker beszéd 2018 egyik prioritásaként a kibertámadások elleni hatékonyabb védelem biztosítását jelölte meg.[11] A beszédet követően az Európai Bizottság javaslatot tett az EU informatikai támadásokkal szembeni ellenálló és reagáló képességének megerősítésére, amelyet az alábbi eszközrendszerrel kíván megvalósítani:

a) az ENISA átalakítása Uniós Kiberbiztonsági Ügynökséggé, amely források és feladatok tekintetében megerősítésre kerül, legfőbb feladata a tagállamok támogatása lesz a kiberbiztonsági irányelv végrehajtásában;
b) a tagállamok között átjárható, a határon átnyúló kereskedelmet segítő uniós szintű kiberbiztonsági tanúsítási keret létrehozása;
c) nagyszabású kiberbiztonsági eseményekre és válságokra való reagálásról szóló terv megalkotása, amely a tagállamok és az uniós intézmények együttműködését feltételezi. A tagállamokban bevonja a nemzeti hatóságokat, a számítógép-biztonsági eseményekre reagáló csoportokat (CSIRT) és a kiberbiztonsági ügynökségeket, európai szinten az ENISA, az Europol Számítástechnikai Bűnözés Elleni Európai Központja, az Európai Bizottság, az Európai Külügyi Szolgálat és annak válságkezelésért felelős szolgálatai, valamint a Tanács vesz részt a tevékenységben;
d) az Európai Kiberbiztonsági Kompetenciahálózat, valamint az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont kialakítása, amely az uniós és tagállami szintű kiberbiztonságot támogató erőforrások kialakítását támogatja új eszközök és technológiák kifejlesztésével és alkalmazásával;
e) a készpénz-helyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló új irányelv kodifikációja, az informatikai támadásokkal szembeni hatékonyabb büntetőjogi válasz kialakítása érdekében,
f) a rosszhiszemű kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretének[12] megerősítése;

---

7 Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012IP0237&qid=1521197299768&from=HU

8 CERT - Computer Emergency Response Team = úgynevezett Számítógépes Vészhelyzeti Reagáló Egység.

9 Kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez. - Ibtv. 1. § (1) bekezdés 26. pont.

10 Lásd: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu

11 Lásd: http://europa.eu/rapid/press-release_SPEECH-17-3165_hu.htm

12 Lásd: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf

g) a kiberbiztonsággal kapcsolatos nemzetközi együttműködés megerősítésére irányuló intézkedések meghozatala a globális kiberstabilitás megteremtése érdekében (például a NATO és az EU közötti szorosabb kiberbiztonsági együttműködés a kiberbiztonsági szerveik közötti információmegosztás, valamint a párhuzamos és összehangolt gyakorlatok révén).

1.2.2 Nemzeti stratégiák

Az Europa 2020 stratégiában megfogalmazottakra is figyelemmel, továbbá a magyarországi digitalizáció felgyorsítása és a hazai IKT szektor erősítése érdekében – a 2014-2020-as uniós költségvetési időszakhoz igazodva – elkészült a *Nemzeti Infokommunikációs Stratégia* 2014-2020[13] című dokumentum (a továbbiakban: Stratégia), amelynek elfogadásáról a Kormány a Magyarország Nemzeti Infokommunikációs Stratégiájáról szóló 1069/2014. (II. 19.) Korm. határozattal döntött. A kormányzat, az intézményi és a piaci szereplők együttműködését feltételező Stratégia négy pillére (Digitális infrastruktúra, Digitális kompetenciák, Digitális gazdaság és Digitális állam) mentén végzett helyzetelemzést és határozta meg a célokat, valamint a kapcsolódó eszközrendszert.

A Digitális állam pillérben tervezett intézkedések átfogó célja, hogy létrejöjjön egy stabil kormányzati és közigazgatási informatikai háttér, amely biztonságos módon támogatja a közigazgatás belső folyamatait, és egyúttal hozzájárul ahhoz, hogy a lakosság és a vállalkozások számára egyszerűbben, elektronizált módon elérhetővé váljon a közigazgatási szolgáltatások széles köre. Ez az általános irány az alábbi célrendszerben – és a kapcsolódó indikátorok mentén – kerül kidolgozásra:

a) stabil, biztonságos, valamint infrastrukturális és üzemeltetési szempontból egységes kormányzati IT-háttér megteremtése;
b) kormányzati ASP szolgáltatások kialakítása;
c) nyílt forráskódú alkalmazások arányának növelése;
d) elektronikus közigazgatás és elektronikus ügyintézés fejlesztése;
e) az állam által kötelezően nyújtandó szabályozott elektronikus ügyintézési szolgáltatások elérhetővé tétele;
f) jelentősebb állami nyilvántartások közötti interoperabilitás megvalósítása;
g) digitális adatvagyon hozzáférhetővé tétele.

A Stratégia mellett kiemelten fontos kormányzati döntés a Közigazgatás- és közszolgáltatás fejlesztési stratégiával kapcsolatos feladatokról szóló 1052/2015. (II. 16.) Korm. határozattal elfogadott Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia[14] (a továbbiakban: KKFS). A KKFS tovább hangsúlyozta és megerősítette a Stratégiában részletezett célrendszer fontosságát (közigazgatás belső folyamatainak elektronizálása, ügyfélközpontú közigazgatás, interoperabilitás), és a végrehajtása ellenőrzését célzó monitoring rendszerben olyan indikátorokat is megfogalmazott, amelyek a közigazgatás elektronizálását mérik:

a) átlagos ügyintézési időtartam (-20%),
b) adminisztratív terhek csökkenése (-20%),
c) elektronikusan intézhető ügyek aránya (+30%),
d) összekapcsolt adatbázisok aránya (80%).

A Stratégiában foglaltak végrehajtásához kapcsolódva és a négy pillér megvalósítása érdekében indult el 2014-ben a *Digitális Nemzet Fejlesztési Program,*[15] amelynek folytatása a jelenleg megva-

[13] Lásd: http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf

[14] Lásd: http://www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljeszt%C3%A9si_strat%C3%A9gia_.pdf

[15] A „Digitális Nemzet Fejlesztési Program” megvalósításáról szóló 1631/2014. (XI. 6.) Korm. határozat.

lósítás alatt álló, számos intézkedést tartalmazó *Digitális Jólét Program* (a továbbiakban: DJP) első[16] és második[17] üteme.

Fenti dokumentumok közös jellemzője, hogy az EU irányvonalaihoz igazodva és a Stratégia pilléreinek horizontális tényezőjeként rögzítik a *biztonság* fontosságát a szolgáltatók és felhasználók szintjén egyaránt.

A Biztonság célrendszerében a Stratégia és a KKFS az alábbiakat emeli ki:

a) kritikus információs infrastruktúrák, a közigazgatási belső rendszerek és külső alkalmazások, valamint az ezekben megjelenő felhasználói adatok védelme,
b) megfelelő szintű rendelkezésre állás és biztonsági paraméterek garantálása,
c) szemléletformálás, a lakosság átfogó tájékoztatása a valós biztonsági kockázatokról és megelőzésükről,
d) jogszabályi környezet felülvizsgálata,
e) számítógépes bűnözés visszaszorítása, gyermekek védelme.

A biztonságtudatosság, a biztonságos internethasználat és a gyermekek védelmének erősítése kiemelt elemként jelenik meg a DJP első ütemében elkészült Digitális Oktatási Stratégiában,[18] a Digitális Gyermekvédelmi Stratégiában[19] és azok intézkedési tervében. A DJP második ütemében konkrét intézkedések kerültek megfogalmazásra a kiberbiztonság területén is. A DJP2.0 Korm. határozat egyrészt rögzítette az 1139/2013. (III. 21.) Korm. határozattal közzétett Nemzeti Kiberbiztonsági Stratégia felülvizsgálatát, másrészt elrendelte továbbá:

a) egy, a tételes feladatokat és felelősöket rögzítő intézkedési terv elkészítését,
b) a biztonságtudatosság további erősítése érdekében az elektronikus információbiztonsági és kiberbiztonsági ismeretek beépítését a köznevelési és szakképzés tantervekbe,
c) olyan javaslat kidolgozását, amely a közigazgatási szervek és a vállalkozások elektronikus információbiztonsági és kiberbiztonsági tevékenységét támogatja,
d) a hazai kis- és középvállalkozások versenyképességének javítása érdekében kibervédelmi képességük felmérését és támogatását,
e) a közigazgatási és a rendvédelmi szervek kibervédelmi képességének felmérését, valamint
f) a jelenlegi jogszabályi környezet felülvizsgálata mellett a Juncker beszédben foglaltak figyelembe vételével a már létező kormányzati GovCERT mellett nemzeti kiberbiztonsági eseménykezelő központ létrehozását.

1.3. Az eu irányai, a nis hatása és a gdpr

A stratégiaalkotás szintjén már korábban megfigyelhető, az EU és a tagállamok összehangolt fellépését ösztönző javaslatok uniós jogi norma szintjén csak 2016-ban jelentek meg, az alábbiak szerint:

– az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (a továbbiakban: NIS irányelv),[20]

---

16 Az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról szóló 2012/2015. (XII. 29.) Korm. határozat.

17 A Nemzeti Infokommunikációs Stratégia 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről szóló 1456/2017. (VII. 19.) Korm. határozat (a továbbiakban: DJP2.0 Korm. határozat).

18 A köznevelési, a szakképzési, a felsőoktatási és a felnőttképzési rendszer digitális átalakításáról és Magyarország Digitális Oktatási Stratégiájáról szóló 1536/2016. (X. 13.) Korm. határozat..

19 A Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról szóló 1488/2016. (IX. 2.) Korm. határozat.

20 Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148&from=HU

– illetve az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) az Európai Unió Általános Adatvédelmi Rendelete[21] (angolul: General Data Protection Regulation, a továbbiakban: GDPR).[22]

1.3.1 NIS irányelv

A NIS irányelv[23] a belső piac működése szempontjából alapvetőnek tartja a hálózati és információs rendszerek és szolgáltatások megbízhatóságát, biztonságát. Célja, hogy a tagállamoknak a biztonsági események megelőzése és kezelése terén tapasztalható eltérő felkészültségében egyenszilárdságot teremtsen a közös minimumszabályok megalkotásával. A biztonsági intézkedések tekintetében egy átfogó, ugyanakkor differenciált megközelítést alkalmaz az alanyi hatály, valamint a kapcsolódó jogok és kötelezettségek meghatározásakor.

A NIS irányelv hatálya alá tartozó alanyi kör magában foglalja *az alapvető szolgáltatásokat nyújtó szereplőket* és a *digitális szolgáltatókat,* amelyek biztonságos, folyamatos és megbízható működése elengedhetetlen a fenntartható biztonság megteremtéséhez.

*Alapvető szolgáltatásokat nyújtó szereplő*nek minősül az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és -elosztás, valamint a digitális infrastruktúra ágazatában működő – tagállami szinten kijelölt – közjogi vagy magánjogi szervezet, amely megfelel az alábbi kritériumoknak:[24]

a) a szervezet a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt;
b) az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ;
c) az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában.

A hatálya tehát csak azon alapvető szolgáltatásokat nyújtó szereplőre vonatkozik, amelyek kiesése komoly társadalmi vagy gazdasági károkat okozna.

*Digitális szolgáltató*nak minősül a NIS irányelv szempontjából minden digitális szolgáltatást nyújtó szereplő, amelynek szolgáltatása ugyan nem nélkülözhetetlen, de társadalmi szempontból kiemelt jelentőséggel bír. Digitális szolgáltatás az online piactér, az online keresőprogram és a felhőalapú számítástechnikai szolgáltatás, de a közösségi szolgáltatást nyújtók nem tartoznak a szabályozás hatálya alá.[25]

A NIS irányelv védett jogi tárgya az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók hálózati és információs rendszere,[26] amely:

a) a 2002/21/EK irányelv[27] 2. cikkének a) pontja szerinti elektronikus hírközlő hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt, vagy kapcsolatban álló eszközök cso-

---

21 A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679 rendelet.

22 Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=EN

23 A NIS irányelv 2016. augusztus 8-án lépett hatályba. Az irányelv az uniós jogi norma sajátosságából adódóan az elérendő célt tekintve valamennyi címzett tagállamot kötelez, de a tagállamok szabadon dönthetnek arról, hogy az uniós szabályok milyen módszerek és eszközök révén válnak a nemzeti jog részévé. A rendelkezések átültetési határideje 2018. május 9, amely azt jelenti, hogy ezen időpontig köteles minden tagállam a vonatkozó jogi környezetet áttekinteni és összhangba hozni az irányelv előírásaival.

24 NIS irányelv 4. cikk, 4 pont; 5. cikk, 2. pont.

25 NIS 4. cikk, 6. pont, III. melléklet.

26 NIS 4. cikk, 1. pont.

27 Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról.

portja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) az általuk működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

A NIS irányelv az alanyi kör pontos körülírása mellett meghatározza a hálózati és információs rendszerek biztonságára vonatkozó nemzeti kereteket, a határon átnyúló együttműködési formákat, valamint az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók hálózati és információs rendszereinek biztonsága érdekében szükséges lépéseket. Ennek érdekében:

a) valamennyi tagállam számára kötelezettségként rögzíti a hálózati és információs rendszerek biztonsága nemzeti stratégiájának elfogadását és rögzíti annak főbb tartalmi elemeit;[28]
b) előírja egy vagy több nemzeti hatóság kijelölését, amely felügyeli a NIS irányelv átültetését és végrehajtását;[29]
c) előírja egy olyan, a hálózati és információs rendszerek biztonságáért felelős nemzeti egyedüli kapcsolattartó pont megnevezését, amely összekötő feladatokat lát el a tagállami hatóságok és más tagállamok, továbbá az unió illetékes intézményei felé;[30]
d) előírja annak meghatározását, hogy ágazatonként milyen kritériumok alapján kerül egy-egy szolgáltató az irányelv hatálya alá, és ezt követően ezen szolgáltatók (az alkalmazás időpontjától számított hat hónapon belüli) kijelölését;
e) biztonsági és bejelentési követelményeket állapít meg az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára;[31]
f) létrehoz egy együttműködési csoportot a tagállamok, az Európai Bizottság és az ENISA képviselőivel a tagállamok közötti stratégiai együttműködés, tapasztalat- és információcsere támogatása és elősegítése céljából;[32]
g) létrehozza a nemzeti számítógép-biztonsági eseményekre reagáló csoportok, a CSIRT-ek hálózatát a tagállamok közötti bizalom erősítéséhez való hozzájárulás, valamint a gyors és hatékony operatív együttműködés előmozdítása céljából, és leírja a CSIRT-ek hálózatának feladatait[33].

Fenti megfelelés érdekében került sor az Ibtv. és végrehajtási rendeleteinek a 4. pontban ismertetett módosítására.

1.3.1 Az Általános Adatvédelmi Rendelet

Míg a NIS irányelv szabályozásának célcsoportját a szolgáltatók képezik és elsődleges célja a hálózatbiztonság megteremtése, addig a GDPR rendelet[34] fókuszában a természetes személyek, mint felhasználók állnak, illetve a személyes adatok és a magánszféra védelmét szolgáló rendelkezéseket tartalmazza. A

28 NIS irányelv 7. cikk.
29 NIS irányelv 8. cikk.
30 NIS irányelv 8. cikk.
31 NIS irányelv 14-17. cikk.
32 NIS irányelv 11. cikk.
33 NIS irányelv 12. cikk.
34 Az Általános Adatvédelmi Rendelet 2018. május 25-én lép hatályba. Olyan uniós jogi norma, amely teljes egészében kötelező és közvetlenül alkalmazandó, implementációs kötelezettség nélkül a nemzeti jog részévé válik, és felváltja a rendeletben foglalt szabályokkal összhangba nem hozható tagállami rendelkezéseket.

GDPR az EU adatvédelmi reformja részeként a személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 95/46/EK irányelvet váltja fel. Az adatvédelmi reform a személyes adatok védelme és az információbiztonsági követelmények egységesen magas szintjét és koherenciáját kívánja megteremteni, ezáltal is növelve a felhasználói bizalmat az online felületek és digitális szolgáltatások iránt.

A GDPR a személyes adatok kezeléséből már ismert alapelveknek (jogszerűség, tisztességes eljárás és átláthatóság, célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság, integritás és bizalmas jelleg) való megfelelés mellett rögzíti az adatkezelő számára az elszámoltathatóság alapelvét is. Utóbbi alapelv lényege, hogy az adatkezelő felelőssége, hogy biztosítsa az érintettnek a személyes adatok megfelelő védelméhez fűződő alapvető jogát a belső szabályzóiban és folyamataiban, és ezt bármikor megfelelő módon igazolni is tudja a felügyeleti hatóság irányába[35]. Az új szabályozás szerint nem elvárás az adatkezelés adatvédelmi hatósághoz történő bejelentése, azonban mind az adatkezelő, mind az adatfeldolgozó részéről felmerül a naprakész nyilvántartás vezetési kötelezettség, valamennyi általa végzett adatkezelési tevékenységről.[36]. Ehhez elsőként a szerveknek fel kell mérniük, hogy milyen adatokat, milyen célból és milyen módon kezelnek, azaz adatvagyon leltárt kell készíteniük és azt naprakészen kell tartaniuk, hogy ezzel is igazolni tudják az adatkezelés jogszerűségét az elszámoltathatóság elvének megfelelően.

A GDPR rögzíti a beépített adatvédelem elvét[37] is, amely szerint az adatkezelőnek az adatkezelés módjának meghatározásakor és az adatkezelés teljes folyamata során figyelemmel kell lennie a tudomány és technológia állására, a megvalósítás költségeire, az adatkezelés jellegére, hatókörére, körülményeire és céljaira, valamint a személyes adatok kezelésével járó kockázatokra, és ez alapján kell meghatároznia az adatkezelés módját, illetve megtennie azokat a technikai és szervezési intézkedéseket (például álnevesítés), amelyek a követelmények maradéktalan betartását segítik elő.

Bizonyos feltételek megléte esetén a GDPR biztosítja az érintett számára az adathordozhatóságot,[38] amely szerint az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban (ez az adatkezelő oldaláról azt a kötelezettséget eredményezi, hogy rendelkeznie kell az ilyen módon történő adatátadás műszaki, technikai feltételeivel) megkapja, és ezeket az adatokat egy másik adatkezelőnek továbbítsa.

Ugyancsak az érintettnek a személyes adatai felett meglévő rendelkezési jogát erősíti az „elfeledtetéshez" való jog.[39] Ennek megfelelően – adott esetekben – az érintett kérheti, hogy az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, amely teljesítésére az adatkezelő köteles. Emellett ha az adatkezelő nyilvánosságra hozta a személyes adatot és a törlési kötelezettség feltételei fennállnak, az adatkezelő az elérhető technológia és a megvalósítás költségeinek figyelembevételével köteles megtenni az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében is, hogy tájékoztassa az adatokat kezelő többi adatkezelőt, hogy azok is töröljék és tegyék elérhetetlenné az adatokat (ide értve a személyes adatokra mutató linkek vagy e személyes adatok másolatát, illetve másodpéldányát is).

A GDPR szabályozza az adatvédelmi hatásvizsgálat[40] intézményét és azt, hogy mely esetekben szükséges különösen ezen hatásvizsgálat elvégzése. Az adatkezelőnek adatvédelmi hatásvizsgálatot akkor kell végeznie az adatkezelés megkezdése előtt, ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Az adatvédelmi hatásvizsgálat annak feltárására irányul, hogy a tervezett adatkezelés miként érinti a személyes adatok védelmét.

A jelenleginél szélesebb körben teszi kötelezővé a GDPR az adatvédelmi tisztviselő[41] kijelölését, amelyet meg kell tenni:

35 GDPR 5. cikk.
36 GDPR 30. cikk.
37 GDPR 25. cikk.
38 GDPR 20. cikk.
39 GDPR 17. cikk.
40 GDPR 35. cikk.
41 GDPR 37. cikk.

a) az adatkezelést végző közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek esetében;
b) olyan adatkezelést vagy adatfeldolgozást végző szervnél, ahol a fő tevékenységek olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé (például profilozás);
c) abban az esetben, ha az adatkezelő vagy adatfeldolgozó különleges személyes adatokat kezel.

Az adatvédelmi incidensek bejelentésének kötelezettsége[42] a GDPR szerint valamennyi adatkezelő számára kötelező. A kockázattal járó adatvédelmi incidenst indokolatlan késedelem nélkül, de legkésőbb az adatkezelő tudomására jutását követő 72 órán belül be kell jelenteni a felügyeleti hatóságnak. Ha az adatvédelmi incidens a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal jár, az adatkezelő indokolatlan késedelem nélkül köteles az érintetteket is tájékoztatni.

A GDPR fenntartja a közigazgatási bírság[43] kiszabásának lehetőségét az adatkezelő és az adatfeldolgozó vonatkozásában egyaránt, mértékére két kategóriát határoz meg, rögzítve, hogy mely jogsértések melyik kategóriába tartoznak:

a) az enyhébb jogsértések esetén a bírság maximális mértéke 10 millió euró, vagy személyes adatot kezelő szervezetek esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeg azzal, hogy a kettő közül a magasabb összeget kell kiszabni,
b) súlyosabb jogsértések esetén a maximálisan kiszabható bírság mértéke 20 millió euró, vagy személyes adatot kezelő szervezetek esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeg azzal, hogy a kettő közül a magasabb összeget kell kiszabni.

A GDPR alapján[44] az Európai Adatvédelmi Testület, illetve a nemzeti adatvédelmi hatóságok iránymutatásokat, ajánlásokat bocsáthatnak ki a nem szabályozott kérdések értelmezése, alkalmazása kapcsán, így joggal várható, hogy az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény további előírásokkal kerül pontosításra a 2018. évi őszi jogalkotás során.

1.4. Változások a nemzeti jogban

Az előzőekben ismertetett uniós és nemzeti stratégiai törekvések, valamint joganyagok meghatározták a nemzeti jogalkotás irányultságát, így az öt éves Ibtv. novelláris felülvizsgálata még várat magára. A törvényi szintű módosítás az elmúlt időszakban minimális volt, markánsabb változások a végrehajtási rendeletek szintjén jelentek meg, amelyeket elsősorban az uniós hatás indokolt, főként a NIS irányelv átültetési kötelezettségéből keletkezően.

1.4.1 Az Ibtv. változása

Az Ibtv. módosítására az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési törvény) 2018. január 1-jétől történő kötelező alkalmazásával összefüggően került sor. A módosítás a Nemzeti Elektronikus Információbiztonsági Hatóság[45] (a továbbiakban: Hatóság) feladataként írja elő az Elektronikus Ügyintézési

42 GDPR 33. cikk.
43 GDPR 83. cikk.
44 GDPR 70. cikk g) és h) pontja.
45 Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 187/2015. (VII. 13.) Korm. rendelet (a továbbiakban: 187/2015. (VII. 13.) Korm. rendelet) 1. § 3. pontja.

Felügyelettel[46] való együttműködést a szabályozott elektronikus ügyintézési szolgáltatás[47] szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében.[48] E rendelkezés kapcsolódik a stratégiai szinten megjelenő együttműködési kötelezettség igényéhez.

További módosítás a 2018. január 1-jén hatályba lépő, az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban. Ákr.) által bevezetett eljárási rendhez kapcsolódik, amely szerint a Hatóság eljárásaiban az ügyfél értesítése az eljárás megindításáról mellőzhető, illetve a Hatóság által elrendelt szakértői eljárásban a szervezet közreműködési kötelezettségét írja elő.[49] Az Ákr.-rel összefüggő további módosítása az Ibtv.-nek, hogy a zárt célú és honvédelmi célú elektronikus információs rendszerek hatósági feladatainak ellátására kijelölt szervnek a véglegessé vált határozata az ügyfélen és az Ákr. alapján iratbetekintésre jogosult személyen[50] kívül más számára nem ismerhető meg.

A NIS irányelvnek való megfelelés céljából jogharmonizációs klauzula beépítésére is sor került az Ibtv-be, amely 2018. május 10-től hatályos.[51]

1.4.2 A végrehajtási rendeletek változásai

Az Ákr. hatálybalépésével a hatósági nyilvántartások vezetésére vonatkozó szabályok felülvizsgálata is megtörtént, így az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény hatálybalépésével összefüggésben egyes belügyi tárgyú miniszteri rendeletek módosításáról, valamint egyes belügyi tárgyú miniszteri rendeletek módosításáról és hatályon kívül helyezéséről szóló 44/2017. (XII. 29.) BM rendelet 2018. január 1-jével hatályon kívül helyezte a hatósági nyilvántartásba vétel rendjéről szóló 42/2015. (VII. 15.) BM rendeletet. Ez a rendelet az Ibtv. 15. § (1) bekezdése szerinti adatokat tartalmazó hatósági nyilvántartásba vételre vonatkozó részletszabályokat tartalmazta, amely deregulálásával a részletszabályok átkerültek az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendeletbe.[52] Meg kell jegyezni, hogy a 42/2015. (VII. 15.) BM rendelet megalkotására felhatalmazást adó rendelkezést, az Ibtv. 24. § (3) bekezdését az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról szóló 2015. CXXX. törvény 8. § (40) bekezdés j) pontja már 2015. július 16-án hatályon kívül helyezte.

A NIS irányelvnek való megfelelés céljából jogharmonizációs klauzula beépítésével került sor:

a) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet;[53]
b) a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.)

---

46 Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban. E-ügyintézési tv.) 1. § 18. pontja.

47 E-ügyintézési törvény 29. §.

48 Ibtv. 14. § (2) bekezdés h) pont.

49 Ibtv. 14. § (3b) bekezdés.

50 Harmadik személy akkor tekinthet be a személyes adatot vagy védett adatot tartalmazó iratba, ha igazolja, hogy az adat megismerése joga érvényesítéséhez, illetve jogszabályon, bírósági vagy hatósági határozaton alapuló kötelezettsége teljesítéséhez szükséges. - Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény 33. § (3) bekezdés.

51 Ibtv. 29. §.

52 187/2015. (VII. 13.) Korm. rendelet 4/A. A hatóság regisztrációs eljárása és a hatósági nyilvántartásba vétel alcíme.

53 41/2015. (VII. 15.) BM rendelet 7. §-a, hatályos 2018. május 10-től.

Korm. rendelet[54] (a továbbiakban: 185/2015. (VII. 13.) Korm. rendelet),

c) az előzőt hatályon kívül helyező, az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet[55] (a továbbiakban: 271/2018. (XII. 20.) Korm. rendelet), valamint

d) az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet[56] (a továbbiakban: 187/2015. (VII. 13.) Korm. rendelet),

módosítására.

A NIS irányelvnek való megfeleltetéshez kapcsolódóan a 187/2015. (VII. 13.) Korm. rendelet – a megfeleltetési klauzula mellett – több helyen is módosításra került. A Hatóság feladatai[57] között előírták, hogy:

a) együttműködési kötelezettség terheli a hálózati és információs rendszerek biztonságáért felelős nemzetközi szervekkel, így különösen az Európai Unió e feladatra létrehozott Együttműködési csoportjával, valamint

b) a hálózati és információs rendszerek biztonságáért felelős nemzetközi szervezetekben ellátja Magyarország képviseletét.

További a NIS irányelvhez kapcsolódó, 2018. május 10-én hatályba lépő módosítás[58] a Hatóság számára újabb feladatok ellátását írja elő. Ezek közé tartozik, hogy a Hatóság:

a) ellátja a NIS irányelv szerinti egyedüli kapcsolattartó pont feladatait, amelynek keretében biztosítja a hatóságok és az érintett EGT tagállamok hatóságai közötti együttműködést;

b) ellátja a hatáskörébe tartozó elektronikus információs rendszerek esetében a NIS irányelvnek megfelelően azonosított alapvető szolgáltatásokat nyújtó vagy bejelentés-köteles szolgáltatást nyújtóként azonosított szolgáltatók[59] elektronikus információs rendszerei esetében a megfelelés vizsgálatával összefüggő adatokat, valamint a vizsgálat eredményét megküldi az Európai Bizottság részére;

c) együttműködik a NIS irányelvnek való megfelelés vizsgálata érdekében a kormányzati eseménykezelő központtal;

d) megküldi Magyarország vonatkozásában az Európai Bizottság részére a NIS irányelv szerinti nemzeti stratégiát;

e) tájékoztatja az érintett EGT tagállamokat a biztonsági eseményről, ha a biztonsági esemény az adott tagállamban jelentős zavart okozott a szolgáltatás nyújtásában, illetve az Együttműködési csoport részére összefoglaló jelentést küld e biztonsági eseményekről; valamint

f) konzultációt folytat és együttműködik a rendvédelmi szervekkel, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

A b) pont szerinti tájékoztatás keretében az Európai Bizottság részére megküldött adatok köre[60] a következő:

a) az alapvető szolgáltatásokat nyújtó szereplők azonosítását lehetővé tevő nemzeti intézkedések;

b) a NIS irányelv szerinti kritikus társadalmi, gazdasági tevékenységek fenntartásához nyújtott alapvető szolgáltatások jegyzéke;

c) az alapvető szolgáltatásokat nyújtó szereplők száma, valamint az érintett ágazat szempontja szerinti jelentőségük;

---

54 185/2015. (VII. 13.) Korm. rendelet 23. §-a hatályos 2018. május 10-től.

55 271/2018. (XII. 20.) Korm. rendelet 31. §-a hatályos 2019. január 2-től.

56 187/2015. (VII. 13.) Korm. rendelet 31. §-a, hatályos 2018. május 10-től.

57 187/2015. (VII. 13.) Korm. rendelet 6. § (1) bekezdés, hatályos 2018. május 10-től.

58 187/2015. (VII. 13.) Korm. rendelet 6. § (1) bekezdés i)–n) pont, hatályos 2018. május 10-től.

59 NIS irányelv.

60 187/2015. (VII. 13.) Korm. rendelet 6. § (1a) bekezdés, hatályos 2018. május 10-től.

d) az adott szolgáltatásra támaszkodó felhasználók száma, vagy az alapvető szolgáltatásokat nyújtó gazdasági szereplő ellátási szintje;
e) az információbiztonságra vonatkozó nemzeti rendelkezések megsértése esetén alkalmazandó szankciókat tartalmazó szabályok és módosításai; valamint
f) a 185/2015. (VII. 13.) Korm. rendelet szerinti CSIRT-ek[61] hatásköréről, valamint a biztonsági események kezelésére szolgáló eljárásról szóló tájékoztatás.

A NIS irányelvvel összefüggésben a 187/2015. (VII. 13.) Korm. rendelet 2018. május 10-től az alapvető szolgáltatásokat nyújtó szereplővé kijelölt szereplők hálózati és információs rendszerei biztonságának felügyeletét ellátó hatóságként – a kijelölt létfontosságú rendszerek és létesítmények információbiztonsági hatóságaként eljáró – Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságot (a továbbiakban: BM OKF) jelöli ki.[62] A módosítás a BM OKF feladataként nevesíti az alábbiakat:[63]

a) Az alapvető szolgáltatásokat nyújtó szereplők elektronikus információs rendszereit érintő biztonsági esemény bekövetkezése esetén:
   aa) a nyilvánosság saját honlapon történő tájékoztatása, illetve
   ab) a szolgáltatók határozatban történő kötelezése a tájékoztatásra, ha saját mérlegelése szerint a biztonsági esemény nyilvánosságra hozatalának hiánya a közérdeket sértené vagy veszélyeztetné.
b) A Hatóság tájékoztatása a fentiekben részletezett, az Európai Bizottság részére megküldött adatok rendelkezésre állása érdekében:
   ba) az alapvető szolgáltatásokat nyújtó szereplők azonosítását lehetővé tevő nemzeti intézkedésekről,
   bb) a NIS irányelv szerinti kritikus társadalmi, illetve gazdasági tevékenységek fenntartásához nyújtott alapvető szolgáltatások jegyzékéről,
   bc) az alapvető szolgáltatásokat nyújtó szereplők jegyzékéről, valamint az érintett ágazat szempontja szerinti jelentőségükről,
   bd) az adott szolgáltatásra támaszkodó felhasználók számáról, vagy az alapvető szolgáltatásokat nyújtó gazdasági szereplő ellátási szintjéről.

A 187/2015. (VII. 13.) Korm. rendelet további módosítása az E-ügyintézési törvény végrehajtásához kapcsolódik, amellyel összefüggésben az értelmező rendelkezések körében bevezetésre került az elektronikus űrlap[64] fogalma. További módosítás 2018. január 1-től a szervezet[65] fogalmának átvétele az Ibtv-ből, illetve a hatósági nyilvántartás[66] fogalmának bevezetése a fentiekben említett 42/2015. (VII. 15.) BM rendelet hatályon kívül helyezéséhez kapcsolódóan. A hatósági nyilvántartásba vétellel összefüggő szabályozás – ahogy fentebb már említettük – új alcímben[67] jelenik meg a 187/2015. (VII. 13.) Korm. rendeletben, amely kapcsolódik az E-ügyintézési törvény végrehajtásához is. Ezen rendelkezések rögzítik,[68] hogy:

a) a szervezet és az elektronikus információs rendszer biztonságáért felelős személy jogszabályban előírt adatait a Hatóság részére biztonságos elektronikus kézbesítés útján, ennek hiányában postai úton kell bejelenteni;
b) a szervezet regisztrációját követően adatbejelentés vagy adatváltozás – utóbbi a változást követő 8 napon belül – csak regisztrált szervezet nevében az alábbiak szerint tehető meg:

---

61 CSIRT: számítógép-biztonsági eseményekre reagáló csoport. E rendelet 2. és 6. §-ai szerinti eseménykezelő központok CSIRT-nek minősülnek. - 185/2015. (VII. 13.) Korm. rendelet 1. § 15. pont - hatályos 2018. május 10-től.

62 187/2015. (VII. 13.) Korm. rendelet 25. § (1) bekezdés, hatályos 2018. május 10-től.

63 187/2015. (VII. 13.) Korm. rendelet 25. § (4) bekezdés, hatályos 2018. május 10-től.

64 Elektronikus űrlap: a hatóság által biztosított és közzétett, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet 2. § 2. pontja szerint meghatározott elektronikus űrlap - 187/2015. (VII. 13.) Korm. rendelet 1. § 4. pont.

65 Szervezet: az Ibtv. 2. § (1) és (2) bekezdésében – az Ibtv. 2. § (3)–(6) bekezdése szerinti információs rendszert üzemeltető szervezet kivételével – meghatározott szervezet, - 187/2015. (VII. 13.) Korm. rendelet 1. § 5. pont.

66 Hatósági nyilvántartás: a hatóság által vezetett, az Ibtv. 15. § (1) bekezdése szerinti adatokat tartalmazó nyilvántartás - 187/2015. (VII. 13.) Korm. rendelet 1. § 6. pont.

67 187/2015. (VII. 13.) Korm. rendelet 4/A. A hatóság regisztrációs eljárása és a hatósági nyilvántartásba vétel alcíme.

68 187/2015. (VII. 13.) Korm. rendelet 10/A. – 10/D. §-ok.

ba) a Hatóság által az elektronikus tájékoztatás szabályai szerint közzétett elektronikus űrlappal, amelyet a hatóság elektronikus adatbejelentési felületén keresztül kell megküldeni,

bb) az űrlapot és mellékleteit a Hatóság tartalmilag ellenőrzi, megfelelés esetén a bejelentett adatokat nyilvántartásba veszi és elektronikus úton erről értesítést küld, vagy hiányosság esetén hiánypótlást ír elő;

c) az a) pont szerinti elektronikus adatközlés mellett a hatóság elektronikus adatbejelentési felületén keresztül meg kell küldeni az informatikai biztonsági szabályzatot és a Hatóság által meghatározott és közzétett formátumban be kell jelenteni:

ca) a szervezet elektronikus információs rendszereinek bejelentés időpontja szerinti biztonsági osztályát, az ehhez kapcsolódóan meghatározott fizikai, logikai és adminisztratív védelmi intézkedéseknek való megfeleléseket,

cb) a szervezet vagy szervezeti egység bejelentés időpontja szerinti biztonsági szintjét, az ehhez kapcsolódóan meghatározott védelmi intézkedéseknek való megfeleléseket.

Az Ákr.-rel összefüggő módosítása a 187/2015. (VII. 13.) Korm. rendeletnek a hatósági eljárásra vonatkozó általános rendelkezések változása, amely szerint a Hatóság eljárása során a kérelem kormányablaknál való előterjesztése kizárt, illetve hiánypótlás esetén kétszeri felszólítással élhet a Hatóság.[69]

A 185/2015. (VII. 13.) Korm. rendelet módosítására szintén a NIS irányelvvel összhangban került sor, amely alkalmával az értelmező rendelkezések közé bekerült a CSIRT fogalmi meghatározása.[70]. Ilyen csoportnak minősül a kormányzati eseménykezelő központ[71] (a továbbiakban: GovCert), az Információs Hivatal szervezeti keretén belül működő eseménykezelő központ (IntCERT), a BM OKF keretein belül működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (a továbbiakban: LRLIBEK), valamint a honvédelemért felelős miniszter irányítása, vezetése alatt álló eseménykezelő központok. A módosítás a GovCert feladatkörét kiegészítette azzal, hogy a biztonsági események és fenyegetések kezelésével összefüggésben előírta:

a) a magyar és a nemzetközi hálózatbiztonsági szervekkel, így különösen az Európai Unió számítógép-biztonsági eseményekre reagáló csoportjával,

b) az iparági szereplőkkel, valamint

c) a Hatósággal

való együttműködés kötelezettségét.[72]

Rögzítette továbbá, hogy a GovCert:

a) részt vesz a CSIRT-ek hálózatának tevékenységében, amelynek keretében ellátja a többi eseménykezelő központ képviseletét,[73]

b) jogosult az LRLIBEK-től a jelentős hatást gyakorló biztonsági eseményekről tájékoztatást kérni, amely alapján tájékoztatja a többi tagállamot és vizsgálja az alapvető, valamint a bejelentés-köteles szolgáltatást nyújtók szolgáltatásaira jelentős hatást gyakorló biztonsági események határon átnyúló hatását.[74]

A BM OKF-et mint a létfontosságú rendszerelemmé kijelölt rendszerelemek elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelésére kijelölt szervezetet,[75] 2018. május 10-től a NIS irányelvvel összhangban az alábbi kötelezettségek terhelik:

a) felelős a biztonsági eseményekre történő reagálásért, ennek érdekében információt kérhet a hatáskörébe tartozó szervektől,

b) dinamikus kockázat- és eseményelemzéseket, valamint a biztonsági eseményekkel kapcsola-

69 187/2015. (VII. 13.) Korm. rendelet 3. §, 25. § (6)-(7) bekezdés.

70 185/2015. (VII. 13.) Korm. rendelet 1. § 15. pont - hatályos 2018. május 10-től.

71 Ibtv. 19. §.

72 185/2015. (VII. 13.) Korm. rendelet 3. § (1) bekezdés h-j) pontok - hatályos 2018. május 10-től.

73 185/2015. (VII. 13.) Korm. rendelet 5. § (2) bekezdés e) pont - hatályos 2018. május 10-től.

74 185/2015. (VII. 13.) Korm. rendelet 5/A. § - hatályos 2018. május 10-től.

75 185/2015. (VII. 13.) Korm. rendelet 6. § (3) bekezdés - hatályos 2018. május 10-től.

tos helyzetképet készít,

c) felelős a kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatásért, korai előrejelzéséért, koordinációért,
d) a hatáskörébe tartozó elektronikus információs rendszerek tekintetében – a GovCert útján – részt vesz az EU számítógép-biztonsági eseményekre reagáló csoportjának tevékenységében
e) a CSIRT szolgáltatási, operatív és együttműködési képességeivel kapcsolatos információkat átadjaa GovCert részére.[76]

A BM OKF az észlelt, valamint a tudomására jutott biztonsági eseményekről haladéktalanul tájékoztatja a GovCertet, amely tájékoztatásnak tartalmaznia kell:[77]

a) a biztonsági esemény által érintett felhasználók számát,
b) a biztonsági esemény időtartamát,
c) a biztonsági esemény által érintett terület földrajzi kiterjedését,
d) a szolgáltatás működésében támadt zavar mértékét,
e) a gazdaságra és társadalomra gyakorolt hatás mértékét.

Az a)-e) pontokban felsorolt információk alapján a BM OKF-et a GovCert felé a határon átnyúló hatások jelentőségének vizsgálata érdekében tájékoztatási kötelezettség terheli az alapvető, valamint a bejelentés-köteles szolgáltatást nyújtók szolgáltatásaira jelentős hatást gyakorló biztonsági eseményekről. Emellett tájékoztatni köteles a Hatóságot, mint egyedüli kapcsolattartó pontot a biztonsági események kezelésére vonatkozó, jogszabályban nem részletezett eljárásrendjéről.[78]

Fenti módosítások a Hatóság és az eseménykezelő központok tekintetében mind a Juncker beszéd, mind az uniós és nemzeti stratégiai irányokhoz igazodnak, az együttműködést és a fenntartható biztonságot erősítik.

A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet 2018. január 1-jei módosítása az Ibtv. 24. § (1) bekezdés g) pontjában kapott felhatalmazás alapján, az elektronikus közigazgatási és a nemzeti stratégiából levezethető követelmények teljesítéséhez kapcsolódik. A módosítás szerint a Nemzeti Infokommunikációs Szolgáltató Zrt. mint központi szolgáltató köteles a Kormányzati Adatközpont révén nyújtott szolgáltatásai körében az azt igénylő ügyfelei számára biztosítani a korai figyelmeztető rendszerhez való kapcsolódást az ahhoz szükséges műszaki feltételek megteremtésével és fenntartásával.[79] A részletszabályokat a Kormányzati Adatközpont működéséről szóló 467/2017. (XII. 28.) Korm. rendelet tartalmazza.

Az információbiztonságot érintő jogszabályok 2018 végén újabb változtatásokon mentek keresztül, tovább központosítva a magyar kibervédelem intézményrendszerét. A 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól a Nemzetbiztonsági Szakszolgálatot jelölte ki eseménykezelő központnak, így az LRLIBEK eseménykezeléssel kapcsolatos feladatköre átkerült az NBSZ-en belül működő Nemzeti Kibervédelmi Intézethez.

További fontos változás a 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról kiadása, mely ágazati stratégiának minősül ugyan, de fontos kiegészítése Magyarország Nemzeti Kiberbiztonsági Stratégiájának. A következő

[76] 185/2015. (VII. 13.) Korm. rendelet 6. § (3a)-(3b) bekezdései - hatályos 2018. május 10-től.
[77] 185/2015. (VII. 13.) Korm. rendelet 6. § (3c) bekezdése - hatályos 2018. május 10-től.
[78] 185/2015. (VII. 13.) Korm. rendelet 6. § (3d)-(3e) bekezdései - hatályos 2018. május 10-től.
[79] A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet 2/A. §.

években ez a két stratégia együttesen jelöli ki Magyarország kibertéri feladatainak irányát.

1.5. Irodalomjegyzék

1. Európai Biztonsági Stratégia – Biztonságos Európa egy jobb világban
Elérhetőség: http://www.consilium.europa.eu/media/30811/qc7809568huc.pdf (utolsó letöltés: 2018. március 31.)
2. A Bizottság közleménye a kritikus informatikai infrastruktúrák védelméről – „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása
Elérhetőség: http://ec.europa.eu/transparency/regdoc/rep/1/2009/HU/1-2009-149-HU-F1-1.Pdf (utolsó letöltés: 2018. március 31.)
3. EURÓPA 2020 – Az intelligens, fenntartható és inkluzív növekedés stratégiája Elérhetőség: http://ec.europa.eu/eu2020/pdf/1_HU_ACT_part1_v1.pdf (utolsó letöltés: 2018. március 31.)
4. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér:
Elérhetőség: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (utolsó letöltés: 2018. március 31.)
5. Jean-Claude Juncker elnök beszéde – Az Unió helyzete (2017)
Elérhetőség: http://europa.eu/rapid/press-release_SPEECH-17-3165_hu.htm (utolsó letöltés: 2018. március 31.)

6. A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”)
Elérhetőség: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf (utolsó letöltés: 2018. március 31.)
7. Nemzeti Infokommunikációs Stratégia:
Elérhetőség: http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf (utolsó letöltés: 2018. március 31.)
8. Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia
Elérhetőség: http://www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljesztt%C3%A9si_strat%C3%A9gia_.pdf (utolsó letöltés: 2018. március 31.)

2. BODÓ ATTILA PÁL – ZÁMBÓ NÓRA: A KÖZREMŰKÖDŐK KÖTELEZETTSÉGEI A CÉLZOTT TÁMADÁSOK ELHÁRÍTÁSÁBAN AZ IBTV. SZERINT[80]

2.1. Bevezető gondolatok

Az elektronikus információbiztonsággal összefüggő feladatok ellátásánál, így különösen a fenyegetések felismerésénél, szükség esetén a biztonsági események kezelésénél mind szervezeti, mind személyi oldalon azonosíthatóak, azok a szereplők és kötelezettségeik, amelyek a védelmi intézkedések hatékony megvalósítását szolgálják. A hatályos jogszabályi rendelkezések igen szűk kereteket adnak mind az értelmező rendelkezések, mind a jogok és kötelezettségek megállapításánál a fentiekben említett személyi kör azonosításához. Ebből ered, hogy az érintett személyek és feladataik meghatározásához egyéb szervezetszabályozó eszközöket és a különböző dokumentumokban megjelenő „mindennapi gyakorlatot" is szükséges számba venni.

A mindennapi gyakorlatban jelentkező probléma, hogy a számítógépes hálózatokon keresztül történő fenyegetések egyre nagyobb veszélyt jelentenek, és ebben a körben az interneten terjedő kártevők mellett a célzott támadások a leggyakoribbak. Ezek a fenyegetések mind a felhasználókat, mind a technikai eszközöket érintik és az egyik legelterjedtebb veszélyforrások közé tartoznak.

Jelen tananyagban az elektronikus információbiztonságban közreműködő személyek körét és kötelezettségeit vesszük sorra az előzőekben említett szűk keretek között, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és egyes végrehajtási rendeletei alapján a célzott támadások kezelésével összefüggésben.

2.2. Alapvetés és értelmezési keretek

A jogok és kötelezettségek ismertetése és megismerése megköveteli, hogy a szakanyagban tárgyalt témakör szempontjából releváns alapfogalmakat és azok értelmezési kereteit rögzítsük. Ennek érdekében szükséges meghatározni, hogy mely szereplő és milyen körülmények között minősül közreműködőnek, illetve milyen fenyegetést, és mely biztonsági esemény(eke)t tekinthetünk célzott támadásnak.

---

[80] A fejezet az *Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018 – Célzott kibertámadások* című közszolgálati továbbképzési program szakanyagához készült (Bodó Attila Pál – Oroszi Eszter Diána – Sági Gábor János – Szappanos Gábor – Szarvák Anikó – Zámbó Nóra: *Célzott kibertámadások*. Budapest, Dialóg Campus Kiadó, 2018).

2.2.1 Mely szereplőt tekintjük közreműködőnek?

Az elektronikus információbiztonságban közreműködő szereplőket két személyi körre adaptálva szükséges vizsgálni. Az egyik a természetes személyek, a másik a jogi személyek köre. A vizsgálat alapját biztosító jogszabályi környezet elsődlegesen az Ibtv. értelmező rendelkezésein[81] alapul. A közreműködő meghatározását az Ibtv. nem rögzíti önálló fogalomként, ettől függetlenül mindkét személyi kör tekintetében az értelmezéshez iránymutatást nyújt az üzemeltető, az adatfeldolgozó és az adatkezelő meghatározása.

Az Ibtv. 1. § (1) bekezdésének 45. pontja szerint az állami és önkormányzati szervek elektronikus információbiztonságának körében üzemeltetőnek minősül *„az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős*". *Adatfeldolgozónak* az a természetes vagy jogi személy, minősül, aki vagy amely az Ibtv. személyi hatálya alá tartozó szervezeteknél szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.[82]

Az Ibtv. személyi hatálya alá tartozó szervek[83] köre igen széles, ide tartoznak:

a) a központi államigazgatási szervek, ezen belül:
   aa) a minisztériumok,
   ab) az autonóm államigazgatási szervek,
   ac) a kormányhivatal, mint törvény által létrehozott, a Kormány irányítása alatt működő szerv,
   ad) a központi hivatalok, mint kormányrendelet által létrehozott, miniszter irányítása alatt működő szervek,
   ae) a rendvédelmi szervek,
   af) az önálló szabályozó szervek,
b) a Köztársasági Elnöki Hivatal,
c) az Országgyűlés Hivatal,
d) az Alkotmánybíróság Hivatala,
e) az Országos Bírósági Hivatal és a bíróságok,
f) az ügyészségek,
g) az Alapvető Jogok Biztosának Hivatala,
h) az Állami Számvevőszék,
i) a Magyar Nemzeti Bank,
j) a fővárosi és megyei kormányhivatalok,
k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatala (polgármesteri hivatal, megyei önkormányzati hivatal, közös önkormányzati hivatal), a hatósági igazgatási társulások,
l) a Magyar Honvédség, valamint

az a)-l) pontokban meghatározott szervek számára adatkezelést végzők.

Az adatkezelő fogalmi meghatározása tágabb kört ölel fel, hiszen visszahivatkozik az adatfeldolgozói körre. E szerint *adatkezelő* az a természetes vagy jogi személy, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.[84]

Az Ibtv. szerinti, fentebb rögzített fogalmi megahatározások – adatfeldolgozó, adatkezelő – 2015. július 16-tól[85] az Ibtv. és az információs önrendelkezési jogról és az információszabadságról szóló

[81] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 1. §-a.

[82] Ibtv. 1. § (1) bekezdés 3. pont.

[83] Ibtv. 2. §.

[84] Ibtv. 1. § (1) bekezdés 5. pont.

[85] Az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról szóló 2015. évi CXXX. törvény 8. § (1) bekezdése.

2011. évi CXII. törvény (a továbbiakban: Infotv.) közötti összhang megteremtését célzó Ibtv. módosítást követően egyeznek az Infotv. 3. §-a szerinti fogalmi meghatározásokkal. A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679 rendelet, azaz az EU Általános Adatvédelmi Rendeletének (a továbbiakban: GDPR) hatálybalépése és kötelező alkalmazása 2018. május 25-ét követően szintén felveti a fogalmi kérdések további tisztázását. Jelen tananyag készítésekor az Infotv. GDPR miatti módosítása még várat magára – várhatóan erre a 2018. őszi parlamenti ülésszakban kerül sor – így a fogalmak értelmezési keretei kötöttek.

Speciális szereplőnek minősül az Ibtv. személyi hatálya alá tartozó azon szervek köre, akik a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói feladatait[86] látják el. Ez utóbbi szervezetek körét a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet melléklete[87] tartalmazza.

Mindhárom fogalom – üzemeltető, adatfeldolgozó, adatkezelő – mindkét személyi körre vonatkozóan azonosítható, így a fogalmak alá tartozó személyi és szervezeti kör az Ibtv. szerint az elektronikus információbiztonság szervezeti érvényesülését illetően közreműködőnek minősül. Az adatkezelést illetve az adatfeldolgozást végző vagy végeztető jogi személyt vagy egyéni vállalkozót, valamint az üzemeltetőt az Ibtv. együttesen szervezetként definiálja.[88]

Az adatfeldolgozón, az adatkezelőn és az üzemeltetőn túl közreműködőnek tekinti továbbá az Ibtv. az elektronikus információs rendszer[89] létrehozásában, auditálásában, karbantartásában vagy javításában, továbbá tervezésében, fejlesztésében, vizsgálatában, kockázatelemzésében és kockázatkezelésében részt vevők körét.[90]

Az Ibtv. személyi hatálya alá tartozó szervek közül a központi államigazgatási szervek egy részénél[91] megjelenik a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet (a továbbiakban: 309/2011. (XII. 23.) Korm. rendelet) alapján egy speciális szereplő, az 1. §-ban kijelölt központi szolgáltató, a Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: központi szolgáltató).

A 309/2011. (XII. 23.) Korm. rendelet 1. melléklete tartalmazza a központi szolgáltató által kötelezően biztosítandó központosított informatikai és elektronikus hírközlési szolgáltatások körét.[92] A központi szolgáltató a 309/2011. (XII. 23.) Korm. rendeletben biztosított szolgáltatások körében mint üzemeltető és adatkezelő jár el, ez alapján közreműködőnek minősül. Ugyanígy közreműködőnek minősül a 309/2011. (XII. 23.) Korm. rendelet 3. mellékletében[93] meghatározott szolgáltatások körében az IdomSoft Informatikai Zártkörűen Működő Részvénytársaság (a továbbiakban: IdomSoft Zrt.).

További támpontot ad a közreműködő fogalmi meghatározásának rögzítéséhez az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet (a továbbiakban: KIM rendelet). A KIM rendelet tartalma az Ibtv. 13. § (11) bekezdésében előírt kötelezettség teljesítéséhez kapcsolódik, amely szerint

86 Ibtv. 2. § (2) bekezdés b) pont.

87 Lásd 3. melléklet.

88 Ibtv. 1. § (1) bekezdés 43. pont.

89 Elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese - Ibtv 1. § (1) bekezdés 14b. pont.

90 Ibtv. 11. §.

91 A központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet 2. melléklete.

92 Lásd 1. melléklet.

93 Lásd 2. melléklet.

az elektronikus információbiztonságban érintett személyi kör, így az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen kötelesek részt venni. E kötelezettség szempontjából a személyi kör csak természetes személyre értelmezhető.

A KIM rendelet értelmező rendelkezései szerint[94] a képzési kötelezettség teljesítésével összefüggésben elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személynek – témánk szempontjából közreműködőnek – minősülnek:

a) az állami és önkormányzati szervek esetében a szervezeti és működési szabályzat és a munkaköri leírások alapján,

b) az Ibtv. hatálya alá tartozó egyéb szervek esetében a munkaköri leírásban vagy egyéb módon

az elektronikus információbiztonsági feladatok ellátásával megbízott személyek.

Fentieken túl közreműködőnek tekinthetők a felhasználók[95] is, akik az értelmező rendelkezések szerint az egy adott elektronikus információs rendszert igénybevevő személyek. Ilyen személynek tekinthető minden olyan munkatárs, aki az adott elektronikus információs rendszerhez felhasználói jogosultsággal rendelkezik (utóbbi szervezetenként és elektronikus információs rendszerenként eltérő, kereteit a szervezet Informatikai Biztonsági Szabályzata tartalmazza).

Összegzésként megállapítható, hogy minden olyan feladat, tevékenység és szolgáltatás, amely az elektronikus információbiztonsághoz kapcsolódik és leíró jelleggel, mint kötelezettség megjelenik valamely szervezetszabályzó dokumentumban, munkaköri leírásban vagy szerződésben közreműködői tevékenységhez köthető. Ez alapján bár az Ibtv. és a fentiekben ismertetett jogszabályok nem határozzák meg a közreműködő fogalmát, véleményünk szerint az az alábbiak szerint rögzíthető. Közreműködőnek minősül egy szervezet működése során minden olyan természetes és jogi személy, amely feladat- és hatásköréből adódóan magatartásával, tevékenységével hozzájárul az elektronikus információbiztonság szervezeten belüli érvényesüléséhez (a továbbiakban együtt: közreműködő).[96]

2.2.2 Mi minősül célzott támadásnak?

Az értelmezési keretek rögzítéséhez a közreműködő adekvát fogalmi használata mellett szükséges, hogy meghatározásra kerüljön mi minősül célzott támadásnak. A célzott támadás az internetről érkező fenyegetések körébe tartozik, amely során a támadó az elektronikus információs rendszer infrastrukturális szegmensét célozza annak érdekében, hogy e szegmensben felügyelet nélkül „tevékenykedjen". Ezen magatartás arra irányul, hogy a támadó az adott célpont eszköze feletti rendelkezési jogosultság gyakorlását megszerezze. Rendkívül összetett módszereket és magas szakértelmet igénylő támadási forma, amely ellen nehéz védekezni és így gyakran jár „eredménnyel".

Ebből eredően a célzott támadások egyaránt minősülnek fenyegetésnek és ha a kívánt célt elérik biztonsági eseménynek. Az Ibtv. és a hatályos jogszabályi környezet – a közreműködő fogalmához hasonlóan – a célzott támadások meghatározását sem rögzíti az értelmező rendelkezések között, azonban a szükséges kereteket a fenti két fogalom meghatározásával megadja.

Az Ibtv. szerint fenyegetésnek kell tekinteni minden olyan lehetséges műveletet vagy eseményt, illetve mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer és elemei vé-

[94] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet (a továbbiakban: KIM rendelet) 2. § 3. pont.

[95] Ibtv. 1. § (1) bekezdés 18. pont.

[96] Szerzők fogalom meghatározása.

dettségét, biztonságát.[97] Ha a fenyegetések ellen hozott tevékenységek és intézkedések összessége nem megfelelő a fenyegetésből biztonsági esemény lesz. Biztonsági eseménynek az Ibtv. azt a nem kívánt vagy nem várt egyedi esemény vagy eseménysorozatot tekinti, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.[98]

A biztonsági esemény fogalmának az értelmezéséhez segítséget nyújt, hogy az Ibtv.-ben önálló fogalomként jelenik meg a *bizalmasság,*[99] a *sértetlenség,*[100] a *rendelkezésre állás.*[101] Az értelmező rendelkezések rögzítik, hogy:

a) Bizalmasságnak az elektronikus információs rendszer azon tulajdonságát kell érteni, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.
b) Sértetlenségnek az adat azon tulajdonságát kell érteni, amely szerint:
   ba) az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyeznek, az adat az elvárt forrásból származik, azaz hiteles, és
   bb) az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága is, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
c) Rendelkezésre állás alatt annak biztosítását kell érteni, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak.

A hatályos szabályozási környezet megkülönbözteti a biztonsági esemény fogalmát a súlyos biztonsági esemény fogalmától. Súlyos biztonsági eseménynek kell tekinteni azt az informatikai eseményt, amely bekövetkezése esetén:

a) az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet,
b) emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
c) súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben,
d) alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.[102]

2.2.3 A közreműködők helye és szerepe az elektronikus információbiztonságban

Az előzőekben rögzítettük és elhatároltuk egymástól azokat az alapfogalmakat, amelyek zsinórmértékként szolgálnak a témakör ismertetéséhez, ezáltal ismerjük a közreműködő szereplők fogalmát és körét. Ezen ismeretek birtokában szükséges elhelyezni az elektronikus információbiztonság környezetében az ismertetett szereplőket és meghatározni szerepüket.

A közreműködők elektronikus információbiztonsággal kapcsolatos helye egy szervezetben az által határozható meg, hogy milyen alaptevékenységet végeznek feladat- és hatáskörükkel összefüggésben. Az értelmezési keretekből kiindulva ezek lehetnek:

a) üzemeltetői,
b) adatkezelői,

97 Ibtv. 1. § (1) bekezdés 19. pont.
98 Ibtv. 1. § (1) bekezdés 9. pont.
99 Ibtv. 1. § (1) bekezdés 8. pont.
100 Ibtv. 1. § (1) bekezdés 39. pont.
101 Ibtv. 1. § (1) bekezdés 38. pont.
102 Ibtv. 1. § (1) bekezdés 41a. pont.

c) adatfeldolgozói,
d) központi szolgáltatói,
e) felhasználói,

szerepkörökkel összefüggő alaptevékenységek. Ezen tevékenységi körök a szervezeti struktúrában bárhol elhelyezhetők és gyakorlati megjelenési formájukat tekintve lehetnek önálló vagy kapcsolt munkakörök, szerződés vagy jogszabály által ellátott feladatok. A munkakör alapú megközelítés esetében a szervezeti hierarchia megjelenési formája a vezetői szerepkör és a szervezeti egység szintjén is azonosítható. Szerződéses jogviszony és jogszabályi kijelölés esetén az ellátott feladat mennyisége és mélysége rögzített keretek között mozog. A betöltött szerepkörök sokszínségétől és a szervezetben elfoglalt hely változatosságától függetlenül az alapvető kötelezettségek köre minden közreműködőre kiterjed, amely kötelezettségek az Ibtv.-ben megjelenő támogató védelmi intézkedésekre[103] és a biztonságtudatos működésre is visszavezethetőek.

2.3. Kötelezettségek az ibtv. És végrehajtási szabályai tükrében

A közreműködők kötelezettségeire vonatkozó generális szabály az Ibtv.-ben előírt követelmények teljesülése a szervezet elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenységük során. Ennek teljesülését az elektronikus információs rendszer biztonságáért felelős személy[104] biztosítja. A közreműködőt a biztonsági követelmények teljesülésével kapcsolatban tájékoztatási kötelezettség terheli az elektronikus információs rendszer biztonságáért felelős személy részére. Ezen tájékoztatás keretében további kötelezettsége, hogy:

a) a követelményeknek való megfelelőség alátámasztásához szükséges, a közreműködői tevékenységgel kapcsolatos adatokat, illetve
b) az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot az elektronikus információs rendszer biztonságáért felelős személy rendelkezésre bocsássa.[105]

Az Ibtv. az elektronikus információbiztonsági követelmények között alapvetésként rögzíti,[106] hogy a védelmi intézkedéseknek – a PreDeCo (Preventive–Detective–Corrective) elvet alapul véve – támogatniuk kell:

a) a megelőzést, azaz a fenyegetés által okozható hatás bekövetkezésének elkerülését;[107]
b) a korai figyelmeztetést, azaz olyan aktív szervezeti cselekvést, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;[108]
c) az észlelést, azaz a biztonsági esemény bekövetkezésének felismerését;[109] illetve
d) a reagálást, amely a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedéseket foglalja magába,[110] és magát
e) a biztonsági események kezelését, amely magába foglalja a dokumentálást, a következmények felszámolását, a bekövetkezés okainak és felelőseinek megállapítását, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet.[111]

103 Ibtv. 6. §.
104 Ibtv. 13. § (5) bekezdés.
105 Ibtv. 13. § (7) bekezdés.
106 Ibtv. 6. §.
107 Ibtv. 1. § (1) bekezdés 36. pont.
108 Ibtv. 1. § (1) bekezdés 32. pont.
109 Ibtv. 1. § (1) bekezdés 17. pont.
110 Ibtv. 1. § (1) bekezdés 37. pont.
111 Ibtv. 1. § (1) bekezdés 10. pont.

Fentiekből következik, hogy minden közreműködőnek a feladat- és hatáskörébe tartozó tevékenysége során a célzott támadások elhárítása érdekében úgy kell eljárnia, hogy azzal hozzájáruljon:

a) a célzott támadások megelőzéséhez,
b) a célzott támadásokra vonatkozó korai figyelmeztetés megvalósulásához,
c) magának a célzott támadásnak az észleléséhez, valamint
d) célzott támadás bekövetkezése esetén a reagálás hatékony megvalósulásához, és a biztonsági esemény kezeléséhez.

Minden fenti résztevékenység során szükség szerint érvényesülnie kell az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben (a továbbiakban: BM rendelet) előírt védelmi intézkedéseknek, amelyek az alábbiak:

a) adminisztratív védelem (a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések összessége, és az oktatás);[112]
b) fizikai védelem (a fizikai térben megvalósuló fenyegetések elleni védelem, ide sorolva a természeti csapás elleni és a mechanikai, az élőerős védelmet, az elektronikai jelzőrendszert, a beléptető és a megfigyelő rendszert, a tápáramellátást, a sugárzott és vezetett zavarvédelmet, a klimatizálást és a tűzvédelmet);[113]
c) logikai védelem (az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem).[114]

A védelmi intézkedések körét a BM rendelet az elektronikus információs rendszer biztonsági osztályba[115] sorolt értékéhez igazodva határozza meg. De melyek azok a védelmi intézkedések, amelyek a biztonsági osztályba sorolás eredményétől és a közreműködő szerepvállalásának mértékétől függően szükség szerint a célzott támadások elhárításához kapcsolódnak?

Az adminisztratív védelmi intézkedések terén a jogi személy közreműködőnek a közreműködés mértékétől függően rendelkeznie kell:[116]

a) alapfeltételként elektronikus információs rendszerek biztonságáért felelős személlyel,
b) a megelőzés érdekében:
ba) informatikai biztonsági szabályzattal,
bb) kockázatelemzési és kockázatkezelési eljárásrenddel,
bc) üzletmenet folytonosságra vonatkozó eljárásrenddel,
bd) a biztonságtudatosságot szem előtt tartó képzési eljárásrenddel,
be) az elektronikus információs rendszerek nyilvántartásával,
c) a megelőzés, a korai figyelmeztetés, az észlelés, a reagálás és a biztonsági esemény kezelésére vonatkozóan olyan biztonsági eseménykezelési eljárásrenddel, amely kitér a biztonsági események figyelésére, jelentésére és a képzésre,
d) a megelőzés és a korai figyelmeztetés érdekében olyan személybiztonsági eljárásrenddel,

[112] Ibtv. 1. § (1) bekezdés 6. pont.
[113] Ibtv. 1. § (1) bekezdés 20. pont.
[114] Ibtv. 1. § (1) bekezdés 34. pont.
[115] Ibtv. 7-8. §-ok.
[116] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben (a továbbiakban: BM rendelet) 3. melléklet 3.1. alpontja, amely az egyes védelmi intézkedések alábontását is tartalmazza, ezek szükségessége és teljesülése egyedi vizsgálat tárgya.

amely kitér a munkakörök, feladatok biztonsági szempontú besorolására és az interneten tanúsítandó viselkedési szabályokra.

A fizikai védelmi intézkedések terén a jogi személy közreműködőnek a közreműködés mértékétől függően rendelkeznie kell:[117]

a) a megelőzés érdekében a belépési engedélyezésre vonatkozó eljárásrenddel,
b) a korai figyelmeztetés és az észlelés érdekében behatolás riasztással, észlelő berendezésekkel, hőmérséklet és páratartalom ellenőrzéssel, tűzvédelemmel,
c) a reagálás érdekében tartalék áramellátással, vészkikapcsolási renddel és vészvilágítással, tűzelfojtó berendezéssel, víz- és más, csővezetéken szállított anyag okozta kár elleni védelemmel.

A logikai védelmi intézkedések terén a jogi személy közreműködőnek a közreműködés mértékétől függően rendelkeznie kell:[118]

a) a megelőzés érdekében szükség esetén:
aa) biztonságtervezési szabályzattal,
ab) rendszerbiztonsági tervvel,
ac) az elektronikus információs rendszerre vonatkozó tesztelési, képzési és ellenőrzési tervvel,
ad) konfigurációkezelési eljárásrenddel,
ae) rendszer karbantartási eljárásrenddel,
af) adathordozók védelmére vonatkozó eljárásrenddel,
ag) azonosítási és hitelesítési eljárásrenddel,
ah) hozzáférés ellenőrzési eljárásrenddel,
ai) rendszer- és információsértetlenségre vonatkozó eljárásrenddel, amelyet üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell érvényesíteni,
b) a megelőzés és a korai figyelmeztetés érdekében szükség esetén biztonságértékelési tervvel és az eredmény elemzésével, naplózási eljárásrenddel valamint rendszer- és kommunikáció védelmi eljárásrenddel.

Az előzőekben felsorolt adminisztratív, fizikai és logikai védelmi intézkedések annál nagyobb mértékben és mélységben kell, hogy rendelkezésre álljanak, minél magasabb az elektronikus információs rendszer biztonsági osztálya, és minél sokrétűbb a közreműködő szerepvállalása. Különösen igaz ez a logikai védelmi intézkedések rendelkezésre állása esetén. Látható, hogy a közreműködőket alapvetően a megelőzést célzó védelmi intézkedések terhelik, azonban adott esetben egy adatfeldolgozó, adatkezelő vagy üzemeltető a teljes védelmi intézkedési katalógus megvalósításában is érintett lehet. Főszabályként kell, hogy érvényesüljön, hogy jogi személy közreműködő esetében a BM rendeletben előírt védelmi intézkedések szükségességét és teljesülését egyedileg kell vizsgálni.

Fenti védelmi intézkedések elsődlegesen tehát a jogi személy közreműködő esetében értelmezhetők, természetes személy közreműködő esetén ezek a kötelezettségek az adott magatartásban megjelenő cselekvések és viselkedési formák révén érvényesülnek azzal, hogy a közreműködőnek úgy kell eljárnia, ahogy az az adott helyzetben tőle elvárható. A szervezeti szabályzókban megjelenő kötelezettségek betartása esetükben alapvető munkajogi kötelezettség.

A BM rendeletben előírt és fent részletezett védelmi intézkedések mellett a megelőzést szolgáló további kötelezettség a biztonságtudatosságot, a tudás szinten tartását és a szakmai fejlődést célzó, a KIM rendeletben előírt képzésen való részvétel. A közreműködő fogalmi kereteinek meghatározásánál rögzítettük, hogy a KIM rendeletben szereplő, az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek (a továbbiakban: részt vevő személyek) köz-

[117] BM rendelet 3. melléklet 3.2. alpontja, amely az egyes védelmi intézkedések alábontását is tartalmazza, ezek szükségessége és teljesülése egyedi vizsgálat tárgya.

[118] BM rendelet 3. melléklet 3.3. alpontja, amely az egyes védelmi intézkedések alábontását is tartalmazza, ezek szükségessége és teljesülése egyedi vizsgálat tárgya.

reműködőnek minősülnek. A részt vevő személyeket az alábbi képzések érinthetik:

a) két féléves, szakirányú továbbképzés választható jelleggel,[119]

b) 50 órás továbbképzés, amelyen egy alkalommal kötelező részt venni, kivéve ha a közreműködő már elvégezte az a) pont szerinti szakirányú továbbképzést, vagy a KIM rendeletben meghatározott, érvényes oklevéllel rendelkezik,[120]

c) 25 órás éves továbbképzésben, kötelező jelleggel, amely alól mentességgel nem rendelkezik.[121]

A KIM rendelet alapján a részt vevő személyek esetében az 50 órás továbbképzés alóli felmentésnek minősül:

a) az Information Systems Audit and Controll Association (ISACA) által kiadott:

aa) Certified Information System Auditor (CISA), vagy

ab) Certified Information Security Manager (CISM), vagy

ac) Certified in Risk and Information Systems Control (CRISC),

b) az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP)

érvényes oklevél megléte.[122]

A felhasználók részére a KIM rendeletben előírt 25 órás éves továbbképzés elvégzése kötelező, azonban ettől függően a szervezet belső szabályzóiban (például informatikai biztonsági szabályzat, képzési terv) célszerű a biztonságtudatosságra vonatkozó képzési lehetőségeket rögzíteni. Ennek összhangban kell állni a BM rendelet 3. melléklet Adminisztratív védelmi intézkedések 3.1.7.2. alpontjában előírt – és az 1. biztonsági osztálytól kötelező – képzési eljárásrenddel.

A központi szolgáltatónak és közreműködőnek minősülő szervezetnek az információbiztonsággal kapcsolatos speciális feladatait a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet (a továbbiakban: 186/2015. (VII. 13.) Korm. rendelet) tartalmazza. A 186/2015. (VII. 13.) Korm. rendelet a központi szolgáltató részére a biztonsági események kezelésével összefüggésben együttműködési kötelezettséget ír elő a szervezet, a Nemzeti Elektronikus Információbiztonsági Hatóság és az eseménykezelő központok[123] irányába.[124]

A központi szolgáltató kötelezettsége továbbá a célzott támadások elhárításával összefüggésben,[125] hogy:

a) a megelőzés érdekében kialakítsa informatikai biztonsági irányítási rendszerét,

b) a megelőzés érdekében azonosítsa és nyilvántartsa:

ba) a szolgáltatások végfelhasználóit, az üzemeltető felhasználókat, valamint a szolgáltatás biztosításához igénybevett támogatókat és fejlesztőket (a továbbiakban együtt: felhasználók), továbbá a hozzáférési jogosultságaikat,

bb) a szolgáltatásokhoz kapcsolódó távoli hozzáféréseket,

c) a megelőzés érdekében elvégezze a szolgáltatások kockázatértékelését és meghatározza a szolgáltatások biztosításához szükséges és a kockázatokkal arányos védelmi intézkedéseket és folyamatosan felülvizsgálja azokat,

---

119 KIM rendelet 4-8. §-ok.

120 KIM rendelet 9-13. §-ok.

121 KIM rendelet 14-18. §-ok.

122 KIM rendelet 7. § (2) bekezdés.

123 Ibtv. 19. §.

124 A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet (a továbbiakban: 186/2015. (VII. 13.) Korm. rendelet) 3. §.

125 186/2015. (VII. 13.) Korm. rendelet 2. §.

d) a korai figyelmeztetés, az észlelés és a reagálás érdekében folyamatosan ellenőrizze a szolgáltatások biztonsági állapotát, elvégezze az üzemi és biztonsági információk gyűjtését és elemezését, az elemzések alapján a megelőzés érekében biztonságnövelő intézkedéseket vezet be,
e) a reagálás és a biztonsági esemény kezelése érdekében intézkedik a bekövetkezett biztonsági események által okozott kár csökkentéséről,
f) a biztonsági események kezelése során tájékoztatja az eseménykezelő központokat az azonosított biztonsági eseményekről és fenyegetettségekről, biztosítja az azonosításához, elemzéséhez és kezeléséhez szükséges, bizonyíték értékű információkat részükre,
g) a biztonsági események kezelése érdekében a biztonsági eseményről szóló adatszolgáltatással, vizsgálat elvégzésével, az elrendelt biztonságnövelő intézkedések végrehajtásával közreműködik az eseménykezelő központok által végzett informatikai biztonsági eseménykezelésben.

A központi szolgáltató a Kormányzati Adatközpont szolgáltatásai[126] körében az azt igénylő ügyfelei számára korai figyelmeztető rendszerhez való kapcsolódást biztosít az alábbi műszaki feltételek megteremtésével és fenntartásával:

a) a hálózati forgalom másolatának átadása,
b) az internet felé menő, illetve onnan érkező hálózati forgalom SSL/TLS csatornáinak szelektív feloldása az ügyfél által meghatározott házirend szerint az SSL/TLS csatornák terminálásával vagy SSL/TLS átjáró megvalósításával,
c) a korai figyelmeztető rendszer fenntartójával az ügyfelek kapcsolódásának kialakítása, változás- és eseménykezelése terén.[127]

Kiegészítő szabály az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet szerint előírt kötelezettség, amely szerint a Nemzeti Elektronikus Információbiztonsági Hatóság[128] helyszíni ellenőrzése során a szerződéses jogviszony alapján érintett közreműködő köteles együttműködni a hatósággal.[129]

2.4. Összegzés

Az elektronikus információs rendszereket naponta érik az internet irányából azok a fenyegetések, amelyek elhárítása és a fenntartható biztonsági környezet megteremtése komoly kihívást jelent minden szereplő számára. A célzott támadások elhárítása során megjelenő kötelezettségek köre a közreműködő szereplők tekintetében – mint olvashattuk – szerteágazó és sokrétű tevékenységet ölel fel, hiszen minden intézkedésük kihat a szervezeti működésre. Éppen ezért ezen intézkedésekre vonatkozóan a jogi szabályozás megléte kiemelt jelentőségű, így időszerű volt egy olyan szakanyag készítése, amely a jogértelmezést és a jogalkalmazást támogató céllal foglalja össze és mutatja be a szabályozási környezetet. Szándékaink szerint jelen tananyag ezeknek az elvárásoknak felel meg. A szabályozási környezet elemeit vizsgálva egyértelműen levezethető, hogy a jogalkotónak nem az volt a szándéka, hogy a legapróbb részletekig szabályozza ezt a területet. Úgy gondoljuk, hogy a meglévő és bemutatott szabályozás megfelelő keretet biztosít a fenntartható biztonság állapotának megterem-

126 A Kormányzati Adatközpont működéséről szóló 467/2017. (XII. 28.) Korm. rendelet.

127 186/2015. (VII. 13.) Korm. rendelet 2/A. §.

128 Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 2. §-a.

129 Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 5. § (6) bekezdése.

téséhez, azzal, hogy a további részletszabályokat a szervezeti szabályozás egyéb eszközével szükséges biztosítani.

2.5. Mellékletek

1. Melléklet: a 309/2011. (xii. 23.) Korm. Rendelet 1. Mellékletében felsorolt, kötelezően biztosítandó központosított informatikai és elektronikus hírközlési szolgáltatások köre

A) Végfelhasználói infokommunikációs infrastruktúra biztosítása és üzemeltetése

1. Alapvető informatikai és elektronikus hírközlő eszközökkel, kellékanyagokkal való ellátás (papír kivételével), valamint üzembe helyezés

1.1. Asztali és hordozható munkaállomás biztosítása

1.2. Alap irodai alkalmazások biztosítása (levelezés és irodai munkákhoz kapcsolódó dobozos alkalmazások)

1.3. Felhasználó – munkával kapcsolatos – anyagainak tárolásához központi tárterület biztosítása

1.4. Nyomtatáshoz szükséges eszközök biztosítása

1.5. Mobiltelefon biztosítása

1.6. Helyhez kötött telefon (berendezés) biztosítása

1.7. Helyi informatikai és elektronikus hírközlési hálózat és ezzel kapcsolatos eszközök biztosítása

1.8. Faxoláshoz szükséges eszközök biztosítása (multifunkciós fax készülék vagy fax szerver útján)

1.9. Nyomtatók, multifunkcionális eszközök biztosítása

1.10. Nyomtatók és multifunkcionális berendezések festékkazettával való ellátása

1.11. Egyéb alapvető informatikai és elektronikus hírközlő eszközökkel és kellékekkel való ellátás, üzembe helyezés és telepítés

1.12. Végfelhasználói eszközökön futó vírus- és rosszindulatú kód (malware) elleni védelem biztosítása

2. Alapvető informatikai és elektronikus hírközlő eszközök munkaidőben és a központi, illetve az egyedi szolgáltatási megállapodásban rögzített felhasználói kör munkaidőn túli használatának támogatása, üzemeltetése és karbantartása

2.1. Személyi használatú számítógépek normál és kiemelt szintű helyszíni informatikai támogatása (szoftver és hardver meghibásodások kezelése)

2.2. Helyi informatikai hálózat üzemeltetése, karbantartása

2.3. Internet-hozzáférés működtetése, a központi, illetve az egyedi szolgáltatási megállapodásban rögzített felhasználói kör számára hordozható eszközön is (mobil-internet)

2.4. Levelező rendszer üzemeltetése a kiegészítő biztonsági szolgáltatásokkal

2.5. Piaci (nem kormányzati célú) hírközlési szolgáltatótól igénybe vett standard mobil rádiótelefon előfizetés, valamint internet biztosítása

2.6. Piaci (nem kormányzati célú) hírközlési szolgáltatótól igénybe vett standard helyhez kötött telefon előfizetés biztosítása

2.7. Nyomtatók, multifunkcionális eszközök üzemeltetése

2.8. Elektronikus hírközlő berendezések üzemeltetése (mobil és vezetékes telefonkészülék, fax készülék)

2.9. Központi tárolóhely, nyomtatási várakozási sorok és központi levelezési szolgáltatások üze-

meltetése
2.10. Dobozos és egyedi fejlesztésű alkalmazásoknak a központi vagy egyedi szolgáltatási megállapodás szerint történő üzemeltetése
2.11. Egyéb alapvető informatikai és elektronikus hírközlő eszköz üzemeltetése, karbantartása
3. Informatikai problémák ügyfélszolgálati kezelése
3.1. Végfelhasználói állományok visszaállítása mentésből – igény szerint
3.2. Általános informatikai segítségnyújtás ügyfélszolgálaton keresztül
3.3. Elfelejtett jelszó kezelése
3.4. Felhasználó felvétele, törlése a támogatott rendszerekre és alkalmazásokra
3.5. Felhasználó informatikai jogosultságainak adminisztrálása a támogatott rendszerekre és alkalmazásokra
3.6. Felhasználói, munkacsoport adatok archiválása optikai lemezre igény szerint
3.7. Informatikai ügyelet – munkaidőn kívül
3.8. Költözések során az informatikai eszközök költöztetéshez történő előkészítése, illetve költözést követő installációja – megelőző egyeztetést követően
3.9. Speciális problémák továbbítása szakértői csoportok felé
3.10. Szolgáltatási paraméterek méréséhez szükséges adatok kinyerése az ügyfélszolgálati rendszerből
3.11. Alap irodai alkalmazásokkal kapcsolatos hiba kezelése
3.12. Végfelhasználói használatú számítógépekkel és perifériáikkal kapcsolatos hiba kezelése
3.13. Jogosultsággal kapcsolatos felhasználói incidens kezelése
3.14. Informatikai és elektronikus hírközlési hálózati hibabejelentések kezelése
4. Új igények új technológiai megoldásokkal való kielégítése és a meglévő eszközök technológiai megújítása során a végfelhasználói használatba kerülő eszközökhöz kapcsolódó infokommunikációs szolgáltatások ellátása.

B) Központi infokommunikációs infrastruktúra biztosítása és üzemeltetése
1. Címtár üzemeltetés
2. Központi szerver infrastruktúra elemek biztosítása
3. Igény szerint alkalmazások karbantartása, támogatása és üzemeltetése
4. Eszköz-nyilvántartási szolgáltatások jellemzően saját tulajdonú eszközök esetében
5. Informatikai raktár és tartalék raktárkészlet biztosítása
6. Informatikai és elektronikus hírközlési beszerzésekről való gondoskodás
7. Az ellátáshoz kapcsolódó informatikai projektek vezetése
8. Az ellátáshoz kapcsolódó informatikai rendszerintegráció új eszközök és alkalmazások telepítéséhez
9. A standard ellátáshoz kapcsolódó IT alkalmazások és licencek biztosítása
10. Az ellátáshoz kapcsolódó IT beszerzések technikai nyilvántartása (hardver és szoftver nyilvántartás) jellemzően saját tulajdonú eszközök esetében
11. Az ellátáshoz kapcsolódó IT eszközök garanciális és garancián túli javítása, javíttatása
12. IT jogosultságok kezelése, adminisztrálása
13. Központi vírusvédelem biztosítása
14. Rendszer monitorozási szolgáltatások
15. Rendszeroptimalizálás, normalizálás
16. Telefonközpont kezelés
17. Elektronikus hírközlési szolgáltatással kapcsolatos számlák feldolgozása
18. Elektronikus hírközlési szolgáltatással kapcsolatos forgalmi és hívásinformációk szolgáltatása
19. Tűzfal biztosítása és üzemeltetése
20. Új igények új technológiai megoldásokkal való kielégítése és a meglévő eszközök technológiai megújítása során a központosított használatú eszközökhöz kapcsolódó infokommunikációs szolgáltatások ellátása

C) Egyéb informatikai igények ellátása

1. Informatikai oktatóteremben informatikai eszközök biztosítása
2. Szabványos IT eszköz kölcsönzése tartalék raktári készletből
3. Egyedileg igényelt perifériákkal való ellátás (szkenner, nyomtató) raktári készletből
4. A lakosság részére készített kormányzati tájékoztató levelekkel, kiadványokkal, illetve kérdőívekkel kapcsolatos adatfeldolgozói és adminisztrációs tevékenység, valamint a postai szolgáltatásokról szóló 2012. évi CLIX. törvény 2. § 35. pontja szerinti postai küldeménynek minősülő küldemények címzettek részére postai úton történő soron kívüli megküldésével kapcsolatos feladatok ellátása a Magyar Posta Zrt. bevonásával.

2. Melléklet: az idomsoft informatikai zártkörűen működő részvénytársaság által kötelezően biztosítandó központosított alkalmazás-üzemeltetési és e rendszereket érintő alkalmazás-fejlesztési szolgáltatások köre

1. Az önkormányzati ASP rendszer keretében működő gazdálkodási szakrendszer
2. Külön jogszabályban meghatározott személyiadat-és lakcímnyilvántartáshoz kapcsolódó rendszerek (SZL, SZIG, eSZIG, LIG, cím és körzetnyilvántartás, TSZR, ESZF, Nemzeti Arcképtár /NAT/)
3. Külön jogszabályban meghatározott központi címregiszter (KCR)
4. Külön jogszabályban meghatározott központi idegenrendészeti nyilvántartáshoz kapcsolódó egyes rendszerek (IDR, ISZL, IDEGEN)
5. Külön jogszabályban meghatározott közúti közlekedési nyilvántartáshoz kapcsolódó rendszerek (JÁRMŰ, Vezetői engedély /VEN/, Származásellenőrzés /SZENY/, Közlekedési Okmánytár, PARKIG, eredetiségvizsgálat /KERT/, Útdíj-díjmentes, EUCARIS)
6. Külön jogszabályban meghatározott közlekedési biztonsági kiszolgáló rendszer (KBKR)
7. Külön jogszabályban meghatározott elektronikus útdíj rendszer gyorsítótár (e-Útdíj)
8. Külön jogszabályban meghatározott kötelező gépjármű-felelősségbiztosítási rendszer (IGFB)
9. Külön jogszabályban meghatározott közúti közlekedési előéleti pontrendszer (Pontrendszer)
10. Külön jogszabályban meghatározott elektronikus anyakönyvi rendszer (EAK)
11. Külön jogszabályban meghatározott arcképelemzési nyilvántartás és arcképelemző rendszer (ÁAAR)
12. Külön jogszabályban meghatározott egyéni vállalkozó nyilvántartási rendszer (EVNY)
13. Külön jogszabályban meghatározott szabálysértési nyilvántartási rendszerhez kapcsolódó egyes rendszerek (SZNYR, STAT-VIR)
14. Külön jogszabályban meghatározott bűnügyi nyilvántartási rendszerhez kapcsolódó egyes rendszerek (HCR-bűnügyi, ERHAB)
15. Külön jogszabályban meghatározott központi útiokmány nyilvántartási rendszer (EPASS)
16. Külön jogszabályban meghatározott elektronikus ügyfél-azonosítást segítő és elektronikus ügyintézést támogató rendszerek (UKAPU, Összerendelési Nyilvántartáshoz kapcsolódó rendszerek / ÖNY/, Az elektronikus ügyintézést igénybe vevő, külföldön élő természetes személyek személyi nyilvántartása /3NYT/, Időszakos Értesítési Szolgáltatás /RÉR/, Részleges Kódú Telefonos Azonosítás /RKTA/, Elektronikus hatósági ügyintézést és tájékoztatást segítő internetes szolgáltató rendszer
17. Elektronikus hatósági ügyintézést és tájékoztatást segítő internetes szolgáltató rendszer – Webes Ügysegéd /WÜ/
18. Elektronikus hatósági ügyintézést és tájékoztatást segítő telefonos szolgáltató rendszer (Effector)
19. Külön jogszabályban meghatározott Schengeni Információs Rendszer magyar nemzeti részének központi informatikai elemei (SIS II NS.CP)
20. Külön jogszabályban meghatározott nemzeti egységes kártya-kibocsátási keretrendszer (NEK)
21. Külön jogszabályban meghatározott a jogügyletek biztonságát szolgáló keretrendszer üzemeltetése (JÜB)
22. Külön jogszabályban meghatározott jármű figyelőztetési rendszer üzemeltetése (Figyelőztetés)

23. Külön jogszabályban meghatározott központi tanúvédelmi rendszer üzemeltetése (KTR, BÁSTYA)
24. A 13/2013. (IV. 11.) ORFK utasítás alapján kialakított szolgálati lőfegyverek nyilvántartásának (Fegyver)
25. Külön jogszabályban meghatározott Magyar igazolvány rendszer (MIG)
26. Külön jogszabályban nevesített Központi Ügyfél-regisztrációs Nyilvántartás (KÜNY)
27. Szakrendszeri Kódképző és Kapcsolatkezelő Alkalmazások
28. Általános Közigazgatási Statisztikai Adatgyűjtő Rendszer
29. Elektronikus Felügyeleti és Ellenőrzési Rendszer
30. A központi okmány keretrendszer mellett kialakított Integrált Napló
31. Vezetői Információs Portál
32. Központi Jogosultságkezelő Rendszer
33. Központi Okmánytár Okmányfeldolgozó és Lekérdező Rendszer (KOTAR)
34. Iratérvényességi Nyilvántartás rendszer
35. Központi Közigazgatási Adatszolgáltató és Adatfogadó Rendszer (KAAR)
36. Központi okmánygyártás (SZIG, Útlevél, VEN, Magyar igazolvány), (MOKA)
37. Okmányügyek Intézését Segítő Mobilalkalmazás rendszer (OkmányApp)
38. Okmányok Képfelvételező és adatfeldolgozó rendszere (Fotoshop)
39. Központi Okmány megszemélyesítő Rendszer (Erkölcsi bizonyítvány, Származásellenőrzési határozatok, Gépjármű törzskönyv)
40. Egyéb okmánymegszemélyesítő rendszerek: Szolgálati igazolványok, Diákigazolvány, Vitorlás kártya, Polgárőr kártya
41. Integrált Portál alapú lekérdező rendszer (IPL)
42. Központi Certifikáció és tanúsítvány generáló rendszer
43. Elektronikus Kormányiroda (EKI)
44. Hivatalos Lapok – Magyar Közlöny website
45. Jogtár menedzsment rendszer
46. Központi Időpontfoglaló Alkalmazás
47. KIÜSZI Központi Szakalkalmazások
48. Nemzeti Konzultációk IT kiszolgáló rendszere
49. Központi Közigazgatási Naplórendszer (NLR)
50. A Magyar Nemzeti Public Key Directory
51. Mobil okmányirodai időpontfoglalás
52. Szerződés Nyilvántartó rendszer
53. Kormányablakok Tudástárát működtető Szerkesztőségi rendszer és Portál
54. Külön jogszabályban meghatározott, az Európai unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásához kapcsolódó rendszerek (HCR-tagállami)
55. Központi Kormányzati Hírlevélküldő rendszer

3. Melléklet: a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói:

	A	B	C	D
	A nyilvántartás megnevezése	**Adatfeldolgozó**	**Az adatfeldolgozó által végzett adatfeldolgozás köre**	**Az adatfeldolgozó igénybevételének jellege**
	Foglalkoztatási és Közfoglalkoztatási Adatbázis	NISZ Zrt.	teljes adatfeldolgozás	az adatkezelő döntésétől függő
	Az állami foglalkoztatási szerv feladatainak ellátásához szükséges adatbázis	NISZ Zrt.	teljes adatfeldolgozás	az adatkezelő döntésétől függő
	Egységes szociális nyilvántartás	Magyar Államkincstár központi szerve	teljes adatfeldolgozás	az adatkezelő döntésétől függő
	Az európai uniós források felhasználásához kötődő adatfeldolgozói feladatok	NISZ Zrt., Új Világ Nonprofit Szolgáltató Korlátolt Felelősségű Társaság	elektronikus adatfeldolgozás	kötelező
	A polgárok személyi adatainak és lakcímének nyilvántartása	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Elektronikus anyakönyvi nyilvántartás	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Földhasználati nyilvántartás	Budapest Főváros Kormányhivatala és megyei kormányhivatalok járási hivatalai	teljes adatfeldolgozás	kötelező
	Az államhatár adatbázisa, az állami nagyméretarányú topográfiai térképi adatbázisok, az állami távérzékelési adatbázisok, a Földrajzinév-tár adatbázis	Budapest Főváros Kormányhivatala	teljes adatfeldolgozás	kötelező
	Az alapponthálózati pontok adatbázisa, az állami földmérési alaptérképi adatbázis, az archív analóg és digitális térképi adatok adatbázisai.	földmérési és térinformatikai államigazgatási szervként eljáró Budapest Főváros Kormányhivatala	teljes adatfeldolgozás	kötelező

	Ingatlan-nyilvántartás, az állami ingatlan-nyilvántartási térképi adatbázis	földmérési és térinformatikai államigazgatási szervként eljáró Budapest Főváros Kormányhivatala, fővárosi és megyei kormányhivatalok ingatlanügyi hatósági hatáskörében eljáró járási (fővárosi kerületi) hivatalai	teljes adatfeldolgozás	kötelező
	Közepes és kisméretarányú állami topográfiai térképek	MH Geoinformációs Szolgálat és HM Térképészeti Közhasznú Nonprofit Kft.	teljes adatfeldolgozás	kötelező
	Nyugdíj-biztosítási nyilvántartás	kizárólagos állami tulajdonú gazdálkodó szervezet	teljes adatfeldolgozás	az adatkezelő döntésétől függő
	Egészségbiztosítási nyilvántartás	kizárólagos állami tulajdonú gazdálkodó szervezet	teljes adatfeldolgozás	az adatkezelő döntésétől függő
	Központi útiokmány-nyilvántartás	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Szabálysértési nyilvántartási rendszer	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Közúti közlekedési nyilvántartás	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	A Magyar igazolvány és a Magyar hozzátartozói igazolvány tulajdonosainak nyilvántartása	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Kulturális örökségvédelmi nyilvántartás	államigazgatási szerv	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő
	A Nemzeti Adó- és Vámhivatal által kezelt adóhatósági és vámhatósági adatok nyilvántartása	Pillér Pénzügyi és Számítástechnikai Kft.	teljes adatfeldolgozás	az adatkezelő döntésétől függő
	A Nemzeti Adó- és Vámhivatal által kezelt, a 19. pont alá nem tartozó adatok nyilvántartása	Pillér Pénzügyi és Számítástechnikai Kft.	teljes adatfeldolgozás	az adatkezelő döntésétől függő
	Cégnyilvántartás	Magyar Közlöny Lap- és Könyvkiadó Korlátolt Felelősségű Társaság	teljes adatfeldolgozás	kötelező

	Központi idegenrendészeti nyilvántartás	IdomSoft Zrt., Nemzeti Szakértői és Kutató Központ	elektronikus adatfeldolgozás	kötelező
	A Magyar Államkincstár mezőgazdasági és vidékfejlesztési támogatási feladataihoz kapcsolódó nyilvántartási rendszerek	kizárólagos állami tulajdonú gazdálkodó szervezet	teljes adatfeldolgozás	az adatkezelő döntésétől függő
	N.SIS	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Kötvénynyilvántartás	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Az egyéni vállalkozók nyilvántartása	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Bűnügyi nyilvántartási rendszer	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
	Egységes örökbefogadási nyilvántartás	Magyar Államkincstár központi szerve	elektronikus adatfeldolgozás	kötelező
	Természetes személyek közhiteles országos adósságrendezési nyilvántartása, az adósságrendezési eljárással összefüggő hirdetményi rendszer	Magyar Közlöny Lap- és Könyvkiadó Korlátolt Felelősségű Társaság	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő
	Természetes személyek adósságrendezési eljárásával összefüggő nyomtatványellenőrzési és nyomtatványkitöltő informatikai rendszer	NISZ Zrt.	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő

2.5. Irodalomjegyzék

Berzsenyi Dániel et al. (2017): Incidensmenedzsment. Dialóg Campus Kiadó, Budapest.

Leitold Ferenc (2014): Sebezhetőségvizsgálatok a gyakorlatban. Nemzeti Közszolgálati Egyetem, Budapest.

Legális szoftverekkel támadnak a kiberbűnözők – 2017. február 13. hétfő – 10:45/piacesprofit.hu. Elérhetőség: http://www.piacesprofit.hu/infokom/legalis-szoftverekkel-tamadnak-a-kiberbunozo (utolsó ideje: 2018. március 25.)

3. LATTMANN TAMÁS: NEMZETKÖZI JOGI SZABÁLYOZÁS CÉLZOTT KIBERTÁMADÁSOK ESETÉN

3.1. Bevezetés

A jelen tanulmány azt a kérdést járja körbe, hogy a nemzetközi jog hogyan tudja szabályozni a célzott informatikai támadásokat. Átfogóan vizsgálja a támadások lehetséges elkövetési környezeteit, és rámutat a fennálló különbségekre. Emellett megvizsgálja az informatikai támadásokhoz kapcsolódó személyi, jogszerűségi kérdéseket, és kitér az esetleges nemzetközi büntetőjogi felelősségre vonás lehetőségére is.

3.2. Informatikai támadások lehetséges nemzetközi jogi környezete

Egy informatikai támadásra sor kerülhet tényleges fegyveres konfliktus fennállása során, valamint anélkül is, állami háttérrel vagy valamiféle magán kezdeményezésre. Ezek mind különböző helyzetekre vezetnek, ami a létező nemzetközi jogrend más és más elemeinek alkalmazhatóságát váltják ki. Négy különböző lehetőséget tudunk azonosítani:

- nincs fegyveres konfliktus, nincs állami háttér;
- nincs fegyveres konfliktus, de van állami háttér;
- folyamatban van fegyveres konfliktus, és a támadás mögött van állami háttér;
- folyamatban van fegyveres konfliktus, de a támadás mögött nincs állami háttér.

3.2.1. Informatikai támadás fegyveres konfliktus és állami háttér nélkül

Amennyiben nem áll fenn fegyveres konfliktus az államok között, azaz nincsenek katonai tevékenységek, és a támadás mögött nincs állami háttér, akkor a kibertámadás a jelenlegi jogszabályi környezet alapján az érintett állam belső jogi előírásai szerinti bűncselekménynek minősül. Az államok belső joga meghatározza ezeket a bűncselekményeket, így például Magyarországon a Büntető Törvénykönvről szóló 2012. évi C. törvény, amelynek az információs rendszer elleni bűncselekményekről szóló XLIII fejezetében jelennek meg ilyen bűncselekmények. E mellett még számos más bűncselekmény is kapcsolódhat ezekhez az előírásokhoz, például a Btk. 287. §, 314. §, 375. § előírásai határoznak meg.

Ilyen helyzetekben a nemzetközi jog szerepe csupán kiegészítő. Amellett, hogy elismeri e belső jogi meghatározásokat, segíti azok összhangjának megteremtését, valamint megteremtik az államok között az ilyen bűncselekményekkel szembeni fellépéshez feltétlenül szükséges nemzetközi büntető együttműködés kereteit és főbb szabályait. A témában elfogadott legfontosabb nemzetközi szerződésnek jelenleg az Európa Tanács keretében elfogadott számítógépes bűnözés elleni egyezmény

tekinthető.[130] Az egyezmény szerkezete és tartalma jól mutatja e kettős feladatkört: bűncselekményeket határoz meg, valamint rendelkezik az államok közötti együttműködésről. Elsődlegesen nem a kibertámadásokra alkották, hanem a számítástechnikai eszközökkel elkövetett egyéb, többnyire az üzleti szférának jelentős károkat okozó bűncselekményekkel szemben. Jelentőségéről árulkodik, hogy bár az Európa Tanács keretében fogadták el, részesévé vált Ausztrália, Japán és az Egyesült Államok is, hiszen ezeknek az államoknak érdekében áll a részvétel ebben a rendszerben, tekintettel arra, hogy a szerzői jog által védett termékeik illegális másolásával és terjesztésével folyamatos veszteségeket szenvednek.

Egy területen válik ez igazán érdekessé, nevezetesen a nemzetközi jogilag lehetséges állami ellenintézkedések köre tekintetében. A jelenlegi nemzetközi jogi értelmezések többsége nem ismeri el azt, hogy nem állami szereplők a nemzetközi jog szerint értelmezhető „támadást" kövessenek el. amivel szemben az államok az önvédelem eszközéhez nyúlhatnának,[131] ami látszólag szűkíti e kört. Azaz jelenleg azt állíthatjuk, hogy egy ilyen helyzetben az informatikai támadással érintett állam nem gyakorolhat önvédelmet. Ugyanakkor meg kell jegyezni, hogy az utóbbi két évtized állami gyakorlata – leginkább a terrorista szervezetekkel és a nemzetközi terrorizmussal szembeni fellépés keretében – azt az ettől eltérő értelmezést látszik erősíteni, hogy az államok fenntartják az önvédelem alkalmazhatóságát olyan helyzetben is, ha a támadást nem egy államtól, hanem egy nem állami szereplőtől szenvedik el.[132] Ez azt jelenti, hogy egyelőre nem tudunk egyértelműen állást foglalni a kérdésben.

3.2.2. Informatikai támadás fegyveres konfliktus nélkül, állami háttérrel

Egészen más, bonyolult helyzetre vezet, ha informatikai támadásra állami háttérrel vagy állami intézmények által, valamiféle politikai célok szolgálata érdekében kerül sor, de az államok között amúgy nincs fegyveres konfiktus. Az ilyen támadásokban részt vevő személyek aktusai továbbra is a fentiek szerint minősíthetők, ám amennyiben azok betudhatók egy államnak, ez az állam felelősségét is keletkezteti. Ez nem csupán azt jelenti, hogy az állam köteles az okozott károk megtérítésére, hanem adott esetben arra is vezethet, hogy abban feloldódhat a részt vevő egyének büntetőjogi felelőssége. Újfent analógiákkal tudunk élni: ahogy egy állam által egy másik állam ellen felállított katonai blokád személyzetét sem vonhatjuk büntetőjogilag felelősségre csupán amiatt, hogy a blokád maga a nemzetközi jog alapján jogsértőnek bizonyul, ugyanez a kérdés merülhet fel az ilyen helyzetben végrehajtott informatikai támadások elkövetőivel szemben.

Természetesen ilyenkor meghatározó fontosságú kérdés, hogy a nemzetközi jog hogyan határozza meg az ilyen lépések jogszerűségét. Ma az ENSZ Alapokmányára épülő nemzetközi jogi rezsimen belül a *ius ad bellum* előírásai segítenek annak megállapításában, hogy adott helyzetben egy állam jogszerűen alkalmaz-e erőt egy másik állammal szemben, azaz hogy milyen esetben jogszerű egy támadás végrehajtása. Ennek fő vonalait a mai rendszer akként határozza meg, hogy arra csak fegyveres támadásra adott önvédelem, vagy az ENSZ Biztonsági Tanács által az Alapokmány VII. fejezete alapján elrendelt módon kerülhet sor jogszerűen.

Ám az első kérdés annak tisztázása, hogy egy informatikai támadás a nemzetközi jog fenti kérdésben kialakított mércéinek megfelelő *fegyveres támadásnak* tekinthető-e. Az elmúlt időszakban született szakértői értelmezések többsége ezt nem támogatja, többnyire amiatt az aggodalom miatt, hogy az informatikai támadások ilyenként való elismerése azonnal felvetné az önvédelem kérdését, és az elemzők többsége az erő alkalmazásának tilalmának abszolút jellegének fellazulása miatt aggódik – azaz egy végrehajtott informatikai támadás könnyedén vezethetne tényleges erő alkalmazásához önvédelem jogcímén. Ugyanakkor a kérdés vizsgálata során nem hagyhatjuk figyelmen kívül az álla-

---

130 *Convention on Cybercrime.* CETS No.: 185. Magyar nyelven kihirdette: *2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.*

131 Ehhez lásd pl. Kajtár, 2015.

132 Ennek bemutatásához bővebben lásd pl. Lattmann, 2011; Dinstein, 2011, 230. o.

mok gyakorlatát, amely az önvédelem területén amúgy is sokkal inkább egy megengedőbb értelmezést vezet át a gyakorlatba, ennek megfelelően pedig a szakértői értelmezések egy része is állást foglal annak lehetősége mellett, hogy adott esetben egy informatikai támadást tényleges fegyveres támadásnak tekintsünk, azaz óvatosan ugyan, de nyitva hagyják a lehetőséget. Erre jó példaként szolgál Stéphane Abrial tábornok, a NATO Szövetséges Átalakítási Parancsnokság (NATO ATC) vezetőjének 2011-ben közzétett véleménycikke a New York Times hasábjain,[133] valamint a NATO CCD COE által 2012-ben kiadott útmutató, amely kijelenti, hogy egy informatikai támadás adott esetben beilleszthető az agressziós cselekmények fogalmi körébe, és ezzel egyidejűleg kiválthatja az önvédelem gyakorolhatóságát is.[134] A Nemzetközi Bíróság a nukleáris fegyverek alkalmazhatóságával kapcsolatos tanácsadó véleményében korábban úgy értelmezte az „erő alkalmazásának tilalma“ fogalmát, hogy az bármilyen eszközzel megsérthető, az előírás nem meghatározott fegyverekre vonatkozik – ebből következően érvelhetővé válik, hogy egy informatikai támadás is alkalmas lehet e tilalom megsértésére.[135]

Amennyiben arra a következtetésre jutunk, hogy egy informatikai támadás megfelel a nemzetközi jogi értelemben vett „fegyveres támadás” fogalmának, abból következően számos további kérdés merül fel. A nemzetközi jog jelenlegi rendszerében egy fegyveres támadás az annak áldozatául esett állam oldalán kiváltja az önvédelem gyakorlásának jogát, ami lehetővé teszi a fegyveres erő jogszerű alkalmazását. Ez rögtön felveti az informatikai támadásokkal szembeni önvédelem eszköztárának kérdését. Az nem vitatott, hogy a passzív védelmi rendszerek alkalmazása jogszerű, hiszen ezek célja éppen a támadások azonnal elhárítása, ám amennyiben mégis sor kerül ilyenre, milyen reakciókat enged meg a nemzetközi jog? Ketté kell választanunk az önvédelem lehetséges körén belüli lehetséges válaszlépéseket: egyrészt vizsgálni kell az azonos eszközökkel elkövetett informatikai „ellentámadások” jogszerűségét, másrészt pedig az ennél jóval kényesebb tűnő, fegyveres erő alkalmazásával történő önvédelmi intézkedések lehetőségét, azaz azt a kérdést, hogy jogszerű lehet-e egy katonai támadás az informatikai támadáshoz felhasznált eszközök vagy infrastruktúra ellen.

Az első eset messze nem annyira egyértelmű, mint ahogy gondolnánk. Mert bár logikusnak tűnik, hogy egy támadással szemben megengedhető az azonos mértékű és jellegű ellentámadás, a nemzetközi jog gyakorlata a fegyveres önvédelem esetében tiltja,[136] a nem fegyveres ellenintézkedések esetében viszont bizonyos mértékig tolerálja a megtorló jellegű ellenlépéseket, azaz az olyan intézkedéseket, amelyek nem az adott jogsértő cselekmény közvetlen elhárítására alkalmasak, hanem a további ilyenektől való távoltartásra. Ebből következik egy logikai csapdahelyzet: amennyiben az informatikai támadásokat nemzetközi jogi értelemben vett támadásoknak tekintjük, úgy a védekező állam nemzetközi jogi lehetőségei szűkülnek. Mivel fentebb arra a következtetésre jutottunk, hogy lehetséges egy informatikai támadást nemzetközi jogi értelemben vett támadásnak tekintetni, ezt azt jelenti, hogy csak azok az informatikai ellentámadások jogszerűek, amelyek egy folyamatban lévő támadás elhárításához szükségesek, tehát ez a döntő szempont a jogszerűség megállapításához. Amennyiben viszont az informatikai támadásokat nem tekintjük nemzetközi jogi értelemben vett támadásnak, hanem „csupán“ nemzetközi jogsértésnek, úgy a nemzetközi jogsértésekkel szemben alkalmazott ellenintézkedések (retorzió, represszália) alkalmazásával a fenti korlátozás helyébe egy arányossági vizsgálat kötelezettsége lép, ami adott esetben tágabb mozgásteret biztosít az áldozatul esett állam számára.

A fegyveres erő alkalmazása egy informatikai támadással szembeni önvédelemként a fentebb említett korlátozás megléte mellett kiegészül azzal a kötelezettséggel is, hogy az ilyen önvédelmi célú erő-alkalmazásnak teljesítenie kell az önvédelemmel kapcsolatos egyéb kritériumokat is, azaz a támadás

133 Abrial, 2011.
134 Klimburg, 2012.
135 *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion.* I.C.J. Reports 1996, p. 226, Para. 39.
136 Dinstein, 2011, 231. o.

elhárítására nincs más mód (szükségességi kritérium), az nem okoz nagyobb kárt (arányossági kritérium), valamint arra akkor kerül sor, amikor az erre az elhárításra képes (azonnalisági kritérium).[137] Ezek egységes fennállása biztosítja, hogy az intézkedés ne megtorló jellegű legyen, amely tilalomra fentebb utaltam. Bár egy informatikai támadás esetében nem könnyű ezek teljesülését biztosítani, úgy vélem, hogy nem lehetetlen, ami azt jelenti, hogy adott helyzetben nem zárható ki a fegyveres önvédelem egy informatikai támadással szemben.

Egyelőre nincs kikristályosodott, széles körben elfogadott álláspont, és jó eséllyel egy ideig nem is lesz – e kérdés ugyanúgy az eltérő értelmezések szövevényes hálójában fog vergődni, mint maga az önvédelem kérdése, illetve az annak különböző formái (lásd az előző pontban). Személyes véleményem, hogy a mai digitalizált társadalmakban bőven lehetséges olyan informatikai támadást végrehajtani, amely olyan mértékű károkat, adott esetben civil károkat (gondoljunk csak a különböző automatizált, számítógépek irányította rendszerekre, amelyek meghibásodása halálhoz, vagy tömeges szerencsétlenséghez vezethet) okozhat, aminek a hatásai mérhetők egy klasszikus fegyveres támadáshoz, sőt, akár túl is szárnyalhatják azokat. Egy ilyen esetben a politikai kényszer hatására még egy olyan állam is könnyen megváltoztatja az álláspontját, amely eddig elutasította az önvédelem alkalmazhatóságát ilyen helyzetekben, a nemzetközi jog világában ez nem ritkán fordul elő.

3.2.3. Informatikai támadás fegyveres konfliktus során, állami háttérrel

Az informatikai támadások jogi megítélése egyszerűsödik abban a helyzetben, ha az államok között amúgy fennáll egy fegyveres konfliktus, amellyel az adott támadás kapcsolatban áll, és amelynek végrehajtója az államhoz tartozik, hiszen ilyen esetben vitathatatlan, hogy a felhasznált informatikai eszközök a folyamatban lévő ellenségeskedések során az egyik érintett állam katonai céljainak szolgálatában állnak. Az informatikai támadások ebben a kontextusban többféle célra is alkalmasak lehetnek, így például ellenséges katonai adatok gyűjtésére, az ellenséges katonai vezetés félrevezetésére vagy pszichológiai hadviselésre, irányító vagy egyéb informatikai eszközök megzavarására, vagy adott esetben akár tényleges támadásra, hiszen a fegyverek mellett DoS vagy DDoS eszközökkel vagy előre telepített vírusokkal is lehetséges jelentős károkat okozni.

Kérdés, hogy milyen módon – ha egyáltalán – szabályozza a jog az ilyen cselekményeket. Álláspontom szerint minden ilyen cselekményre a hadviselésre vonatkozó nemzetközi joganyag, a *ius in bello* előírásainak teljes körét megfelelő módon alkalmazni kell, hiszen az 1949-ben elfogadott Genfi egyezmények[138] közös 2. cikke annak előírásait minden „fegyveres konfliktus" esetén alkalmazni rendeli. Erre bővebben a következő részben térek ki.

A teljesség kedvéért itt érdemes hozzátenni, hogy egy államon belüli fegyveres konfliktus esetén annyiban lehet más a helyzet, hogy ilyenkor az alkalmazható humanitárius jogi szabályok köre szűkebb ugyan, de az érdemi különbségek a szokásjogilag kötelező normák között elenyészőek, tehát a következő részben foglaltak nagy részét megfelelően lehet alkalmazni itt is.

---

137 Dinstein, 2011, 231-233. o..

138 *Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.* Geneva, 12 August 1949. UNTS vol. 75. (továbbiakban: I. Genfi egyezmény); *Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea.* Geneva, 12 August 1949. UNTS vol. 75. (továbbiakban: II. Genfi egyezmény); *Convention (III) Relative to the Treatment of Prisoners of War.* Geneva, 12 August 1949. UNTS vol. 75. (továbbiakban: III. Genfi egyezmény); *Convention (IV) Relative to the Protection of Civilian Persons in Time of War.* Geneva, 12 August 1949. UNTS vol. 75. (továbbiakban: IV. Genfi egyezmény); Megerősítette azokat az *1954. évi 32. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, az 1949. évi augusztus hó 12. napján kelt nemzetközi egyezményeknek a Magyar Népköztársaságban való törvényerejéről,* közzétette azokat: sorrendben 2000/17., 2000/18., 2000/19., 2000/16. sz. nemzetközi szerződések a külügyminisztertől.

3.2.4. Informatikai támadás fegyveres konfliktus során, állami háttér nélkül

Amennyiben folyamatban van egy fegyveres konfliktus az államok között, de a konkrét informatikai támadás mögött nincs állami háttér, vagy annak végrehajtója nem állami szereplő, a kialakult helyzet nemzetközi jogi szempontból igen nehezen kezelhető. Hozzá kell tenni, hogy ezt nem informatikai hadviselési helyzetben is nehezen kezeli a nemzetközi jog, hiszen a különbségtétel elvének ilyen fokú sérelme fenntarthatatlanná teszi azt a követelményt, hogy az összeütköző feleknek folyamatosan különbséget kell tenniük a személyek között annak alapján, hogy tevékenységük a nemzetközi jog alapján jogszerű-e: a III. Genfi egyezmény alapján kombattánsként, azaz jogszerű harcosként elismert személyek cselekményeinek más a jogkövetkezménye, mint a civileké, ahogy a velük való bánásmódra is eltérő szabályokat írnak elő az egyezmények, különösen a polgári lakosság védelméről szóló IV. Genfi egyezmény.

E kérdés fontossága okán a következő külön fejezetben térek ki az egyéni részvétel kérdésére.

3.3. A „támadás" után: a hadviselés jogának analóg alkalmazása

A jelenlegi nemzetközi jogrendben nincsenek kötelező formában létező olyan hadijogi szabályok, amelyek kifejezetten az informatikai hadviselésre vonatkoznának. E látszólagos hiányosságnak legfőbb oka, hogy a nemzetközi humanitárius jogi előírások nemzetközi szerződésekbe foglalásának idejében az „informatikai hadviselés" nem volt olyan tényező, amivel számolni kellett volna. Amikor a hadviselés jogát 1949-ben és 1977-ben, a Genfi egyezmények és annak kiegészítő jegyzőkönyvei elfogadásával az államok a létező körülmények figyelembe vételével kodifikálták, nem foglalkoztak ezzel a fajta sajátos konfliktusos helyzettel, így szerződésalkotó akaratuk sem terjedt ki arra. Ez azt jelenti, hogy a nemzetközi jog egyik nagyon fontos jogalkotó tényezője, a szerződő államok eredeti akarata (amit általában a nemzetközi szerződések előkészítő irataiból, a történelmi-politikai körülményekből, állami nyilatkozatokból tudunk rekonstruálni vagy igazolni) nem áll rendelkezésünkre. Amire viszont lehet támaszkodni, az az a feltevés, hogy a nemzetközi humanitárius jog alapelvi szintű szabályai és a hadviselés jogának szokásjogi normái tekintetében továbbra is megvan a konszenzus államok között, de ezeken túlmenően bármilyen kötelező erő meglétét külön bizonyítani kell, és e területeken további, célzott nemzetközi jogfejlesztése van szükség, ami tevékeny nemzetközi jogalkotást igényel, adott esetben újabb nemzetközi szerződés(ek) elfogadását.

Mint azt egy korábbi tanulmányban már jeleztem, az informatikai hadviselés jogi szabályozása több komoly problémával kell szembenézzen.[139] Az egyik ilyen a megfogható „tér", mint elem hiánya, azaz az informatikai támadások helye, amit nem könnyű szabályozási területként kezelni. A nemzetközi jog szempontjából ez azért fontos, mert az egész modern nemzetközi jogrendünk a területük felett szuverenitást gyakorló államok rendszerén alapszik, emiatt pedig mind az erő alkalmazását szabályozó joganyag (jus ad bellum), mind pedig a nemzetközi humanitárius jog (jus in bello) nehezen elválaszthatató az államterület kérdésétől. Viszont az informatikai támadások esetében nem könnyű a területiségre alapozni, hiszen míg a fizikai csatatereken vannak államhatárok, demarkációs vagy frontvonalak, ezek a kibertérben nehezen értelmezhetők. Egy informatikai támadást államterülethez kötni annak megindítása és hatása tekintetében tudunk, valamint az ahhoz felhasznált informatikai eszközök fizikai elhelyezkedése alapján, azaz itt lehetséges kapcsolatot teremteni a „virtuális tér" és az államok területe, valamint joghatósága között. Ezek összességében nem teszik lehetetlenné a feladatot, ám jogalkotási terhet rónak az államokra, azaz szabályozniuk kell a területükön folytatott

[139] Lattmann, 2013.

informatikai tevékenységeket, még pedig olyan módon, hogy azok konformitásban álljanak a már létező, vagy a jövőben kialakítandó nemzetközi jogi normákkal.

Egy másik, már hadviselési természetű nehézség az informatikai hadviselés jogi szabályozása tekintetében, hogy az úgynevezett „virtuális csatatér" nem tisztán katonai jellegű. Léteznek ugyan természetesen kifejezetten katonai használatú informatikai rendszerek és eszközök, ám az adatforgalom nagyon jelentős része a polgári használatú hálózaton zajlik, ahogy magának az internet eredeti koncepciójának is lényegi eleme az volt, hogy az adatforgalom több különböző szálon is futhasson, adott esetben olyan központ nélkül, amit egy nukleáris csapás megsemmisíthet. Ez azzal a következménnyel jár, hogy az informatikai támadások nagy része mindenképpen civil, vagy legalábbis kettős rendeltetésű objektumok ellen fog irányulni, ami ráadásul igaz lehet az ellenintézkedések, ellentámadások tekintetében is. Ennek következménye az egyik alapvető hadviselési szabály, a különbségtétel elvének gyakorlati alkalmazásának a nehézsége. Ilyen körülmények között nem könnyű meghatározni, hogy mi minősül jogszerűen támadható katonai célpontnak, sem az előzetes műveleti tervezés, sem pedig egy esetleges azonnali ellentámadás során. Ugyanígy, az is nehezen állapítható meg, hogy informatikai támadások során ki minősül hadijogi terminológia szerinti „jogszerű harcosnak", vagy kinek az informatikai eszközeit tekinthetjük harceszköznek, ami pedig meghatározó fontosságú abban a kérdésben, hogy milyen személyekkel szemben milyen állami intézkedéseket tartunk megengedhetőnek. Ehhez kapcsolódik végül, de nem utolsósorban az esetleges jogsértésekkel szembeni fellépés nehézsége, mind a jogsértő ellenségeskedésekbe bocsátkozás, mind pedig a hadijogi szabályok megsértése miatt. Az előbbi problémát, azaz a fizikai hadviselés során a harcokba közvetlenül bocsátkozó civil cselekményének jogsértő jellegét fel lehet ismerni a Genfi egyezmények meghatározta kritériumok hiányában a helyszínen, és az azzal szembeni büntetőjogi fellépésre lehetőséget biztosítanak az egyezmények. Informatikai támadások esetében ugyanakkor ez több száz, vagy akár ezer kilométeres távolságból nehezen elképzelhető, az érintett civil személy saját állama pedig nyilvánvaló okokból nem fog büntető együttműködés keretében segítséget nyújtani ehhez. A második kérdést, azaz az informatikai támadásokkal megvalósítható háborús bűncselekmények problémáját a következőkben vázoljuk majd röviden.

A kodifikált szabályok hiánya ugyanakkor nem jelent teljes szabályozatlanságot. A nemzetközi humanitárius jog szokásjogi alapon kötelező elveinek alapul vételével kialakíthatók olyan szabályok, amelyek alkalmazhatósága nehezen megkérdőjelezhető egy informatikai támadás, vagy akár egy átfogó „kiberháború" során. Ehhez alapként 1977-ben elfogadott I. Kiegészítő jegyzőkönyvet[140] lehet használni, amely számos olyan hadviselési normát foglalt írásos, nemzetközi szerződési formába, amelyek informatikai támadások esetében is alkalmazhatóak. E munka első eredménye a 2013-ban megjelent Tallinni kézikönyv,[141] amely első alkalommal tett kísérletet e szabályok rendszerbe foglalt megjelenítésére, majd ezt 2017-ben egy újabb kiadás követte.[142] Ezek a munkák olyan szakértői értelmezést jelentenek, amelyek célja, hogy a létező hadviselési jogi normák felhasználásával állítsanak elő egy olyan szabálygyűjteményt, ami egyrészt tükrözi a jelenleg létező alkalmazható szabályokat, másrészt pedig egy későbbi nemzetközi szerződés alapjául is szolgálhatnak akár. Nemzetközi jogi értelemben a kézikönyvek tartalma nem kötelezi az államokat – ám a szokásjogi erejű normák alkalmazásától nem térhetnek el.

A különbségtétel fent leírt elvét például a Kiegészítő jegyzőkönyv 48. cikke a hadviselés területén úgy határozza meg, hogy az ellenségeskedések során az összeütközők kötelesek katonai műveleteiket a szembenálló fél katonai objektumai ellen irányítani, amely szabály szokásjogi ereje vitán felül

---

140 *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I).* Geneva, 8 June 1977. UNTS vol. 1125. (továbbiakban: I. Kiegészítő jegyzőkönyv). Megerősítette és magyar nyelven kihirdette az *1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben 1949. augusztus 12-én kötött Egyezmények I. és II. kiegészítő Jegyzőkönyvének kihirdetéséről.*

141 Schmitt, 2013.

142 Schmitt, 2017.

áll.[143] A nemzetközi jog nem enged eltérést ettől, így természetesen még informatikai támadás során is alkalmazni kell. Ez az előírás a Tallinni kézikönyv 31. számú szabályában teljesen azonos módon jelenik meg egy informatikai támadás esetében is.

Érdemes újra kitérni a „támadás" fogalmára is, amelynek „jus ad bellum" szerinti értelmezését megadtuk korábban, és megvizsgálni annak „jus in bello", azaz hadijogi tárgyú értelmezését egy informatikai támadás esetében. A hadviselési jogában a Jegyzőkönyv 49. cikke azt „erőszakos" cselekményként írja le, mégpedig a szövegezés szerint „bárhol folyó mindennemű" támadás lehet. Az „erőszakos" és „bárhol" kifejezések kiterjesztő értelmezése lehetővé teszi, hogy a meghatározás magába foglalja az informatikai támadásokat is. Ezzel látszólag szemben áll, hogy a Jegyzőkönyv hivatkozott cikkének következő bekezdésének szövegezése „szárazföldi, légi vagy tengeri hadviselésre" hivatkozik, kihagyva a felsorolásból az informatikai hadviselést, utalva arra, hogy a szerződés szövegezésekor a szerződő államok nem céloztak az informatikai támadásokra. Tény, hogy a szövegező államok számára a hetvenes években még nem volt hadviselési realitás a célzott informatikai támadások lehetősége, ezért az utalás kihagyása nem értékelhető szándékosként, és erre a szerződés előkészítő dokumentumai, illetve a korszak szakirodalmi forrásai sem tartalmaznak bármilyen utalást.[144] A szövegező államok még a fizikai terület szempontjából gondolkodtak a támadás meghatározásáról, és nem a támadások hatásai, hanem eszközei irányából közelítették meg a kérdést. A Tallinni kézikönyv viszont már a hatás-elven gondolkodva, az eszköz alkalmazásának színterének kritériumait megkerülve, a 30. szabály megfogalmazásakor informatikai támadásként az olyan, akár támadó, akár védekező jellegű informatikai műveleteket határozza meg, amelyek „megalapozottan személyek sérülésével vagy halálával, vagy anyagi javak megsemmisülésével vagy megrongálódásával járhatnak".

A polgári javak védelmének és a „katonai célpontok" meghatározásának kérdése alapvető fontosságú a hadviselés szabályozása szempontjából. A jegyzőkönyv 51-52. cikke tartalmazza az ezekre vonatkozó, mára már szokásjogi erejűnek tekintett szabályokat. Ezek az előírások megfelelően alkalmazandók egy informatikai támadás esetében is, a Tallinni kézikönyv 32-40. számú szabályai kimerítően foglalkoznak e kérdéssel. A kézikönyv által felvázolt szabályozás összehasonlítása a jegyzőkönyvben foglalt, és a nemzetközi szokásjog által is ismert előírásokkal azt mutatja, hogy az informatikai támadásokra kialakított előírások egy párhuzamos szabályozási rezsimet alakítottak. A polgári javak védelméhez szorosan hozzátartozik a hadviselés során kötelezően megteendő óvintézkedések kötelezettsége, a bizonyos objektumok számára biztosított különleges védelem (egészségügyi létesítmények, kulturális javak stb.), és még számos egyéb szabály, amelyek esetében ugyanezt a párhuzamosságot tudjuk felfedezni.

Terjedelmi okokból további összehasonlításokat most nem teszünk, összességében megállapíthatjuk, hogy a nemzetközi humanitárius jog alapelvei és kötelező alapvető szabályainak alkalmazása a célzott informatikai támadások, valamint általánosságban az informatikai hadviselés során is kötelező.

3.4. Egyének aktív részvétele az informatikai támadásokban és ennek nemzetközi jogi hatásai

A hadviselés elmúlt évtizedekben megjelent és elterjedt új módszerei, különösen az aszimmetrikus hadviselési helyzetek egy új problémát helyeztek a figyelem fókuszába. A kérdés, hogy mit tud kezdeni a nemzetközi jog azzal a helyzettel, amikor szándékoltan és módszeresen olyan személyek válnak az ellenségeskedések aktív résztvevőivé, akik arra a nemzetközi hadijog szabályai alapján nem bírnak felhatalmazással, ám ezt ők vagy saját döntésükkel, vagy pedig az állam belső jogi parancsára

[143] A szokásjogi erő tekintetében lásd a Vöröskereszt Nemzetközi Bizottságának szokásjogi tanulmánya által felállított 7., 146. és 147. sz. szabályait. Henckaerts – Doswald-Beck, 2009, 25, 519, 523. o.

[144] A jegyzőkönyv szövegezését kísérő vitákról és kérdésekről bővebben lásd pl. Herczegh, 1981.

figyelmen kívül hagyják. A nemzetközi humanitárius jogi szerződések ezt a helyzetet bizonyos mértékig próbálják szabályozni a kombattáns-civil státusz elhatárolásával, ahogy ennek szokásjogi alapjai is többé-kevésbé tisztázottak,[145] mindennek ellenére a kérdés gyakorlatban felmerülő problémái a szakirodalmi szerzők körében is élénken kutatott problémákká váltak.[146] Ennek gyakorlati jelentősége az, hogy a nemzetközi jog a kombattáns státusz keretében jogi védettséget biztosít az ellenséges fél számára ártó cselekmények végrehajtójának, amennyiben azokat a cselekményeket a hadijogi szabályokkal összhangban hajtotta végre.

Ahogy egy korábbi tanulmányban már szintén jeleztem, a „civil részvétel" problémája hatványozottan jelentkezhet az informatikai támadások esetében, a kisebb veszélyérzet, valamint a tevékenység viszonylagosan egyszerű természete okán.[147] Ez felveti azt a kérdést, hogy a genfi egyezmények és a gyakorlat által kialakított kettős felosztást lehet-e analóg módon alkalmazni az informatikai támadások tekintetében, különösen egy olyan helyzetben, ahol ennek az elméletinek tűnő kérdésnek hirtelen nagy gyakorlati jelentősége keletkezik. Nem csupán amiatt, hogy eldönthessük, valakinek joga van-e részt venni egy informatikai támadásban, hanem sokkal inkább azért, hogy megállapíthassuk a vele szemben alkalmazható ellenintézkedések lehetséges körét, beleértve ebbe nem csupán az esetleges büntetőjogi következmények alkalmazását, hanem akár a valamiféle ellentámadások lehetséges körét.

Az informatikai hadviselés nemzetközi jogi kérdéseit körbejáró Tallinni kézikönyv szerzői érintették ezt a kérdést, és a fent jelzett létező forrásokba foglalt normatartalmat próbálták meg analóg módon alkalmazni. Alapvetésként rögzítették a 35. számú szabályt, amely evidens jelleggel mondja ki, hogy a polgári személyek elveszítik védettségüket az ellenségeskedésekben való közvetlen részvétel esetén,[148] ami értelmezésükben azt jelenti, hogy jogszerűen támadhatóvá válnak mind informatikai, mind „egyéb jogszerű módszer" alkalmazásával.[149] A szöveg kritikai elemzése annak látszólagos logikája mellett felvet értelmezési kérdéseket, így különösen a „jogszerű" kitétellel kapcsolatban, valamint nyitva hagyja a „passzív", azaz a nem szándékos, de mégis közvetlennek tekinthető részvétel problémáját.

Aktív részvétel alatt azt a helyzetet értem, amikor valaki szándékosan, a cselekményről tudva és annak eredményét kívánva cselekszik, vagy mulaszt el cselekvést. Passzív részvétel alatt azt értem, amikor egy polgári személy gondatlanságból válik egy informatikai támadás résztvevőjévé, például úgy, hogy elmulasztja saját számítástechnikai eszközeinek védelmét, ezért válik a számítógépe ilyen támadás áldozatává. Értelmezésemben elsősorban a támadásról való tudomás megléte vagy hiánya, másodsorban pedig annak eredményének kívánalmának vagy hiánya vezet az aktív és a passzív részvétel közti különbségtételre.

Aktív részvétel esetében a fenti, Tallinni jegyzőkönyvi értelmezés megfelelőnek, a hadijogi szabályokkal és szokásokkal összhangban lévőnek tűnik. A „jogszerű" kitétel értelmezésével kapcsolatban viszont több lehetséges forgatókönyvet vizsgálnunk kell a szó lehetséges jelentéstartalmai tekintetében. A „jogszerű" ugyanis jelentheti a hadijogi szabályoknak megfelelőt, vagy a nemzetközi jog szabályainak általában megfelelőt, ami különbségtétel a *jus ad bellum – jus in bello* elválasztottság okán válik döntő jelentőségűvé. Vajon egy informatikai támadást végrehajtó személlyel szembeni ellentámadásnak csupán hadijogi szempontból kell jogszerűnek lennie (azaz a támadásokra vonatkozó jogi elvárásokat kell kielégítse, vagyis ne okozzon aránytalan károkat védett személyekben vagy javakban stb.), vagy az erő alkalmazására vonatkozó általános nemzetközi jogi normáknak is meg kell felelnie? Utóbbi esetben ugyanis sokkal nehezebb egy támadás „jogszerű" jellegét biztosítani, ha figyelembe kell vennünk az önvédelem gyakorolhatóságának szűk nemzetközi jogi feltételeit, és igen széttartó gyakorlatát. A kézikönyv szövegezőinek a szövegkörnyezetből és annak logikájából következtethető szándéka a „jogszerű" kitétel itt hadijogi természetű jogszerűséget vár el.

145 Henckaerts – Doswald-Beck, 2009.
146 Melzer, 2009.
147 Lattmann, 2013, 209-220. o.
148 Schmitt, 2013, 118. o.
149 Schmitt, 2013, 119. o., 3. bek.

Passzív részvétel esetében az okozhat gondot, hogy miközben ekkor az adott személy szándéka hiányában nem tekinthető aktív résztvevőnek,[150] ugyanakkor az általa üzemeltetett, a támadáshoz felhasznált számítástechnikai eszközről a megtámadott fél sem tudja megállapítani, hogy az vajon szándékosan vagy csupán gondatlanságból vesz részt az ellene intézett támadásban. Emellett nem csak a képessége nincs meg az adott helyzetben erre, de a szándéka sem lesz adott erre, és semmilyen jogi kötelezettséget sem tudunk azonosítani, amely szerint adott körülmények között a megtámadott félnek erre kellene törekednie, ez életszerűtlen elvárás is lenne ilyen helyzetekben. A kézikönyv a támadásokra általánosságban előírja az elővigyázatosság[151] és a gondos mérlegelés kötelezettségének[152] a hadijogi szabályokból ismert kötelezettségeit, de ezek teljesítése egy informatikai támadásra adott intézkedéssel összefüggésben nem jelentenek egyszerű kihívást, tekintettel arra, hogy a támadás végrehajtója és a végrehajtás körülményei az érintett államhoz képest akár beláthatatlan távolságban vannak. Érdemes hadijogi analógiában gondolkodnunk újfent: vajon az ismeretlen támadótól tüzet kapó katonától elvárja-e a hadijog, hogy a támadás viszonzása előtt meggyőződjön a támadó jogi helyzetéről, esetleges védettségéről? A válasz a fenti kötelezettségek kivételével többnyire nemleges lesz. Ugyanezt a megközelítést kell alkalmaznunk az informatikai támadások esetében is, azzal az eltéréssel, hogy ha mégis megvan a megtámadott állam lehetősége erre, akkor azt nem mulaszthatja el.

A passzív részvétel problémája rámutat ugyanakkor a modern informatikai társadalom egyik nagy gondjára, az informatikai eszközök értő alkalmazására, valamint az annak hiánya által okozott veszélyekre. Ahogy a hadijog szabályaival kapcsolatban a genfi egyezmények előírják az ismeretterjesztés kötelezettségét, úgy vélem, ugyanerre van szükség az informatikai eszközök használata tekintetében is: tudatosítani kell mindenkiben, hogy a számítástechnika alkalmazása is járhat veszélyekkel, és ehhez kapcsolódóan felelősséggel is. A sajtát eszközök és rendszerek védelme egyfajta kötelezettség lehet, ám az ennek elmulasztása miatti felelősség terjedelmét (például az otthoni vezeték nélküli hálózat tulajdonosának felelősségét, ha az általa jelszóval nem védett hálózatot mások bűncselekmény elkövetésére használják fel) egyelőre nem határozta meg a joggyakorlat. Lehetséges, hogy a büntetőjog a bűnsegédlet vagy a társtettesség valamely formáját alakítja majd egy ilyen helyzetre, de egyelőre nincs ilyen kiforrott gyakorlat.

3.5. Jogi felelősségre vonás kérdése: alkalmazhatók-e a nemzetközi büntetőjog normái és intézményei?

Érdemes kitérni röviden arra a kérdésre, hogy mennyiben alkalmazható a jelen nemzetközi jogrend, amennyiben egy informatikai támadás olyan súlyú jogsértést valósít meg, amit háborús bűncselekménynek is tekinthetünk.

Leszögezhetjük, hogy e kérdés vizsgálata a fentebb vázoltak közül csak olyan helyzetekben lehetséges, amikor az érintett államok között fegyveres konfliktus áll fenn, vagy amikor létezik egy államon belüli fegyveres konfliktus. A nemzetközi jog a háborús bűncselekmények kategóriáját csak ezekben a helyzetekben alkalmazza. Külön vizsgálat tárgyát képezheti, hogy emberiesség elleni bűncselekményt, vagy népirtást megvalósíthat-e egy informatikai támadás, ám erre a jelen vizsgálat keretében terjedelmi okokból nem kerítünk sort, ahogy azt sem vizsgáljuk, hogy agresszió bűntettét megvalósíthatja-e.

A nemzetközi büntetőjogi rezsim alapokmányának tekinthető nemzetközi szerződés, a Nemzetközi Büntetőbíróság 1998-ban elfogadott, és 2002-ben hatályba lépett alapokmánya[153] mind nemzetközi, mind pedig belső konfliktus esetén elkövethetőnek tartja a háborús bűncselekményeket, külön felsoro-

[150] Ezt a szempontot emelik ki a szakirodalmi források is, lásd pl. Melzer, 2009, 60. o.

[151] 52. és 55. szabályok – Melzer, 2009, 165, 170. o.

[152] 40. szabály – Melzer, 2009, 137. o.

[153] *Rome Statute of the International Criminal Court.* Rome, 17/07/1998, UNTS vol. 2187.

lását adja azoknak a két különböző típusú konfliktus esetében.[154] Ezek vizsgálatával megállapíthatjuk, hogy egy informatikai támadás alkalmas lehet a következő bűntettek bármelyikének megvalósítására: szándékos emberölés; súlyos szenvedések okozása, illetőleg a testi épség vagy az egészség súlyos károsítása; vagyontárgyak katonai szükséglet által nem indokolt, tömeges, jogellenes és önkényes elpusztítása és eltulajdonítása; a támadásoknak szándékosan a polgári lakosság, mint olyan, vagy az ellenségeskedésben közvetlenül részt nem vevő polgári személyek elleni irányítása; a támadásoknak szándékosan polgári létesítmények, azaz nem katonai célpontok elleni irányítása; a támadásoknak az Egyesült Nemzetek Alapokmányával összhangban tevékenykedő humanitárius segély- vagy békefenntartó misszió személyzete, felszerelése, eszközei, egységei, vagy járművei elleni, szándékos irányítása, ha azok jogosultak a polgári személyeknek vagy polgári létesítményeknek a fegyveres konfliktusok nemzetközi joga által biztosított védelemre; támadás szándékos indítása, azt tudva, hogy az adott támadás a polgári lakosság körében emberi életeket követelhet, polgári személyek sérülését, polgári létesítményekben olyan kárt, vagy a természeti környezetben olyan nagy kiterjedésű, hosszantartó és súlyos károsodást okozhat, amely összességében nyilvánvalóan túlzott mértékű a várható tényleges és közvetlen katonai előnyökhöz képest; olyan városok, falvak, lakóhelyek vagy épületek bármilyen módon történő támadása vagy bombázása, amelyek védtelenek, és nem katonai célpontok; támadások szándékos indítása vallási, oktatási, művészeti, tudományos, vagy jótékony célú épületek, történelmi műemlékek, kórházak vagy olyan helyek ellen, ahol a betegeket és sebesülteket gyűjtik össze, feltéve, hogy azok nem katonai célpontok.

Ezek mellett még több olyan bűntettet sorol fel a Statútum, amelyek esetében a kapcsolat nem közvetlen, de megállapítható. Így például lehetséges az ellenfél állampolgárainak arra kényszerítése, hogy a saját államuk elleni hadműveletekben részt vegyenek, valamint bizonyos fajta informatikai támadás minősülhet olyan bűntettnek minősített harci módszernek is, amely jellegénél fogva felesleges sérüléseket vagy szükségtelen szenvedést okoz, megkülönböztetés nélkül hat. Összességében azt állapíthatjuk meg, hogy számos olyan háborús bűncselekmény létezik, amit megvalósíthat egy informatikai támadás.

Az ezekkel szemben való fellépés a nemzetközi jog szintjén egy következő kérdést jelent. Tisztázni kell, hogy e bűntettek az államok belső joga alapján is bűncselekménynek kell minősüljenek, azaz a fellépés elsődleges területe nem a nemzetközi, hanem a belső jog, azaz a büntetőjogi felelősség megállapítása elsődlegesen az állami bíróságok feladata. A Nemzetközi Büntetőbíróság kiegészítő (komplementer) joghatóságot gyakorol, azaz akkor jár el, ha az egyébként az adott bűncselekménnyel kapcsolatban területi vagy személyi alapon joghatósággal bíró állam nem tud, vagy nem akar,[155] ez a bíróság általános működési elve minden, a joghatósága alá tartozó bűntett esetében, tehát az informatikai támadások sajátos jellege nem jelent kivételt. Ami azok esetében viszont bonyolíthatja a képet, azok a bizonyítási és egyéb nehézségek, amelyek az internet nemzetközi hálózatos természetéből fakadnak. Így például bonyolult kérdést vet fel annak végrehajtásának és hatásának helyének elváltása egy informatikai támadás esetében, különösen, ha harmadik állam hálózatát is igénybe veszik ahhoz. Ez visszautal a nemzetközi büntető együttműködés fontosságára, azaz az állami hatóságoknak kell lefolytatniuk a szükséges vizsgálatokat, a Nemzetközi Büntetőbíróság vagy bármilyen egyéb nemzetközi fórum az ezek során megszerzett információk és adatok alapján tud csak eljárni.

Van lehetőség olyan eseti büntetőbírói fórumok létrehozatalára is, amelyek nem a komplementaritás, hanem az elsőbbség elvén működnek, erre példát az 1993-ban létrehozott Jugoszlávia-, majd az 1994-ben létrehozott Ruanda-törvényszékek jelentenek.[156] Ezek esetében az érintett állam nem bír elsőbbséggel, köteles együttműködni a nemzetközi fórummal. Abban az elméleti esetben, ha egy informatikai támadás egy ilyen bírói fórum elé kerül, az érintett állam együttműködési kötelezettsége jelenthet gyakorlati problémát.

154 *Rome Statute.* 8. cikk.

155 *Rome Statute.* 17. cikk.

156 Az egyes büntetőbírói fórumok közötti lényegi különbségekről lásd például Lattmann, 2009.

3.6. Konklúzió

Mint a fentiekből láthattuk, az informatikai támadásokat továbbra sem szabályozza kifejezetten a nemzetközi jog, de a létező normák rendszeréből megfelelő értelmezéssel kikristályosodott egy olyan szabályozó korpusz, amit egy állam sem hagyhat figyelmen kívül, valamint nem hivatkozhat a szabályozatlanságra sem. Ebből fakadóan kettős feladat áll előttük a jövőre nézve: konstruktív jogalkotó együttműködéssel fejlesszék a nemzetközi jog anyagát, ezzel párhuzamosan pedig a saját belső joguk területén gondoskodjanak a nemzetközi jog anyagának egyrészt megfelelő, másrészt pedig annak további fejlődését elősegítő szabályok megalkotásáról. E folyamatok, ahogy maga a nemzetközi és a belső jogrend is, kölcsönös összhatásban és együttműködésben vannak egymással.

3.7. Nemzetközi szerződések

Convention on Cybercrime. CETS No.: 185. Magyar nyelven kihirdette: *2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.*

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. UNTS vol. 75. Megerősítette az *1954. évi 32. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, az 1949. évi augusztus hó 12. napján kelt nemzetközi egyezményeknek a Magyar Népköztársaságban való törvényerejéről,* közzétette azt: 2000/17. sz. nemzetközi szerződés a külügyminisztertől.

Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea. Geneva, 12 August 1949. UNTS vol. 75. Megerősítette az *1954. évi 32. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, az 1949. évi augusztus hó 12. napján kelt nemzetközi egyezményeknek a Magyar Népköztársaságban való törvényerejéről,* közzétette azt: 2000/18. sz. nemzetközi szerződés a külügyminisztertől.

Convention (III) Relative to the Treatment of Prisoners of War. Geneva, 12 August 1949. UNTS vol. 75. Megerősítette az *1954. évi 32. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, az 1949. évi augusztus hó 12. napján kelt nemzetközi egyezményeknek a Magyar Népköztársaságban való törvényerejéről,* közzétette azt: 2000/19. sz. nemzetközi szerződés a külügyminisztertől.

Convention (IV) Relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949. UNTS vol. 75. Megerősítette az *1954. évi 32. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, az 1949. évi augusztus hó 12. napján kelt nemzetközi egyezményeknek a Magyar Népköztársaságban való törvényerejéről,* közzétette azt: 2000/16. sz. nemzetközi szerződés a külügyminisztertől.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I). Geneva, 8 June 1977. UNTS vol. 1125. (továbbiakban: I. Kiegészítő jegyzőkönyv). Megerősítette és magyar nyelven kihirdette az *1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben 1949. augusztus 12-én kötött Egyezmények I. és II. kiegészítő Jegyzőkönyvének kihirdetéséről.*

Rome Statute of the International Criminal Court. Rome, 17/07/1998, UNTS vol. 2187. Megerősítette a 72/2001. OGY határozat, magyar nyelven nincs kihirdetve. Magyar szöveg elérhető: *T/4490. számú törvényjavaslat az Egyesült Nemzetek Diplomáciai Konferenciája által, a Nemzetközi Büntetőbíróság Rómában, 1998. július 17-én elfogadott Statútumának kihirdetéséről.*

3.8. Magyar jogszabályok

2012. évi C. törvény a Büntető Törvénykönyvről.

3.9. Bírói határozatok

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion. I.C.J. Reports 1996, p. 226.

3.10. Irodalomjegyzék

Stéphane Abrial (2001): NATO Builds Its Cyberdefenses. The New York Times, February 27. Elérhetőség: http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html?_r=0 (utolsó letöltés: 2018. április 10.)

Yoram Dinstein (2011): War, Agression and Self-Defence (5th ed.). Cambridge University Press.

Jean-Marie Henckaerts – Louise Doswald-Beck (2009): Customary International Humanitarian Law. Vol I. ICRC and Cambridge University Press.

Herczegh Géza (1981): A humanitárius nemzetközi jog fejlődése. Közgazdasági és Jogi Kiadó, Budapest.

Kajtár Gábor (2015): A nem állami szereplők elleni önvédelem a nemzetközi jogban. ELTE Eötvös Kiadó, Budapest.

Alexander Klimburg (szerk.) (2012): National Cyber Security Framework Manual. NATO CCD COE Publication, Tallinn.

Lattmann Tamás (2009): A nemzetközi büntetőbírói fórumok működésének rendszere, különös tekintettel a Nemzetközi Büntetőbíróság rendszerére: politika, parancs vagy jog? In: Kirs Eszter (szerk.): Egységesedés és széttagolódás a nemzetközi büntetőjogban. Miskolc, Bíbor Kiadó.

Lattmann Tamás (2011): A 2001. szeptember 11-i támadások hatása a nemzetközi jognak a fegyveres erő alkalmazására vonatkozó előírásaira. Külügyi Szemle. 2011/3. 105-115. o.

Lattmann Tamás (2013): A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén. In: Csapó Zsuzsanna (szerk.): Emlékkötet Herczegh Géza születésének 85. évfordulójára – A ius in bello fejlődése és mai problémái. PTE ÁJK, Pécs.

Nils Melzer (2009): Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. ICRC.

Michael N. Schmitt (szerk.) (2013): Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Michael N. Schmitt (szerk.) (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

4. VÁCZI DÁNIEL: CÉLZOTT TÁMADÁSOK MÓDSZERTANA

4.1. A célzott támadások sikerességét meghatározó körülmények

A célzott támadások sikerességének megértéséhez ismernünk szükséges az internetalapú társadalom működését. Fontos megvizsgálni, hogy mik azok a körülmények, melyek lehetővé teszik a támadó tevékenységet. A társadalmi berendezkedésünk, a technikai és különösen az okoseszközökhöz való hozzáállásunk magától értetődőnek tűnhet számunkra, hiszen ebben élünk. Azonban vannak olyan tényezők, összefüggések, melyeket fontos kiemelni a konkrét módszertan megismerése előtt.

4.1.1. A fogyasztói társadalomban rejlő biztonsági problémák

A mai társadalmunk egyik jellemzője, hogy a technológia rohamos fejlődésének köszönhetően folyamatosan új termékek jelennek meg a piacon. Ez a műszaki cikkekre kiemelten igaz. A hardvergyártók a legritkább esetben fordítanak erőforrást arra, hogy egy adott terméküket piacra dobás után javítsák. Amennyiben ez megtörténik, akkor azt inkább egy új verzióként teszik meg. Természetesen vannak kivételek, de az esetek nagy többségében a rendező elv az, hogy inkább egy új termékkel állnak elő, hiszen a versenytársak is valószínűleg már a következő cikkel jelentek meg a piacra.

Az eszközök életciklusát figyelembe véve az is előfordul, hogy már a két-három verzióval későbbi termékek is a raktáron vannak, azonban ezek csak késleltetve kerülnek ki a boltok polcaira. Ebben az esetben könnyű belátni, hogy ha egy adott eszközt T_0 időpontban terveznek meg a fejlesztőmérnökök, akkor T_1 pillanatban készül el a legyártott modell. Ezt raktáron tartják és csak T_2-kor szállítják ki a boltok polcaira. T_3-kor jut el a vevőhöz, aki csak ez után kezdi el használni azt. Valószínűleg a gyártósort eddigre már átállították a következő széria elemeire, így ha valami biztonsági hibát észlel a felhasználó, akkor gazdaságosabb a gyártó számára új termékre cserélni, mint a régi verziót újra előszedni és azt áttervezés után újra legyártani.

A hardverek szoros összefüggésben vannak a rajtuk futó szoftverekkel és a két réteget összekötő firmware-ekkel. Mindkettőről, de az utóbbiról különösen, elmondható, hogy a biztonsági javításukkal nagyon keveset foglalkoznak. Tegyük fel, hogy van egy otthoni okos tévénk. Az ezen futó firmware-t a lehető legritkább esetben vizsgálják felül, főleg biztonsági szempontból. Amennyiben mégis történik ilyen jellegű fejlesztés, jó eséllyel csak rövid ideig lesz az eszköz támogatott. Ez azt jelenti, hogy egy felhasználónál az adott készülék akár évekig is üzemelhet úgy az internetre kötve, hogy a rajta lévő szoftverek sérülékenységének ténye már napvilágra került, és gyártói beavatkozás nélkül, bárki kihasználhatja azt támadásra. A nem frissített, vagy nem frissíthető eszközök tehát nagyobb valószínűséggel lesznek kitéve támadásnak. Ez a fajta gyártói mentalitás is az egyik oka a 2016. szeptember 16-án az Amerikai Egyesült Államokban számos nagyvállalat (például GitHub, Twitter, Reddit, Netflix, Airbnb stb.) ellen elkövetett megosztott túlterheléses (DDOS) támadásnak. Az eset során IoT[157] eszközök botnetként sikeresen lehetetlenítették el a sokak által használt szolgáltatásokat. Ha megfelelő lett volna az eszközök frissítésének folyamata, kisebb eséllyel tudta volna a támadó felhasználni azokat.

[157] Internet of Things – dolgok internete: Az internetre kötött „okos” eszközök gyűjtőneve (IP kamerák, routerek stb.).

Az internetre kötött okos eszközök patchelésének problémája nem csak a gyártói oldalon jelentkezik, hanem a felhasználóin is. A biztonsági javítások, ha rendelkezésre is állnak egy termék kapcsán, nagy valószínűleg az átlagfelhasználó nem fog tudomást szerezni róla, hiszen nincs ismerete arra vonatkozóan, hogy ezzel neki egyáltalán foglalkozni kell. Ha esetleg mégis hallott már ilyen jellegű teendőkről, akkor sem biztos, hogy a frissítések telepítését véghez fogja tudni vinni. Megoldás lehet, egy szakember felkeresése, aki a megfelelő lépéseket véghez tudja vinni, de mivel a felhasználó nem érzi a biztonsági rések befoltozásának fontosságát, ezért erre pénzt nagy valószínűséggel nem fog kiadni.

Az okos eszközök közül talán ilyen szempontból kivételek a telefonok és tabletek. Ezekre operációs rendszer és alkalmazás szinten is gyakrabban érkezik biztonsági javítás, ha az eszköz még támogatott. Léteznek olyan eszközök és operációsrendszerek, melyek biztonságosnak mondhatóak, azonban ezek mögött mindig olyan erős gazdasági érdekek húzódnak, melyek túlmutatnak a hétköznapi felhasználáson.

4.1.2. Információs társadalom jelentette veszélyek

Jelenlegi információs társadalmunk sajátos szociológiai és pszichológiai vonatkozásait széles körű szakirodalom elemzi. A célzott támadások szempontjából azt fontos kiemelni, hogy napjainkban folyamatosan ki vagyunk téve a különböző helyekről érkező információknak. A hétköznapi szóbeli kommunikációnk során is valószínűleg a korábbinál szélesebb körű ismeretre tehetünk szert, de a különböző médiumok segítségével még inkább kitárul az emberek előtt a világ. Az első lépés a nyomtatott sajtótermékek széleskörű elterjedése, majd a rádió és a televízió hétköznapivá válása volt. Ennek hatása ma már mérhető. Példaként elég csak azt említeni, hogy a rádió megjelenése előtt a mai Olaszországban a lakosság alig 20%-a beszélte csak a hivatalos olasz nyelvet, azt követően ez az érték néhány évtizeden belül 90% lett. Természetesen már az internetet megelőző írott sajtóból és a rádióból, televízióból is könnyebben lehetett hozzájutni információkhoz, azonban az internet forradalmasította és gyorsította fel igazán a tartalmak generálását. Korábban, amíg a médiumok nem voltak elterjedtek és elérhetőek, csak az elit részére, addig a hétköznapi ember számára nem volt elegendő információ arról, hogy mi történik a szűk lakterületén kívül. Napjainkra a különböző típusú írásos, hang és videó formátumú anyagok könnyű és szabad létrehozhatósága azt eredményezte, hogy az embereknek más problémája alakult ki. Jelenleg már nem az információ rendelkezésre állása a probléma, hanem hogy a felhasználók meg tudják szűrni a számos fellelhető közül lényegeseket és a hiteleseket.

Mi áll mögötte? Az online sajtó, a különböző hírportálok jelenleg úgy működnek, hogy az esetek többségében közvetlenül nem kell értük fizetni. Így gyakorlatilag mindenki tudhatja, hogy mi történik a világ másik oldalán. Természetesen be kell látni, hogy ingyen semmi sem működik. Az oldalak a reklámokból élnek, amiket a hatékonyság érdekében célzottan helyeznek el a felhasználók számára. Külön iparág szerveződött a felhasználói szokások gyűjtésére. A meglátogatott honlapokból, a megnyitott cikkekből, a kereséseinkből cookie-k[158] ezrei küldik az információkat tartózkodási helyünkről, érdeklődési körünkről, vásárlási szokásainkról. Sok esetben megéri az oldalakat üzemeltetői számára „ingyen" adni az információt. Belátható az is, hogy nem csak a hivatalos sajtó szolgáltat információkat. Az egyének is bátran nyilváníthatnak véleményt, készíthetnek blogot, vlogot (videó blogot) és az közösségi médián keresztül gyakorlatilag bármit megoszthatnak. [2] Az információk minősége, és megszületésük indoka azonban eltérő. Ezt sajnos sokszor az emberek nem veszik figyelembe. Ezért lehetséges, hogy a tájékoztatási célon messze túlmutatóan megjelennek a befolyásolási célú álhírek, amelyek szakmailag már a célzott támadás kategórájába tartoznak. A legjobb példa erre a 2016-os Amerikai Egyesült Államok elnökválasztása. Sokan kételkedtek abban, hogy igaz lehet az oroszok álhírekkel történő befolyásolásának a ténye, azóta azonban sok helyről megerősítésre került az eset. Többek között a The Guardian folyóirat is foglalkozott az üggyel. Olivia Solon és Sabrina Siddiqui 2017. októberi cikkükben [3] beszámoltak a Facebook egyik ügyvédje, Colin Strech által az igazságügyi bizottságnak tett vallomásáról. Colin elmondása szerint több 10 millió

[158] A cookie, azaz süti egy olyan információcsomag, mely egy weblap meglátogatása után adatokat tárol el a felhasználói szokásokról.

amerikai állampolgárhoz jutottak el ezek a tartalmak közvetve vagy közvetlenül. A kutatók megvizsgálták az álhírek hatásmechanizmusát is, illetve meghatározták az elsődleges célközönséget is. [4] A nagy szolgáltatók, pontosan a Trump-eset által gerjesztett felháborodás hatására algoritmusokat dolgoztak ki az álhírek kiszűrésére, és olyan alkalmazást is lehet már telepíteni, amely felhívja a figyelmet, ha valamely álhírgyártó portál termékére kattintottunk. A legérdekesebb azonban mégis az, hogy ezeknek a híreknek az olvasása magával hozza, hogy egyre több ilyen hírhez fogunk kéretlenül is hozzájutni. Az úgynevezett „szűrőbuborék hatás" [5] azt jelenti, hogy mivel a szokásainkat feltérképező algoritmusok nem hivatottak arra, hogy mérlegeljék, hogy a minket érdeklő tartalom valós, vagy sem, egyre több hasonló hírhez fognak elvezetni minket, mígnem a kereső-szűrők csapdájába, és egy alternatív valóságba kerülünk. Mivel a véleményformálás e durván manipulatív és félrevezető formája maga is egy IT alapú célzott támadás, így az álhírek olvasása maga is kiszolgáltatottá tesz minket.

Másik felület, ami szintén megemlítendő az információs társadalom és a célzott támadások összefüggése kapcsán, az elektronikus levelezés. Az e-mail forgalomnak csak a töredéke hasznos, emberek közötti információcsere. A legnagyobb része reklám, illetve kéretlen levélszemét. Ezek az ingerek is folyamatosan érnek minket és a mindennapi életünk részévé váltak. Ezért lehetnek olyan sikeresek az adathalász, az úgynevezett phishing támadások. Ezeknek a leveleknek az alkotói valamilyen formában szeretnék átverni a felhasználókat, hogy így megszerezhessék belépési jelszavukat vagy más adataikat. Sokszor nem fontos, hogy ki lesz az áldozat, azonban speciális esetekben lényeges az, hogy kihez jut el a levél. Ilyenkor célzottan egy adott személynek vagy embercsoportnak készítik el a tartalmat úgy, hogy az érdeklődési körüknek megfelelően építik fel a szöveget. Ez az úgynevezett spearphishing. A támadási formát úgy lehet még eredményesebbé tenni, ha a levélben valamilyen linket küldünk, mely utal a szövegben megfogalmazott tartalomhoz. Például áramszolgáltatással kapcsolatos phishing e-mailnél a www.veIetlenceg.hu/lakossagiugyfelek/ajanlat/otthon honlap linkje látszik, melyre rákattintva a www.veletlenceg.hu/lakossagiugyfelek/ajanlat/otthon honlap tükrözött, a támadó által preparált honlap működik. Ez tűnhet ugyanannak, azonban a példa az első esetében a véletlen szó „L" betűje nagy „i" betűvel van írva, addig a második valóban a megfelelő karakter. Az eredeti oldal tükrözése, annak minden grafikai és más elemének az átvétele akár egy ingyenes alkalmazással is könnyűszerrel elvégezhető.

Egy célzottan megírt levél nem csak arra lehet alkalmas, hogy adatot gyűjtsön be. Az internetes támadások sikerességéhez a felhasználók interakciója is sok esetben nélkülözhetetlen. Az egyik legkönnyebb módja a fertőzésnek, ha egy e-mailben elküldött olyan linkre kattint a gyanútlan áldozat, mely mögött egy fertőzött weboldal található. A megnyitáskor a háttérben lefut valamilyen script[159] és települ valamilyen dropper.[160] Hasonló eredmények érhetőek el az elektronikus levelek csatolmányaiként küldött rosszindulatú kódokkal is.

Ezeket a támadási, fertőzési módokat a végtelenségig lehet finomítani. Amennyiben kellő energiát fektet a támadó a célpont megismerésébe nagyon jó eséllyel tud olyan e-mailt gyártani, aminek a segítségével el tudja valamilyen módon juttatni a kártevő kódját, hogy annak segítségével további támadásokat tudjon véghezvinni. Mindezek a személyre szabott tartalom mellett azért lehetnek sikeresek, mert hozzászoktunk, hogy folyamatosan információk bombáznak minket különböző felületeken keresztül. Fontos tehát, hogy jó hatásfokkal meg tudjuk ezeket szűrni.

4.1.3. Hidegháború a kibertérben

2001. szeptember 11-én az Amerikai Egyesült Államok ellen terrortámadást követtek el. Sokakat ez az esemény világította rá arra, hogy a békének titulált időszak csak a felszínen létezik. A terrorizmus hatására a nemezállamok elkezdték növelni a védekezési képességeiket. Nem csak a harcászat terén,

[159] A script egy erre alkalmas programnyelven írott utasítássor.

[160] A dropper egy vírus telepítéséért felelős kód.

de más területeken is születtek előrelépések. Erre egyik példa a jogi oldal erősítése. Ugyan már 2001 előtt is felismerték, hogy ezek olyan kiszolgáló ágazatai a társadalmunknak, melyek kiesése nagyobb fennakadásokat okozna az állampolgárok életében. A terrortámadás következtében Egyesült Államok törvénnyé [6] is emelte az 1998-as kritikus infrastruktúrák elleni direktíváját. [7] Ennek a jogszabálynak a tartalmát később különböző nemzetállamok átültették saját jogi környezetükbe.

Ezzel párhuzamosan a technológia fejlődése, az informatikai eszközök és az internet számos olyan lehetőséget adott mind a támadó, mind a védekező oldalnak, melyekre korábban nem, vagy sokkal kisebb mértékben volt lehetőség. Korábban az atomfegyverkezés jellemezte a hidegháborút, azonban napjainkban ez már kiegészült a kiberfegyverekkel. [8] A probléma az, hogy ezt a fenyegetettséget sokkal kevesebben tudják elképzelni, így nem tulajdonítanak nagyobb jelentőséget neki, nem kezelik a valós súlyának megfelelően, csak ijesztgetésnek tartják.

Az elmúlt húsz évben a szakértők, a politikusok felismerték, hogy foglakozni kell a kibertérrel és a kiberbiztonsággal. Az, hogy Magyarország jelenleg milyen szinten áll ezen a téren a szövetségi rendszereinek is köszönheti. Egyik meghatározó esemény történelmileg, hogy a NATO[161] hadszíntérnek nyilvánította ki a kiberteret, illetve a másik, hogy az Európai Unió megfogalmazta stratégiai szinten a tagállamok számára kiberbiztonság kialakítását [9] 2003-ban *„Egy biztonságos Európa egy jobb világban. Az Európai Biztonsági Stratégia”* címmel, és annak 2008-as felülvizsgálata utána a növelését a 2016-ban kiadott *„Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitika stratégiája”* címmel. [10] Az Erópai Bizottság egy külön kiberbiztonsági stratégiát is kiadott 2013-ban *„Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér”* néven. [11]

Mindezekre azért volt szükség, mert olyan események történtek az elmúlt időszakban, amik felhívták a tagállamok figyelmét a kibervédelmi képességeik növelésére. Talán az első jelentős támadás az iráni atomdúsító elleni Stuxnet malware támadás volt, ahol annak sikeressége miatt, az iráni atomprogram szakértők szerint több évvel vetette vissza az ország atomprogramját, jelentős hátrányt generálva ezzel nemzetközi viszonylatban. [12] A következő kiemelendő esemény Észtország esete, ami ellen megosztott túlterheléses támadást indítottak 2007-ben Oroszország felől. Az első olyan kibertámadás, mely hagyományos háborús cselekményekkel párhuzamosan történt, az 2008-ban a dél-oszét háborúban kapcsán történt, mely Oroszország és Grúzia között zajlott. [13]

A közelmúlt eseményei rávilágítanak arra, hogy nem feltétlen az általános kibertámadások okozhatnak csak nehézségeket a nemzetállamoknak. A korábban említett 2016-os amerikai elnökválasztás kérdése is idetartozik. Az eset érdekessége, hogy gyakorlatilag legális csatornán keresztül történt a támadás, mely az egyik, világgazdaságot meghatározó ország elnökének megválasztását befolyásolta [14], így közvetve kihatással volt számos más országra is. Amennyiben fontos mérföldköveket szeretnénk említeni a közelmúltból, figyelembe kell vennünk 2017-ben két globális támadást. Egyik a WannaCry néven ismert zsarolóvírust. Az eset megmutatta a világ számára, hogy mekkora kárt tud okozni egy ismert sérülékenység nem megfelelő kezelése. Sok más ország mellett, az Egyesült Királyság kórházainak egy részét is megtámadta a malware, így lehetetlenítve el a kórház bizonyos funkcióinak ellátását. [15] A másik globális támadás a NotPetya kártevő volt, melynek valószínűleg az egyetlen célja a rombolás volt.

Az említett esetek mögötti kártékony kódok eredete különböző forráskód-analízisek és politikai helyzetek elemzései után sejthető. Azonban biztosra nem jelenthető ki egyik sem. A célzott támadások ismertetése kapcsán azonban azt fontos megérteni, hogy számos módja és indítéka lehet egy nagyobb kibertámadásnak. Az említett esetekben is valószínű, hogy komoly munkát megelőzően a háttérben a befektetett anyagi erőforrások mellett hosszú tervezés és – döntően nyílt forrású – információszerzés állt.

[161] North Atlantic Treaty Organisation = Észak-atlanti Szerződés Szervezete.

4.1.4. Mitől lesz célzott egy támadás?

A fejezet második felében bemutatásra kerül egy informatikai támadás általános felépítése, ismertetésre kerülnek humán és IT alapú támadási technikák. Felmerülhet a kérdés, hogy mégis miért kell külön foglalkozni módszertani szempontból a **célzott** támadásokkal?

A jó gyakorlat szerint a cégek a kockázatarányosság mentén kezdik kialakítani az informatikai rendszereik – technikai és fizikai – védelmét. Jó esetben ezzel párhuzamosan az információbiztonsági – papír és humán oldali – folyamatok is kiépítésre kerülnek annak megfelelően, hogy melyik oldalról érheti támadás a cég által kezelt elektronikus és papír alapú információkat.

Minden esetben kritikus terület az információ szóbeli terjedésének megakadályozása. A cégen belüli pletyka, a rosszindulatú üzleti titkok, jelszavak ellen irányuló social engineering[162] támadások sikerességének megakadályozása mindig nagy kihívás elé állítja a biztonsági szakembereket. Az ilyen jellegű információszivárgások csökkentése szabályzatok bevezetésével és azok megfelelő kihirdetésével, tudatosítással (előadásokkal és e-learning anyagokkal), valamint célzott auditokkal és azok eredményeinek prezentálásával lehetséges.

A kockázatarányosság elve azt jelenti, hogy megvizsgálásra kerül, mik azok a felületek, ahol a legkönnyebb behatolni egy rendszerbe és sikeres támadás esetén milyen károkat szenved el az érintett cég, valamint ezt hogyan tudja a legmegfelelőbben orvosolni.

Mit is jelent tehát a védekezés kiépítése a gyakorlatban? Olyan adminisztratív, logikai és fizikai kontrollok bevezetését, melyek működése esetén nagy valószínűséggel egy sikeres támadásba fektetett energia nem térül meg a támadónak. Ez sok szinten értelmezhető. Megfelelően kiépített és jól konfigurált hálózatbiztonsági elemek, jól szeparált hálózatok, alaposan végiggondolt és frissen tartott hozzáférési jogosultsági rendszer, a felelősségi körök pontos meghatározása és azok kölcsönös elfogadása. Több szabvány, kvázi szabvány, ajánlás, jó gyakorlat foglalkozik ezzel a kérdés körrel. [16] Ilyen az ISO 27000-es szabványcsalád, a COBIT, a Magyar Nemzeti Bank által kiadott informatikai rendszer védelméről szóló ajánlás stb.

Jelen informatikai alapú társadalmunkban elemi érdeke a vállalatoknak a védelmi szintek kialakítása. Azonban azt kell szem előtt tartani, hogy a cégek profitorientáltak és az egyes állami szereplőknek is figyelembe kell venni a költségvetést. Mivel a biztonság közvetlenül csak anyagi ráfordítást jelent, ezért erre általában nem fordítanak elegendő erőforrást. Ezen kívül figyelembe kell azt is venni, hogy nem elég egy rendszer telepítése, hanem azt megfelelően, magas hozzáértéssel kell tudni konfigurálni. A minőségi munkának természetesen ára van. A különböző szereplők sokszor azonban csak a törvényi vagy más jellegű megfelelésnek szeretnének eleget tenni, ezért az elégséges, olcsóbb megoldást választják. A fő probléma az, hogy ezzel csak hamis biztonságérzetet teremtenek maguknak.

A nem megfelelő kiépítésnek és konfigurációnak az lesz a következménye, hogy számos kiskapu keresztül meg fogja tudni kerülni a biztonsági kontrollokat. Egy célzott támadás alkalmával a támadónak van ideje feltérképezni az informatikai hálózatot, információt gyűjteni a védelmi megoldásokról, az alkalmazott hardverekről, szoftverekről és az őket üzemeltetőkről. Gyakorlatilag ismert a támadó számára az infrastruktúra, vagy annak bizonyos része. Amennyiben ezek valóban rendelkezésre álló információk, akkor nincs más teendője a támadónak, mint az ismert vagy nem publikált (zero day)[163] sérülékenységeket kihasználni és lépésről lépésre bentebb kerülni a rendszerben, hogy eljusson a célig.

A célzott támadások mögött általában mindig egy adott konkrét indíték áll. A cél lehet információszerzés, károkozás, zsarolás, hátráltatás, pénzszerzés és még számos más ok. Mivel feltételezhető, hogy elegendő idő és erőforrás van a károkozó kezében, ezért nem az a kérdés, hogy sikerrel jár-e, hanem hogy mennyi idő alatt tudja végrehajtani a célját. Az idő azonban radikálisan lerövidíthető megfelelő eszközökkel, mely célzott támadásnál konkrétumokká válnak. Mivel nem arról van szó

[162] A social engineering az emberek megtévesztésén alapuló támadási forma.

[163] Nulladik napi.

ezekben az esetekben, hogy egy hacker megír (vagy vásárol) például egy zsarolóvírust, azt feltölti az internetre és hagyja, hogy a program működjön. Egy általános támadás során lényegtelen, hogy ki lesz megfertőződve, ha a végén sikerül például pénzhez jutni. Egy célzott támadás során tudatosan egy objektum vagy személy ellen irányul a cselekvés. De hogy lehet gyorsítani a folyamaton? Mi sem egyszerűbb annál, mint hogy egy elégedetlen, megsértett, alulfizetett munkavállalót megkörnyékeznek és felajánlanak neki egy megfelelő összeget azért cserébe, hogy helyezzen be egy pendrive-ot a vállalat valamelyik számítógépébe. Megnyugtatják, hogy neki semmi mást nem kell csinálni, hiszen csatlakoztatás után a programkód lefut. Amennyiben a közbenjáró fél hajlandó erre, a támadó máris közelebb van a céljához. Márpedig számos olyan személy van, aki a körülményei miatt meg fogja ezt tenni. A célzott támadásoknál tehát az a fontos, hogy a cél ismert a támadó számára és megvannak azok a lehetőségei, módszerei, amelyek segítségével sikerrel tud járni. Ez az, amiért nagyon nagy valószínűséggel sikeresek lesznek az ilyen ezek a cselekvések.

4.1.5. Használjuk az informatikát, de nem értünk hozzá

A körülöttünk lévő különböző technikai eszközök már a mindennapjainkká váltak. A probléma azonban az, hogy megfelelően működtetni kevesen tudják azokat. A tudatos és biztonságos használatuk pedig az átlag felhasználó számára nincs is kellő súllyal kezelve. Tekintsük egy napjainkban átlagosnak tűnő családi környezetet. Feltehetően valamilyen router segítségével az adott szolgáltatótól érkező internet egy Wi-Fi router segítségével van megosztva. Az esetek nagy százalékában ez szakértelem híján alapbeállításokkal üzemel. Jó estben ez a konfiguráció egy WPA2 titkosítást jelent, de a gyárilag beállított kód van használatban, mely az eszköz aljára van ragasztva. Az router elérési neve (SSID-ja) szintén a gyári néven fut. Feltételezve, hogy egy célzott támadás áldozatai leszünk, vizsgáljuk meg mi a probléma ezzel.

Egy átlagos otthoni elérési pont SSID-ja a szolgáltató nevéből, majd néhány számjegyből áll. Másik gyakran előforduló kombináció a hálózati eszköz gyártója és az azt követő numerikus karakterek. Egy-egy ilyen hálózati azonosítóból következetni lehet a router típusára. Ha már önmagában a névben megtalálható, akkor alapvetőnek tűnik az összefüggés. Nincs ez másként a szolgáltatóról elnevezett esetekben sem, hiszen a cégek általában egy adott eszközparkkal dolgoznak. Ezáltal a pontos típusok megismerése kis utánjárással, illetve social engineeringgel könnyű feladat. Az eszközöknek pedig megvannak a sérülékenységei, melyeknek a nagy része az interneten ingyen elérhető. Arra is jó esély van, hogy a korábbi fejezetben kifejtettek miatt, nincs frissítve a felhasználó hálózati eszköze, így a támadónak még egyszerűbb dolga lehet. Amennyiben ez a sérülékenység a céljának megfelel, már meg is van a leggyengébb rés a célrendszerben.

Továbbmenve az otthoni környezet vizsgálatában, manapság sok helyen találhatóak – az alapvetően nem megfelelően konfigurált router segítségével – csatlakoztatott televíziók, játékkonzolok, a ház/lakás védelmét szolgáló IP alapú kamerák, esetleg a kényelem fokozása miatt beszerelt hálózaton keresztül elérhető és programozható épületgépészeti megoldások, illetve más okos háztartási gépek. Ezek az úgynevezett IoT eszközök, melyek nem megfelelő kezelése legalább akkora problémát jelentenek, mint a hálózati aktív eszközök alapértelmezett beállításai. Ezek a passzív készülékek annyiban térnek el a routerektől, hogy az utóbbiak az elmúlt években a szakemberek törekvéseinek köszönhetően kezdenek figyelmet kapni és a felhasználók legalább sejtik, hogy figyelni kellene rájuk. Egy internetre kötött fűtés biztonsági problémája azonban maximum rémhírként, sci-fi-ként kerül be a köztudatba.

Amikor a PC-k és a laptopok széleskörűen is kezdtek elterjedni és az emberek egyre több eszközt vásároltak, akkor a felhasználók könnyen nyithattak meg olyan tartalmakat, melyek segítségével például egy bot-hálózat[164] részeivé tehették számítógépeiket, hogy így tudtuk nélkül rosszindulatú támadások

[164] A bot-hálózat, más néven botnet a robot network szóból ered. A hálózatba kötött zombi számítógépekkel, a tulajdonosuk tudta nélkül, a támadó nagyobb teljesítményű támadást tud végrehajtani.

részeseivé váljanak. Jelenleg hasonló tendencia figyelhető meg az IoT eszközök kapcsán is, hiszen kevés információ jut el a háztartásokba a problémáról. Ennek egyik oka a szakemberhiány, hiszen akik ezekhez a problémákhoz értenek azok jellemzően a piaci szereplőknél dolgoznak „nagyobb" problémák kiküszöbölésével. Másik ok pedig a folyamatos eszköz- és információdömping, amiben nehezen lehet a felhasználók figyelmét felhívni olyan veszélyekre, melyeket nem értenek, így nem is vesznek komolyan.

Egy jól szemléltethető példa a probléma súlyosságára az egyre több helyen található biztonsági IP alapú kamerák. Ezeknek a hackelhetősége valószínűleg a szakmabeliek számára ismertek. Több IT biztonsági konferencián bemutatták már, hogy feltörésük nem csak a filmekben létezik. A legtöbb esetben ezeken az eszközökön is valamilyen Unix/Linux alapú rendszer fut. Lényegében ugyanannyira sebezhetőek, mint bármelyik másik ilyen operációs rendszerrel rendelkező számítógép. Ráadásul a felhasználónak nincs is tudomása arról, hogy valójában mi szolgálja ki készüléke működését. Belátható tehát, hogy számos problémához vezet az, ha a hálózaton keresztül hozzáférhető egy otthoni biztonsági kamera és annak képét a támadó követni tudja, adott esetben még módosíthatja is. Azon kívül, hogy senki nem szereti, ha idegenek figyelik, a kamerához történő hozzáféréssel egy célzott támadás profilozásához remek alapot adhat a célszemély megfigyelése. Az, hogy ez nem csak a filmes forgatókönyvgyártók fejében létező történet, talán a legkönnyebben azokból az internetes oldalakból látható, melyek összegyűjtik a nem védett ipari közterületi kamerák képeit. Ezekhez a tartalmakhoz oldaltól függően ingyen vagy előfizetéssel bárki hozzáférhet.

4.1.6. Miért pont engem érne támadás?

Sokan úgy gondolják, hogy felesleges a saját eszközeiken védelmet kialakítani. Többen fel is teszik a kérdést, hogy ők miért lennének egy támadás célpontjai? Nem olyan fontos emberek ők, hogy kíváncsi lenne bárki az adataikra. Ha esetleg mégis, úgy sem tudnak mit kezdeni azokkal. A probléma az, hogy akárki lehet áldozata egy támadásnak. Most már vannak olyan esetek, amik a hétköznapi embereket számára is látható és hatásuk érezhető. Ilyen lehet, ha egy támadó egy ransomware segítségével meg tudja fertőzni a személyes használatban lévő laptopot, okostelefont. Az esetek nagy részében a felhasználók nem készítenek biztonsági másolatot a fontos adataikról (például családi képek), így ebben az esetben könnyen elveszhetnek azok. Az okos eszközökön annak a valószínűsége, hogy ne férjenek hozzá a képeinkhez egy fokkal kisebb, hiszen a különböző operációs rendszer gyártók alapbeállításként felszinkronizáltatják ezeket a felhőkbe. Persze ez mit sem ér akkor, ha a tulajdonos kikapcsolja ezt a funkciót, mondván, hogy nem bízik meg a cloud technológiában és a „nagy testvérben".

Arra, hogy céges adatokat nem tesznek fel a felhőbe, még nagyobb esély van. Így ha például egy zsarolóvírus támadás ér egy KKV-t, akkor gyakorlatilag a teljes adatvagyona el tud veszni, ha nincs megfelelő adatmentési folyamata. Márpedig a tapasztalatok azt mutatják, hogy Magyarországon, a nagy és multinacionális cégeken kívül, kevesen foglalkoznak a megfelelő IT biztonsági folyamatok kialakításával. A kérdésre tehát, hogy miért alakítaná ki valaki az információbiztonságot maga körül, az lehet egy válasz, hogy anélkül nagyobb eséllyel veszíti el személyes vagy céges adatait.

A következő példa szintén azt mutatja be, hogy egy támadónak bárki a kiszemelt áldozata lehet. Tételezzük fel, hogy „A" cég egy családi műanyagipari vállalkozás, ahol többnyire dísztárcsákat gyártanak. A bevételi forrását az adja, hogy „B" autógyárnak szállítja be a termékeit. Feltehetően a gyárban megfelelően kialakított a biztonsági infrastruktúra és az ehhez kapcsolódó folyamatok is alaposan átgondoltak. A támadó ezért nem közvetlenül „B"-t fogja megtámadni ipari titkok megszerzése céljából, hanem „A" vállalatot, ahol nem foglalkoztak a biztonsággal. Hogy férhet „A"-n keresztül „B"-hez az ipari kém? A támadó, miután megvizsgálta a fröccsöntő cég munkatársait, meglátja, hogy az egyik munkatársnak van egy nyolc éves gyereke. Eléri, hogy a kisfiú vagy kislány letöltsön egy online játékot, ami segítségével települ egy kártékony kód a család otthoni gépére. A szülő később a fertőzött gépbe helyezi a pendrive-ját, mivel valamit a munkahelyén szeretne kinyomtatni, hiszen ott

nem kerül pénzbe. A már valamilyen kártevővel rendelkező külső meghajtó csatlakoztatva a céges környezetbe egy hátsókaput (backdoort) nyit valamelyik porton. Ezen keresztül a támadó hozzáfér a levelezéshez és küld „B" gyártónak egy phishing levelet „A" cég nevében. Ha azt a gyár munkatársai elindították, máris elősegítették az információ kifelé történő áramlását. Ezt nevezik supply chain attack-nek.[165] Ha kiderül, egy idő múlva, hogy egy beszállító figyelmetlensége miatt került a gyár jelentős versenyhátrányba, valószínűleg „B" felbontja a szerződést „A" céggel. Mivel a családi vállalkozásnak ez jelentette a legfőbb bevétel forrását, így akár csődbe is mehet, nem beszélve az erkölcsi kárról, amit a piacon elszenvedhet.

A példa a valóságtól nem elrugaszkodott. Egyes szakértők szerint az iráni atomdúsítót megtámadó Stuxnet malware is hasonló módon fertőződhetett meg. Ebből kiindulva, ha valaki egy kis vállalatnál dolgozik, legalább annyira lehet veszélyben, mint aki egy kritikus infrastruktúránál vagy az állami szektorba, ahonnan nem ipari, hanem nemzeti titkok szivároghatnak így ki. Mindenegyes esetben a megtámadott személy életére nagy hatással lehet egy ilyen támadás, holott ő azt gondolta jelentéktelen ahhoz, hogy egy támadás áldozata legyen.

4.1.7. Közösségi média

Jelen társadalmunkban mindenki számára ismert fogalom a közösségi média, még azoknak is, akik nem aktívak egyik felületen sem. Az átlagember kapcsolattartásra és személyes vagy általános tartalmak megosztására használja a különböző oldalakat. Mások viszont ezeket az önkéntesen megosztott adatokat elemzik, és újfajta összefüggésekbe helyezve saját céljaikra használják. A szakértők sokszor felhívják a figyelmet a különböző posztolási szokások veszélyeire. Ilyen például, hogy ne tegyünk fel olyan fényképet magunkról, amiket később megbánunk, hiszen akár egy munkalehetőségtől is eleshetünk. Másik gyakran emlegetett veszély az olyan képi és videó tartalmak megosztása, ahol látszódnak a vagyontárgyaink. Ennek oka, hogy erre szakosodott bűnözők törhetnek be otthonunkba és rabolhatnak ki minket. A megfelelő időzítésben is segítünk nekik azzal, hogy mi magunk hirdetjük ki személyes oldalunkon nyaralásunk tényét vagy azt, hogy éppen egy adott rendezvényen vagyunk.

Azonban számos más veszélyt hordoz magában a közösségi média, melyekkel nem csak információbiztonsági szakemberek, de a különböző nemzeti és nemzetközi rendvédelmi szervek is sokat foglalkoznak. Az Europol Szervezett bűnözés internetes fenyegetettségét összegző jelentésben [17] meghatározásra kerültek a legkritikusabb területek. Ilyen például a malwarekkel való visszaélés, a gyerekek szexuális kizsákmányolása, a fizetőeszközzel elkövetett csalás stb. Jellemzően ezek nem csak a közösségi médián keresztül történnek, azonban mindegyik összefüggésbe hozható vele. [18]

A célzott támadásokat figyelembe véve a legfontosabb az, hogy minden támadás információgyűjtéssel kezdődik. A támadó annyi információt gyűjt a célpontról, amennyit csak tud. Ezeket rendszerezi különböző erre kialakított programokkal (például Dradis),[166] majd elkezdi tevékenységét. Az adatgyűjtés megkezdése az esetek többségében nem okoz nehézséget, internet-használati szokásaink miatt. A személyközi interakciók online, virtuális világba történő eltolódásával azt kockáztatjuk, hogy amit eddig szemtől szembe osztottunk meg másokkal, az most kikerül a világhálóra és mindenki számára elérhető lesz. [19] Mivel az emberek – főleg az y, z, α generációk szülöttei – egyre inkább online élnek [20], ezért egyre több dolgot tudnak meg rólunk, akik kíváncsiak ránk. Egy-egy ember online jelenlétéből alkotott profil pedig egy megszemélyesítésnél vagy bármely más támadásnál olyan helyzeti előnyhöz juttathatja a támadót, mely nagyban garantálja a sikerességét.

A begyűjthető információk minősége egy profil tanulmányozásával relatív magas, hiszen a személyek önmagukról általában az igazat posztolják ki, még ha ezt sokszor úgy is teszik meg, hogy csak a pozitívumok jelenjenek meg. Szokások, hobbik, kapcsolatok, lelkiállapotok, anyagi helyzet, ezek

[165] A supply chain attack, azaz az ellátási lánc támadás lényege, hogy a támadó a leggyengébb láncszemen keresztül (például beszállító, munkavállaló stb.) jut el a célrendszerbe.

[166] Lásd: https://dradisframework.com/ce/

mind olyan adatok, amikre például egy malware sikeres célba juttatásához, vagy valamilyen zsarolási, lefizetési alaphoz szükség lehet. Ezeket mind a felhasználók osztják meg magukról.

A célzott támadás kidolgozásának, megindításának számos célja lehet. Napjainkban egyre gyakrabban felmerül az emberek befolyásolása a közösségi médián keresztül. Az alkalmazott módszer miatt a téma meghatározó eseménye volt a 2018 márciusában kirobbant körülbelül 50 millió felhasználót érintő adatlopási botrány, melyet Mark Zuckerberg hivatalosnak mondható nyilatkozata[167] támaszt alá. Az esemény során egy alkalmazás segítségével a felhasználók saját maguk járultak hozzá adataik átadásához. Ez is rávilágít arra, hogy érdemes megfontolni, hogy mit osztunk meg magunkról és milyen alkalmazásoknak engedjük meg, hogy hozzáférjenek azokhoz. Egy célzottan megírt program segítségével a támadó könnyen juthat olyan információkhoz, melyek normál esetben rejtve voltak előtte.

4.1.8. A legújabb problémák

A technológia fejlődésével számos olyan új körülmény egészíti ki a korábbiakat, amelyek tovább bonyolítják ezt a világot és a benne lévő biztonságos létet. Egyik ilyen problémakör az úgynevezett big data, azaz az óriási adattömegek. [21] A folyamatos tartalomgyártás, a különböző informatikai műveletekkel keletkezett bejegyzések és az emberek által hagyott digitális lábnyomok kezelésre szorulnak. Ha az emberiség megfelelően tudja használni, előnyére tudja fordítani a rengeteg adat rendelkezésre állását. Ilyen terület például az egészségügy. Számos olyan következtetést vonhatnak le a kutatók a felhalmozott adatokból, melyek értelmezésére a big data elemzések előtt nem volt módjuk. Azonban mint mindennek, meg van ennek is az ellenpólusa. Például a választópolgárok adataiból egy elemzőcég olyan következtetésekre juthat, melyek akár egy választás kimenetelét is megváltoztathatja.

A big data létrejöttének egyik alapja egy másik nagy informatikai újítás, a felhő alapú infrastruktúra, azaz a cloud technológia. Számos biztonsági kérdést vet fel a felhőben nem felelően tárolt adatok elleni támadások. Egy rosszul kiépített cloud-ból ellopható adatokból, jelszavakból olyan adathalmazt állíthat elő valaki, ami segítségével más informatikai támadásokat tud véghezvinni.

Mind társadalmi, mind információbiztonsági szempontból érdekes kérdéseket vet fel a gépi tanuláson alapuló mesterséges intelligencia (AI)[168] kérdésköre. Számos területe van életünknek, amelyben várhatóan életünk könnyítésére fogjuk tudni használni ezt a technológiát. Persze számos ellenzője van a területnek, akik félnek az „apokalipszis" elszabadulásától, amennyiben sikerül megalkotni a nem csak specifikus célokra – mint például az önvezető autó – alkalmazott mesterséges intelligenciát. A teljesen önmagától „gondolkodó" gépek várhatóan át fogják alakítani a környezetünket. Jó példa erre az AI jogi felelősségi körének tárgyalása. Valószínűleg a jogászoknak majd egy új fogalmat kell kialakítani a természetes és jogi személy mellé, akire ugyanúgy létre kell hozni a vonatkozó jogi szabályozásokat.

4.2. Technológiai módszerek

A kibertér, így a kibertámadások meglétét az informatikai infrastruktúra és annak széleskörű elterjedése teszi lehetővé. Életünk számos területén jelen vannak a technikai eszközök és IT alapú szolgáltatások, melyek felületet adhatnak a különböző típusú támadásoknak. Legyen szó kiberbűnözésről, hactivizmusról, kiberterrorizmusról, kiberkémkedésről vagy kiberhadviselésről. [22] A következő-

[167] Mark Zuckerberg Facebook bejegyzése: https://www.facebook.com/zuck/posts/10104712037900071?pnref=story (utolsó letöltés: 2018. március 31.)

[168] AI = Artificial Intelligence.

ekben bemutatásra kerülnek azok a felületek, melyek egy célzott támadásnál szerepet játszhatnak. A különböző támadási módszerek számossága azonban olyan nagymértékű, hogy a támadási típusok közül csak az ismertebbek kerülnek vázolásra. Nem célunk, hogy mélyreható ismeretet közöljön egy-egy technika kapcsán, csupán hogy egy átfogó képet adjon a célzott támadásokhoz tartozó, technológiát érintő módszerekről.

4.2.1. Technológia környezet Megismerése

Az információgyűjtés szakaszában számos dolgot kell a támadónak megtudnia ahhoz, hogy sikeresen juthasson el a céljához. Mielőtt azonban megismernénk, a kihasználásra alkalmas eszközt meg kell vizsgálni, hogy milyen csoportokba lehet osztani a kihasználhatóság módjait.

- Első ilyen, amikor egy adott technológia, eszköz vagy program valamilyen sérülékenységét használja ki a támadó. Ide tartozik egy alkalmazott technológia vagy szolgáltatás működésében hordozott támadhatóság. (például Wi-Fi WEP titkosítás törése). Ilyen lehet egy rosszul megírt szoftver, vagy hanyagul tervezett hardver.
- A következő csoport, amikor valamilyen kontroll nem megfelelő kialakítását fordítják saját előnyükre a támadók. A rosszul beállított jogosultságkezelés, az objektumba történő beléptetés átgondolatlansága, a helytelen hálózati szegmentáció, a biztonságos kezelés hiányából fakadó adatszivárgás és más hamis biztonsági érzetet keltő rosszul bevezetett kontrollok tartoznak ebbe a kategóriába.
- Harmadik csoportba azok az esetek tartoznak, amikor egy jól működő szolgáltatást vagy technológiát használ a támadó rossz célra. Például lehet ez egy hamis Wi-Fi hozzáférési pont üzemeltetése vagy a levelezés használata adathalász támadásra.

Amennyiben valamilyen ipari adatot szeretne megszerezni egy támadásnál valaki, alapvető, hogy feltérképezi a vállalat infrastruktúráját. Hálózati topológiát, az ott található hálózati biztonsági eszközöket, megpróbálja megismerni milyen nyitott szolgáltatások, portok vannak egy adott eszközön. A hálózatot alkotó gépeken futó operációsrendszereket, használt böngészőket verzióra pontosan érdemes tudni. Információt gyűjt más biztonsági megoldásokról, esetleg a különböző kontrollokról. A megkívánt hatástól és a cél objektum által használt technológiáktól függően fontos lehet ismeretet szerezni az úgynevezett Operation Technology (OT)[169] eszközökről is, hiszen ezek biztonságára általában keveset fordítanak, holott nagy károk okozhatóak megtámadásukkal. Főleg, ha sikerül elérni a Purdue modell[170] szerinti biztonsági zónáig a támadónak.

Érdemes külön információt gyűjteni a szerverekről és munkaállomásokról, a cégben használt mobil eszközökről, az esetleg ezeket védő Enterprise Mobility Management (EMM) rendszerről. Van-e lehetősége a saját eszköz céges környezetben történő bevonásának (Bring Your Own Device – BYOD). Ez azért is fontos, mivel a mobilitás mindenki számára lehetőséget nyújt – kontrollálás hiányában – az otthoni eszközök (például okostelefonok) céges infrastruktúrához (Wi-Fi-hez) történő csatlakoztatására. Igaz ez a munkáltatók által kiadott laptopokra, okos készülékekre is, mellyel nem csak a lakásban tudnak internetelériéshez jutni a használóik, de kávézókban, repereken, tömegközlekedési eszközökön, gyakorlatilag bárhol használhatják azokat. Ráadásul, nem megfelelően titkosított eszközök esetén egyszerűbb dolga lehet egy támadónak, ha ellopja azokat az értékes adatokkal együtt, majd kinyeri a memóriából, háttértárból a szükségeseket.

Mivel azonban célzott támadásról beszélünk a támadó, amennyiben közel szeretne férkőzni egy személyhez, akkor nem csak a céges, hanem az otthoni környezetet is meg kell, hogy vizsgálja. Ide tartozik az adott ember és annak családtagjai által használt eszközök. Az épületben használt külön-

[169] Ipari irányítási rendszerek.

[170] A Purdue modell a biztonságos architektúrát mutatja be az ipari irányítási rendszerekben. 4 biztonsági zóna és 6 szint található benne. Ennek legalsó és legjobban védett része a biztonsági zóna.

böző kényelmet segítő IoT (távolról vezérelhető árnyékolási és más épületgépészeti rendszerek, okos háztartási gépek stb.) és IoHT[171] (egészségi állapotot figyelő rendszerek, online pacemaker stb.) kiemelten potenciális kockázatot jelentenek, mint ahogy a valószínűleg kevésbé védett hálózati otthoni hálózati hozzáférés. Amennyiben van a háztartásban olyan személy, akinek az informatikai tudása, biztonságtudatossága valamilyen, például életkorból, tapasztalatból, vagy szellemi visszamaradottságból fakadóan elmarad még az átlagos alacsony szinttől, az egy támadó által sokkal könnyebben kihasználható. Valószínűleg, akik ilyen támadást hajtanak végre, azokat nem fogják visszatartani az erkölcsi kérdések.

4.2.2. Technikai tudás, biztonságtudatosság felmérése

Szintén nagyon fontos körülmény, hogy egy adott felhasználó mennyi tudással rendelkezik. Nem csak a technikai eszközök ismerete a fontos, hanem biztonságtudatosság megléte is. Meghatározó a támadhatóság szempontjából az, hogy adott személyek mennyi idő után veszik észre az árulkodó jeleket. Egy megfelelően kivitelezett célzott támadás egy szakmában jártas személy ellen is elkövethető úgy, hogy arról nem vagy csak későn szerez tudomást. Számos olyan esetről hallhatunk, amikor titkosszolgálatok a másik ország rendszereiben tevékenykednek, és ezt a tevékenységet természetüknél fogva próbálják elrejteni a másik elől. Erre példa a 2018 januárjában napvilágot látott holland AIVD esete, akik éveken át voltak beépülve az orosz Cozy Bear hackercsoportba a de Volkskrant cikke szerint. [23]

Természetesen másként jár el egy támadó, amennyiben képzett, óvatos ellenfél a célja és másként, ha egy olyan felhasználót szeretne átverni, aki nem ért az informatikához, a technológiához, aki nem járatos a bitek világában. Számos olyan emberi tulajdonság van, amire építeni lehet az ilyen eseteknél. Ilyen a túlzott magabiztosság, a hiszékenység, a naivitás és a figyelmetlenség is. Ezek kihasználhatósága a későbbiekben kerül kifejtésre. Például egy vállalat rendszergazdája sokszor lehet kiszemelt áldozat, hiszen az esetek többségében más jogosultságokkal rendelkezik a cég rendszereihez, mint a többi felhasználó. Mivel azonban az ilyen munkakört betöltő személyek is esetenként egyszerűsíteni szeretnék a munkájukat és sokszor érezhetik úgy, hogy több dolgot megtehetnek, mivel másnak nincs hozzáférése rajtuk kívül. A következő tényező, ami segítheti a támadó dolgát, az eszközhasználat. Vajon a felhasználó védi-e készülékeit valamilyen zárolással, titkosítással? Mennyire figyel oda rájuk? Van-e esély egy kávézóban ellopni azokat? Hogyan kezeli a jelszavait? Felírja azokat egy cetlire, amit a pénztárcájában hordoz? Meglepő módon sok olyan hasznos következtetést lehet levonni egy személy közösségi média profiljáról, ami sejteti a személyiségét és a biztonságtudatosságát.

4.2.3. Fizikai környezetből fakadó problémák

Az objektumok elhelyezkedése fontos tényező lehet egy célzott támadásnál. Két fő szempontot kell megvizsgálni. Azt, hogy milyen könnyű az objektum közelébe kerülni és azt, hogy mennyire kelt feltűnést maga az ott tartózkodás.

A könnyebb érthetőség kedvéért tételezzük fel, hogy egy fertőzött pendrive-ot szeretnénk a célterületen direkt elejteni, hogy azt valaki megtalálja és a kíváncsisága miatt behelyezze remélhetőleg a célhálózatra kötött számítógépbe. Ez az úgynevezett baiting támadás.

Ahhoz, hogy el tudjuk így helyezni a fertőzött pendrive-ot, az objektum területéhez közel kell kerülni. Adott esetben, a nagyobb siker érdekében, be is kell jutni nem csak a kerítésen belülre, de az épület belső területére is. Fontos tehát annak a vizsgálata, hogy mennyire ütközik akadályba a támadó. Van-e kerítés, van-e beléptetés? Érdemes vizsgálni azt is, hogy milyen módon közelíthető meg az objektum. Gépjárművel el lehet-e hajtani a kiszemelt cél mellett? Ha csak gyalogosan lehet

[171] Internet of Health Things – egészségügyi internetre kötött eszközök.

az objektumot megközelíteni, az azt jelenti, hogy nő a helyszíni tartózkodás ideje. Persze az adott hely közlekedési kultúrája is ebbe a tényezőbe tartozik. Feltűnő lehet, hogyha ugyan megközelíthető gépjárművel a helyszín, de a helyiek inkább kerékpárt használnak a közlekedésre.

A másik vizsgálandó szempont, hogy mennyire lehet úgy „elejteni" egy pendrive-ot, hogy a kivitelező személy jelenléte ne tűnjön fel a biztonsági személyzetnek. Nehezebb észrevétlennek maradni, ha az objektum egy város szélén található, ahol nincs a környezetben csak sík terület és általában kevés ember fordul meg. Tovább nehezíti a támadó munkáját, ha erős védelemmel is rendelkezik az objektum. Ilyen megoldás lehet, ha az élőerős védelem nem csak megfelelően van megtervezve, de a résztvevő biztonsági szolgálatot teljesítők kellően kvalifikáltak és motiváltak a hatásos munkavégzés ellátására. Amennyiben ez megfelelő fizikai határvédelemmel és elektronikus jelzőrendszerrel, megfigyelőrendszerrel van megtámogatva, a támadónak sokkal nehezebb dolga van. Belátható, hogy ezzel szemben, egy nagyváros forgatagos utcáján található objektumnál, ahol semmi határvédelem nincs és a biztonságra keveset fordítanak sokkal egyszerűbb dolga van a támadónak abban, hogy úgy kerüljön közel a célterülethez, hogy jelenléte ne keltsen feltűnést.

A példa alaphelyzetben arra irányult, hogy egy bizonyos épületen belülre szeretne a támadó behatol, hogy ott rejtse el a pendrive-ot. Azonban egy célzott támadásnál előfordulhat, hogy a kiszemelt áldozat napi rutinjába tartozik, hogy gépkocsival érkezik a munkahelyére és minden nap egy számára kijelölt parkolóban hagyja azt. Ilyenkor a támadó nagyobb eséllyel juttathatja célba a fertőzött eszközt, ha ehhez a parkolóhoz tud odaférkőzni, mint magába az épületbe.

Egy célzott támadást kivitelezéséhez sok esetben nem elegendő távolról tevékenykedni. Amennyiben egy kritikus infrastruktúra ellen szeretnének informatikai támadást indítani, lehetséges, hogy az objektum környezetébe szeretnének férkőzni. Az indok többféle lehet.

Egyik az, hogy információt szeretnének gyűjteni a célpontról. Egy fizikai körüljárás során több dolog is kiderül. Megismerhető, hogy mennyire őrzött valójában az objektum. Ebből – ha nem is teljes bizonyossággal – következtetni lehet a biztonsághoz való viszonyuláshoz. Ha egy vezetőség alaphelyzetben nem figyel arra, hogy őrzött legyen a telephelye, nagyobb eséllyel az IT biztonságra sem fog adni. Amennyiben az tapasztalható egy objektumnál, hogy a beléptető ponton egy nem megfelelően képzett portás dolgozik csak, joggal feltételezhető, hogy a behatolás jelző- vagy zártláncú kamerarendszer sincs kiépítve megfelelően. Arra is következtetni lehet, hogy az informatikai biztonságra sem költöttek sokat. Természetesen lehet ez alól kivétel. Előfordulhat, hogy legalább egy tűzfal és valamilyen alap malware védelem ki van alakítva, de ez sajnos nem elegendő egy jól kivitelezett támadás ellen. Egy felmérés [24] szerint a cégek közel 100%-a rendelkezik valamilyen alap hálózatbiztonsági és antivírus megoldással. Azonban a korszerű támadások ellen (például: APT)[172] ezek a védelmi megoldások nem jelentenek védelmet. Joggal feltételezhetjük, hogy ha a fizikai biztonságra nem figyelnek oda, akkor más oldalon sem költenek megfelelően a védelemre.

A beléptetés folyamata is egy olyan terület, amit érdemes lehet feltérképezni az objektum üzemeltetői számára. A gyakorlat azt mutatja, hogy az esetek nagy részében nem fordítanak kellő odafigyelést a különböző biztonságtechnikai megoldások megfelelő kialakításához. A nem megfelelően végiggondolt beléptetés már önmagában kockázatot jelent egy objektum üzemeltetői számára. Elegendő az egyszerű zsebtolvajra gondolni, aki a vállalat, a munkavállalók, az ügyfelek anyagi javait tulajdoníthatják el, ha szabadon járkálhatnak ki és be az épületen belül.

A célzott támadások tekintve belátható, hogy ez a kockázat sokkal magasabb. Amennyiben a támadó kontroll nélkül tud ki és bejárni, akkor lényegesen egyszerűbb a kivitelezése a támadásának.

A beléptetést több különböző területről kell megvizsgálni. Legalapvetőbb a megfelelő fizikai határvédelem kialakítása. Belátható, ha megfelelően vannak kiépítve a kerítések, nyílászárók, úgy jelentősen nehezebb a behatolás. Amennyiben ez a feltétel adott, akkor a bejárás már a dedikált bejáratokon keresztül történik. Ettől eltérni természetesen lehet, azonban nagy valószínűséggel a támadó kerülni szeretné a feltűnést, így nem próbál meg olyan helyen bejutni, ahol könnyen feltűnik a bejutás ténye.

[172] Az APT (Advanced Persistent Threat) rejtett, célzott támadás, melynek célja általában az információszerzés.

A bejáratok védelme alapvetően több módon történhet. A legalapvetőbb módszer, az élőerős őrzés, illetve a beléptető rendszerek kialakítása. Általában a kettő egyszerre történő alkalmazása magasabb hatásfokot eredményez. Tételezzük fel, hogy csak a biztonsági őr áll a bejáratnál. Teljesen rá van bízva, hogy kit enged be. Ilyen esetben a támadónak több lehetősége is van kihasználni az őr emberi mivoltát. Ahhoz, hogy az ellenük irányuló sikeres átverések könnyebben érthetőek legyenek, át kell tekinteni egy átlagos biztonsági őr munkakörülményeit. A nyolc órában szolgálatot teljesítő őrök a legritkábban fordulnak elő. Általában tizenkettő vagy sok esetben huszonnégy órán keresztül végzik a tevékenységüket. Egy relatív monoton munkát hosszú ideig folyamatosan, koncentráltan végezni nagyon nehéz. Legyen szó pusztán arról, hogy segítse az irodaházba történő beléptetést vagy akár a CCTV rendszer monitorainak figyeléséről. Akármennyire törekszik az őr, valószínűleg a legfelkészültebbek sem tudnak teljesíteni úgy szolgálatot, hogy folyamatosan 100%-os teljesítményt nyújtsanak. Vannak természetesen olyan kiemelt helyek, ahol fontos közelíteni ezt a teljesítményt, ilyenkor általában többen végzik egyszerre ezt a feladatot. A teljes képhez hozzátartozik, hogy a biztonsági őrök sok esetben nincsenek kellően megfizetve, így nem eléggé motiváltak a munkavégzésre.

A vagyonőrök többféle képen is kijátszatóak. Nem kell hozzá más, mint türelem. Tételezzük fel, hogy a célobjektum dohányzásra kijelölt helye nem messze van a bejárattól, ahova a biztonsági őrök is járnak cigarettázni. A támadó könnyen megismertetheti az arcát azzal, hogy egy ideig rendszeresen jár oda ő is. Néha váltanak pár szót, majd egy-két hét után, mivel ismerős lesz az arca, egyszerűen a támadó csak besétál az épületen belülre, mondván, hogy fent hagyta a kártyáját. De persze, ha a célvállalat rendeltetéséből fakadóan van ügyfélszolgálat, ügyintézési lehetőség, akkor az is egy járható útja az arc megismertethetésének. Mivel nem minden esetben van megfelelően kiépítve a beléptetés, még akkor sem, ha van valamilyen erre kialakított rendszer, ilyen egyszerű trükkök alkalmazhatóak a támadók által.

4.2.4. IT támadás felépítése

Egy-egy IT támadás felépítése minden esetben különbözhet, azonban felismerhető egyfajta általános felépítés. Ennek ismertetése a Certified Ethical Hacker (CEH) kurzus 9. verziójának tanulási segédletében fellelhető terminológia szolgál alapul. [25]

1. *Footprinting*: azaz a passzív információgyűjtés szakasza. Tipikusan az először passzív módon megszerezhető információk tartoznak ide. Azoknak az információknak az összegyűjtése, melyek egy célzott támadás alapját tudják szolgálni. A korábban említett közösségi média tartalmakon kívül ide tartoznak például az úgynevezett whois rekordok, ahonnan többek között egy-egy domainhez tartozó alapinformációkat lehet megismerni. Következő információ forrás lehet a különböző keresőmotorok célzott használata, amelyek segítségével hozzá juthatunk olyan tartalmakhoz, melyek alaphelyzetből rejtve maradnának előttünk. Meglepően konkrét kereséseket lehet indítani, amelyek segítségével egy adott weblapon felejtett érzékeny adatokhoz is hozzáférhetünk. A megfelelő keresőszavak kialakításához segítséget nyújthat az internetről elérhető Google Hacking Database (GHDB), mely egy adatbázisa a keresőmotor célzott használatának. E két példán kívül természetesen számos más módja van a szükséges adatok megismeréséhez.

2. *Scanning*: tehát a szkennelés szakasza. Ez a lépés alkalmával a támadó felhasználja a korábban szerzett információkat és sokkal finomabb, precízebb felderítést tud végezni a különböző erre dedikált eszközökkel (például Nmap), hogy megismerhesse az elérhető szolgáltatásokat, eszközöket. Információt gyűjthet itt például a használt operációs rendszerek típusáról, illetve megfelelő gyakorlattal a hálózati biztonsági megoldások egy része, a topológia is felderíthető ennek segítségével.

3. *Enumeration:* e szakasz alatt a támadó kiszűri a hasznos információkat a korábbi lépések-

ből és mélyebb vizsgálatok útján el tud jutni a rejtett információkhoz, a felhasználónevekhez, a felhasználói csoportok, alkalmazások, használt protokollok, bannerek listájához. E lépés alatt történik általában a jelszavak megszerzése is.

4. *System Hacking*: a rendszer hackelése követi. A korábbi lépések alapján a támadó meg tudja tervezni a konkrét lépéseket. Ki tudja találni, milyen módszereket hajtson végre, közéállásos, injekciós támadást hajtson végre, használjon valamilyen malwaret, túlterheléses támadást, keylogger használatát preferálja.

5. *Escalation of privilege* a felhasználói jogosultságok kiterjesztését foglalja magában. A cél, hogy a korábbi támadások segítségével a támadó minél magasabb szintű hozzáféréssel és jogosultággal rendelkezzen a cél rendszerben, hogy ott a valódi tevékenységet később el tudja végezni.

6. *Covering tracks:* a nyomok eltüntetéséről szól. Ez egy célzott támadásnál kiemelt jelentőséggel bírhat, hiszen a támadó még kevesebb információt szeretne magáról hagyni ezekben az esetekben, mint máskor. A profi támadó addig tevékenykedik, amíg el tudja úgy fedni, tüntetni a tevékenysége által okozott nyomokat, hogy arra ne, vagy csak nagyon későn jöjjenek rá.

(A védekezési oldalon nagy probléma a különböző rendszer és tevékenységnaplók megfelelő beállítása és azok visszaellenőrzése. Meg kell találni az optimumot. A szükséges, de elégséges naplóállományra kell törekedni. A teljes körű, mindenre kiterjedő adatgyűjtés irreális tárhely igénnyel jár, aminek az elemzése képtelenség. Ennek ellentéte az alapértelmezett naplózás, mely nem tartalmazza a biztonsági szempontból szükséges bejegyzéseket. A következő probléma az így keletkezett tartalom értelmezésére. Különböző megoldások segítik a biztonsági szakemberek munkáját, ilyen például a Security Information and Event Managemet (SIEM) rendszer, mely a különböző eseményeket, figyelmeztetéseket gyűjti össze és szervezi egy relatív értelmezhető struktúrába. Az értelmezés azonban további tapasztalatot és szaktudást igényel, melyet külön szervezeti egységbe az úgynevezett Security Operation Centerbe (SOC) szerveznek azok, akik ezt komolyan veszik.)

7. Az utolsó lépés a hackelés folyamán a CEH terminológia szerint a *Planting of backdoors*, azaz a hátsó kapuk nyitva hagyása. Sok esetben szeretné a támadó biztosítani, hogy később is hozzá férhessen a korábban megtámadott rendszerhez, ezért olyan, úgynevezett backdoorokat hagy hátra, ami segítségével ez lehetséges lesz számára. A médiában lehet hallani olyan eseteket, ahol eszközökben, szolgáltatásokban előre dedikált hátsó kapuk találhatóak, melyet a gyártók maguktól, esetleg kormányzati hatásra hagytak termékeikben.

4.2.5. Malware

A malware, azaz malicious software, rosszindulatú szoftverek talán az átlagfelhasználó számára az a szó, amit leginkább össze tud kötni a számítógépek világának sötét oldalával. Ha nem is ebben az alakjában, de amennyiben az utca embere azt hallja, hogy vírusos lett a számítógépe, akkor jó eséllyel tudja, hogy valami rossz történt. Természetesen ez a téma ennél sokkal összetettebb, de van annak alapja, hogy összekötik az IT biztonságot és a rosszindulatú programokat. A számítógépes technológia alapjainak elméleténél letették a különböző malwarek alapjait is. Magyarország méltán híres IT

virológiai szakértője, Ször Péter a több nyelven megjelent A vírusvédelem művészete című kötetének első fejezetét egyfajta történelmi visszatekintéssel kezdi. Bemutatja, hogy már Neumann János gondolkozott az önreprodukáló automatákról, ahol egy parancssor (szalagos egység) végrehajtásával automaták (univerzális gép) képesek lennének reprodukálni magukat. [26] Ma, 2018-ban már a gépi tanulás szintjén beszélünk ezekről a kártevőkről.

Mint ahogy egy összetett célzott támadásnak, úgy egy malware írásának is számos indítéka lehet. Ször a vírusírásról úgy nyilatkozik a magyar kötethez tartozó előszóként megjelent interjúban, hogy „*Teljesen beigazolódott az a tendencia is, amelynek a kezdetét már a 2003-2004 körül éreztük. A vírusírás tökéletesen megváltozott, a hobbifejlesztésből a professzionális maffia szintjére került.*” [27] Maga ez a mondat is megágyaz annak, hogy a károkozás sokszor nem céltalanul történik. Néhány sorral lejjebb találjuk a következőket: „*Máskor az a cél, hogy személyre szabott támadást hajtsanak végre. A legtöbb kártékony program csak néhány, legfeljebb néhány tucat gépen van jelen.*” A szakember bő húsz éves, e téren alkotott munkássága alatt számos malwarrel foglalkozott. A kötetben Ször által összegyűjtött típusokat [28] a következő táblázat foglalja össze:

Malware típusa	Fő jellemzők
Vírusok	Saját magát, vagy önmagának egy fejlettebb változatát másoló kód. Fájlokat, rendszerterületek fertőznek meg.
Férgek	A vírus olyan speciális változata, mely elsősorban a hálózaton terjed. Általában önmagától terjedő programkód, ritkán emberi indikáció szükséges a fertőzés elindítására. (Altípusai: levélférgek, polipok, nyulak.)
Logikai bombák	Normál szoftverbe a programozó által épített működési anomália.
Trójai falovak	Valamilyen más programnak, vagy annak egy részének álcázzák magukat. (Altípusai: Hátsóajtó-programok, jelszólopó vírusok)
Baktériumok	Kezdetleges vírusfajták.
Alkalmazáshibát kihasználó vírusok (Exploit vírusok)	Egy program sebezhető pontját/pontjait célzottan támadják.
Letöltők	Más rosszindulatú programok telepítésében segítenek.
Tárcsázók	Fizetős szolgáltatásokra irányító kód.
Dropperek	Például a rendszerindító szektorba települő vírusok telepítéséért felelős kódok.
Injektorok	A dropper speciális változata, melyek a memóriában aktív állapotba helyezik el a vírusokat.
Automatizált jogosultságszerzők	Magas jogosultságszerzésre alkalmasak általában exploit vírus segítségével.
Kitek (vírusgenerátorok)	Vírusok generálására alkalmas program.
Spammer programok	Kéretlen levelek küldésére alkalmas program.
Flooderek	Szolgáltatásleálláshoz vezető többlet adatforgalmat generáló program.
Billentyűzetnaplózók (keyloggerek)	A billentyűzetleütéseket, adott esetben monitorképet, más beviteli perifériák tevékenységét rögzítő malware. (Létezik hardver változat is.)

Malware típusa	Fő jellemzők
Rootkitek	Rendszergazdai jogosultságú, akár kernelszintű hozzáférést biztosító programcsomag.
Spyware	Felhasználói (például internetes) tevékenységet kutató programok.
Hirdető programok	Kéretlen reklámokat jelenítenek meg például a böngészőkbe. Rendszerint más kárt nem okoznak.

A szerző kiegészítése az elmúlt évek trendjei alapján:

Malware típusa	Fő jellemzők
Ransomware (zsaroló vírus)	Olyan malwarek, melyek visszaállítható vagy visszaállíthatatlan módon titkosítanak a célrendszerben, majd váltságdíjat kérnek a feloldó kulcs megadásáért.
Kripto vírusok	A kriptovaluták lopására alkalmas kártékony kódok.
Destructoware	A trójai falovak egy fajtája. A legitim szoftver valamilyen funkcióját kihasználva kifejezetten romboló hatást ér el.

A fent említett kártékony kódok értelmezhetőek nagyrészt a mobil platformokra is. Azonban ott különbséget kell tenni aközött, hogy a felhasználó magától ad-e jogosultságot egy rossz szándékúan megírt programnak (például telepítés alkalmával) vagy egy rootkitről van szó, amely magától képes megemelni a jogosultságait.

4.2.6. Webes támadások

Korábban esett már szó különböző támadásokról, melyek arra építettek, hogy a támadó közel tud férkőzni egy objektumhoz vagy egy személyhez. Egy célzott támadásnál ez előfordulhat, hiszen mindenáron szeretnék az elérni a célpontot. Az esetek többségében azonban az internet felől közelednek a hackerek, akik különböző sérülékenységek kihasználásával jutnak közelebb pontról pontra, mint ahogy ez az *IT támadások felépítése* fejezetben is bemutatásra került. Sok magától értetődő oka van ennek. A piaci szektor nagy részében, olyan üzleti modellt alkalmaznak, amely megkívánja, hogy a cégek internetelérréssel rendelkezzenek. Emellett a hétköznapjainkat is hálózati függés jellemzi. Az aktív személyek jelentős része valamilyen formában online van. Ha valaki törekszik is arra, hogy kerülje a különböző netes felületeket, vagy egyszerűen távol áll tőle az informatika, valószínűleg lesz a közvetlen környezetében olyan személy, akin keresztül elérhetővé válik. Ezt az információszerzés szakaszában a támadónak fel kell mérnie, és eszerint alakítania a stratégiáját.

A különböző keresőmotorok kihasználásával már akár a korai lépések során találhatunk olyan információkat, amiken elindulva egy támadás sikere garantált lehet. Ha abból indulunk ki, hogy egy weboldal tesztelése során sikerül a webszervert olyan hibára futtatni, ami segítségével az kiírja önmaga adatait, de legalább a típusát, akkor a támadónak csak egy sérülékenységet kell keresni, majd azt kihasználni. Ugyanez igaz például az így beazonosított adatbázisokra vagy más háttérben futó alkalmazásokra.

A következőekben néhány olyan általános, a web felől érkező támadás kerül bemutatásra, melyről valószínűleg a témában keveset olvasottak is hallhattak. Ezen a néhány példán kívül természetesen számos más módja létezik a rendszerek és alkalmazások ellen elkövethető tevékenységeknek.

• DoS, DDoS [29]

A két rövidítés a Denial of Service, illetve a Distributed Denial of Service kifejezéseket takarja, a szolgáltatás megtagadással járó támadást, illetve ennek több (általában botnetbe szervezett) gép általi végrehajtásával létrejövő elosztott túlterheléses támadást jelentik. Ez egy igen egyszerű, nem túl „elegáns", de annál hatásosabb módja a célszemély ellehetetlenítésének. A DoS támadás lényege, hogy annyi kéréssel támadják meg a hálózatot, vagy azon keresztül valamelyik alkalmazást, amennyit a fogadó oldal nem tud feldolgozni. Ennek hatására nem lesz elérhető az adott szolgáltatás, mivel nem tud kiszolgálni egyszerre ennyi kérést a szerver. Célzott esetben könnyű egy adott objektum hálózata, webes szolgáltatásának ellehetetlenítése. Ennek oka az is lehet, hogy a támadó addig, amíg a szakemberek az újbóli elérhetőségen dolgoznak, a tényleges támadást hajtják végre. Alapvetően két féle képpen lehet ellene védekezni, melyek együttes alkalmazása vezet megfelelő eredményre. Első az olyan szolgáltatás igénybevétele, ahol egy kellően nagy hálózati kapacitással rendelkező szolgáltató ki tudja szűrni a hálózati forgalom alsó szintű csomagjait (például SYN csomagokkal történő elárasztás – SYN flood – esetén). Másik megoldás a szervezet hálózati infrastruktúráján (az IPS-en[173], load balanceren[174]) beállított megfelelő alkalmazás szintű szűrés. Ilyenkor letiltásra kerülnek egy adott szolgáltatás ellen irányuló gyanús, túlterhelést okozó kérések.

• XSS [30]

A rövidítés a cross side scripting kifejezéssel oldható fel. Magyarul oldalakon keresztül végrehajtott közvetett szkripthívás. A támadók célja, hogy egy kártékony szkriptet futtassanak le a célgépen. Létezik perzisztens és nem perzisztens fajtája. Ez utóbbi alkalmával a kártékony kód az URL-be kerül beillesztésre, mely rákattintás esetén lefut, és elvégzi a felhasználó által nem kívánt tevékenységet. Az értő szemnek valószínűleg feltűnik, hogy a „script" kifejezést, vagy például a javas scriptre utaló „.js" kifejezés el van bújtatva az URL-ben. Tipikusan phishing támadásoknál alkalmazható jó. A perzisztens változat során magán a webszerveren helyezik el a szkriptet, mely egy weboldal minden megtekintésénél így lefut. Az ilyen módon történő rosszindulatú kódsor elhelyezésre példa a nem megfelelő beviteli védelemmel ellátott blog oldalak bejegyzései adnak lehetőséget.

• SQL injection [31]

Más néven SQL befecskendezés. A webes alkalmazásokat kiszolgáló adatbázisok kerülnek megtámadásra e technikával. A támadás alapja itt is a nem megfelelő programozás. Amikor egy weblapon a felhasználók valamilyen adat megadásával más adatokat kap eredményül, akkor közvetetten eléri az adatbázist egy kéréssel. Ezt használja ki a támadó. Például nem egy adatot fog beírni a beviteli mezőbe, hanem egy kifejezést, mely segítségével nem egy eredményt, hanem akár a teljes tábla tartalmát elérheti.

• Cookie poisoning [32]

A sütimérgezés a weblapok működését segítő dinamikus tartalmak, cookie-k, módosítását és azok a webszervernek történő eljuttatását jelenti. A manipulálás különféle módokon lehetséges.

[173] Inntrudion prevention System=Behatolás védelmi rendszer. Proaktív működésű aktív hálózatbiztonsági eszköz.

[174] Load balancer = Terhelés elosztó. Olyan hálózati eszköz, amely feladata a beérkező kérések egyenletes elosztása a kiszolgáló szerverek felé.

4.3. Humán módszerek

A különböző környezeti, társadalmi, szociológiai körülmények, a technológia jelenléte és a kibertér kialakulása csupán lehetőséget biztosítja egy támadás lebonyolításához. Az, hogy a felsorolt körülmények nem egy tökéletes rendszert, világot alkotnak, a támadókat abban segíti elő, hogy általánosan kihasználhassák a sebezhetőségeket. Azonban a célzott támadásokat az teszi igazán azzá, ami, hogy emberek ellen irányulnak, akik mind egyediek. Még akkor is, ha a cél egy vállalat vagy objektum, a humán faktort fogják kihasználni a legjobban. Ebben a fejezetben bemutatásra kerülnek azok a jellemzők, amelyek segítik a támadót személyre szabni a különböző technikákat.

4.3.1. Személyiség

Az egyik legfontosabb lépés, hogy a támadás által célzott ember személyiségét kell megismerni. Valójában egy összetett támadás kivitelezéséhez nem elegendő technikai ismeretekkel rendelkeznie az ártó szándékú személyeknek. Szociális érzékkel, sok beleérző képességgel, némi pszichológiai, szociológiai tudással is rendelkezniük kell. Vannak esetek, ahol úgy tűnik, hogy egy rosszindulatú kód elindul a támadótól és emberi beavatkozás nélkül végzi a dolgát. Valójában ott is végig kell gondolni azt a folyamatot, amit emberek üzemeltetnek, abban a rendszerben, amit emberek állítottak össze.

Ha egy kifejezett személy ellen azért irányulhat támadás, mert vagy ő a célpont, vagy ő tűnik annak a gyenge pontnak, akinek a segítségével be lehet jutni egy rendszerbe vagy közelebb kerülni a következő lépéshez.

Bármi is az ok, mint a technikai támadásnál, itt is információkat kell gyűjteni az adott emberről. Nem mindegy, hogy egy extrovertált titkárnőt vagy egy teljesen antiszociális programozót kell átverni. A megismeréshez különböző felületeket lehet segítségül hívni az interneten keresztül. Számos információt osztanak meg az emberek önmagukról és a környezetükről, azonban biztos következtetéseket ebből nem lehet levonni. Sokan valamilyen képet szeretnének láttatni önmagukról. Ezzel azonban valós támadást mérsékelten lehet csak végrehajtani. Fontos megismerni a személyiségét, aminek a módja az, hogy el kell hagyni a monitort és a húsvér valójában kell megismerni egy személyt. Christopher Hadnagy mélyrehatóan foglalkozik az emberek befolyásolásának művészetével, a social engineeringgel.

A tapasztalatait összefoglaló könyv [33] alapján ahhoz, hogy egy embert úgy tudj irányítani, ahogy te szeretnéd, meg kell ismerni elsősorban, hogy hogyan jár az agya. A gondolkozási módok összefüggenek azzal, hogy milyen környezeti hatások, ingerek feldolgozása az elsődleges számunkra. A verbális és nonverbális információkat kognitívan értelmezzük, érzékszerveink segítségével jutnak el a tudatunkig. Az eltérő hatásokra azonban másként reagálnak tudat alatt a különböző embertípusok. [34] A nagytöbbséget a vizuális hatások határozzák meg a leginkább. A különböző kereskedelmi, marketing szakemberek is gyakran építenek erre, hiszen számos emberre lehetnek így hatással. A vizuálisan gondolkodó emberek kommunikációjában gyakran tűnnek fel képi elemek. Másokra a hanginger hat a legjobban. Ők azok, akik úgy tudnak tanulni a legjobban, hogy hangosan olvassák a tananyagot. Ez a típus különösen érzékeny a hangerőre, a hangtónusokra, a beszéd gyorsaságára. Harmadik gondolkodási mód a tapintással és az érzelmekkel függ össze. Bizonyos fizikai hatások és a hozzájuk kapcsolt mentális, emocionális állapotok könnyen párosulnak, ennek az embertípusnak az agyában. Egy beszélgetés alkalmával be lehet határolni, hogy valószínűleg melyik érzékszerve hat a legjobban egy személy tudatalattijára. Nincs más dolgunk, mint figyelni egy kommunikáció során, hogy vajon mennyi metaforát használ, hogy próbálja-e az adott ember elképzelni vizuálisan az elmondottakat. Amennyiben nagyon változatos hanglejtéssel beszél egy illető, vagy például a mondandójának sebességével ad nyomatékot, akkor valószínűleg a második kategóriába fog tartozni. A harmadik típusra leginkább az intenzív környezeti körülmények hatnak, mint például a hőmérséklet.

A kommunikáció alatt fontos megszűrni, hogy pontosan milyen érzelmi állapotban van a partner, hiszen annak megfelelően tudja a támadó kihasználni a helyzetet. Ennek egyik legbiztosabb módja az árulkodó gesztusok (microexpression) felismerése. [35] Az emberi mimikában, testbeszédben történő olvasás sok gyakorlást igényel, hiszen ennek hiányában könnyen félreérthetjük a másikat. Ekman által tudományosan bizonyítottan [36], a hét biológiailag elkülönülő alapérzelem – a harag, az undor, a félelem, az öröm, a szomorúság, a meglepődés és a lenézés – olyan módon hat az emberi szervezetre, hogy önkéntelenül elárulja azokat a külvilág számára. Azoknál az embereknél, akiknél jellemzőek a nagy gesztusok (például a kar) használata, a kommunikáló partnernek – jelen esetben a támadónak – könnyebb dolga van a felismeréssel. A hamis információk kiszűrésében [37] fontos, hogy nem csak önmagukban a gesztusokat, a mimikát kell figyelni. A verbális közlésnek ellentmondó testbeszéd árulkodhat arról, hogy a kommunikáló partner valamiért nincs összhangban saját mondanivalójával. Ez persze nem azt jelenti, hogy hazudni akar. Lehet teljesen más is a háttérben. Szélsőséges példa, hogy egy közeli hozzátartozóját veszítette el. Ilyenkor valószínűleg, ha nem is mondja ki a fájdalmát, belülről emészti őt a gyász. Érdemes lehet odafigyelni a kommunikáció során a kérdésünkre adott válasz reakcióidejére. Ha a partner hezitálás után gyorsan felel valamit, van esély arra, hogy nem az igazat tükrözi a válasza. A hirtelen viselkedésmód változás tipikus gyakorlat a valódi gondolatok elrejtésére. Emögött sokszor időnyerés a cél.

A személyes kommunikáció során az első benyomáson kívül [38], számos olyan dolog van, mely elősegíti a támadót abban, hogy elhitesse az átverni kívánt személlyel, hogy bízhat benne. Az összhang- és a szimpátiateremtés tudatos használata [39] azt eredményezi, hogy kiépül egyfajta bizalom. Ennek megszerzése után persze jobban megnyílik az áldozat, és akár számos olyan információt is elmond – főleg ha a támadó tudatosan választ megfelelő kérdezési technikát [40] –, melyet valószínűleg nem tett volna meg.

A támadó sikerességének elérése érdekében alkalmazhat különböző befolyásoló technikákat [41], melyekkel egy célzott támadás során ráveheti arra célszemélyt, hogy az akarata szerint cselekedjen. [42] Tovább növelhető a siker esélye, ha az előzetes információk megszerzése után egy olyan személyiséget vesz fel [43] a támadó, mely az adott szituációban előnyére válik.

4.3.2. Személyes háttér

Egy támadónak ahhoz, hogy kiválaszthassa a módját a célravezető támadásnak, nem csak a személyiségét kell megismerni az átverni kívánt személynek. Fontos látnia, hogy mi motiválja vajon a kiválasztott embert. Motiváció lehet a pénz, vagy az, hogy ne derüljön ki olyan róla, amit elkövetett. A lefizetés és a zsarolás egy adott dolog elvégzésére remek megoldást nyújthat. Ha valakinek az anyagi körülményei szűkösek, csak a lelkiismerete az, ami gátat szabhat abban, hogy elfogadjon egy nagyobb összeget egy „apró” tettért cserébe. Valószínűleg az, aki a mindennapi megélhetésért küzd, emellett nagyobb tartozása is van, élni fog a lehetőséggel, hogy egy kicsit könnyítsen az életén. A zsarolás pedig egyértelműen hatásos lehet, ha valakinek a háttere és személyisége lehetővé teszi ezt. De nem kell csak ilyen szélsőséges dolgokra gondolni. Egy munkavállaló, akit úgy érzi megalázták vagy igazságtalanul bántak vele, könnyen cselekedhet olyat, amivel kielégítheti belső bosszúvágyát. Ennél is egyszerűbb egy el nem ismert munkatárs szakmai tudását igénybe venni, hogy fontosnak érezze és elkötelezze magát az „új barátjának”.

Egy adott személy függőségei szintén olyan paraméterek, melyek könnyen kihasználhatóak. Szélsőséges esetben egy drogfüggő személy egy kis „anyagért” cserébe, sok dologra rábírható. Kicsit árnyaltabb a számítógépes játékfüggőség, mely a célzott kibertámadások szempontjából érdekes lehet. A különböző virtuális világokban egy hozzáértő, ügyesen taktikázó támadó hasonló eredményt érhet el, mint az, aki a hús-vér függőségeket használja ki.

Szükséges azonban azt is megvizsgálnia a támadónak, hogy milyen akadályokba ütközhet. Az olyan személyt, aki erős erkölcsi tartással rendelkezik, nehezebb lesz a céljaira használni. Legalábbis

az eddig felsoroltak alapján. Ilyenkor más emberi tulajdonságot fog keresni a támadó. Ilyen lehet a naivitás, tudatlanság. Nagyon jól működő technika az úgynevezett reverse social engeineering. A támadó megoldást kínál egy még be nem következett problémára, majd később előidézi azt. Jó eséllyel az áldozat, emlékezni fog arra, hogy ki tud neki segíteni, ha baj van. A kártékony kód pendrive-val történő bejuttatásának példáján keresztül ez azt jelenti, hogy a támadó például egy ismerőseinek gyakran segítő számítógépes szakembernek állítja be magát, egy informatikában járatlan ember előtt, akit korábban kiszemelt áldozatául. Tételezzük fel, hogy egy nagyon erkölcsös emberről van szó. A támadónak először közel kell kerülnie hozzá. Ehhez a korábban említett számos közeledési technika alkalmas. Mivel erkölcsileg nehezen lehet megtörni, ezért a lefizetés, zsarolás nem működő megoldás az esetében. Azonban egy otthoni Wi-Fi hálózati hiba generálása egy relatív könnyű megoldás arra, hogy szakember segítségére legyen szükség. Az áldozat felhívja a támadót, aki elvileg korábban már olyan sok embernek segített, és megkéri, nézzen rá a számítógépére. Ő természetesen szívesen tesz eleget a kérésnek. A fertőzött pendrive-ot csatlakoztatja a gépbe, így elérte a célját, majd megszünteti a Wi-Fi hibát, amit ő okozott.

Egy ember befolyásolhatóságát a személyiségén és az anyagi helyzetén kívül más is megszabhatja. A szociális körülmények nagyon meghatározóak tudnak lenni. A szülői háttér, az iskolázottság, a családi erkölcsi alapelvek, a társadalmi hierarchiában betöltött pozíció jelentős mértékben befolyásolják egy ember személyiségét. Figyelembe kell venni azt is, hogy egy személy, az adott ország vagy a világ melyik táján él, honnan származik, milyenek a kulturális, vallási hátterei. Jó példák erre a kiberterrorista támadások. Valószínűleg egy jómódú keresztény családban nevelkedett embert nem vonzana egy kiberterrorista cselekedet. [44]

Az embereknek az a tulajdonsága, hogy szeretettnek érezzék magukat, az alapvető fiziológiai szükségleteik kielégítése és biztonság érzete után áll Maslow szerint. [45] A szeretett hölgy iránti viaskodás a történelem során számos alkalommal vezetett már háborúhoz. Egy apró támadás esetén is jó motiváció lehet annak ígérete, hogy ha az áldozat megtesz valamit, a támadó majd segít a hőn áhított személyhez közel kerülni.

Egy objektum elleni támadásnál lényeges, lehet az, hogy egy személynek a munkahelyén milyen a hierarchiában betöltött szerepe. Kiemelten érdekes a téma kapcsán a tipikusan kihasznált szerepkörök. Ezek a főnök, az asszisztens, az informatikus/rendszergazda, a karbantartó személyzet (takarító, szerelő stb.) és manager. A hivatalos pozíción kívül azonban az új kutatások szerint nagyobb jelentőséggel bír, az informális szerep a cégen belül. [46] Ez a fajta hálózatiság egy értő támadó számára alapanyagot jelenthet a megfelelő személy kiválasztására. [47]

Egy közösség függőségi, társas viszonyainak feltérképezése, gráfban történő ábrázolása, nagy segítséget nyújthat abban, hogy megtaláljuk a közösség gyenge pontját, vagy éppen azt az erőset, akinek a figyelmét el kell terelni a sikeres támadáshoz. A skálafüggetlen hálózatok – mint amilyen a társadalom – matematikai szabályok által leírható módon működnek, így tervezhető a közösség reakciója a beavatkozásra.

4.3.3. Generációs különbségek

A jelenleg (2018-ban) használt kommunikáció teljesen eltér attól, mint amit 10-20-50 éve használtak. Jelenleg a könnyen kezelhető interaktív, interkonnektív webes, mobilos alkalmazásokon keresztül történik az információcserénk nagy része. [48] Ehhez a különböző generáció szülöttei attól függően, hogy mennyire születtek bele ebbe a világba másként viszonyulnak. Természetesen nem jelenthető ki, hogy egy generáció minden tagja ugyanúgy viselkedik, ugyanúgy használja a technikai, informatikai eszközöket és szolgáltatásokat, mint a kortársai. Azonban egy jelenleg nagyszülő korabeli személyt, jó eséllyel más módon kell megközelíteni egy támadás esetén, mint egy harmincas éveiben járó aktív személyt. Megint más egy támadás egy digitális bennszülöttel – egy kamasszal vagy egy gyerekkel – szemben, aki most fedezi fel a világot, amiben él, noha természetes számára az őt körülvevő techno-

lógia. Ennek oka persze nem csak a tudásban, de az érettségi szintben, az életkori sajátosságokban és a nemi különbségekben is keresendő. A gyerekek kíváncsisága, a kamaszok „csakazértis" hozzáállása legalább annyira tud sajátos személyiség lenni, mint a férfi-női sajátosságok. [49]

4.4. Irodalomjegyzék

[1] Steven Kenny (2017): Strengthening the network security supply chain. Computer Fraud & Security, 2017/12. pp., 11-14. Elérhetőség: https://www.researchgate.net/publication/321846131_Strengthening_the_network_security_supply_chain (utolsó letöltés: 2018. március 28.)

[2] Klausz Melinda (2017): Megosztok, tehát vagyok. Antheneum Kiadó, Budapest.

[3] Olivia Solon, Sabrina Siddiqui (2017): Russia-backed Facebook posts 'reached 126m Americans' during US elecition. The Guardian, 2017.10.31. Elérhetőség: https://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million (utolsó letöltés: 2018. március 28.)

[4] David Z. Hambrick, Madeline Marquardt (2018): Cognitive Ability and Vulnerability to Fake News, Scientific America 2018.02.06. Elérhetőség: https://www.scientificamerican.com/article/cognitive-ability-and-vulnerability-to-fake-news/ (utolsó letöltés: 2018. március 31.)

[5] Fehér Katalin, Király Olívia (2017): Álhíresülés – a hamis hírek dinamikája a médiában. Századvég 2017/2 p 44 Elérhetőség: https://szazadveg.hu/uploads/media/59888870e25b0/szazadveg-84-alhirek-201708.pdf (utolsó letöltés: 2018.március 28.)

[6] Egyesült Államok: Uniting and Strengthening America, by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001-es 107-56-os törvény, 1016-os szekció, más nevén a Kritikus Infrastruktúrák védelméről szóló 2001-es törvény. Elérhetőség: https://www.selectagents.gov/resources/USApatriotAct.pdf (utolsó letöltés: 2018. január 14.)

[7] PPD 63 – 1998. május 22. Protecting America's critical infrastructures Elérhetőség: https://fas.org/irp/offdocs/pdd/pdd-63.html (utolsó letöltés: 2018. március 05.)

[8] Berki Gábor (2016): Kiberháborúk, kiberkonfliktusok; Pintér István (szerk.) Műhelymunkák: A virtuális térgeopolitikája. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, pp. 245-284. Elérhetőség: http://mek.oszk.hu/16100/16182/16182.pdf (utolsó letöltés: 2018. március 31.)

[9] Molnár Dóra (2017): Egységes európai kibertér? Az Európai Unió Kiberbiztonsági Politikájának fejlődése; Hadmérnök 2017/1. Elérhetőség: http://hadmernok.hu/171_20_molnar2.pdf (utolsó letöltés: 2018. március 25.)

[10] Az Európai Unió Globális Kül- és Biztonságpolitika Stratégiája (2016) Elérhetőség:http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (utolsó letöltés: 2018. március 28.)

[11] Az Európai Unió Kiberbiztonsági Stratégiája (2013) Elérhetőség: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (utolsó letöltés: 2018. március 28.)

[12] Paulo Shakarian, Jana Shakarian, Andrew (2013): RuefIntroduction to Cyber-Warfare pp. 223–239, Elsevier Inc. Waltham, ISBN: 9780124078147

[13] Lattmann Tamás: A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén Elérhetőség: https://www.academia.edu/8028014/A_nemzetközi_jog_lehetséges_szerepe_az_informatikai_hadviselés_területén (utolsó letöltés: 2018. március 27.)

[14] Kovács László, Krasznay Csaba (2017): Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során, Stratégiai Védelmi Kutató Központ (Elemzések) 2017/9 pp. 1-11.

[15] Tobias A. Mattei (2017): Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack; World Neurosurgery 2017/8. pp. 972-974 Elérhetőség: https://www.sciencedirect.com/science/article/pii/S1878875017309968 (utolsó letöltés:

2018. március 31.)
[16] Szádeczky Tamás (2014): Információbiztonsági szabványok. Budapest, Nemzeti Közszolgálati Egyetem. Elérhetőség: https://lipusz.hu/pedagogia_tanulas/nke_eiv/informaciobiztonsagi-szabvanyok.original.pdf (utolsó letöltés: 2018. március 31.)
[17] Europol The Internet Organised Crime Threat Assesment 2016., Europol, Hága, (2016) Elérhetőség: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (utolsó letöltés: 2018. március 24.)
[18] Bányász Péter: Kiberbűnözés és közösségi média (2017), Nemzetbiztonsági Szemle, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet 2017/4. pp. 55-74. https://www.uni-nke.hu/document/uni-nke-hu/nemzetbiztonsagi-szemle-2017-4-szam.pdf (utolsó letöltés: 2018. március 31.)
[19] Nicholas A. Christakis, James H Fowler (2010): Kapcsolatok hálójában; Budapest, Typotex Kiadó; pp. 280-284.
[20] Tari Annamária (2015): #yz Generációk online, Tericium Kiadó, Dabas.
[21] Viktor Mayer-Schönberger, Kenneth Cukier (2014): Big Data, HVG Kiadó Budapest.
[22] Krasznay Csaba (2012): A polgárok védelme egy kiberkonfliktusban, Hadmérnök, 2012/4 pp. 142–151.
[23] Huib Modderkolk (2018): Dutch agencies provide crucial intel about Russia's interference in US-elections, deVolkskrant. Elérhetőség: https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/amp (utolsó letöltés: 2018. március 31.)
[24] Check Point (2018): Stepping Up to Gen V (5th Generation) of Cyber Security. Elérhetőség: https://www.checkpoint.com/downloads/product-related/brochure/gen_v_brochure-.pdf (utolsó letöltés: 2018. március 31.)
[25] Sean-Philip Oriyano (2016): CEHv9: Certified Ethical Hacker Version 9 Study Guide; Figure 1.2, Joh Wiley & Sons Inc., Indianapolis.
[26] Szőr Péter (2010): A vírusvédelem művészete, pp. 4-5, SZAK Kiadó Bicske.
[27] Szőr Péter (2010): A vírusvédelem művészete, SZAK Kiadó Bicske.
[28] Szőr Péter (2010): A vírusvédelem művészete, pp. 25-34, SZAK Kiadó Bicske.
[29] Fehér Krisztián (2016): Kezdő hackerek kézikönyve; pp. 202-204, BBS-INFO kiadó, Budapest.
[30] Fehér Krisztián (2016): Kezdő hackerek kézikönyve; pp. 178-184, BBS-INFO kiadó, Budapest.
[31] Fehér Krisztián (2016): Kezdő hackerek kézikönyve; pp. 184-192, BBS-INFO kiadó, Budapest.
[32] Fehér Krisztián (2016): Kezdő hackerek kézikönyve; pp.192-202, BBS-INFO kiadó, Budapest.
[33] Hadnagy, Cristopher (2011): Social Engineering – The Art of Human Hacking, Wiley Publishing, Indianapolis.
[34] Hadnagy, Cristopher (2011): Social Engineering – The Art of Human Hacking, pp. 103-109, Wiley Publishing, Indianapolis.
[35] Hadnagy, Cristopher (2011): Social Engineering – The Art of Human Hacking, , pp. 109-135, Wiley PublishingIndianapolis.
[36] Ekman, Paul. Friesen (1975, 2003): Unmaskingthe face: A guide to recognizing emotions from facial cluses. Prentice Hall, New Jersey, 1975. Újranyomtatott kiadás: Malor Books, Cambridge, 2003.
[37] Claudine Biland (2013): A hazugság pszichológiája; Háttér Kiadó, Budapest.
[38] Ann Demarais, Valerie White (2008): Első benyomás; HVG Kiadó, Budapest.
[39] Hadnagy, Cristopher (2011): Social Engineering – The Art of Human Hacking, pp. 162-172, Wiley Publishing Indianapolis.
[40] Hadnagy, Cristopher (2011): Social Engineering – The Art of Human Hacking, pp. 55-76, Wiley Publishing Indianapolis.
[41] Cialdini, Robert (1999): A befolyásolás lélektana, Corvinus kiadó.
[42] Hadnagy, Cristopher (2011): Social Engineering – The Art of Human Hacking, pp. 187-215,

Wiley Publishing Indianapolis.
[43] Hadnagy, Cristopher (2011): Social Engineering – The Art of Human Hacking, pp. 77-100, Wiley Publishing Indianapolis.
[44] Berzsenyi Dániel, Ványi Rajmond (2015): Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei; Nemzet és Biztonság 2015/3, pp 135-138. Elérhetőség: http://www.nemzetesbiztonsag.hu/cikkek/nb_2015_3_12_berzsenyi-vanyi_-_egy_katonapolitikai_dontes_lehetseges_kiberbiztonsagi_kovetkezmenyei_iszlam_allam.pdf (utolsó letöltés: 2018. március 31.)
[45] Abraham H. Maslow (1943, 2003): A theory of Human Motivation, Martino Fine Books. Az eredeti könyv 1943-ban került kiadásra.
[46] Barabási Albert-László (2016): A hálózatok tudománya, Libri Könyvkiadó Kft., Budapest, pp. 47-50.
[47] Kiss Dávid, Váczi Dániel (2018): A vállalatok és a kritikus infrastruktúrák humánhálózata ellen irányuló támadások veszélyei a komplex hálózatok elemélete alapján, Hadmérnök, 2018/1, pp. 151-168, Budapest. Elérhetőség: http://real.mtak.hu/77916/1/HT20181_153_170_u.pdf (utolsó letöltés: 2018. március 31.)
[48] Fehér Katalin (2016): Digitalizáció és új média; pp. 54-62, Akadémia Kiadó, Budapest.
[49] Barbara Annis, John Gray (2013): Nemek intelligenciája; pp. 29-30, Trivium Kiadó, Budapest.

5. SOLYMOS ÁKOS: IDENTITÁS- ÉS JOGOSULTSÁGKEZELÉS MINT A CÉLZOTT TÁMADÁSOK MEGELŐZÉSÉNEK TECHNOLÓGIAI ESZKÖZE

5.1. Bevezetés

Az „Identitás- és jogosultságkezelés, mint a célzott támadások megelőzésének technológiai eszköze” tananyag célja nem az, hogy fellistázza az összes objektumot, szubjektumot, ID-t, metaadatot, jogosultságvezérlő paramétert vagy rendszert és a hozzájuk kapcsolódó minden folyamat minden elágazását.

Az anyag célja az, hogy ha egy információbiztonsági vezető azzal a feladattal szembesül a munkahelyén – és ez legyen versenyszféra vagy állami szektor – hogy meg kell valósítania egy felhasználó és jogosultságkezelési rendszert – akkor tudja, hogy mi is ez az egész, hogy vannak szegmensek, ahol már évek óta szabályozott ez a téma, és ezért érdemes megismerni azt, hogy ott mikre helyezték a hangsúlyokat és elvárásokat. Fontos tudnia, hogy egy szervezetnél kik ennek a szerteágazó témának a szereplői, kikkel kell együttműködni, milyen feladatokkal és szituációkkal kell szembenéznie egy információbiztonsági vezetőnek egy szervezetnél, ahol a külsősök és belsősök jönnek-mennek, a HR osztályokat mozgat át egy tollvonással egyik szervezettől a másikhoz, egyik napról a másikra, ahol külső és belső auditorok firtatják, hogy ki, mit, mikor hagyott jóvá, vagy egyik pillanatról a másikra meg kell válni kollégáktól, a lehető legfájdalommentesebben, de mégis úgy, hogy a szervezet működése zavartalanul menjen tovább.

5.2. Felhasználó és jogosultságkezelés a törvények és szabványok tükrében

A felhasználó és jogosultságkezelés az egyik alap problematikája az informatikai rendszereknek, ezért számos törvény és jogszabály foglalkozik ezzel a témával. Ahhoz, hogy egy szervezet pontosan nyomon tudja követni, hogy a felhasználói mikor, mihez férték hozzá, ráadásul úgy, hogy a jogosultsághoz jutást és annak fenntartását is igazolni tudja, ahhoz nagyon nagy elhatározás, megfelelő tervezés és a szükséges folyamatok precíz megvalósítása szükséges.

Ott, ahol a hozzáférés védelem és ennek igazolhatósága elengedhetetlen, ott különböző jogszabályokban szabályozza az Állam a területet. Vannak szektorok, ahol régóta, vannak, ahol kevésbé régóta szabályozott a felhasználó és jogosultságkezelés, de az közös minden szabályozásban, hogy a hozzáférésvédelem megvalósítása egyike az információvédelem alap kontrolljainak.

Ott, ahol nincsen törvényi szintre emelve a felhasználó és jogosultságkezelés, hosszú évek alatt kifejlődött szabványok és ajánlások nyújtanak segítséget a legjobb gyakorlatok kialakításában.

Ezen jogszabályokat, szabványokat és ajánlásokat mutatjuk be ebben a fejezetben.

5.2.1. Törvények és jogszabályok/Felügyeleti ajánlások

5.2.1.1. 2013. évi L. törvény

A *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*.

A jogszabályban megjelenik a bizalmasság mint fogalom, mint az információvédelem egyik alapkövetelménye az alábbi magyarázattal: „az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;" [1]

Ezen alapkövetelményre alapozva, illetve a jogszabály *II. Fejezet elektronikus információbiztonsági követelmények – 3. Alapvető elektronikus információbiztonsági követelmények* fejezetéből vezethető le a szervezeteknél a felhasználó és jogosultságkezelési folyamatok kialakításának szükségessége:

„5. § Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint

b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét." [2]

5.2.1.2. 41/2015. (VII. 15.) BM rendelet

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

A *41/2015. BM Rendeletben a 4. melléklet 3. Védelmi intézkedés katalógus alcímben* meghatározott védelmi intézkedések besorolásának táblázataiban az

A) 3.1 Adminisztratív védelmi intézkedések,

B) 3.2. Fizikai védelmi intézkedések és a

C) 3.3 Logikai védelmi intézkedések

alább felsorolt követelményei kapcsolhatók össze a felhasználó és jogosultságkezelés témaköreivel, nem vizsgálva azon szempontrendszert, hogy milyen biztonsági osztályba sorolások esetén kötelező vagy nem kötelező használni az adott követelményt:

A) Adminisztratív védelmi intézkedések

Adminisztratív védelmi intézkedések esetén a felhasználók munkakörével, a személyek ellenőrzésével, az áthelyezések, átirányítások és kirendelések kezelésével kapcsolatos szabályokat kell rögzíteni. Ennek a tevékenységnek két fő célja van:

„1) Feladatok szétválasztása (separation of Duties)

• Célja, hogy egy folyamat lépéseit különböző személyek végezzék el.

• Ehhez a folyamatot meg kell tervezni.

• Meg kell akadályozni, hogy egy személy a teljes folyamatot ellenőrizze és manipulálja. (Például egy könyvelési osztályon nem fogadhatja be ugyanaz a személy a számlákat, és nem kezdeményezheti ezek ki zetését.) 2) Legkevesebb jogosultság (Least Privilege)

• az elv betartásával a rendszer a felhasználók és az alkalmazások erőforrásokhoz való hozzáférését csak a leg- szükségesebbekre korlátozza.

• Ehhez meg kell határozni a felhasználók munkájához szükséges jogosultságok minimális halmazát.

• a felhasználók ehhez a halmazhoz kapnak csak hozzáférést, se többhöz, se kevesebbhez." [3]

Azon esetekben, amikor egy szervezet nem veszi figyelembe ezen elveket, akkor a felhasználó és jogosultságkezelés eseti jelleggel, egyedi döntéseken fog alapulni. A gyakorlatban ilyenkor korábbi dolgozók már meglévő és szervezeti hagyományokon alapuló jogosultságait veszik alapul, ami által jellemzően többletjogosultságokhoz jut a felhasználó. Ezen kívül, ha nincsenek pontos szabályok a szervezet elhagyására, vagy felhasználók áthelyezésére vonatkozóan, akkor előfordulhat, hogy megmaradnak felhasználói fiókok és jogosultságok, amelyekkel később visszaéléseket lehet elkövetni.

B) FIZIKAI VÉDELMI INTÉZKEDÉSEK

„A legtöbb információbiztonsági fenyegetés a hozzáférés-vezérlési kontrollok kijátszására irányul. a fenyegetések ki- használásával egy támadó nem engedélyezett hozzáférést szerezhet a rendszerhez, alkalmazásokat futtathat, információt olvashat, hozhat létre, adhat hozzá és törölhet. az információvédelem legtipikusabb feladata éppen ezért az, hogy a hozzáférés-vezérlési szabályokat kikényszerítse, és az ezekkel kapcsolatos kockázatokat csökkentse.” [4]

Számos biztonsági esemény a fizikai hozzáférési kontrollok sérüléséből fakad. Például, ha egy támadó bejut egy épületbe, és ott rá tud fizikailag csatlakozni a hálózatra, vagy ha egy hordozható számítógépet vagy adathordozót felügyelet nélkül hagynak, és a támadó el tudja azt tulajdonítani.

C) LOGIKAI VÉDELMI INTÉZKEDÉSEK

A jogszabály ezen fejezete tartalmazza az felhasználói azonosításra, hitelesítésre, hozzáférés ellenőrzésre és vezérlésre vonatkozó szabályokat és követelményeket.

„A hozzáférés-vezérlés olyan biztonsági mechanizmusok gyűjteménye, mely meghatározza, hogy a felhasználók mit tehetnek a rendszerben, azaz milyen erőforrásokhoz férhetnek hozzá és milyen műveleteket hajthatnak végre. azok a védelmi intézkedések tartoznak ide, melyek szabályozzák, hogy egy felhasználó

- milyen felhatalmazással férhet a rendszerhez,
- milyen alkalmazásokat futtathat,
- milyen információkat olvashat, hozhat létre, adhat hozzá és törölhet.

Általánosságban magába foglalja az azonosítás (identifcation), a hitelesítés (authentication), a hozzáférés-engedélyezés (access approval) és az audit (hozzáférés-ellenőrzés) lépéseit, de bizonyos esetekben a hozzáférés-vezérlés részének tekintik az elszámoltathatóságot (accountability) is.” [5]

A logikai védelmi intézkedések kialakítása és működtetése az egyik legkomplexebb feladat, ami egy információbiztonsági felelősre vár. A szabályok meghatározása mellett igazodni kell a szervezet lehetőségeihez, együtt kell tudni működni az informatikai rendszerek üzemeltetőivel, fejlesztőivel és nem utolsó sorban a szervezeti alaptevékenységet végző felhasználókkal. A leggyakoribb felhasználói panasz a hitelesítéssel, a rendszerek hozzáférésével (felhatalmazás, feljogosítással) kapcsolatos.

Napjainkban szinte minden folyamatot informatikai rendszerek támogatnak, amelyeknél az azonosítás, hitelesítés és a feljogosítás, illetve az elszámoltathatóság alapkövetelmény. Ez pedig azzal jár, hogy a felhasználóknak egyre több informatikai rendszert kell használniuk, ami egyre több megjegyezendő vagy birtoklandó azonosítási és hitelesítési információ megjegyzésével és kezelésével jár.

5.2.1.3. 2013. évi CCXXXVII. Törvény a hitelintézetekről és a pénzügyi vállalkozásokról

A *Hitelintézetekről és pénzügyi vállalkozásokról szóló törvény 67/A §* írja elő azon alapkövetelményt, amely a felhasználó és jogosultságkezelés kialakításának szükségességére vonatkozik, mely szerint: „(1) A pénzügyi szolgáltatói tevékenység – a kiegészítő pénzügyi szolgáltatás kivételével – végzésére csak olyan informatikai rendszer felhasználásával kerülhet sor, amely biztosítja a rendszerelemek zártságát, és megakadályozza az informatikai rendszerhez történő jogosulatlan hozzáférést, valamint észrevétlen módosítását.” [6]

Ezen kívül még az informatikai rendszerek tanúsítására (beleértve a hozzáférés-védelem rendszerének és folyamatainak ellenőrzését is) vonatkozóan vannak további jogszabályok: *2016. évi CLXXXII.*

Törvény egyes pénzügyi és gazdasági tárgyú törvények módosításáról, valamint ilyen a *2015. évi LXXXV. Törvény egyes törvényeknek a pénzügyi közvetítőrendszer fejlesztésének előmozdítása érdekében történő módosításáról*. Ezen kívül még a *2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról*, valamint az általuk végezhető tevékenységek szabályairól *– Bszt. 12. § (12)-(14), a 2013. évi CCXXXV. Törvény az egyes fizetési szolgáltatókról – Fsztv. 12/A. és a 2014. évi LXXXVIII. törvény a biztosítási tevékenységről Bit. 94. § (4)-(6)* tartalmaznak az informatikai rendszerek védelmével kapcsolatos olyan követelményt, amely áthivatkozik a *42/2015. a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló kormányrendeletre*. Bővebben a következő fejezetben ejtünk szót a fenti rendeletről.

Ezen jogszabályokban azonban nem történik meg annak részletes kifejtése, hogy mit is értenek a jogszabályok azon, hogy meg kell akadályozni az informatikai rendszerekhez történő jogosulatlan hozzáférést.

Korábban, 2015 előtt, az egyes pénzintézet típusok (bank, befektetési szolgáltató, biztosító, pénzügyi szolgáltató stb.) saját ágazati törvényeiben voltak az informatikai rendszerek biztonsági követelményei megfogalmazva – bár nagyon hasonló formátumban.

5.2.1.4. 42/2015. (III. 12.) Korm. rendelet

A 2015. márciusában lépett hatályba a *42/2015. a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről* szóló kormányrendelet, amely egységes keretbe foglalta a korábban külön jogszabályokban rögzített követelményeket.

A felhasználó és jogosultságkezelés kapcsán az alábbi paragrafusok lettek a mérvadók:

„3. § (1) Az intézmény kiépíti az informatikai rendszere biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működteti.

(2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

a) a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról” [7]

A fenti paragrafus tartalmának abban van nagy szerepe, hogy ha nincsenek az eszközök, informatikai rendszerek (és jogosultságok), illetve személyek nyilvántartva, akkor nem is lehet ezeket összerendelni és az egész hozzáférés vezérlés ad-hoc módon működik. Ha a nyilvántartások rendelkezésre állnak, akkor mondhatjuk, hogy megvan az alapja a felhasználói adminisztráció elvárható szintű kialakításának.

„c) a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események).

4. § (1) Az intézménynél mindenkor rendelkezésre kell állnia

d) az adatokhoz történő hozzáférési rend meghatározásának,

ca) a jogosult általános (emberek és program entitások) és privilegizált (speciális jogokkal felruházott) felhasználók – így különösen rendszergazdák – kizárólag a szigorúan szabályozott szerepkörüknek megfelelően férhetnek a védendő információkhoz és az azokat kezelő rendszer elemeihez, kezdeményezhetnek aktivitásokat, valamint kizárólag meghatározott privilegizált felhasználók adhatnak szabályozott szerepkörüknek megfelelően és ellenőrzött módon hozzáférési jogosultságokat;” [8]

A kiemelt vagy privilegizált jogosultságokkal bírók mindig kiemelt kockázatot is hordoznak. Ha ezen felhasználói jogosultságok nem megfelelően kezeltek a szervezetben, akkor egy potenciális támadónak is sokkal könnyebb dolga van, illetve előfordulhat, hogy olyan személyek is rendelkeznek adminisztrátori jogosultságokkal – például munkaállomásokon – ahol lehetőségük van akár a biztonsági beállítások módosítására vagy védelmi elemek kikapcsolására. Jelentősen

csökkentve ezáltal a teljes informatikai rendszer védekezési képességeit és biztonsági szintjét.

5.2.2. Ajánlások és szabványok

Az Magyar Nemzeti Bank és korábban a Pénzügyi Szervezetek Állami Felügyelete rendszeres időközönként kiadott ajánlásokat, amelyeket erősen ajánlott volt – és manapság is az – figyelembe venni minden pénzintézetnek. Útmutatóként bármilyen szervezet magáévá teheti az ajánlásban foglaltakat, garantáltan növekedni fog a biztonsági szint, ha eddig a témával nem foglalkoztak behatóan.

5.2.2.1. MNB 7/2017. (VII.5.) számú ajánlása

A legfrissebb ilyen ajánlás a *Magyar Nemzeti Bank 7/2017. (VII.5.) számú ajánlása az informatikai rendszer védelméről* címet viseli. Az ajánlás a felügyeleti vizsgálati tapasztalatok és az általános informatikai biztonság kibocsátáskor ismert és elvárható követelményei alapján készült.

Ezen ajánlás azt a célt szolgálja, hogy a korábban említett és idézett pénzintézetekre vonatkozó jogszabályokat részletesen elmagyarázza és akár gyakorlati példákkal, konkrétumokkal segítse azon szereplőket, akiknek feladatok van a szervezetüknél az információvédelemmel kapcsolatban.

Az ajánlás 9. Hozzáférési rend című fejezete ismerteti részletesen a szabályozásra, hozzáférés rendre, felhasználói adminisztrációra és ezek ellenőrzésére vonatkozó követelményeket és szabályokat.

Egy pontot emelnék ki, amely tapasztalatok alapján még olyan szervezeteknél is el szokott maradni, ahol egyébként a nyilvántartások és a jogosultsági folyamtok megfelelően ki vannak alakítva. Ez pedig a felhasználók és jogosultságaik rendszeres felülvizsgálata.

„Az intézmény az informatikai biztonsági szabályozási rendszerben meghatározott eljárásrend szerint, az abban meghatározott időközönként, de legkésőbb évente a felhasználói azonosítók és a hozzájuk kapcsolódó jogosultságok ellenőrzésével meggyőződik a hozzáférési és felhasználói adminisztrációs szabályok betartásáról.” [9]

Amennyiben elmaradnak a fenti hozzáférés vezérléshez kapcsolódó ellenőrzési feladatok, úgy ellenőrizhetetlenné válik, hogy ténylegesen ki milyen rendszerhez fér hozzá, illetőleg nem igazolható, hogy adott műveletet ténylegesen melyik felhasználó hajtotta végre, ami ellehetetleníti a számonkérhetőséget. Extrém esetben, ha egy támadó bejut az informatikai rendszerbe és sikerül felhasználót létrehoznia, akkor erre sem fog fény derülni.

A jogosulatlan tevékenységek megtörténte komoly bizalmi válságot okozhat egy-egy üzleti tevékenység során, ha annak következménye érinti az ügyfeleket vagy az adott szolgáltatást igénybe vevőket. Nem beszélve arról, hogy ha személyes adatokat is érintő incidensről beszélünk, akkor akár komoly büntetésre is számíthat a szervezet.

5.2.2.2. MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági-irányítási rendszerek. Követelmények

Az ISO27001 szabvány [10] mint követelményszabvány a világ minden részén elterjedt. Magyarországon is, ha egy szervezet nem tartozik olyan törvény alá, amely tartalmaz a felhasználó és jogosultságkezelésre, illetve bármilyen IT és információvédelemre vonatkozó előírást, akkor célszerű az ISO27001 szabvány előírásait követnie, amikor a kontrollrendszerét kezdi tervezni és bevezetni.

A szabvány „A” melléklete tartalmazza többek között azon előírásokat, amelyek a felhasználó és jogosultságkezelésre vonatkoznak.

Nem idézzük be a szabványszöveget, de azt érdemes látni, hogy a szabvány is jelen dokumentumban meghatározott életciklus lépéseket követi. A felhasználók kezelésével kapcsolatban a szabvány meghatározza azon szakaszokat, amelyek kapcsán – még nem jogosultsági témákat részletezve – követelményeket kell támasztani, hogy később a felhasználók felelősségteljesen tudják ellátni azon tevékenységeket, amelyet a szervezet rájuk bíz.

5.2.3. Egyéb iparági jó gyakorlatok

5.2.3.1. CIS Top 20 Security control

A *CIS – Center for Internet Security*[175] meghatározta azt húsz kontroll intézkedést, amit minden szervezetnek, aki elektronikus információt kezel, célszerű bevezetni és működtetni. A CIS Top 20 kontrollból [11] több is kapcsolódik a felhasználó és jogosultságkezeléshez.

1. ábra – CIS Top 20 biztonsági kontroll

Ezen kontrollok a következők:

CIS Control 5.: Adminisztrátori/kiemelt jogosultságú felhasználói fiókok ellenőrzött használata (Controlled use of Administrative Privileges).

CIS Control 14.: Ellenőrzött hozzáférés-kezelés a szükséges és elégséges hozzáférés elvét követve. (Controlled Access Based on the Need to Know).

CIS Control 16.: Felhasználói fiókok kontrollált kezelése és ellenőrzése (Account Monitoring and Control)

[175] CIS – Center for Internet Security – https://www.cisecurity.org

5.2.3.2. NIST – National Institute of Standards and Technology

A *NIST (National Institute of Standards and Technology)*[176] az Amerikai Egyesült Államok Kereskedelmi Minisztériuma által kiadott szabvány. A NIST 800 sorozata 1990-ben jött létre mint közérdekű dokumentumok gyűjteménye, amelyek az Amerikai Egyesült Államok szövetségi kormánya számítógépes biztonsági politikáit, eljárásait és irányelveit írják le. A NIST 2015-ben elkezdett egy SP – Special Publication sorozatot is kiadni, amelyben napjainkig több felhasználó és jogosultságkezeléssel kapcsolatos kiadvány is megjelent – igaz, egyelőre „draft" státusszal. Ezzel együtt érdemes tanulmányozni a következő kiadványokat:

- SP 1800-2 Identity and Access Management for Electric Utilities – Draft, Relase date: 8/25/2015 [12];
- SP 1800-3 Attribute Based Access Control (2nd Draft) – Draft, Release Date: 9/20/2017 [13];
- SP 1800-9 Access Rights Management for the Financial Services Sector – Draft, Release Date: 8/31/2017 [14];
- SP 1800-12 Derived Personal Identity Verification (PIV) – Draft, Release Date: 9/29/2017 [15].

A NIST elindított egy projektet *Access Control Policy and Implementation Guides*[177] *(Hozzáférési Kontroll Szabályok és Bevezetésük Kézikönyvei)* címmel, valamint a hozzá tartozó értékelési szempontrendszert.

5.2.3.3. NIST IR 7316, Assessment of Access Control Systems

Ezen kiadvány ismerteti az informatikai rendszerek legáltalánosabban használt hozzáférés kezelési szolgáltatásait, azok struktúráját, előnyeiket és hátrányaikat. [16]

5.2.3.3. NIST IR 7874, Guidelines for Access Control System Evaluation Metrics

Ezen dokumentum tartalmazza a fenti Access Control Systems [NIST IR 7316] értékelési rendszerét, amely bemutatja a szabályokat, modelleket és működési mechanizmusukat. [17]

5.3. Azonosítás, hitelesítés, feljogosítás összefüggései

Az informatikai rendszerekbe történő belépéshez a felhasználókat azonosítani és hitelesíteni kell, valamint ahhoz, hogy a számukra rendelt funkciókat és szerepköröket elérhessék, meg kell vizsgálni, hogy fel vannak-e jogosítva az elérni kívánt funkciók és szerepkörök elérése.

Összefoglaló néven e tevékenységet hozzáférés-vezérlésnek hívjuk.

„A hozzáférés-vezérlés olyan biztonsági mechanizmusok gyűjteménye, mely meghatározza, hogy a felhasználók mit tehetnek a rendszerben, azaz milyen erőforrásokhoz férhetnek hozzá és milyen műveleteket hajthatnak végre. Azok a védelmi intézkedések tartoznak ide, melyek szabályozzák, hogy egy felhasználó:

- Milyen felhatalmazással férhet a rendszerhez,
- Milyen alkalmazásokat futtathat,
- Milyen információkat olvashat, hozhat létre, adhat hozzá és törölhet." [18]

[176] NIST - National Institute of Standards and Technology https://www.nist.gov/

[177] Lásd: https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides

5.3.1. Azonosítás

Az első lépés egy informatikai rendszerbe történő belépéshez, hogy a felhasználó rendelkezzen egy, az adott rendszerben érvényes azonosítóval – az adott rendszerbe történő belépéskor meg kell győződni arról, hogy kinek állítja magát a kérelmező.

5.3.1.1. Mesterséges úton képzett/előállított azonosító alapján történő azonosítás

A rendszerekben használt felhasználói azonosítókat célszerű egységes rendszerben kezelni, és már a rendszer tervezésekor meghatározni az azonosító képzés logikáját.

Azonosító sokféleképpen kinézhet, lehet a felhasználó neve, egyszerűsített neve, e-mail címe, illetve lehet futó sorszám vagy egyéb logika mentén felállított karaktersorozat.

Az azonosítási rendszer kialakításánál vegyük figyelembe, hogy a felhasználó neve, e-mail címe, szervezeti egysége stb. változhat bizonyos idő elteltével, így bonyodalmakat okozhat, ha ezeket azonosítási célból belekódoljuk az azonosítóba.

Az azonosító nem csak a rendszerbelépésnél kerül alkalmazásra, hanem a rendszerhasználat során ezen azonosító is szerepel a naplóállományokban. Emiatt nem célszerű egy adott rendszerben változtatni a felhasználói azonosítót, ha például a felhasználónak megváltozik a neve, és a neve képezte az azonosító, akkor az megnehezíti a naplóelemzés során az érintett felhasználói tevékenység visszakövethetőségét.

Ebből a szempontból a legpraktikusabb megoldás, ha olyan azonosítót használunk, ami semmilyen, a felhasználóra vonatkozó információt nem tartalmaz. Például XYZ123456. A betű és számnévtér nagysága biztosítja, hogy akár millió fölötti azonosítót is képezni tudjunk.

Meg kell említeni, hogy szervezeten belül célszerű előírni az alkalmazásokban ugyanazon azonosító használatát. Ez több dolog miatt is praktikus. Egyrészt a felhasználóknak nem kell többféle azonosítót megjegyezni, másrészt a naplóállományokban ugyanaz az azonosító fogja jelölni ugyanazt a felhasználót. Amennyiben annyira fejlett a szervezet, hogy van biztonsági naplógyűjtő és elemző (SIEM) rendszere, és nem elkülönülten kerülnek az egyes rendszerek elemzésre, hanem már korrelációs szabályok is működnek, akkor nem kell kereszttáblákban összerendelni a rendszerekben használt azonosítókat.

A rendszerek bejelentkezési felületén ügyelni kell arra, hogy amennyiben a bejelentkezés során a felhasználó hibás azonosítót és/vagy jelszót ad meg, ne adjon a rendszer arról információt, hogy melyik komponens lett elrontva.

Ugyanez igaz a jelszó emlékeztető funkcióra is.

5.3.1.2. Biometrikus jellemzők alapján történő azonosítás

A biometrikus jellemzők alapján történő (rövid nevén biometrikus) azonosítás különböző fajtáinak működése egyaránt azon alapul, hogy a rendszer az emberi szervezet vagy viselkedés valamely egyedi sajátosságáról mintát vesz, azt digitális adattá konvertálja és adatbázisban tárolja, majd az aktuálisan levett mintát összeveti az ebben az adatbázisban tárolt mintákkal. A hivatalos definíció szerint a biometria az alapján azonosít, ami az ember maga, nem pedig az alapján, amit tud (kód, jelszó), vagy amije van (kártya, token).

A biometrikus azonosításhoz soroljuk arcképünk fotóját vagy aláírásunkat, melyekkel nap mint nap bizonyítjuk, hogy azonosak vagyunk saját magunkkal. A biometrikus beléptető rendszer előnye, hogy ténylegesen az adott személyt azonosítja, és nem olyan közvetett jellemzőket vizsgál, mint amilyen a PIN kód vagy a beléptető kártya. Ez utóbbiak megfejtése vagy eltulajdonítása esetén már valójában nem azt a személyt fogja azonosítani, akihez eredetileg hozzárendelték.

Biometrikus azonosítás alapfeltételei:

- Egyediség (biometriai azonosításhoz szükséges fizikai jellemzői mindenkinek vannak, de

különböznek más személyek hasonló kategóriájú azonosítóitól);
• Állandóság (a biometriai azonosító tulajdonságai a korral, betegségekkel járó változások során nem változnak);
• Mérhetőség (adattá konvertálható);
• Elvárt sebesség és teljesítmény az azonosítás során;
• Az azonosítási módszer elfogadása (a mintavételt, vagy az azonosítási lépést ne utasítsák el például fizikai érintkezés egy ujj, vagy tenyérlenyomat olvasóval);
• Megbízhatóság (hamisítás, kikerülés elkerülésére).[178]

A biometriai azonosítás során használnak fizikai jellemzőket: arc-, hang-, írisz-, retina-, kéz-, ujjlenyomat-, hajszálér azonosítást és DNS elemzést, valamint azonosíthatnak viselkedésbeli jellemzők például aláírás, gépelési stílus, járás, testtartás vagy gesztusok alapján. Ezek közül a felismerési módok közül néhányat már évtizedek óta alkalmaznak a gyakorlatban is, másokat csak elvétve, és vannak rövid múltra visszatekintő módszerek: fülazonosítás, arcthermogram (hőkép az arcról).

Biometrikus azonosítás bevezetése során mindenképpen vizsgálni érdemes három kritériumot:
• Megfelelőség;
• Feldolgozási sebesség;
• Felhasználói elfogadás.

„1. Megfelelőség
• Hibás visszautasítási ráta (False Reject Rate – FRR) – a rendszer hányszor utasít vissza jogosult felhsználót
• Hibás elfogadási ráta (False Accept Rate – FAR) – a rendszer hányszor enged be nem jogosult felhasználót
• Metszésponti hibaarány (Crossover Error Rate – CER) vagy azonos hibaérték (Equal Error Rate – ERR) – a valódi hibaarány, a függvényként értelmezett FRR és a FAR görbéinek metszéspontját mutatja. Javasolt, hogy a boimetrikus eszköz azonosítási munkapontja az ERR+/- 10%-on belül, erős azonosításnál az ERR +/-5%-on belül maradjon.

2. Feldolgozási sebesség: Mennyi idő alatt képes a rendszer a beolvasott jellemzőket feldolgozni.
3. Felhasználói elfogadás: Az adott technológiát mennyire fogadják el azok, akiknek alá kell vetniük magukat. Például egy vérvétellel történő DNS elemzés csekély elfogadási rátára számíthat” [19]

5.3.2. Hitelesítés

Felhasználó és jogosultságkezelés kapcsán a hitelesítés elsősorban felhasználók – és ezen belül személyek hitelesítéséről szól.

„A hitelesítés az a folyamat, mely arra szolgál, hogy az entitás bizonyítsa az önmagáról állítottak valódiságát. A felhasználó bemutatja a rendszernek az azonosítóját, amit a rendszer hitelesít, mielőtt engedné hozzáférni a rendszerhez” [20]

Hitelesítésről beszélhetünk dokumentumok esetében is, amikor az adott dokumentum sértetlenségének és eredetének hitelességéről győződünk meg. Sőt beszélhetünk termékek, márkák hitelességéről és hitelesítéséről is, de ezek a témák most nem kerülnek részletesebben kifejtésre – mivel nem az információvédelmi felelős hatókörébe esnek.

[178] Lásd: http://oktel.hu/szolgaltatas/belepteto-rendszer/biometrikus-azonositas/

5.3.2.1. A hitelesítés három alaptípusa

a) Személy, hatóság, hitelesítés szolgáltató által igazolt azonosság

Az első típusú hitelesítés olyan hiteles személy/hatóság/szolgáltató által adott azonosság igazolását jelenti, aki első kézből bizonyítja, hogy a személyazonosság valódi. A központosított hatósági/hitelesítés szolgáltatói alapú bizalmi kapcsolatok ilyenek például, ahol a közigazgatási hatóságok, vagy a jogszabályok által arra felhatalmazott elektronikus hitelesítés szolgáltatók a megfelelő azonosítás után a saját elektronikus aláírásukkal hitelesítik személyek elektronikus személyazonosságát.

b) Objektumok és fizikai jellemzők összehasonlítása

A második típusú hitelesítés összehasonlítja az vizsgált objektum sajátosságait valamilyen fizikai jellemzővel. Ezt jellemzően pénzügyi eszközök, értékpapírok, készpénz esetében használják. Informatikában és személyek hitelesítése során nem. Ilyen fizikai jellemzők lehetnek például a vízjelezés, hologramos biztonsági csík, dombornyomtatás, gravírozás, amelyek esetében, ha minden jellemző megegyezik, akkor hitelesnek tekinthető az objektum. Ezek fizikai jellemzők nehezen hamisíthatók és képzett szakemberek, vagy akár laikusok számára is felismerhetők.

c) Dokumentumok és más külső megerősítések

A harmadik típusú hitelesítés dokumentumokra vagy más külső megerősítésekre támaszkodik. Informatikában a felhasználó akkor kapnak ilyen harmadik típusú hitelesítési eszközt, ha előzetesen valamilyen szervezet leellenőrizte a felhasználó azonosságát, majd ez után előállítódik a rendszerhez történő hozzáférést biztosító hitelesítési adat. Ilyen például amikor egy rendszergazda legenerálja a kezdőjelszót a felhasználónak, vagy létrehozzák a privát/publikus kulcspárt, vagy átadja a felhasználó részére az egyszer használatos jelszót generáló hardver/szoftver tokent. Ez esetben az eredetiség hallgatólagos, de nem garantált, mivel az ellenőrzési láncban is történhetnek visszaélések/hamisítások, illetve utólag a felhasználó is átadhatja a hitelesítési adatok másoknak, illetve ezeket el is lophatják tőle, jogosulatlanul felhasználva azokat. Ezen esetekben beszélünk felhasználói azonosság lopásról, vagy identitás lopásról.

5.3.2.2. A hitelesítés tényezői

A valódi hitelesítés módjai három kategóriába sorolhatók, a hitelesítés tényezői alapján:

A felhasználó tudta, valamit a felhasználó és a felhasználó valami. Valamennyi hitelesítési tényező kiterjed az azonosítók azonosítására vagy ellenőrzésére használt elemek körére, amelyek a személy hozzáférési jogosultsága, a tranzakciós kérelem jóváhagyása, a dokumentum vagy egyéb munkatermék aláírása, a mások számára engedélyező hatóság és a jogsértési lánc létrehozása előtt vannak. Pozitív hitelesítés esetén legalább két, és lehetőleg mindhárom tényező elemeit ellenőrizni kell. A három tényező (osztály) és az elemek egyes elemei a következők:

A) Tudás alapú hitelesítés

A tudás alapú hitelesítés tényezői: a felhasználó tud valamit (például jelszót, részleges jelszót, jelmondatot, személyes azonosító számot, másnéven PIN kódot, kihívás/választ (a felhasználónak válaszolnia kell egy kérdésre vagy mintára), biztonsági kérdést. Az azonosító után ezt a hitelesítési adatot kell megadni.

B) Birtoklás alapú hitelesítés

A birtoklás alapú hitelesítés tényezők: a felhasználó rendelkezik valamivel: például chipben tárolt egyedi kód, egyedi, bizonyos időközönként változó egyszer használatos jelszót/számsort generáló

biztonsági token, mobiltelefon beépített hardveres tokennel, vagy telefonon futó szoftveres token. Azonosítás után, illetve előfordul, hogy egy azonosítás és tudás alapú hitelesítés után következik a birtoklás alapú hitelesítés.

2. ábra Gemalto ID Prove 100 harver token

C) A felhasználó biometriai jellemzőin alapuló hitelesítés

A felhasználó biometriai jellemzője által hitelesítési adat: például ujjlenyomat, retina minta, arc, kézfej geometria, hang, egyedi bio-elektromos jelek vagy más biometrikus azonosító és hitelesítő adatok.

5.3.2.3. Hitelesítés típusai

Az online felhasználók hitelesítéséhez használatban lévő leggyakoribb hitelesítési típusok különböznek a biztonság szintjén:

A) Egyfaktoros hitelesítés

A leggyengébb hitelesítési szintként a tényezők három kategóriája egyikének egyetlen elemét használják az egyén személyazonosságának hitelesítéséhez. Az egyetlen tényező használata nem nyújt sok védelmet a visszaélés vagy rosszindulatú behatolás ellen, mivel könnyen ellopható, lefigyelhető, illetve kicsalható számos módszerrel. Ez a fajta hitelesítés nem ajánlott – és nem is engedélyezett olyan pénzügyi vagy személyes vonatkozású ügyletekre, amelyek magasabb szintű biztonságot igényelnek.

B) Kétfaktoros hitelesítés (2FA – Two Factor Authentication)

Ha az azonosítást követően a hitelesítéshez két tényezőt kell feltüntetni, a kétfaktoros hitelesítést kell alkalmazni – például egy chipkártyán tárolt privát kulcsot (a felhasználó által birtokolt eszköz és hitelesítő adat) aminek a kiolvasásához szükséges egy PIN kód (amit a felhasználó tud). Vagy egy azonosítást követő sikeres jelszómegadás után egy előre regisztrált telefonszámra érkező SMS, amely egy pár percig használható egyszer használatos jelszót/számsort tartalmaz.

Egyre elterjedtebb a kétfaktoros hitelesítés. A számos, akár milliós vagy milliárdos nagyságrendű adatlopások arra késztetik a szolgáltatókat, hogy jobban védjék a felhasználók adatait. Ajánlott gyűjtemény a kétfaktoros hitelesítést biztosító szolgáltatásokról, témakör szerint összegyűjtve: https://twofactorauth.org/.

C) Többfaktoros (kettőnél több faktoros) hitelesítés

A kétfaktoros azonosítás során használt két tényező használata helyett több hitelesítési tényezőt használnak a tranzakció biztonságának növelésére.

D) Erős hitelesítés

Az Egyesült Államok kormánya (US Federal Government) meghatározta, hogy az állampolgárok részére nyújtott digitális szolgáltatásokhoz erős, multifaktoros hitelesítést kell alkalmazni.[179]

Az európai, valamint az amerikai megértésben az erős hitelesítés nagyon hasonlít a kettő- vagy többfaktoros hitelesítéshez, azonban azoknál szigorúbb követelményeket támaszt.

A Fast IDentity Online (FIDO) szövetség,[180] létrehozott egy tanúsítási programot (FIDO Functional Certification Program), [21] amellyel a FIDO tagjai, illetve külső szervezetek is le tudják mérni a FIDO által létrehozott technikai specifikációknak való megfelelésüket, illetve e specifikációk alkalmazásával biztosítani lehet a rendszerek közötti átjárást az erős hitelesítéssel kapcsolatban.

E) Folyamatos hitelesítés

A hagyományos számítógépes rendszerek a kezdeti bejelentkezési munkamenettel kapcsolatban hitelesítik a felhasználókat csak, ami a kritikus biztonsági hibát okozhatja. A probléma megoldásához a rendszerek folyamatos felhasználói hitelesítési módszereket igényelnek, amelyek folyamatosan figyelik és hitelesítik a felhasználókat bizonyos biometrikus tulajdonságok alapján.

A legújabb kutatások azt mutatták, hogy az okostelefonok érzékelői és tartozékai által rögzített bizonyos viselkedési jellemzők, például érintésdinamika, billentyű használati dinamika, járásfelismerés is felhasználhatók azonosításra. Ezeket az attribútumokat viselkedési biometriának nevezik, és felhasználhatók okostelefonok felhasználóinak folyamatos ellenőrzésére vagy azonosítására. Ezek a viselkedési biometrikus tulajdonságok alapján épített hitelesítési rendszerek aktív vagy folyamatos hitelesítési rendszerekként ismertek.

5.3.3. Feljogosítás

5.3.3.1. Szükséges és elégséges jogosultság elve

Szükséges és elégséges jogosultság elvének hívjuk azt az állapotot, amikor az adott felhasználó pont annyi jogosultsággal rendelkezik egy informatikai rendszerben – vagy bárhol, ahol jogosultság alapon határozzák meg a hozzáférést valamihez – hogy el tudja végezni a feladatát – és semmi többet.

Ahhoz, hogy ezen elvnek a szervezetek megfeleljenek, meg kell határozni az alapjogosultságokat és további igényelhető jogosultságokat, valamint azokat a szervezeti feltételeket, amikhez az alapjogosultságok és a további igényelhető jogosultságok hozzárendelhetők. Az alapjogosultságokról és igényelhető jogosultságokról a későbbiekben lesz bővebben szó.

[179] Lásd: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

[180] Lásd: https://fidoalliance.org/

5.4. Felhasználó-kezelési folyamatban résztvevő alanyok és területek

5.4.1. Felhasználókezelés alanyai

5.4.1.1. Belsős/munkavállaló

Belsős munkavállalói kategóriába esik mindenki, aki az adott szervezetnél munkavállalói státuszban van. A munkavállalói státusz és jogosultságok esetében az, hogy valaki például közalkalmazott, köztisztviselő vagy egyéb munkavállaló, nem játszik szerepet. Az adott szervezet saját szabályozásában kell, hogy definiálja a felhasználó kezelés alanyait.

Alapesetben a munkavállalói státusz az, amely a legelterjedtebb egy-egy szervezeten belül, de természetesen lehetnek kivételek. Például széles körű külsős szakértői kört foglalkoztató szervezetek, pénzintézetek ügyfélkőre, akik igénybe veszik az elektronikus bankolási rendszereket.

5.4.1.2. Külsős partner, alvállalkozó, támogató

Külsős partnerek, alvállalkozók és egyéb szerződéses viszony alapján hozzáférést kapó felhasználói kör speciális abban a tekintetben, hogy a szervezet és a szerződő partner közötti kapcsolatot egyedül a szerződés – és esetenként a vonatkozó jogszabályok (például Ptk.)[181] határozzák meg. Épp ezért a szervezetben definiálni kell, hogy szerződésen alapuló kapcsolat esetén milyen alapjogosultságok illetik meg a szerződő fél felhasználóit.

Figyelembe véve a GDPR [*Az Európai Parlament és a Tanács (eu) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)*] vonatkozó előírásait, amelyben különösen nagy hangsúlyt kap a külsősök személyes adatokhoz történő hozzáférése, a szervezeteknek meg kell határozni azon rendszert, amelyben első körben maguk a külsős szervezetek regisztrálásra és nyilvántartásra kerülnek, majd, hogy a külsősök milyen folyamat és rendszerek mentén igényelhetnek jogosultságot, azokat ki vagy kik hagyják jóvá, mennyi ideig élnek ezek a jogosultságok, mi történik, ha az adott külsős felhasználó kilép a szerződött partnertől és már nem lesz szükség a jogosultságaira, mi történik akkor, ha egy szerződött partner felhasználója több témában, több szerződés keretén belül is rendszerhozzáférésekkel rendelkezik?

Célszerű a belső felhasználó és jogosultságkezelési szabályozás vonatkozó részeire már a Beszerzési terület általános szerződés mintájában is (amennyiben van ilyen) hivatkozni a külsősökre vonatkozó felhasználói és jogosultság kezelési folyamatokra és szabályokra.

5.4.1.3. Hatósági személyek, auditorok

A Hatósági személyek, auditorok mindig kényes pont egy felhasználó és jogosultságkezelési rendszerben. Azért kényes téma, mert ha egy szervezet volt is olyan gondos és szabályozta a témát, könnyen megszegheti ezen szabályokat, ha derült égből villámcsapásként éri egy olyan igény, hogy például a felügyeleti, vagy könyvvizsgálói auditor kér egy, a hálózatra kötött számítógépet, Internet elérést, adatmozgatási lehetőséget, esetleg hozzáférést rendszerekhez ráadásul mindezt nagyon gyorsan.

Ilyenkor melyik ujjába harapjon az ember, ha nem adja meg a kért jogosultságokat az is baj, mert szabotálja a munkát, de ha meg mindenféle ellenőrzés, regisztráció és jóváhagyás nélkül ad hoc módon megadja a hozzáféréseket, az sem jó, mert nem felel meg a saját szabályainak.

[181] 2013. évi V. Törvény a Polgári Törvénykönyvről.

Ezekre az esetekre kell felkészülni oly módon, hogy kialakítjuk azt a folyamatot, amelyben definiált, hogy milyen típusú külső (esetleg belső) auditokra kell felkészülni, melyik szervezeti egység fogja koordinálni az auditor kollégák regisztrációját, felhasználók létrehozását, kezdőjelszavak kiosztását. Célszerű előzetesen kialakítani egy olyan védett hálózati zónát, ahová az auditori számítógépek csatlakozni tudnak – de onnan más zónákba már nincs átjárás, viszont a szervezeten belüli koordinátorok, vagy az auditért felelős belsős kolléga rendelkezik hozzáféréssel. Így biztosítható, egyfajta zsilipként, hogy az auditorokhoz csak ellenőrzött anyagok jussanak el, ráadásul könnyebb az igényelt és átadott anyagok nyilvántartása és végső átadása.

Bár sokan félnek attól, hogy egy felhasználói regisztráció során az auditorok adatait elkérjék és szabályokkal próbálják meg őket „kordában tartani". Nekem az a tapasztalatom, hogy egy jól átgondolt folyamat mentén végrehajtva a külsős auditori felhasználók regisztrációját és jogosultságadását pozitívabb képet ad a szervezetről azzal szemben, mintha nem létező felhasználókat hoznánk létre a rendszerekben vagy egyéb, nehezen hihető indokkal megtagadnánk az auditorok rendszerhasználati kéréseit.

Ráadásul az auditorok – ha csak nem a Gazdasági Versenyhivatal akciójáról van szó – előre be vannak jelentve. Előzetesen el lehet kérni azon igényeket – például rendszerhasználatot igénylő felhasználók listája és adataik – amelyek mentén már elő tudjuk készíteni az auditorok felhasználóinak elkészítését és jogosultsághoz jutását.

Szintén pozitív képet ad az auditált szervezetről, ha az auditoroknak egy rövid 10-15 perces képzés keretén belül bemutatjuk a szervezet őket érintő biztonsági kontrolljait – köztük a felhasználók és jogosultságok kezelésének menetét is.

5.4.1.4. Technikai felhasználók

Technikai felhasználónak hívjuk azon felhasználói fiókokat, amelyek bár jelen vannak az informatikai alkalmazásokban, de nem fizikai személyek használják őket, hanem az egyes informatikai alkalmazások nevében jelentkeznek be más rendszerekbe, hogy ott előre meghatározott tevékenységet végezzenek.

A technikai felhasználókat – bár nem fizikai személyek használják – célszerű valós fizikai személyek felügyeletére bízni, ezzel felelősséget rendelve az adott felhasználóval történő műveletekért. Ez azért is fontos, mert az ilyen technikai felhasználóknak jellemzően beépített jelszava van, amely nem jár le soha – hiszen így adott esetben kizárhatná magát a technikai felhasználó és így megállna az alkalmazás és az üzleti folyamat. A pénzintézeti szektorban a Pénzügyi Felügyelet kifejezett elvárása, hogy legyen nyilvántartás a technikai felhasználókról, a tevékenységükről és felelősükről. A technikai felhasználók esetében tiltani kell a normál felhasználói felületeken történő bejelentkezést, azért, hogy ne lehessen például próbálgatással megtudni a jelszavukat és ezáltal jogosulatlan tevékenységet végezni.

Technikai felhasználók felhasználói névképzési konvencióját is szükséges kialakítani, hogy egy-egy felhasználóról akár a nyilvántartásban, akár a rendszerben, vagy naplóállományokban meg lehessen állapítani, hogy technikai és nem valós felhasználóról van szó. Ezt jellemzően a felhasználónév elejére illesztett „t" vagy „T" betűvel szokás jelölni.

5.4.1.5. Vészhelyzeti fiókok

A vészhelyzeti fiókok olyan adminisztrátori szerepkörrel rendelkező felhasználók, akiket vészhelyzet esetén, például krízishelyzet és a rendes adminisztrátor, vagy adminisztrátorok elérhetetlensége esetén lehet használni. Létrehozásukat, használatuk körülményeit (engedély a használatra) gondosan le kell dokumentálni. Ahhoz, hogy ne lehessen önkényesen vészhelyzeti fiókot használni a felhasználó jelszavát elosztott titokként kell kezelni. Egy ember egymaga sosem tudhatja a teljes jelszót. Amennyiben erős felhasználó azonosítás van bevezetve, úgy a második vagy többedik faktorhoz való hozzáférést kell elosztott titokként kezelni. Vészhelyzeti fiók elosztott titokkal történő hozzáférése

nem működhet biometrikus azonosítással, kivéve abban az esetben, ha erre kifejezetten felkészítették a rendszert. Az üzleti alkalmazások jellemzően nincsenek e képesség birtokában.

5.4.2. Felhasználó és jogosultságkezelés támogató területei

Sokan úgy gondolják, hogy a felhasználó és jelszókezelési tevékenység alapvetően IT vagy IT biztonsági probléma. Ezzel szemben az igazság az, hogy több terület összehangolt munkája és szabályozott folyamatai szükségesek ahhoz, hogy a felhasználó és jogosultságkezelés megfelelően működjön.

Ilyen területek:

- Humánerőforrás kezelésért felelős terület,
- Beszerzés,
- Informatika,
- Információbiztonsági terület,
- Alkalmazásfejlesztésért felelős terület/fejlesztők.

5.4.2.1. Humánerőforrás kezelésért felelős terület

Ahhoz, hogy az IT megfelelő felhasználói nyilvántartást tudjon működtetni, elengedhetetlen, hogy a Humánerőforrás kezelést felelős terület (továbbiakban HR) rendelkezzen megfelelő szervezeti egység nyilvántartással, ahová a munkavállalókat be tudja sorolni (a nem munkavállalókról később lesz szó). Egy szervezet állandó mozgásban van, ezért szükséges, hogy a HR arra is képes legyen, hogy a saját támogató informatikai rendszere kapcsolatban legyen a felhasználó és jogosultságkezelést végző rendszerrel.

A felhasználók a szervezeten belül is mozgásban vannak, a szervezeti egységek nevei rendszeresen változnak, illetve előfordul, hogy komplett szervezeti egységek áthelyeződnek, szétválnak, vagy éppen egyesülnek. Mivel ezek napi, heti szintű feladatok, ezért szükséges, hogy amennyire lehet, automatizáltan történjenek az ilyen szervezeti mozgások. Ellenkező esetben, ha az egyes alkalmazásoknak saját felhasználói nyilvántartásuk van, saját szervezeti egység nyilvántartással, akkor azt egyesével kell lekezelni, ami nagyon nehéz feladat és már rövidtávon is jelentős erőforrásokat vesz el. A szervezetben szabályozni kell az egyedi megbízásos munkavállaláshoz kapcsolódó felhasználó és jogosultságkezelési folyamatokat is. Jellemzően ezen munkatársakat is a HR szokta kezelni és nyilvántartani.

A HR felel a munkavállalók időben való beléptetéséért, illetve azért, hogy a felhasználó és jogosultságkezelést végző informatikai rendszer, vagy ennek hiányában az informatika és az érintett szervezeti egységek minden információ birtokában legyenek időben, akár áthelyezésről, akár kiléptetésről van szó.

5.4.2.2. Beszerzés

A legtöbb cégnél és szervezetnél dedikált szervezeti egység, a Beszerzés foglalkozik a szervezet által használt termékek és szolgáltatások beszerzésével, pályáztatásával és szerződéskötéssel. Emiatt kiváló rálátásuk van arra, hogy a szervezet milyen partnerkapcsolatokkal, beszállítókkal rendelkezik. Erről jellemzően nyilvántartást is vezetnek.

Ez a nyilvántartás alapul szolgálhat arra, hogy a szerződéses, partneri viszonyban lévő cégek és szervezetek felhasználó és jogosultságkezelése rendezett legyen.

Célszerű beépíteni a külsősök – elsősorban szerződött partnerek – felhasználó kezelési folyamatába egy olyan kontrollpontot, hogy csak a Beszerzés által nyilvántartott, élő szerződéssel rendelkező cégeknek lehessen külsős felhasználója.

Ez azért fontos, mert egy cég több szerződéssel is rendelkezhet, egy felhasználó több szerződéshez kapcsolódó feladaton is dolgozhat, azonban ezt célszerű egy darab felhasználóval megoldani. Fenti

problematika miatt, illetve azért, mert a szerződések változhatnak, teljesítési határidők csúszhatnak, ennek összehangolása nagyon nehéz feladat. Célszerű az egyszerűsítés végett előírni, hogy külsős felhasználók élettartama maximum fél vagy egy év lehet. A határidő eljövetel előtt még időben értesíteni kell az érintetteket a lejáratról (belsős kapcsolattartó, maga az érintett felhasználó) a külsős felhasználó, vagy a belsős kapcsolattartó kezdeményezheti a külsős felhasználó mandátumának meghosszabbítását. Amennyiben ez nem történik meg, akkor a határidőhöz elérkezvén el kell, hogy induljon a visszavonási folyamat.

5.4.2.3. Informatika

Az Informatika (van, ahol az információbiztonsági terület) a felhasználó és jogosultságkezelő rendszer adminisztrációját végzi, illetve támogatóként részt kell, hogy vegyen minden jogosultságkezelési folyamatban. Ezen kívül még kiemelt szerepe van a technikai felhasználók kezelésében és a kiemelt jogosultsággal rendelkező felhasználókhoz kapcsolódó folyamatok kezelésében.

A) Alkalmazásfejlesztésért felelős terület/fejlesztők

A szervezetbe mind vásárlás, mind fejlesztés útján kerülhetnek alkalmazások. Mindkét esetben ügyelni kell a felhasználó és jogosultságkezelésre.

„Nem elég olyan terméket vennünk, amelyik kielégíti a biztonsági követelményünket, azzal is tisztában kell lennünk, hogy a gyártók általában – a telepítés megkönnyítése és az egyszerűbb kezelhetőség érdekében – a termék biztonsági beállításait a legalacsonyabb szintre állítják be. A különböző termékkel elérhető legmagasabb szintű biztonság nem az alapértelmezett beállításokkal érhető el!

Az alkalmazásokat úgy kell elkészteni, hogy az operációs rendszer megbízható felhasználó-azonosító rendszerét vagy a szervezetnél alkalmazott biztonsági szerver hasonló szolgáltatásait vegye igénybe. Az egyéb kiegészítő és segédprogramok – minden praktikus hasznuk mellet – számos biztonsági kockázatot jelentenek, mert ellenőrizetlen hozzáférésre adnak alkalmat. Miért? A különböző DBview (adatbázis-nézegető) programok például az alkalmazói rendszer hozzáférési rendszerét megkerülve közvetlenül olvashatóvá tesznek minden adatot” [22]

Alkalmazásfejlesztés kapcsán előzetesen kialakított koncepció mentén kell a felhasználó és jogosultságkezelést kialakítani.

Természetesen minden verziót nem tudunk most kifejteni, de gyakorlati tapasztalatok alapján javasoljuk, hogy törekedjen a szervezet egy olyan felhasználó és jogosultságkezelési struktúra kialakításában, ahol az alkalmazásoknak nincsen saját felhasználó és jogosultságkezelése és nincsenek egyedi jogosultságok, hanem minden jogosultság szerepkörökbe van rendelve és csak szerepköröket kaphatnak a felhasználók.

B) Alkalmazáson belüli felhasználó és jogosultságkezelés vs. központi megoldás

A saját, alkalmazáson belüli felhasználó kezelés legnagyobb hátulütője, hogy a folyamatosan változó szervezeti egység struktúrát nagyon nehéz, ha nem lehetetlen hosszútávon lekövetni. Amennyiben ez nem történik meg, akkor nem lehet majd szervezeti egységekhez, munkakörökhöz rendelni a szerepköröket és jogosultságokat. és nagyon gyorsan teljesen vegyes, egyedi jogosultságokkal tarkított rendszerrel kell majd az üzemeltetésnek megküzdenie. Ezen kívül a fenti probléma a rendszeres felhasználó és jogosultság ellenőrzést és incidenskezelést is megnehezíti, hiszen ha nem megbízhatóak az adatok a felhasználók szervezeti egységeire nézve, akkor az ezekhez kapcsolható (és jó esetben jogosultság engedélyezési/felülvizsgálati/visszavonási jogkörrel rendelkező) vezetők tekintetében sem lesz az. Ráadásul, amennyiben valamilyen ticketing rendszerben vannak a jogosultságigénylések és jóváhagyások dokumentálva, egyesével vissza kell tudni vezetni minden egyes jogosultság ellenőrzésekor, hogy adott vezető jogosult volt-e, illetve nem változott-e meg azóta a státusza, és ha megváltozott, akkor ki most a felelős, akihez tartoznak ezek a jogosultság engedélyezési/felülvizsgálati/visszavonási jogkörök.

C) Egyedi jogosultságok vs. szerepkörösítés

Abban az esetben, ha nincsenek a jogosultságok szerepkörösítve, akkor a felhasználóknak (vagy általában a jogosultságigénylőnek, aki lehet akár egy vezető is) – főleg az újaknak, de a régieknek sem feltétlenül – nem lesz meg azon képessége, hogy olyan szintig ismerjék a rendszert, hogy pontosan meg tudják mondani, hogy adott felhasználónak pontosan milyen jogosultságok halmazára van szükség. Emiatt a rendszerben lévő jogosultságok teljesen kusza módon lesznek megadva és használva, nem fog érvényesülni a szükséges és elégséges hozzáférés elve és hatalmas munka lesz felülvizsgálni a jogosultságokat, valamint rendszermódosítás (például új funkció esetén) esetén mindenkinek egyedileg kell jogokat adni, vagy elvenni.

Egyedi jogosultságokkal operáló rendszereknél jellemző a jogosultságigény olyan formája, hogy „olyan jogokat kérek, mint XY-né.” Ez pedig a kifejezett táptalaja annak, hogy a jogosultságok szóbeszéd útján legyen igényelve, ahol végül senki nem fogja tudni, hogy XY-nak beállított jogosultságok mindegyike valóban szükséges-e az igénylőnek vagy sem? Ráadásul az egyedi jogosultságokkal rendelkező alkalmazási struktúrában nagyon nehéz kialakítani a kizáró jogosultságok rendszerét, ami hogyha nincs, vagy nem megfelelően működik, akkor a táptalaja a belső csalások lehetőségének kihasználására. Könnyen előfordulhat, hogy valaki egyaránt rendelkezik például rögzítő és jóváhagyó funkcióval egy rendszerben, ami belső visszaélésekhez, konkrét anyagi kárhoz, vagy büntetésekhez vezethet.

Mit lehet tenni? Az egyedi jogosultságokkal rendelkező alkalmazásokat fel kell mérni és szerepkörösíteni kell a jogosultságokat. A szerepköröket pedig valamilyen AD/LDAP csoporttagsághoz kell rendelni. Ilyen formán a szerepkörök (és a szerepköröket birtokló felhasználók, vagy csoportok) központi címtárban kezelhetők, ellenőrizhetők. Meghatározhatók a kizáró szerepkörök.

Fentieket természetesen dokumentálni szükséges a rendszertervben. A szerepkörökhöz jóváhagyókat lehet rendelni és ki kell alakítani a jóváhagyási folyamatokat.

5.4.2.4. Információbiztonsági terület

Az Információbiztonsági terület a felhasználó és jogosultságkezelés „üzleti területe”, vagy felelőse. Ez a terület felelős azért, hogy meg legyenek határozva azok a követelmények, amelyek mentén a szervezetnél a megfelelő felhasználó és jogosultságkezelési folyamatokat és támogató rendszereket ki lehet alakítani, illetve be kell vezetni.

Az Információbiztonsági terület írja elő a követelményeket és adott esetben ez a terület ellenőrzi is azokat. Amennyiben a felhasználó és jogosultságkezelési tevékenységet nem az Informatika, hanem az Információbiztonsági terület végzi, úgy fontos, hogy szervezeti egység szinten a feladatkörök elkülönüljenek egymástól.

Az Információbiztonsági terület gondozza a Felhasználó és Jogosultságkezelési Szabályzatot is, amelyben mind az alapkövetelmények, mind a folyamatok, ellenőrzési kritériumok, kötelező nyilvántartások vezetése le vannak fektetve. Amennyiben a szervezet nem rendelkezik az alkalmazásfejlesztésekhez kapcsolódó szabályozással, úgy ebben a szabályzatban kaphat helyet felhasználó és jogosultságkezelésekhez kapcsolódó, a fejlesztéseknél megvalósítandó követelmény struktúra is.

5.5. Felhasználó-kezelés életciklusa

A felhasználó kezelésnek is megvannak a saját folyamatai, üzemeltetési kérdései.

„A biztonságot nem elég megvenni, azt fent is kell tartani. Az információbiztonság tehát nem egy atomi esemény, hanem egy életcikluson átívelő folyamat. A rendszer életciklusának leghosszabb része az üzemeltetés, emiatt különösen fontos az üzemeltetés biztonságával foglalkozni.” [23]

5.5.1. Felhasználó létrehozása

A 4.1 Felhasználó-kezelés alanyai fejezetben szereplő különböző funkcióban megnyilvánuló felhasználók első státusza az, amikor létrejön a számukra használatra rendelt felhasználó. Jellemzően a szervezetek nem teljesen egyedi és semmihez sem kapcsolódó felhasználókat használnak, hanem a felhasználók egy tartományban dolgozva – oda bejelentkezve – végzik mindennapi munkájukat. Alapvetően, ha egy személynek létrejön a tartományi belépést biztosító felhasználója, akkor azzal az úgynevezett alapjogosultságokat kapja meg.

5.5.1.1. Alapjogosultságok

Ezen alapjogosultságok a felhasználók alaptípusai szerint rendszerint eltérnek. Egy belsős munkavállaló jellemzően nem ugyanolyan jogosultságokat kap, mint egy hatósági személy vagy auditor.

A szervezetben az alapjogosultságokat előzetesen meg kell határozni a fenti felhasználói körökre. Alapjogosultságok lehetnek a központi nyomtatás, a fájlszerverhez való hozzáférés szervezeti egység szinten, az elektronikus levelezés, az intranet és internet elérés. Minden olyan rendszerszerepkört és jogosultságot, amit nem előzetesen kapnak meg a felhasználók, igényelhető szerepkörnek vagy jogosultságnak hívunk.

Az alapjogosultság lényege, hogy nem szükséges a felhasználóknak egyesével megigényelni őket és végig várni a különböző szintű jóváhagyásokat, hanem alapból megkapják őket, mivel előzetesen már a szükséges jóváhagyások és ezek dokumentálása megtörtént.

5.5.1.2. Munkakörökhöz rendelt alapjogosultságok

Az alapjogosultságok a fejlettebb szervezeti kultúrával rendelkező szervezetnél kiterjedhetnek a munkakörök szerinti alapjogosultságokra. Ehhez természetesen előzetesen a Humánerőforrás területnek rendelkeznie kell az összes szervezeti munkakörrel, olyan részletességig, hogy az egyes felelős üzleti, támogató és szakmai területek meghatározták, hogy adott munkakörnek milyen rendszerekhez, azon belül pedig milyen szerepkörökhöz kell már alapállapotban hozzáférnie.

Az alapjogosultságok és ezen belül a munkakörhöz rendelt alapjogosultságok előre meghatározásának a lényege, hogy jelentősen lerövidítik azt az időt, amidőn egy újonnan a szervezetbe érkező felhasználó hozzájut a munkájának végzéséhez szükséges rendszerhozzáférésekhez és szerepkörökhöz.

5.5.1.3. Igénylehető jogosultságok

Minden olyan jogosultság, ahol nem alapértelmezett az, hogy valaki megkapja azt, az az igényelhető jogosultságok körébe tartozik. Egy-egy szervezetben rengeteg alkalmazás és rendszer és ez miatt rengeteg szerepkör és jogosultság létezhet. Több tízezer is akár. Ezen szerepköröket és jogosultságokat egyrészt nyilván kell tartani, másrészt oly módon hozzáférhetővé kell tenni, hogy a felhasználók – vagy bárki (erről majd később még lesz szó) megigényelhesse.

Nagyon rossz gyakorlat az, ha egy szervezetnél a jogosultságadás történelmi hagyományokon alapszik, vagy kvázi egy-egy felhasználó és a hozzátartozó szerepkörök és jogosultságok öröklődnek, miközben a személy, akihez eredetileg tartozott, már nincs is a szervezetben. Az ilyen jellegű jogosultságigénylések kezdődnek úgy, hogy „(…) olyan jogosultságot szeretnék kapni, mint XY.” Ezt a legegyszerűbben úgy lehet elkerülni, hogy szabályzatban meghatározzuk, hogy konkrét szerepkört, jogosultságot kell igényelni, és részletesen meg kell indokolni, hogy miért.

Ez azért nem megfelelő, mert nincs konkrétan definiálva benne, hogy valójában mire is van szükség. Jellemzően ilyenkor az igénylőnek fogalma sincs, hogy valójában mihez fog hozzáférést kapni, egyáltalán van-e szüksége rá, vagy csak történelmi okokból így volt egyszerűbb.

Ott, ahol a rendszerek, a hozzájuk tartozó szerepkörök és jogosultságok nyilván vannak tartva,

ott van lehetőség arra, hogy az igénylő pontosan meghatározza, hogy milyen rendszerben, milyen szerepkörre vagy jogosultságra van szüksége. Amennyiben ezen rendszerek, a hozzájuk tartozó szerepkörök és jogosultságok egy Felhasználó és Jogosultságkezelő rendszerben (IAM – Identity and Access Management) vannak kezelve, úgy pár kattintással kiválasztható, hogy mire van szükség, majd a jogosultság jóváhagyási és beállítási folyamatok után már birtokba is veheti a felhasználó a rendszert. Ennek időtartama a jóváhagyókon és a beállítókon múlik, már ha nem automatikus a felhasználó létrehozás és a szerepkörök beállítása.

5.5.1.4. Tömeges jogosultságadás és ősfeltöltés

Előfordulhat szervezeteknél, hogy egy-egy rendszer elindulásával arra van szükség, hogy nagyobb létszámú felhasználó rendelkezzen a rendszer által adott jogosultságokkal, mihamarabb. Ekkor elképzelhető a normál jogosultságigénylési és jóváhagyási folyamat, és idővel minden felhasználó megigényli a szükséges szerepkört/jogosultságot, azt jóváhagyják, majd beállításra kerül. De általában a fejlesztést megrendelő terület nem ilyen türelmes és szeretné, hogy már élesbe állás során a rendszer tartalmazza a felhasználókhoz rendelt szerepköröket. Ezt hívják ősfeltöltésnek.

Ezt természetesen végre lehet hajtani, de előzetesen ugyanúgy a szerepkörök és jogosultságok jóváhagyóit ki kell jelölni, le kell dokumentálni, majd az előre meghatározott felhasználó listákat, az elrendelt szerepkörökkel és jogosultságokkal külön jóvá kell hagyatni, majd az adminisztrátoroknak ezen listát be kell tölteni az éles indulás előtt.

Természetesen az éles indulást követően a szerepkörök és jogosultságok ugyanúgy igényelhetők és lemondhatók, mint minden más szerepkörnél és jogosultságnál, azonban ilyenkor már a jóváhagyói folyamaton végig kell mennie az igénynek.

5.5.2. Áthelyezés

Az áthelyezés alanya lehet személy, felhasználó, de lehet szervezeti egység is.

5.5.2.1. Személy áthelyezése

Amennyiben szervezeten belül egy felhasználó új munkakört kap, és ezáltal új szervezeti egységhez kerül, felmerülhet annak veszélye, hogy amennyiben megmaradnak az előző munkakörhöz kapcsolódó szerepkörei és jogosultságai – és ezek összeférhetetlenek, úgy akár véletlenül, akár akarattal, de nem a feladatköréhez kapcsolódó tevékenységet tud végezni, rossz esetben visszaélést tud elkövetni. Például egy rendszerben megmaradt rögzítő jogosultsága, az új helyen pedig megkapta a jóváhagyó jogosultságot. Ezzel már tipikusan meg lehet kerülni egy négy szem elven alapuló üzleti kontrollt.

Személy áthelyezésénél a legbiztonságosabb megoldás, ha az áthelyezés során a felhasználónak minden korábban igényelt jogosultsága visszavonásra kerül, az új helyen pedig az új jogosultságokat újra meg kell igényelni. Még akkor is, ha adott esetben az egyezik valamely korábbi jogosultsággal. Erre azért van szükség, hogy a felhasználó szervezeti vezetője – mint elsődleges jóváhagyó – tudatában legyen a beosztottja jogosultságainak.

Előfordulhatnak olyan esetek, amikor bár a felhasználót áthelyezik, de vissza kell még dolgoznia az előző helyre. Ebben az esetben kivételkezelési folyamat keretében meg kell tartania a szükséges és elégséges régebbi jogosultságait, természetesen jól dokumentálva a helyzetet, majd amikor már nincs szükség rájuk, akkor az új vezetőnek egy rendkívüli jogosultság felülvizsgálat keretében el kell vennie a nem szükséges szerepköröket és jogosultságokat, hogy csak az maradjon meg, ami az új helyen kell. Érdemes a témával kapcsolatos szabályzatban ezen köztes állapot idejét maximalizálni.

5.5.2.2. Szervezeti egység áthelyezése

Abban az esetben, ha szervezeti egységet helyeznek át, akkor jellemzően nem a tevékenységi kör, vagy a felhasználók munkaköre változik meg, hanem kompletten a szervezet, az eddigi tevékenységével már más szervezethez tartozóan végzi a feladatát. Humánerőforrás rendszerekben ez azonban úgy érzékelhető, mintha tömeges áthelyezések történtek volna. Ez azért lehet problémás, mert ha rendszerrel támogatott a felhasználó és jogosultságkezelés, akkor az IAM rendszer automatikusan elkezdené az érintettek szerepköreit és jogosultságait visszavonni.

Ez könnyen üzletmenet-folytonossági incidenst okozhat, hiszen gondoljunk abba bele, hogy egy komplett szervezeti egység összes dolgozója elveszíti az eddigi napi munkájához rendelt szerepköröket és jogosultságokat. Például, ha egy call center felhasználóival történik ez, akkor adott esetben nem fog tudni működni az ügyfél kapcsolattartás ezen a csatornán, ami ügyfél elégedetlenséggel és akár komolyabb pénzügyi veszteséggel is járhat.

Ahhoz, hogy ilyen ne fordulhasson elő, több kontrollt is be kell vezetnünk. Egyrészt tudatosítani kell a Humánerőforrás területtel, hogy mivel jár, ha előzetes egyeztetés nélkül komplett szervezeti egységet helyeznek át a szervezetben, másrészt a folyamatot támogató rendszerbe be kell építeni olyan kontrollt, hogy ha a rendszer például egy adott szervezeti egység létszámának 10%-át meghaladó jogosultság visszavonást érzékel, akkor további értesítésig függessze fel a folyamatot, és küldjön riasztást az üzemeltetőknek/információbiztonsági területnek, mivel ilyen eset lehet akár szándékos támadás, akár hibás működés, vagy meggondolatlan, előkészítetlen döntés miatt is.

5.5.3. Kilépés/Jogosultságok visszavonása

A kiléptetésnek, jogosultságok visszavonásnak is több változata fordulhat elő a szervezeteknél. Az alábbiakban ezeket mutatjuk be.

5.5.3.1. Normál kiléptetés

Az élet természetes velejárója, hogy fluktuáció van egy szervezetnél. Ilyen esetben információvédelmi szempontból az a cél, hogy a felhasználó a tervezett kilépési dátumához közeledvén rendben, tervezetten átadja munkáit, feladatait. Ezen feladatokhoz rendszeresen kapcsolódnak rendszerjogosultságok és szerepkörök.

Rossz gyakorlat és kerülendő, hogy a felhasználó kilépésével nem vonják vissza a jogosultságait, hanem a felhasználói fiókot megkapja valamelyik kolléga, majd tovább használja. Ez rendkívül veszélyes, hiszen a kilépett felhasználó nevében zajlanak tevékenységek, aki már nincs a szervezetnél, nem is tud erről (ezáltal személyiségi jogai sérülnek, lásd GDPR), ráadásul ilyen esetben az is kérdéses, hogy aki megkapta az előző kolléga felhasználói fiókját „használatra”, az milyen gondossággal vigyáz a hozzáférésre? Auditokon több esetben előfordult olyan eset, hogy rég kilépett felhasználó fiókját használták. Indoklásként az a nehezen védhető mondat hangzott el, hogy „neki sokkal több mindenhez volt jogosultsága”. Érezzük, hogy itt több helyen is sérülnek biztonsági kontrollok. Sem a szükséges és elégséges hozzáférés elve nem valósul meg, sem a kilépett felhasználó fiókjának felfüggesztése, törlése nem történt meg, de még jogosultság felülvizsgálat sem lehetett évek óta, hiszen akkor ki kellett volna derülnie, hogy egy már nem munkavállalónak még él a felhasználói fiókja, és műveleteket végeznek vele valakik.

Tehát felhasználó kilépésekor úgy kell szervezni a munkát, hogy mire a felhasználó kilép, addigra a munkájához szükséges szerepkörök és jogosultságok már megigénylésre és beállításra kerüljenek valamely hasonló szerepkörben tovább dolgozó felhasználónál, és az érintett munkamenetek tovább tudjanak futni. Normál kiléptetés esetén a felhasználó utolsó munkanapjának végén az összes szerepkör és jogosultság visszavonásra kerül, és erről a felhasználó is dokumentált formában bizonyosságot kap, jellemzően egy mindenki által aláírt sétálópapír formájában.

Régebbi rendszereknél elő szokott fordulni, hogy nem lehet munkameneteket átadni menet közben, amelyik felhasználó nevében elindultak, azzal kell lezárni azokat. Ez alapvető tervezési hiányosság, hiszen fluktuáció előfordulhat, de egy-egy betegség, szülés is hosszabb ideig feltarthatja a felhasználót a munkavégzésben, ilyen esetekben is tudni kell az ügyeket folytatni.

Ha és amennyiben semmilyen más módon nem lehet megoldani a feladatot, csak a felhasználói fiók tovább vitelével, úgy kivételkezelési eljárás keretén belül az egészet dokumentálni kell, minden részletes körülménnyel és felelősséggel együtt.

A másik tanulság az ilyen esetekből, hogy ha workflow alapú rendszer tervezésében veszünk részt, gondoljunk mindig a felhasználó és jogosultságkezelési szempontokra és a folytonosság biztosítására is.

Elektronikus levelezés postafiók a másik olyan kardinális témakör, ami problémákat okozhat. Ezen problémákat célszerű időben, az elektronikus levelezési szabályzatban szabályozni. Jellemző gyakorlat, hogy a felhasználó kilépése után a felhasználó e-mail címét és postafiókját nem törlik vagy felfüggesztik, hanem továbbra is élő marad. Valós üzleti igény, hogy a partnerek, üzletfelek, ügyfelek nem értesülnek azonnal a kilépésről, és egy törölt postafiók esetén értékes információk tűnhetnek el, akár üzletektől is eleshet a szervezet.

A rossz gyakorlat ebben az esetben az, hogy az egész postafiókhoz, teljes jogosultsággal odaadnak egy kollégának, aki majd „kezeli" azt. Itt problémás, hogy fokozott ellenőrzést igényel, hogy a volt kolléga nevében nem történt-e levélküldés. A legfájdalommentesebb megoldás ilyenkor a „Házon kívüli üzenet" beállítása, amely minden levélírót tájékoztat a megváltozott kapcsolati információkról, illetve automatikus továbbítást beállítani a kilépett kolléga postafiókjára, valamely másik kolléga részére. Majd záros határidőn belül véglegesen lezárni és archiválni a postafiókot. Praktikusan egy hónap elegendő a változások mindenki általi megismerésére.

Olyan helyeken, ahol diverzifikáltan vannak a felhasználók és szerepköreik nyilvántartva, ott a Humánerőforrás szervezet által napi, heti rendszerességgel kiadott „Kilépő lista" lehet megoldást, amely minden érintett tájékoztat és lehetőséget biztosít arra, hogy az egyes rendszerüzemeltetők leellenőrizzék a saját nyilvántartásaikat, és megtörténjenek a visszavonások. A gyakorlatban sajnos ez a módszer rengeteg hibalehetőséget hordoz magában, nem biztosítja megfelelően a felhasználók és jogosultságaik mielőbbi visszavételét. Gyakorlati tapasztalatok alapján rendszeresek, az „úgy gondoltam majd később megcsinálom, de közbe jött valami", „nem vettem észre a felhasználót", „nem kaptam meg az értesítést/e-mailt" „nem tudtam, hogy ez az én dolgom" típusú kifogások a beragadt felhasználói fiókok esetében.

5.5.3.2. Rendkívüli kiléptetés

Minden szervezetnél előfordul, hogy valakit azonnali hatállyal fel kell menteni a munkavégzés alól. Ez esetben természetesen nincs lehetőség a hosszadalmas munka, feladat és jogosultság átadás-átvételi folyamatoknak.

Azonban az ilyen esetekre is fel kell készülni, le kell szabályozni, hogy ha valaki, akár üzleti, akár vezetőségi vagy Humánerőforrás területről rendkívüli kiléptetéssel kíván megválni a felhasználótól, akkor kik azok a területek, az a szűk kör, akiknek tudniuk kell mégis róla.

Először is meg kell határozni, hogy kik azok a szerepkörök, akik ilyen rendkívüli felhasználó és jogosultság visszavonásra utasítást adhatnak ki. Jellemzően: Humánerőforráskezelés, Biztonsági és Információbiztonsági vezető, Legfelső vezető, Csalásmegelőzési terület vezető. Természetesen ez csak ajánlás, ezt minden szervezet maga kell, hogy eldöntse.

Ilyen esetekben is fontos, hogy a kiléptetést az érintett vezető gondolja végig, legyenek összegyűjtve és dokumentálva a felhasználó által használt rendszerek és jogosultságok, természetesen ezt diszkréten végrehajtva.

Legyen minden érintett a szükséges mértékig tájékoztatva, hogy rendkívüli jogosultságvisszavonás várható és a megfelelő pillanatban kapja meg a visszavonáshoz szükséges információkat.

Kiemelt jogosultságokkal rendelkezők (például rendszeradminisztrátorok) rendkívüli kiléptetése

esetén még szigorúbb és még jobban megtervezett forgatókönyvet kell követni, mivel nem békés elválás esetén komoly károkat tud az illető okozni a meglévő rendszerjogosultságaival.

5.5.3.3. Előre beállított mandátum lejárata

Tipikusan olyan felhasználóknál (partnerek, külsősök), ahol nem lehet pontosan meghatározni egy-egy rendszerszerepkör szükségességének nagyon pontos végét, ott szokták alkalmazni az előre meghatározott időben lejáró szerepköröket. Persze elképzelhető, hogy egy mandátum lejárata definiált, de az élet jellemzően ennél bonyolultabb és számtalan ok miatt szükséges lehet a hosszabbítás, azonban ezen eseteknél is fontos, hogy időnként – ha nincsen olyan kontroll, ami garantálná egy külsős felhasználó vagy annak rendszerhozzáférésének lejárattatását, akkor valamilyen tervezett végdátumot ki kell tűzni.

Ez a mandátum lejárati dátum vonatkozhat konkrétan akár a felhasználó felfüggesztésére is.

Fontos, hogy az előre beállított lejáratok alapvetően azt a célt szolgálják, hogy bizonyos idő elteltével mindenképpen szükség legyen a felhasználóval vagy a rendszer jogosultságokkal valamilyen interakcióra. Amennyiben még szükségesek a továbbiakban is, akkor meg lehet őket hosszabbítani, ha már nem azok szükségesek, akkor meg lehet őket változtatni, végül pedig, ha már nem kellenek, és ezt a tényt senki nem jelezte a rendszerüzemeltetők vagy alkalmazásgazdák felé, akkor vissza legyenek vonva.

Az előre beállított lejáratú jogosultságok vagy felhasználók esetében fontos biztosítani, hogy ne meglepetésként érje a felhasználót a fiókja vagy valamely rendszerjogosultságának visszavonása vagy felfüggesztése, hanem időben kapjon a lejáratról tájékoztatást. Ez – amennyiben nincs automatizmus építve erre a funkcióra – egy napi szintű feladattá válhat, amelyben át kell nézni a nyilvántartásokat és a közeljövőben lejáró felhasználói fiókokról és jogosultságokról tájékoztatni kell az érintetteket. Oly módon kell ezt a tájékoztatást megtenni, hogy legyen elég idő arra, hogy a felhasználó vagy jogosultság meghosszabbítását végre lehessen hajtani.

5.5.3.4. Jogi állományba kerülés

Amikor a munkavállaló felhasználó – külsősöknél ez a fogalom nem értelmezhető – hosszabb távollétre megy el, például szülési szabadságon van, tartós beteg, vagy fizetés nélküli szabadságot vesz ki, akkor, bár a szervezet munkavállalója marad, az informatikai rendszerekhez nem szükséges már a hozzáférése ezért mind a felhasználói fiókot, mind a rendszerjogosultságokat fel kell függeszteni.

Rendszerrel támogatott felhasználó és jogosultságkezelési folyamatban ez gyakorlatilag azt jelenti, hogy aki jogi állományi státuszba kerül, arra vonatkozóan azon, vagy az azt megelőző napon el kell, hogy induljon a visszavonási folyamat.

Amennyiben a felhasználó újra felveszi a munkát, úgy újra meg kell igényelnie az összes abban az időpillanatban szükséges jogosultságot.

Nagyon fontos, és be szoktak próbálkozni a tartós betegállományban lévő felhasználók, illetve vezetőik azzal, hogy a betegség alatt is fontos lenne, hogy a kolléga elérje az informatikai rendszereket. Amennyiben ez megvalósul, akkor a táppénzen lévő kolléga táppénzcsalást követ el, ugyanis táppénz alatt fel van mentve a munkavégzés alól – hiszen nem tud dolgozni. Ezt pedig nagyon könnyen le tudja a Hatóság ellenőrizni, ha bekéri a rendszerlogokat és az kitűnik belőle, hogy táppénz ideje alatt a felhasználói fiók aktív volt, be volt jelentkezve, hozzáfért a rendszerekhez – ergo munkát végzett. A „csak megnéztem a levelezésem” is munkának számít ebben az esetben

5.6. Felhasználó és jogosultságkezelés szoftveres támogatása (iam)

„Nagyszámú entitás azonosságának a kezelése egyáltalán nem triviális feladat.” [24]
Az informatikusok és információbiztonsági felelősök egyik legnagyobb kihívása a sokszor százas vagy ezres nagyságrendű felhasználó napi adminisztrálása, a változások lekövetése. Erre a feladatra rendkívül széles spektrumú eszköztárat használnak a felelős szakemberek, amelyek mindegyike segítség, ahhoz képest, mintha nem lenne semmi, de látni fogjuk, hogy az egyes módszereknek és támogató megoldásoknak sokszor komoly veszélyei is vannak.

5.6.1. Szövegszerkesztő és táblázatkezelő programok

Még mindig számos szervezetnél használják a kinyomtatott, papír alapú jogosultság nyilvántartást, mint folyamattámogató eszközt. A papír alapú formnak számos hátránya van – előnyt nem is tudok említeni – talán annyit, hogy a semminél jobb.

Túl azon, hogy rendkívül nehéz nyomon követni a jogosultság változásokat, szinte lehetetlen nem személyre, hanem informatikai rendszerre vonatkozó következtetéseket vagy állapotinformációt kinyerni az ilyen nyilvántartásból. Minden egyes jogosultságváltozásnál vagy újra kell hitelesíteni a korábbi összes jogosultságot, vagy inkrementális módszerrel csak a változásokat követik le, amelyek már rövid időn belül is átláthatatlanná teszik a felhasználó ténylegesen engedélyezett jogosultságait.

A papírokat valamilyen kartotékrendszerben tárolni kell, illetve védeni kell a fizikai sérülésektől, elveszéstől és nem feledve, hogy a GDPR a fizikai – például papír alapon tárolt személyes adatok kezelését is szabályozza – a jogosulatlan hozzáféréstől is.

Egy fokkal fejlettebb módszer, ha a jóváhagyott papír alapú formok adatait átvezetik egy táblázatba, amely kissé áttekinthetőbbé teszi a felhasználók, rendszerek és jogosultságok sokaságát. Azonban ezen megoldás nem tekinthető hiteles nyilvántartásnak, mivel egy táblázat, az csak egy táblázat. Átírható, letörölhető, maximum statisztikai célokat szolgálhat, hiteles nyilvántartásnak nem.

5.6.2. Ticketing/hibajegy kezelő rendszer

A ticketing vagy hibajegykezelő rendszerek használata előrelépés a jogosultság kezelési folyamat szoftveres támogatása során, hiszen a megjelenő jogosultságigényt (felhasználó igényre ticket nyitása) végig lehet kísérni, lehetőség van jóváhagyói állomásokat a folyamatba illeszteni, majd sikeres beállítás/módosítás/törlés esetén a ticketet lezárni, illetve lehetőség van bizonyos események, státuszok lekérdezésére, riportolására is. Mivel a folyamat naplózott, a naplóállományok megőrzése esetén ellenőrizhető a folyamat. A hibajegy megtekintésével látszódik a teljes folyamat.

A hibajegykezelő rendszereket azonban nem erre tervezték, az olyan kérdésekre, mint például az adott időpontban adott rendszerhez kinek volt érvényes hozzáférése, már nem lehet válaszolni egy hibajegykezelő rendszer adataiból. Ahogy arra a kérdésre sem, hogy adott felhasználónak adott időpontban milyen rendszerhozzáférései voltak.

A hibajegykezelő rendszer az egyes felhasználók állapotváltozásainak – tipikusan a jogosultságokon történő módosítás – lekövetésére használható. Ez azonban távol van egy felhasználó és jogosultságkezelő rendszer funkcionalitásától.

5.6.3. Felhasználó és jogosultságkezelő szoftver

A Felhasználó és jogosultságkezelő szoftvereket (Identity and Access Management – IAM) – rendszereket kifejezetten arra tervezték, hogy a teljes folyamatot szoftveresen támogassák, beleértve a felhasználók és jogosultságaik nyilvántartását, a jogosultságkezelési munkafolyamatokat (például jóváhagyások kezelése, felülvizsgálata), a riporting és audit funkciókat.

Sokan úgy gondolják, hogy egy ilyen rendszert kis vállalatoknál nem éri meg bevezetni, mert drága, bonyolult üzemeltetni, azonban ez nem így van. Látható a fenti két „szoftveres támogatásból", hogy azok sok-sok sebből vérzenek, sem jogszabályi, sem valós kockázatcsökkentési képességeik nem kielégítők.

Az IAM rendszerek nagy előnye, hogy az eszközkészlet adott, minden attól függ, hogy a szervezet mennyire felkészült a fogadására. Egy IAM projektnél a legnagyobb kihívás a különböző előfeltételek megteremtése, amelyek nélkül nem lehet sikeresen bevezetni a szoftvert.

5.6.3.1. IAM bevezetés előfeltételek

- Belső szervezeti egységek nyilvántartása és a munkakörök „kitakarítása és rendberakása".
- Belsős dolgozók nyilvántartásának és ehhez kapcsolódó folyamatok rendbetétele.
- Külsős felhasználók (lásd fent) nyilvántartásának és a kapcsolódó folyamatoknak a rendbetétele.
- Tesztfelhasználók létrehozása, a szervezet eredeti méretéhez igazodva. GDPR szempontból aggályos az éles felhasználói adatokat tesztelésre használni.
- Döntés az IAM-ben kezelendő rendszerekről. Érdemes a kevesebb néha több elvet követni.
- IAM-be bevezetendő szoftverek megfelelősége és dokumentáltsága.
- Fentivel párhuzamosan az alkalmazásfejlesztésekhez kapcsolódó, felhasználó és jogosultságkezelési alapelvek bevezetése és kikényszerítése, biztosítandó a jövő alkalmazásainak IAM kompatibilitását.
- Jogosultságigénylések jóváhagyói szintjeinek definiálása, kivételkezelés meghatározása. Nem érdemes három szintnél többet választani, mert elbonyolítja és lassítja az összes folyamatot.
- Felkészülés a hibrid felhasználó és jogosultságkezelési működésre.
- Felülvizsgálati és riporting igények definiálása.

Láthatjuk, hogy még egy árva szó nem volt magáról az IAM rendszerről. Természetesen magának az IAM szoftvernek is meg kell tervezni a működését, ami célszoftver kiválasztásával kezdődik. Kiválasztás alatt értem a tervezést, specifikálást, RFI-t, POC-t, pénzügyi tervezést, tendereztetést, kiválasztást és beszerzést.

5.6.3.2. IAM szoftverek

Az elmúlt közel másfél évtized alatt rengeteget fejlődtek az IAM szoftverek. Érdemes részletesebb piaci áttekintést végezni. Jelen dokumentum terjedelme nem engedi meg, hogy az IAM szoftverek részletes összehasonlító elemzését elvégezzük, ám vannak szakavatott cégek, akik kifejezetten ezzel a témával foglalkoznak.

Fontos megemlíteni, hogy Magyarországon is vannak cégek, akik jó minőségű, itthonról támogatott felhasználó és jogosultságkezelő rendszerek fejlesztésével foglalkoznak, mind az általános, mind a kiemelt felhasználók kezelése terén. Érdemes ezen lehetőségeket is figyelembe venni, mielőtt valamelyik nagy gyártó terméke mellé tesszük le a voksunkat.

A) Gartner

A Gartner kiadott egy „*2017 Planning Guide for Identity and Access Management"* [25] dokumentumot, amelyet érdemes áttekinteni mielőtt IAM bevezetés projektbe fogunk. Ezen kívül szintén a Gartner minden évben kiadja a „Magic Quadrant" nevű elemzését, ahol a vezető gyártók termékeit elemzik és értékelik.

B) Forrester Research

A Gartner mellett másik jelentős kutató cég a Forrester Research, aki szintén jelen van IAM szoftverek terén elemzéssel, ezt is érdemes áttekinteni.

A Forrester IAM elemzése ezen a címen keresve található meg: „*The Identity And Access Management Playbook For 2018*" [26]. Egy másik hasznos dokumentum a „*Forrester's IAM Maturity Assessment*". [27] Egyik szerzője a magyar Cser András.

5.6.3.3. SSO – Single Sign On

Bár maga a technológia már évtizedek óta rendelkezésre áll (*Kerberos protokoll, Athena project, MIT és IBM , 1983*), csak manapság kezd elterjedni az SSO – Single Sign On – Egyszeri belépés – módszerét.

Ez egy centralizált modell, amelynek lényege, hogy a felhasználó jogosultsági információi központilag tároltak, és ha egyszer valamely pontján a rendszernek sikeresen azonosította és hitelesítette magát, akkor a rendszer többi helyén ezt már nem kell végrehajtania, automatikusan hozzáférést kap a számára előre meghatározott rendszerekhez, funkciókhoz.

5.7. Irodalomjegyzék

[1] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. 1. Értelmező rendelkezések, 8. bizalmasság
[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
[3] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.1 Hozzáférés-vezérlés 62. oldal, Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[4] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.1 Hozzáférés-vezérlés 62. oldal, Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[5] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.1 Hozzáférés-vezérlés 62. oldal, Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[6] 2013. évi CCXXXVII. Törvény a hitelintézetekről és a pénzügyi vállalkozásokról, 67/A §.
[7] 42/2015. a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló kormányrendelet. 3. §.
[8] 42/2015. a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló kormányrendelet. 4. §.
[9] A Magyar Nemzeti Bank 7/2017. (VII.5.) számú ajánlása az informatikai rendszer védelméről. 9. Hozzáférési rend.
[10] MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági-Irányítási Rendszerek. Követelmények.
[11] CIS – Center for Internet Security TOP 20 Security Control. Elérhetőség: https://learn.cisecurity.

org/20-controls-download (utolsó letöltés: 2018. február 20.)
[12] NIST SP 1800-2 Identity and Access Management for Electric Utilities – Draft, Relase date: 8/25/2015
[13] NIST SP 1800-3 Attribute Based Access Control (2nd Draft) – Draft, Release Date: 9/20/2017.
[14] NIST SP 1800-9 Access Rights Management for the Financial Services Sector – Draft, Release Date: 8/31/2017.
[15] NIST SP 1800-12 Derived Personal Identity Verification (PIV) – Draft, Release Date: 9/29/2017.
[16] NIST IR 7316 Assessment of Access Control Systems. Elérhetőség: https://csrc.nist.gov/publications/detail/nistir/7316/final (utolsó letöltés: 2018. február 20.)
[17] NIST IR 7874 Guidelines for Access Control System Evaluation Metrics. Elérhetőség: https://csrc.nist.gov/publications/detail/nistir/7874/final (utolsó letöltés: 2018. február 20.)
[18] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.1 Hozzáférés-vezérlés, 62. oldal, Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[19] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.1.1 Azonosítás, hitelesítés – Tulajdonság alapú hitelesítés, 65. oldal Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[20] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.1.1 Azonosítás, hitelesítés – Hitelesítés, 64. oldal Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[21] FIDO Functional Certification Program https://fidoalliance.org/certification/ (utolsó letöltés: 2018. február 23.)
[22] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.3.5 Egyéb kiegészítő és segédprogramok, 78. oldal, Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[23] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.6 Az üzemeltetés biztonsági kérdései, 85. oldal, Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[24] Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése 8.1.1 Azonosítás, hitelesítés – Azonosságkezelés 65. oldal Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, Budapest.
[25] Gartner – 2017 Planning Guide for Identity and Access Management. Elérhetőség: https://www.gartner.com/binaries/content/assets/events/keywords/identity-access-management/iame11/2017-planning-guide-for-identity-and-access---13oct16.pdf (utolsó letöltés: 2018. február 22.)
[26] Forrester – The Identity And Access Management Playbook For 2018. Elérhetőség: https://www.forrester.com/playbook/The+Identity+And+Access+Management+Playbook+-For+2018/-/E-PLA220 (utolsó letöltés: 2018. február 22.
[27] Forrester – Forrester's IAM Maturity Assessment. Elérhetőség: https://www.forrester.com/report/Forresters+IAM+Maturity+Assessment/-/E-RES140079 (utolsó letöltés: 2018. február 23.)

6. KACZUR GÁBOR: SPEAR PHISHING

6.1. Phising – adathalászat

Az adathalászat (angolul phising) egy olyan támadási forma, mely során a támadó a célpont (vagy célpontok) fontos/személyes adatait, belépési azonosítóit (felhasználó nevek, jelszavak) vagy egyéb értékes információit (bankkártya adatok, adóazonosító jel, édesanyja leánykori neve stb.) kívánja megszerezni.

A közhiedelemmel ellentétben az adathalászat nem a kezdők technikája. Sokszor olyan mértékű előkészületek szükségesek egy-egy sikeres adathalászati kampány lebonyolításához, mely szakmai hozzáértést és jelentős befektetett tőkét igényel.

A mai világban már kezd kialakulni az érzékenység az átlagos emberekben is, hogy kiszűrjék, észrevegyék a nem megfelelő körültekintéssel előkészített adathalász támadásokat.

Általánosságban elmondható, hogy a nem megfelelően felépített adathalász próbálkozások sikerességi rátája meglehetősen alacsony, míg egy jól felépített adathalász támadás sikeressége akár 90% feletti is lehet. Ez is lehet az oka annak, hogy az adathalászat napjaink egyik leggyakoribb és legnagyobb rétegeket érintő támadási formája.

Az Anti-Phishing Working Group (APWG) jelentése alapján 2017 első felében több mint 291000 egyedi adathalász weboldalt és több mint 592000 egyedi adathalász kampányt regisztráltak a hozzájuk befutó jelentések alapján.

	Január	Február	Március	Április	Május	Június
Egyedi adathalász web-oldalak	42889	50567	51265	50328	45327	50720
Egyedi adathalász email kampányok	96148	100932	121860	87453	93285	92657

1. sz. táblázat: APWG jelentése 2017 első félév

6.1.1. Phising történelem

1990-es évek – America Online (AOL) belépési és bankkártya adatok megszerzésére irányuló támadások.

1996 január 2 – Az első alkalom, hogy a phising szó publikus használatban megjelenik egy AOHell elnevezésű Usenet-es hírcsoport által.

2001 június – Az első valódi adathalász támadás az E-Gold ellen, mely bár nem volt sikeres, fontos mérföldkőnek számít.

2003 július 25. – Andrew Shain újságíró Phising to steal your information című cikkében egy FBI szóvivő azt nyilatkozza, hogy a phising támadások a legfelkapottabb és legtöbb problémát okozó internetes csalási forma.[182]

[182] Andrew Shain, "Phishing to steal your information," Charlotte Observer, July 25, 2003.

6.1.2. Adathalász támadási formák

Az alábbiakban pár alapvető phising támadási technika bemutatása következik. Fontos, hogy a valóságban ezen technikák változatos kombinációiból épül fel egy-egy phising kampány.

6.1.2.1. Deceptive Phishing – A megtévesztés művészete

A kezdetekkor, mikor a phising még az AOL account-ok ellopásáról szólt, azonnali üzenetküldéseken (instant messaging) történt az áldozatok megkeresése. Mára a legelterjedtebb megoldás olyan email-t küldeni a célpontoknak, melyek megtévesztésig hasonlítanak egy-egy számukra fontos vagy érdekes szolgáltatás által küldött üzenetre. Az ilyen levélküldést „call to action" fázisnak is nevezik a phising támadások esetében, ekkor történik meg a „beetetés".

A megtévesztő levelek célja minden esetben az, hogy a címzett ellátogasson az email-ben elhelyezett linkre, mely a támadóhoz tartozó áloldal.

Az alábbiakban pár példa a „beetetésre":

- Értesítés egy pénzügyi intézettől vagy esetleges üzleti partnertől, miszerint valamilyen probléma merült fel a címzetthez tartozó profillal vagy fiókkal. Természetesen az email tartalmaz egy linket, mely megtévesztően hasonlít az adott megkereső hivatalos linkjeihez és használatával gyorsan és kényelmesen megoldható a felmerült probléma.
- Értesítés, miszerint a címzetthez tartozó account támadásnak eshetett áldozatul és a levélben található linken keresztül a címzett csatlakozhat egy csalás elleni szolgáltatáshoz.
- Fiktív számla küldése egy termék vagy szolgáltatás megvásárlásáról. Amennyiben a címzett nem kéri a terméket, úgy a levélben található linken keresztül lemondhatja azt.
- Értesítés, miszerint valamilyen nem várt változás történt a címzetthez tartozó fiókkal vagy profillal kapcsolatosan. A levélben található linken keresztül visszaigazolható vagy törölhető a változtatás.
- Egy új szolgáltatás indulásáról szóló értesítés, melyet a címzett most akciósan vagy egy időre akár ingyen is igénybe vehet a levélben található linken keresztül.

Minden esetben a cél az, hogy a csaló egy megtévesztő weboldalon keresztül, olyan esszenciális információkat, adatokat szerezhessen meg az áldozattól, melyeket később visszaélésre, haszonszerzésre vagy az áldozat megszemélyesítésére használhat fel, esetleg kártékony programot telepítsen az áldozat gépére a böngészőn keresztül.

A „halász" (phisher) nem feltétlenül önmaga fog visszaélni a megszerzett adatokkal. Sokan az adathalászat eredményeit listákba foglalva árulják harmadik félnek, akik lehetnek kiberbűnözők, internetes csalók, de akár egy konkurens vállalat is.

A megtévesztés eszköztára

- Mimikri

  Az áldozatnak szánt levél külalakja és szövegezése minél pontosabban megegyezik egy hivatalos értesítéssel, annál kevésbé fog gyanakodni a felhasználó. Az olyan levelek esetében, mely helyesírási hibákkal, rossz fordítással esetleg a hivatalos formátum hiányával készülnek, sokkal nagyobb az esélye, hogy a célpontban felmerül a gyanú, és nem sikerül az átverés. Azonban, ha valaki látszólag a bankjától kap egy hivatalos értesítést, akkor a már meglévő bizalmi kapcsolat miatt nagyobb eséllyel válik áldozattá.

  A HTML alapú levelek esetében nagy előnye még a támadónak, hogy a linket akár egy belépési gomb vagy más grafikus elem mögé is elrejtheti, így az áldozatnak nem tűnik fel, hogy a link, amelyet megnyit a böngészőben, egy átverő oldalra mutat.

• Címsor módosítás

JavaScript használatával megoldható, hogy a böngésző címsorában a támadó által meghatározott tartalom jelenjen meg, így az áldozat számára úgy tűnhet, hogy a valós oldalhoz csatlakozott.

• Domain név elrejtése

Amennyiben a támadónak nincs más lehetősége, úgy a link IP címet tartalmaz domain név helyett.

• Cousin domain támadás

A támadó regisztrál egy olyan domain-t, mely elnevezésében megtévesztő módon hasonlít a valós domain-hez. Például: az eredeti domain **www.validbank.hu**, a megtévesztéshez felhasznált link pedig a **www.validbank-security.hu** domaint használja.

• Homográf támadás

Amikor a megtévesztéshez használt domain neve külsőre hasonlít az eredeti domain névre, de bizonyos karakterek lecserélésre kerülnek egy másik, megjelenésben megtévesztő karakterre. Példa: **ellato.hu** homográf megfelelője lehet az **el1lato.hu**

Szintén ide tartozik az úgynevezett **IDN** (Internationalized Domain Name) homograph támadás, amikor egyes karaktereket más karakterkészletből származó karakterre cserélnek.

6.1.2.2. Malware-Based Phishing

Ahogy a megtévesztés, úgy a kártékony kódok használata is sokrétű és az egyes phishing támadási módokkal jól kombinálható technika. A lényege, hogy valamilyen módon egy programot juttasson az áldozat számítógépére, kihasználva biztonsági sérülékenységeket, vagy – felkeltve az áldozat érdeklődését – az úgynevezett emberi tényezőt. Fontos, hogy sok esetben a malware letöltéséhez szükséges weboldal kéretlen levelek (spam) útján jut el az áldozatokhoz.

Hogyan kerülhet a malware az áldozat gépére:

• Egy weboldalon keresztül, mely érdekeltté teszi a felhasználót, hogy letöltsön egy file-t. Ez többnyire felnőtt tartalom, vagy egy celebbel kapcsolatos bulvár ígéretével történik.

Olyan program ajánlása, melyre jó eséllyel szüksége van a felhasználónak, és a program telepítésével a kártékony kód is települ a számítógépre. Az ingyenes biztonsági programok ajánlása az egyik legelterjedtebb módszer.

• Valós oldalak módosításával is elérhető a kártékony kód telepítése. Kedvelt célpontok lehetnek a hírportálok és az egyes file-megosztó oldalak.

Az alábbiakban az egyes malware típusok kerülnek bemutatásra, melyek az adathalászatban segítik a támadót.

Keylogger és screenlogger

A keylogger olyan malware, mely eszköz driverként vagy böngésző kiegészítésként települ. Alapértelmezett működése, hogy figyelje a begépelt adatokat és előre definiált események bekövetkeztekor a támadónak elküldje a rögzített információt a phishing szerverre (az adathalászathoz használt szerver vagy szerver cluster).

A keyloggerek többféle módon is elvégezhetik a feladatukat:

- A böngészőbe épülő segéd alkalmazásként, mely képes detektálni az URL-ben beállt változásokat és rögzíteni azokat, ha a felhasználó olyan weboldalon tartózkodik, mely megegyezik egy előre definiált hitelesítést elváró oldallal.
- Billentyűzet vagy egér driverként, mely képes figyelni a felhasználó tevékenységét.

A screenlogger egy összetett malware, mely egyszerre képes figyelni a felhasználó által bevitt adatokat és a képernyőn található információkat is, ezáltal képes kijátszani a képernyő alapú beviteli megoldásokat, például egy on-screen billentyűzet használatát.

A keyloggerek előre paraméterezett módon végzik feladatukat, figyelik, hogy a felhasználó milyen platformon vagy weboldalon végez adatbevitelt. Ha a bevitt adat megfelel a malware beállításaiban szereplő feltételek egyikével, akkor a bevitt adatokat rögzíti, és meghatározott időpontban elküldi. Általában pénzügyi intézetekkel, információs vagy ügyintézési portálokkal és vállalati VPN oldalakkal kapcsolatos információk válnak a keyloggerek célpontjaivá.

Session hijacker

A session hijacking, magyarul munkamenet-eltérítés, egy olyan támadási forma, ahol a kártékony kód a böngésző komponensként figyeli a felhasználói tevékenységet. Amikor a felhasználó belép egy oldalon a felhasználói fiókjába vagy egyéb hitelesítést igénylő tranzakciót végez, a malware „eltéríti" az adott munkamenetet, hogy felhasználva a megszerzett hitelesítő adatokat egyéb akciókat hajtson végre a felhasználó jogosultságával.

A munkamenet-eltérítés nem csak lokálisan települt malware segítségével lehetséges. Lehetőség van távoli telepítéssel működő session-hijacker áldozatává válni egy man-in-the-middle támadás keretén belül. A man-in-the-middle támadásról részletesebben az 6.1.2.5. fejezet értekezik.

Fontos, hogy egy lokálisan működő session-hijacker esetében az egész tevékenység úgy tűnik kívülről, mintha a felhasználó végezné az általa felügyelt számítógépről, így egy esetleges visszakövetés esetén maga a felhasználó lesz gyanúsítható egy elkövetett kártékony akció felelőseként.

Web trojans

Olyan kártékony kódok, melyek a bejelentkezési oldalak esetén tűnnek fel, úgynevezett pop-up felületként (például böngészők saját hitelesítési ablaka). A felhasználó jóhiszeműen beírja a hitelesítő adatait, melyek azonban nem az általa meghívott weboldalhoz, hanem a trójai által a phisher-hez kerülnek.

Host File Poisoning

Amikor egy felhasználó el akar érni egy weboldalt (például www.penzintezet.hu) és a böngésző címsorába begépeli az URL címet, akkor a beírt címet a számítógépnek át kell fordítania numerikus karakterekké, azaz a domain nevet IP címmé kell alakítania. Alapértelmezetten ez egy DNS (Domain Name System) lekérdezéssel történik. Annak érdekben, hogy ezt ne kelljen minden egyes alkalommal elvégeznie a számítógépnek, a már egyszer meglátogatott domain nevekhez tartozó IP címeket több operációs rendszer is úgynevezett host file-okban tárolja. Ha ennek a file-nak a tartalma módosításra kerül, akkor a felhasználó által megadott www.penzintezet.hu domain helyett a támadó által kívánt IP címen található oldalt fogja betölteni a böngésző. Ezen az oldalon általában egy megtévesztő másolata jelenik meg az eredeti oldalnak, így a felhasználó gyanútlanul megadhatja az eredeti oldalhoz tartozó belépési adatait, melyek így a támadóhoz kerülnek.

System reconfiguration attack

A rendszer konfiguráció módosítása egy olyan támadási forma, mely előkészítő vagy megvalósító fázisa lehet egy man-in-the-middle támadásnak. A legelterjedtebb rendszer konfiguráció módosítások az alábbiak:

- DNS szerver megváltoztatása

  A felhasználó egy, a támadó által üzemeltetett DNS szerver felé küldi el a DNS lekérdezéseket, amelyekre a támadó által meghatározott, hamis válaszok érkeznek.

- Web proxy beállítás megváltoztatása

  A felhasználó számítógépének proxy beállítása úgy módosul, hogy minden webes forgalom a támadó által üzemeltetett web proxy szerveren keresztül történjen. Ekkor a támadó teljes bepillantást kap a felhasználó weben keresztül továbbított adataiba.

- Wireless evil twin támadás

A felhasználó számítógépének wifi beállításai módosulnak úgy, hogy a támadó által üzemeltetett Wi-Fi hálózathoz kapcsolódjon. Így minden hálózati kommunikációt rögzíteni képes a támadó, melyből később bármilyen adatot kinyerhet.

Data theft

Amennyiben lehetőség van a felhasználó gépén kártékony kódot futtatni, úgy az a kód már önmagában elvégezheti az adathalászatot. Az adatlopó kódok előre meghatározott információkat keresnek az áldozat gépén és azokat küldik el a phisher-nek. Ilyen információk lehetnek:

- jelszavak,
- licenszkulcsok,
- aktiváló kódok,
- email-ek,
- bankkártya adatok,
- személyes adatok,
- bármilyen, keresőszavaknak vagy keresőkifejezéseknek megfelelő tartalom.

Ez a fajta támadás a vállalati kémkedés legkedveltebb eszköze, mert azok az érzékeny információk, melyek egy jól védett szerveren tárolódnak, a legtöbb esetben megtalálhatóak a kliens gépeken is valamilyen formában. A kliens gépek védelme pedig általában alacsonyabb szintű, mint a szerverek védelme.

6.1.2.3. DNS-Based Phishing (Pharming)

A DNS alapú adathalászathoz – mely külön elnevezést is kapott, Pharming – tartozik minden olyan adathalász támadás, mely DNS manipulációra épül. Az előző fejezetben részletezett **host file poisoning** és DNS beállítás módosítás is ide sorolható. Ebben a fejezetben a DNS alapú adathalászat azon részeit fejtjük ki, melyek a DNS alapvető működésének kihasználására épülnek így nincs szükség a kliensek direkt támadására ahhoz, hogy sikeres eltérítéseket valósítsanak meg.

Domain név elfoglalása

Minden domain nevet regisztrálni kell, ezzel kerül az meghatározásra, hogy egy adott domain név milyen IP címen érhető el. A domain nevek regisztrációját bizonyos időnként meg kell újítani. Azon domain-ek esetében, melyek regisztrációjának átvétele magas haszonnal kecsegtet, a phisher-ek igyekeznek a lejárat után elsőként bejelentkezni, hogy a domain hozzájuk tartozzon. Szerencsére a doma-

in megújításról idejében küld értesítést a domain szolgáltató, így ma már kicsi az esélye annak, hogy egy ismert domain rossz kezekbe kerüljön, de mindenképpen érdemes odafigyelni erre.

Alternativ domain név elfoglalása

Sok esetben egy ismert domain-t nem regisztrálnak minden nemzeti domain végződéssel. Ennek többnyire kereskedelmi okai vannak. Ha a phisher regisztráltatja magának a www.ceg.com domain-t, és azon a www.ceg.hu domain név alatt található oldal klónját üzemelteti, akkor a felhasználók figyelmetlenségét vagy jóhiszeműségét kihasználhatja. Ugyanez a helyzet az ismert weboldalak jellemző elírásaival.

DNS Spoofing

A DNS spoofing támadás helytelen névfeloldási információ sikeres beillesztését jelenti olyan gazdagép esetén, amely nem rendelkezik jogosultsággal az ilyen információ biztosítására.

Annak érdekében, hogy érthető legyen, hogyan is működik a DNS spoofing, fontos kitérni arra, hogy hogyan működik maga a DNS szolgáltatás. A világ DNS szerverei szigorú hierarchia alapján épülnek fel. A legmagasabb szinten az úgynevezett root DNS szerverek helyezkednek el, ezekből összesen tizenhárom szolgálja ki a világot. Ezekhez a szerverekhez fordulnak a Top-Level Domain (TLD) DNS szerverek, melyek az úgynevezett top-level domain-eket (például .com, .net, .edu, .gov) és az ország domain-eket (például .hu, .jp, .fr) szolgálják ki. Ezekhez a TLD DNS szerverekhez kapcsolódik minden más, úgynevezett authoritative DNS szerver. A DNS szerverek a már lekérdezett névfeloldási adatokat egy zóna file-ban tárolják. Egy-egy host név – IP cím rekord annyi ideig tárolódik a zóna file-ban, amennyi a hozzá tartozó TTL érték, ezután törlődik, és újra le kell kérje a DNS szerver.

Amikor egy kliens meg akar látogatni egy weboldalt, melynek URL címe a www.peldadomain.hu, akkor a kliens DNS szervere a saját tárolt listájából átadja az IP címet. Ha a zóna file nem tartalmazza ezt a rekordot, akkor a kliens DNS kiszolgálója a .hu TLD szervertől kérdezi le, a peldadomain.hu névkiszolgáló szerverét. Ezután a peldadomain.hu DNS szerverétől lekérdezi a www.peldadomain.hu címhez tartozó IP címet, és ezt átadja a kliens gépnek.

A DNS szerverek nagy többsége azonban elfogad a válasz során kiegészítő DNS rekordokat is, melyek hitelességét nem ellenőrzi. Ez alapján egy DNS spoofing támadás az alábbi módon épülhet fel:

A kliens gépet a támadó arra készteti, hogy feloldja a www.phiser.com címet. Ez történhet egy spam emailben található link vagy egy ismert weboldal feltörése és háttérben történő átirányítás útján is akár. A kliens gép elindítja a DNS lekérdezési folyamatot a phiser.com domain névre. A phiser.com DNS szervere, melyet a támadó már előre felkészített, kiegészítő válaszként visszaküldi, hogy a kedvencbank.hu domainhez tartozó IP cím az 1.1.1.1. Ezután a kliens, ha el akar látogatni a www.kedvencbank.hu weboldalra, akkor már a módosított IP címre fog érkezni, ahol a támadó által előkészített weboldal várja.

6.1.2.4. Content injection phishing

A content-injection phishing olyan módszert jelent, amikor rossz szándékú tartalmat helyez el a támadó egy legitim oldal kódjában. Ez a tartalom legtöbbször átirányítja a látogatót egy, a phisher által előkészített weboldalra, kártékony kódot telepít a felhasználó számítógépére, vagy a felhasználó által a módosított weboldalon bevitt adatokat azonnal továbbítja a támadó számára.

A content-injection phishing során általában az alábbi három módszer egyikét vagy ezek ötvözetét használja a támadó:

- A támadó a weboldalt üzemeltető szerver biztonsági sérülékenységét kihasználva lecseréli vagy módosítja a legitim tartalmat.

• A támadó kihasználja a weboldalt üzemeltető szerver hibás beállításait és az ebből eredő cross-site scripting sérülékenységet. A cross-site scripting sérülékenység egy olyan programozási hiba, mely lehetővé teszi külső forrásból származó tartalom feldolgozását. Ez a tartalom többnyire olyan kód, mely az adathalászat során segíti a támadót. Az ilyen kódok a látogató böngészőjében futnak le.
• SQL-injection sérülékenység kihasználása, mely lehetővé teszi, hogy adatbázis vezérlő parancsokat futtasson a támadó egy szerveren, mely így információ szivárgáshoz, adatlopáshoz vezethet.

Fontos megjegyezni, hogy mind a cross-site scripting, mind az SQL-injection programozási hibából, illetve a weboldalt üzemeltető szerver biztonsági hiányosságaiból adódóan hajthatóak végre. A kártékony kódot vagy a weboldal tartalmába kell illeszteni – melyhez a támadónak a weboldalt üzemeltető szervert kell uralma alá hajtania, vagy URL-be ágyazottan futtatható. Ez utóbbi esetben a kód akkor aktiválódik, amikor a látogató meghívja a módosított URL-t, melyet a támadó akár email-ben is eljuttathat hozzá.

6.1.2.5. Man-in-the-middle phishing

A man-in-the-middle támadás során a phisher beékelődik a felhasználó és az általa elérni kívánt szerver közé. Ez a beékelődés azt jelenti, hogy a kliens által közölt adatokat a phisher szervere fogadja és továbbítja a legitim szerver felé, majd az onnan érkező válaszokat, mint kliens fogadja és továbbítja a felhasználó felé. Annak érdekében, hogy ez megtörténhessen, a támadónak már komoly előkészületeket kellett tennie, hiszen biztosítania kellett, hogy a kliens az eredeti szerver helyett először a támadóhoz csatlakozzon. Erre megoldás lehet a már fentebb részletezett DNS-spoofing vagy a kliens proxy beállításainak módosítása. Normál HTTP alapú oldalak esetében a felhasználó sok esetben nem is veheti észre, hogy nem direkt az általa meglátogatott weboldal kiszolgáló szerverével kommunikál. Ha sikeresen beékelődött a támadó, akkor minden információ, amit a kliens és a weboldal között áramlik, átfolyik a phisher szerverén így az érzékeny információk megszerezhetővé válnak. SSL titkosított kommunikáció során (például egy HTTPS oldal) már problémássá válhat egy beékelődő támadás, hiszen a támadó nem rendelkezik a legitim oldal tanúsítványával, mely nélkül nem tudja a kliens és az oldal közötti kommunikáció titkosítását feloldani. Ha mégis megpróbálkozik a támadó a HTTPS kapcsolat bontásával, akkor egy saját tanúsítványt kell használjon, mely esetben a kliens számára már feltűnő lehet, hogy az eddig megbízhatónak ítélt oldal most nem megbízható tanúsítványt használ. Ennek elkerülése érdekében a támadó megpróbálhatja a saját tanúsítványát telepíteni a kliens gépére, hogy a felhasználónak továbbra is úgy tűnjön, hogy egy megbízható tanúsítvánnyal hitelesített oldallal kommunikál.

6.1.2.6. Search engine phishing

Az internetes keresők phishing célú felhasználása esetén, hasonlóan a DNS-spoofing támadáshoz, egy technológia sajátosságát használják ki a támadók arra, hogy az esetleges áldozatok „horogra akadjanak”.

A támadó létrehoz egy weboldalt, mely tartalma egy felkapott, sokak számára érdekesnek ígérkező tartalom. Ez többnyire egy termék értékesítése nagyon jó feltételekkel, nagy leárazások ígéretével. A létrehozott oldalt ezután indexelik a kereső szolgáltatók, és ahol lehet, ott a támadó esetleg még fizet is azért, hogy adott keresések során az oldala kiemelt találat legyen. Innentől, ha valaki rákeres a támadó által hirdetett termékre, megtalálja az oldalt a keresési találatok között. A támadó weboldalán pedig akár malware is töltődhet a kliens gépére, de még bankkártya és egyéb kritikus adatokat is gyűjthet a jóhiszemű felhasználóktól. Ezután, ha a felhasználó valóban meg kívánja vásárolni a hirdetett terméket, és az online fizetést választja, akkor a támadó oldalán akár meg is adhatja banki vagy egyéb elektronikus fizetéshez szükséges adatait, melyet a támadó rögzíthet.

6.2. Spear-phising, célzott adathalászat

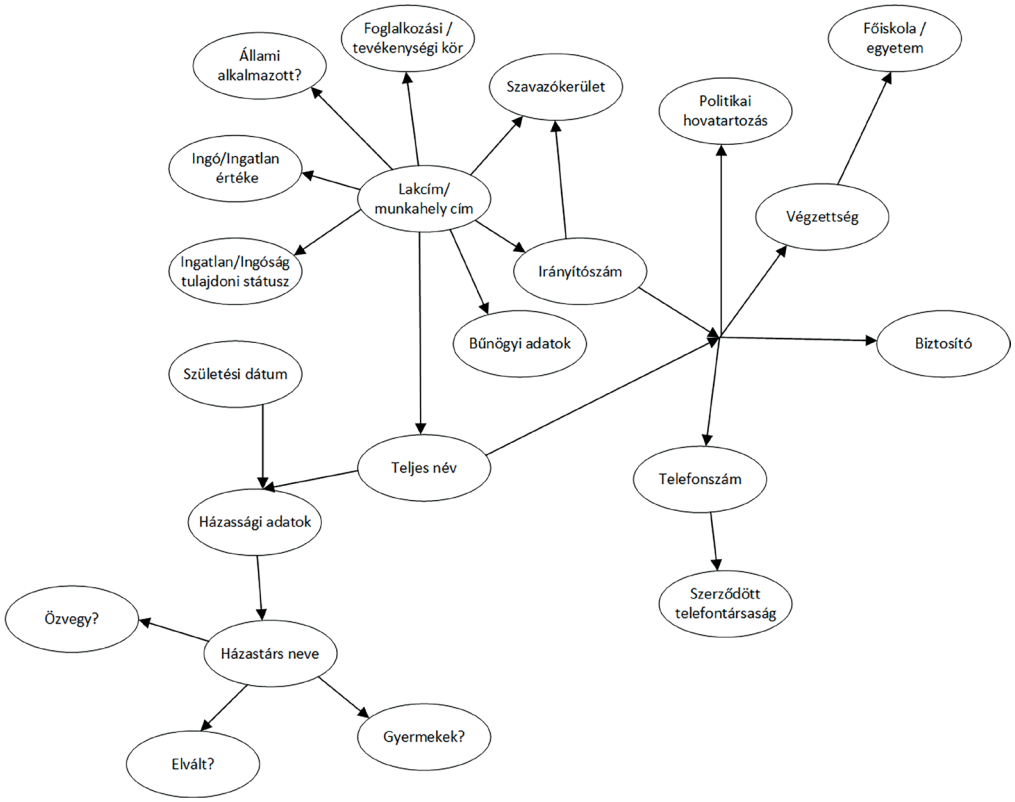
Az eddigi módszerek emberek csoportjait célozták, érdeklődési kör vagy hovatartozás alapján. A célzott adathalászat azonban egy adott személy ellen indított támadás. A célzott támadás sokkal körültekintőbben van felépítve és előkészítve, mint egy általános adathalászat, éppen ezért az áldozat sokszor észre sem veszi, hogy egy adathalász célpontja lett.

6.2.1. Információgyűjtés (Data mining)

A célzott adathalászat legfontosabb tényezője, hogy minél többet megtudjon a támadó, magáról a célpontról. Minél több információval rendelkezik, annál könnyebben találhatja meg a módját annak, hogy a célpont áldozattá váljon.

A lehető legrészletesebb adatgyűjtés egyrészt szükséges, hogy az adathalászat minél sikeresebb legyen. Ugyanakkor megfelelő mennyiségű személyes információ megszerzése már arra is lehetőséget biztosít, hogy a phisher megszemélyesítse áldozatát, esetleg eltulajdonítsa az áldozat által igénybe vett szolgáltatásokat, szélsőséges esetekben pedig akár annak pénzügyi életébe is beavatkozzon (webbanking, az áldozat nevére szóló kölcsön vagy jelzálog felvétele stb.).

Az elsőkörös információ gyűjtés lényege a kiszemelt célpont általános, publikus információinak megszerzése. Ezekkel az információkkal az emberek többsége nagyvonalúan bánik, holott sok esetben kritikus fontosságúak lehetnek. Az édesanya születési neve, kedvenc háziállat neve akár jelszómódosításnál ellenőrző kérdésre adandó válasz is lehet. A születési dátumokat, vagy rokon/hozzátartozó születési dátumait sokan jelszóként használják. Az alábbi ábra azt szemlélteti pár példán keresztül, hogy az egyes általános információk hogyan kapcsolódhatnak egymáshoz, egyik megszerzése esetén mely további információ megszerzésére nyílhat lehetőség:



1. ábra: Információ-kapcsolati gráf
Forrás: Markus Jakobsson, Steven Myers (2007): Phishing and Countermeasures "6.6 Public records phishing graph" ábra alapján.

6.2.1.1. Social data mining

A mai világban szinte mindenki tagja valamilyen social media szolgáltatásnak. Csak az itthon is elterjedtek közül pár példa:

- Facebook
- Google +
- Instagram
- YouTube
- Twitter
- LinkedIn

A felsoroltakból látszik, hogy egy ember akár több social networking platformnak is tagja lehet. A tapasztalatok szerint és a felhasználói kényelemből adódóan sokan ugyanazokat a bejelentkezési adatokat használják az egyes platformok esetében, sőt lehetőség van az egyik mediához tartozó belépési azonosítójával egy másikba regisztrálni (Például Facebook – Instagram; Google – YouTube)

A social media felületek sajátosságaiból adódóan, az alapértelmezett beállítások nagyon engedékenyek. Az egyes tagok tevékenységei és adatai nyilvánosak, annak érdekében, hogy minél könnyebben egymásra találhassanak és kapcsolódhassanak az egyes felhasználók egymáshoz. A felhasználó feladata lenne a biztonsági és nyilvánossági beállítások megfelelő elvégzése, azonban ez sok esetben hanyagságból vagy ennek fontosságának ismeretének hiányából adódóan, hiányos vagy nem megfelelő. Ilyen esetekben a posztok, kedvelések teljesen nyilvánosak alapértelmezett beállítás szerint. Ennek hátránya, hogy bárki számára hozzáférhetőek a célpont kedvenc filmjei/könyvei/zenéi, szórakozási szokásai, események iránti érdeklődései, sőt személyes adatai és családi kapcsolatai is. Egy jól megtervezett social media alapú támadás így nem csak a célpont, de annak ismerőseinek adatait is könnyen begyűjtheti, ezáltal akár nem várt eredményekhez, előnyökhöz juttatva a támadót.

A közösségi portálokhoz kapcsolódóan számtalan program és alkalmazás generálható. Ezek egy része játék, esetleg érdekesnek ígérkező kvíz vagy felmérő, mely az emberi kíváncsiságra épít. Ezen alkalmazások már most is, nyíltan vagy titkoltan, de arra használatosak, hogy információt gyűjtsön az őt használó emberekről, melyet később marketing célokra felhasználhatnak. Figyelembe véve, hogy az emberek döntő többsége mindenféle fenntartás nélkül veszi igénybe ezeket az alkalmazásokat, akár úgy is, hogy a saját social media accountjával kell azonosítsa magát a használatukhoz, nem meglepő, hogy az adathalászok számára ezek az alkalmazások egy új és biztonsági oldalról nehezen ellenőrizhető felületet jelentenek, mely esetben még annyi fenntartása sincs az esetleges áldozatoknak, mint az emailben történő megkeresések esetében.

Az általános adatok mellett sokszor nagyon is konkrét információkat is megosztanak az emberek ismerőseikkel. Ez átlagos emberi viselkedés viszont a phisher számára aranybányát is jelenthet. Az egyik legérzékenyebb megosztás lehet az utazási és látogatási információk közzététele. Ezen adatokból nagyon jól felépíthetőek a célpont mindennapi szokásai, kedvenc helyei, ételei, szórakozási típusai, sőt akár az is, hogy mikor, várhatóan hol tartózkodik. Egy példa alapján, ha valaki rendszeresen bejelentkezik a kedvenc vendéglátó ipari egységéből, akkor a támadó felhasználhatja a hely vélhetően alacsonyabb biztonsági beállításokkal rendelkező vezeték nélküli hálózatát arra, hogy a célpont eszközeihez hozzáférjen.

6.2.1.2. Böngésző előzményeken alapuló adatgyűjtés

A web böngészők eltárolják a meglátogatott weboldalak URL címeit. Ennek kettős oka van: egyrészt a felhasználó számára egy kényelmi funkció, hogy ő maga visszakereshesse a már meglátogatott és érdekesnek talált oldalakat, másrészt gyorsítótárként is működnek az eltárolt előzmények.

Amíg a felhasználó életét kényelmesebbé teszik, addig egy phisher számára jelentős információkat tárolhatnak ezek a böngészési előzmények. Két fő útja lehet annak, hogy egy támadó megsze-

rezze az eltárolt böngészési adatokat. Az egyik módszer, hogy a phisher malware-t telepít a kliens számítógépére, mely kigyűjti ezeket az információkat és eljuttatja számára. Ennél azonban sokkal kényelmesebb megoldás, ha ismét az egyébként létező legitim megoldásokat használja a támadó. Jelenleg is vannak olyan megoldások – többnyire hirdetések alkalmazzák – melyek képesek rögzíteni, hogy egy felhasználó milyen oldalakat látogat. Gondoljunk csak arra, hogy ha többször rákeresünk egy-egy elektronikai cikkre a Google keresőjét használva, akkor egy idő után a Facebook-on ezzel kapcsolatos hirdetésekkel fogunk találkozni. Ezt hívják célzott marketingnek, melynek jogosságán és törvényességén még ma is vitatkoznak a jogászok, de mindenképpen működik.

Ennél is kellemetlenebb, hogy a támadó számára a weboldalok kinézetét szabályozó CSS is biztosít megoldást arra, hogy begyűjtse a felhasználó böngészési előzményeit. Az url() függvény felhasználásával megoldható, hogy egy weboldalon megjelenítendő link megjelenési stílusa (például háttere) egy másik oldalról töltődjön be. Továbbá a :visited nevű pszeudo osztály használata lehetővé teszi, hogy egy CSS kód akkor érvényesüljön, ha a felhasználó böngészőjének előzményeiben szerepel az adott URL. Ezt az egyes weboldalak arra szokták használni, amikor más stílussal kívánnak megjeleníteni egy visszatérő felhasználónak, és más stílussal egy első alkalommal érkező látogatónak.

A fenti két megoldással a támadó felépíthet egy olyan weboldalt, mely tartalmazza akár több ezer jellemző URL linkjét. Az oldal CSS-e úgy van felépítve, hogy ha a felhasználó böngészője valamelyik URL-t már rögzítette az előzmények között, akkor lépjen érvénybe a :visited pszeudo osztály és az url() függvény kapcsolatával létrehozott CSS rész, mely meghívja az adott URL-t. Ezáltal a preparált oldalon található link listán végigfutva a végeredmény alapján a phisher pontosan tudni fogja, hogy mely URL-ek voltak a felhasználó által látogatottak. Természetesen a felhasználó számára mindezt el lehet rejteni, ugyanis, ha a linkek nem tartalmaznak megjelenítendő szöveget, akkor nem lesz vizuális visszajelzése a CSS kód működésének. Több ezer link ellenőrzése már a felhasználó számára zavaró ideig is eltarthat. Ha nem akarja a támadó, hogy a felhasználó gyanút fogjon vagy elálljon az oldal betöltésének végigvárásától, akár egy „betöltés folyamatban” állapotjelzőt is megjeleníthet a felhasználónak, amíg a háttérben minden linket végigellenőriz a böngésző.

Egyes böngészők a könyvjelzőként eltárolt oldalak esetén is úgy járnak el, mint a gyorsítótárban, előzményekben rögzített oldalak esetén.

6.2.1.3. Automatikus kitöltés funkció kihasználása

Több böngésző is alkalmazza az úgynevezett automatikus kitöltési funkciót (autofill feature). Ennek lényege, hogy ha a felhasználó egy jellemző űrlapot (form-ot) már kitöltött, akkor a böngésző eltárolja az itt megadott adatokat, és amikor legközelebb hasonló form-ot kell kitölteni, akkor felajánlja annak automatikus elvégzését. Ilyen például, amikor egy termék megrendelésekor megadjuk a számlázási vagy szállítási címünket, és amikor legközelebb egy másik rendelés kapcsán elkezdünk egy ilyen űrlapot kitölteni, akkor a böngésző felajánlja az automatikus kitöltést. Ennek kihasználása az alábbi módon történhet:

A támadó egy olyan weboldalra irányítja a felhasználót, ahol annak meg kell adnia a nevét vagy email címét, viszont a háttérben egy adatbekérő form található és az email cím vagy a név kivételével minden más mező el van rejtve. A böngésző ekkor is felajánlja az automatikus kitöltést, ha a felhasználó elkezdi beírni a nevét vagy email címét. Ha a látogató nem elég figyelmes és elfogadja az automatikus kitöltést, akkor az autofill funkció az egyébként rejtett mezőket is kitölti, a felhasználó tudta nélkül.

Egy valós veszély, ha a felhasználó a bankkártya adatokat bekérő form-ot már eltároltatta a böngészője automatikus kitöltési segédével és a phisher egy ilyen módszerrel megszerzi a felhasználó bankkártya adatait.

6.3. Hogyan lehet felismerni, hogy adathalász támadással állunk szemben?

Az eddigi fejezetekben részletezett módszerekből kiderül, hogy egy adathalász támadás sikerességéhez – még ha célzott is – több tényezőnek is teljesülnie kell:

- „Beetetés" avagy Call to action, fel kell kelteni a célpont érdeklődését és rá kell venni, hogy kapcsolódjon egy olyan felülethez, amelyet a támadó megfelelő módon előkészített.
- A célpont számítógépes környezetének olyan biztonsági hiányosságokat kell tartalmaznia, melyeket a phisher kihasználhat.
- A támadónak el kell nyernie a célpont bizalmát, vagy annyira fel kell keltenie az érdeklődését, hogy bizonyos szituációkban a biztonságtudatosság ellenében döntsön, ha szükséges.

Az alábbiakban azokat szempontokat részletezzük melyekre, ha odafigyel a felhasználó, akkor jó eséllyel még időben felismerheti, hogy adathalászat célpontjává válhat.

6.3.1. Körültekintő email kezelés

Nagyon fontos, hogy milyen elektronikus üzeneteket kap a felhasználó. Gyanúra adhatnak okot az alábbiak:

- Olyan szolgáltatótól vagy partnertől kapunk üzenetet, akivel már nem állunk kapcsolatban.
- Olyan felhívást kapunk, hogy erősítsünk meg egy-egy új szolgáltatást, esetleg segítsük a biztonsági beállítások jóváhagyását. Ilyenkor mindig győződjünk meg róla, hogy valós-e a megkeresés.
- Ha hivatalos levél érkezik, de nem tartalmaz elérhetőséget. Ha tartalmaz és a megkeresés váratlan számunkra, mert az adott szervezettől nem vártunk levelet, akkor a levélben található elérhetőségen ellenőrizzük az üzenet valódiságát.
- Az email szövegezése rossz helyesírással, hibás karakterkódolással vagy nyelvtani hibákkal van megírva.

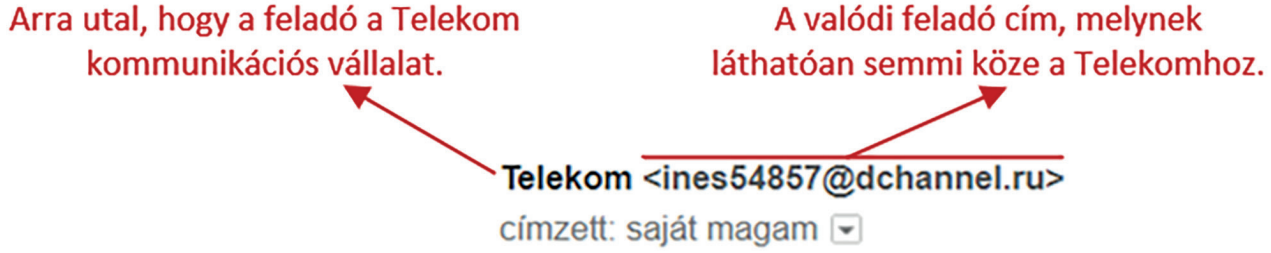
Sok esetben a külföldi adathalászok sima fordítóprogrammal alakítják át az eredeti nyelvű csalinak szánt üzeneteket.

Példa:

„Remeljuk, hogy a szamla kifizeteset a megadott hataridon belul. Vagy az elA'fizetes velunk automatikusan kikapcsol

Most mar fizetni a szamlakat egyszeru es sima utat a bankkartya vagy a bankszamla es biztonsagosan"

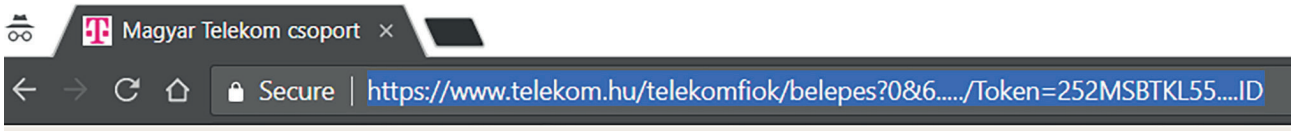
- A feladó hiányzik vagy a domain címe nem egyezik a levél által sugallt szervezet domain címével:



2. ábra: Megtévesztő feladó
Forrás: Saját szerkesztés

• Előre paraméterezett linket tartalmaz az email:

Az adathalászok sokszor előre paraméterezett linkeket illesztenek az email-ekbe. Ezáltal lehetővé teszik az esetleges áldozat azonosítását, illetve az erre érzékeny weboldalak esetén további web-alapú folyamatok, akciók indítását.



3. ábra: Adathalász link
Forrás: Saját szerkesztés

4. ábra: Valódi link
Forrás: Saját szerkesztés

6.3.2. Tudatos internethasználat

A csalinak szánt weboldal iránti érdeklődés felkeltése az adathalászat egyik legfontosabb eleme. Az internet tudatos használatával, ha el is jut valaki egy adathalász weboldalra, több tényező is felkeltheti a gyanúját:

- **Személyes és bankkártya adatok megadására történő felhívás sima http oldalon**

  Az egyes cégek szigorú adatvédelmi szabályok szerint kell kezeljék az ügyfeleik adatait. Ennek egyik alapvető kitétele, hogy adatbekérést csak titkosított csatornán keresztül lehet végezni. Amennyiben egy weboldalon nem titkosított csatornán keresztül kell adatokat megadnunk, tehát nem HTTPS oldal, ne tegyük meg. A titkosítás nélküli kapcsolaton történő adatmegosztás további veszélye, hogy a velünk azonos vezeték nélküli hálózathoz csatlakozó kliensek is láthatják ezeket az információkat, így ez olyan, mintha a tömegben hangosan kiabálnánk a felhasználó nevünket és a jelszavunkat.

- **„Túl szép, hogy igaz legyen" szemléletmód**

  Az egyik legnagyobb érdeklődést kiváltó csali, ha egy ismert, egyébként jelentős árú terméket vagy szolgáltatást óriási kedvezménnyel (80% – 90%), vagy akár ingyen kínálnak. Az ilyen oldalakon szinte mindig megtalálhatóak a már szállóigévé vált „Csak most, csak önnek" és a „Sehol máshol" valamint a „Kihagyhatatlan ajánlat" hívó mondatok. Ha ilyen akcióval találkozunk, mindig érdemes a termék gyártói oldalán utána nézni, hogy valóban van-e ilyen akció, vagy a partnerek között fel van-e tüntetve az akciót hirdető szervezet.

- **Problémás HTTPS tanúsítvány használat**

  A böngészők minden HTTPS kapcsolat esetén ellenőrzik az SSL tanúsítvány érvényességét. Az ellenőrzés az alábbi szempontok szerint történik:

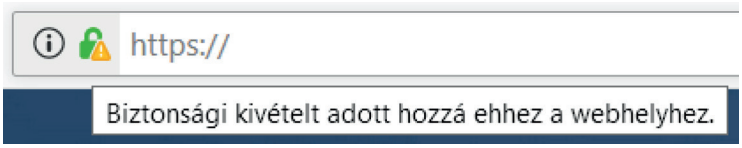
  • A tanúsítvány érvényességi ideje nem járt-e le?
  • A tanúsítvány titkosító algoritmusa elfogadható-e?
  • A tanúsítvány kiállítója egy ismert nemzetközi hitelesítésszolgáltató-e?

• A tanúsítvány ahhoz a meglátogatott oldalhoz (vagy domain-hez) tartozik-e?
Amennyiben a fenti ellenőrzések bármelyike hibára fut, úgy a böngészők az oldal betöltése előtt egy figyelmeztető oldalt jelenítenek meg, melyen a tanúsítvány hibája is megjelenítésre kerül. Az ilyen figyelmeztető oldalak esetében alapértelmezetten a felhasználó közreműködése kell, hogy tovább engedje a weboldalra. Amennyiben ez az oldal nem jelenik meg, vagy valamilyen okból a felhasználó továbblép a hibás tanúsítványú oldalra, a böngészők továbbra is jelzik, hogy gond van az oldal tanúsítványával, a címsor megfelelő formázásával:

5. ábra: Internet Explorer hibás tanúsítvány jelzése
Forrás: Saját szerkesztés

6. ábra: Microsoft Edge hibás tanúsítvány jelzése
Forrás: Saját szerkesztés

7. ábra: Google Chrome hibás tanúsítvány jelzése
Forrás: Saját szerkesztés



8. ábra: Mozilla Firefox hibás tanúsítvány jelzése
Forrás: Saját szerkesztés

6.3.3. Partnerek alapvető viselkedésének ismerete

Elterjedt adathalász módszer a regisztráció megújítására, adategyeztetésre, jelszócserére vagy valamilyen biztonsági funkció jóváhagyására történő felhívás email útján. A pénzügyi intézetek soha nem kérnek be banki vagy regisztrációs adatokat emailben. Ez többnyire igaz minden más szolgáltatóra, ahol valamilyen felhasználói regisztrációt használnak (webshop, levelező rendszerek, közösségi oldalak stb.) Ha emailben a fentiekhez hasonló adatot kérnek tőlünk, az már alapból gyanús kell legyen. Maximum arra küldenek felhívást, hogy jelentkezzünk be a felületükre és ott végezzük el az esetleges adminisztratív vagy beállítás jóváhagyási feladatokat. Ilyen esetben, még ha kényelmi szempontnak is gondoljuk, ne használjuk az email-ben található gyors linket azonnal, csak miután meggyőződtünk róla, hogy a megfelelő oldalra irányít minket. Ennek legjobb módja, ha egy külön böngésző ablakban a hagyományos módon belépünk az adott partner felületére és elvégezzük a szükséges feladatokat, ha valóban léteznek ilyenek. Ha bármi gyanúsat tapasztalunk, hívjuk fel az érintett partnert és kérjünk megerősítést az email-ben küldött akciók valódiságát illetően.

Általános hozzáállás, hogy az Általános Szerződési Feltételeket és az Adatkezelési Szabályzatot nem olvassák el az emberek. Tegyük ezt meg mindig, hogy pontos ismereteink legyenek arról, hogy az adott partnertől milyen viselkedésre, milyen megkeresésekre számíthatunk, és ha vele kapcsolatban ettől eltérőt tapasztalunk, akkor gyanakodjunk arra, hogy nem valós megkereséssel van dolgunk.

6.4. Hogyan lehet védekezni a spear-phising ellen?

Az emberi tényezőn kívül az alábbi technológiai megoldások segíthetnek az adathalász támadások kiszűrésében, meghiúsításában. Fontos, hogy nincs százszázalékos védelem. A technológia segít, de mint minden eszköz, csak annyira lehet jó, amennyire jól használják. Az előző fejezetben részletezett gondolkodásmóddal és körültekintő, tudatos hozzáállással az olyan esetekben is megvédhetjük magunkat, amikor az alábbi technológiákon átcsúszik egy-egy támadás.

6.4.1. Email szűrés

Az adathalász támadás első lépése az email útján történő kapcsolatfelvétel a célponttal. Az email védelmi megoldások képesek több szempont alapján is ellenőrizni a bejövő leveleket:

- Küldő domain tagja-e bizonyos reputációs fekete listáknak (RBL)?
- A levél tartalmaz-e futtatható kódot?
- A levél csatolmánya tartalmaz-e kártékony kódot?
- A levélben található URL-ek tagjai-e valamilyen biztonsági kockázatokat tartalmazó listának vagy ismert adathalász oldalakat tartalmazó listának?
- A levél tartalma alapján ismert spam üzenetnek számít-e?

6.4.2. Webvédelem

Manapság az adathalász kapcsolatfelvétele akár tisztán web-alapú is lehet, amennyiben egy közösségi portálon egy hirdetéssel vagy az előző fejezetekben részletezett kereső-manipulációval kívánja az esetleges áldozatokat az oldalára csábítani. Ekkor a webvédelem nagy szerepet játszik, hogy a felhasználó ne kerüljön a phisher hálójába.

Ezen felül még olyan esetekben is, amikor az email útján eljut a címzetthez az adathalász megkeresés, még mindig kiszűrhető az URL, amelynek megnyitása a következő lépés az adathalászatban. Megfelelő webvédelem esetén ez a szakasz kiszűrhető és blokkolható. Többféle megoldás is létezik, a sima URL szűréstől kezdve az aktív csomag és kommunikáció vizsgálatig.

Javasolt minél fejlettebb webvédelmi megoldást alkalmazni, mely akkor is aktív védelmet tud biztosítani, amikor a kliens nem tartózkodik a vállalati védett környezetben.

A technológia mellett az alábbi viselkedési normák is védelmet biztosítanak. Nevezzük ezeket körültekintő webes jelenlétnek.

- Az egyes rendszerek biztonsági és adatvédelmi beállításait mindig tegyük meg és rendszeresen ellenőrizzük, hogy milyen rendszereknek milyen szintű hozzáférése van az adatlapjainkhoz, profiljainkhoz.
- A böngésző előzményeit tartsuk karban, töröljük rendszeres időközönként.
- Ne használjuk az automatikus kitöltési funkciót, vagy ha mégis, akkor mindig ellenőrizzük, hogy az adott form-on milyen adatokat adna át a böngésző a weboldalnak (autofill settings).
- A böngészőben tárolt cookie-kat tartsuk karban, a tárolt cookie-kat rendszeres időközönként töröljük.

• Minden webes felülethez használjunk egyedi jelszót, mely csak az adott szolgáltatáshoz tartozik. Ezáltal, ha egy bejelentkezési azonosítónk korrumpálódik, a többi hozzáférésünk még biztonságban lehet.

6.4.3. Vírusvédelem

A naprakész antivirus megoldások képesek megvédeni a klienseket azoktól a malware-ektől, melyek további segítséget biztosíthatnak a támadónak, vagy akár a tényleges adathalászatot is megvalósíthatják.

A kliens gépeken üzemelő antivirus megoldások mellett javasolt a vállalati környezetekben az email és web csatornákon is antivirus védelmet kialakítani. Amellett, hogy így tehermentesíthetjük a kliens oldalt, akár két vagy három féle megoldás vírusdefiníciós adatbázisa is a rendelkezésünkre áll, mely fokozza a védelem hatékonyságát.

Amennyiben a felhasználó mobil eszközein is kezelheti a levelezését, úgy javasolt a mobil eszközökre is telepíteni vírusvédelmi megoldásokat.

6.4.4. Több faktoros hitelesítés

Annak érdekében, hogy a kritikus rendszereinkhez ne lehessen egy eltulajdonított jelszóval belépni, javasolt a több faktoros azonosítás használata. Javasolt, hogy a második faktor egy fizikailag elkülönített eszközzel történhessen, tehát vagy egy offline tokennel, de legalább egy mobiltelefon alapú alkalmazás, vagy SMS-ben történő kódküldés legyen a második faktor. A netbank felületek, közösségi médiák, webes email szolgáltatások legtöbbje és a nívós webes szolgáltatások is biztosítják a lehetőséget a több faktoros hitelesítésre, sőt ezen felületek esetében még akár a böngésző validációja is beállítható.

6.4.5. Verziókövetés

Ahogy nincs tökéletes védelem, úgy nincs tökéletes program sem. Az egyes szoftvergyártók a feltárt sérülékenységek javítását, újabb biztonsági megoldásokat az új program verziókban biztosítják. Minden rendszert javasolt frissen tartani annak érdekében, hogy egy ismert sérülékenysége vagy biztonsági rés jelentette veszély a lehető leghamarabb elhárítható legyen.

Magánszemélyek esetében javasolt a számítógépen található programoknál az automatikus frissítési beállításokat használni, valamint havonta ellenőrizni, hogy az általunk használt programokhoz adtak-e ki új verziót vagy biztonsági frissítést, és ha igen, akkor telepítsük azt.

Vállalati környezetben olyan programok használata javasolt, melyek képesek feltérképezni a kliens gépeken található programokat és azokat naprakészen tudják tartani. A szoftver leltár abból a szempontból is hasznos, hogy a vállalat biztonsági felelőseinek rálátása legyen az ismert sérülékenységek jelentette kockázatokra és fel tudjanak készülni azok limitálására.

6.4.6. Emberi tényező csökkentése, képzések

Az adathalászok legerősebb fegyvere az emberi hiszékenységből és bizalomból adódó figyelmetlenség kihasználása. Ezt a veszélyt biztonságtudatos gondolkodással lehet leginkább csökkenteni. Az átlagos felhasználók számára erre lehetőséget biztosítanak az egyes webes szolgáltatások adatvédelmi és biztonsági útmutatói.

Vállalati környezetben erősen javasolt a dolgozók számára rendszeresen olyan előadásokat tartani, amelyek a biztonságtudatosságra nevelnek. Példákon keresztül felhívni a felhasználó figyelmét azokra az elhárítási, illetve megoldási módszerekre, melyek használatával töredékére csökkenthető a felhasználói hibából adódó biztonsági kockázatok száma. Ahogy tűzmegelőzési és balesetvédelmi oktatáson kötelező részt venni, úgy az informatikai biztonsági oktatásokat is be kell vezetni.

Amennyiben a vállalaton belül nincs megfelelő kompetencia a biztonsági oktatások megtartására, úgy fel kell venni a kapcsolatot az erre szakosodott felnőttképzési intézetekkel illetve IT biztonsági cégekkel, hogy helyszínen biztosítsanak oktatást vagy képezzenek ki erre embereket cégen belül.

6.5. Mi a teendő, ha adathalász támadásra gyanakszunk?

Az adathalászattal kapcsolatos gyanút mindig jelentsük egy olyan szervnek, ami képes érdemben eljárni ilyen esetekben. Vállalati dolgozó esetén a vállalat informatikai biztonságáért felelős személyeket kell értesíteni, átadva részükre minden információt, ami a gyanúnkat megalapozza (URL címek, lementett emailek stb.)

Magánszemélyként vagy a vállalat informatikai biztonságáért felelős személyként az adathalász kísérleteket jelentsük az erre a célra kialakított felületeken:

Magyar adathalász-bejelentő oldalak:

- https://e-nmhh.nmhh.hu/e-nhh/4/urlapok/esf00120/
- http://phishing.eset.com/report/hun

Külföldi adathalász-bejelentő oldalak:

- Google: https://www.google.com/safebrowsing/report_phish/
- US-CERT: phishing-report [at] us-cert [dot] gov”>https://www.us-cert.gov/report-phishing , phishing-report@us-cert.gov
- Symantec: https://submit.symantec.com/antifraud/phish.cgi
- ESET: http://phishing.eset.com/report
- GoDaddy: https://supportcenter.godaddy.com/AbuseReport/Index
- PhishTank: http://www.phishtank.com/index.php – bejelentő és kereső oldal

6.6. Irodalomjegyzék

Weboldalak

Anglia Ruskin University Library - Harvard System. Elérhetőség: http://libweb.anglia.ac.uk/referencing/harvard.htm (utolsó letöltés: 2017. január 06.)

APWG. Elérhetőség: https://www.antiphishing.org/resources/apwg-reports/ (utolsó letöltés: 2018. március 15.)

GovCERT-Hungary. Elérhetőség: http://www.cert-hungary.hu/phishing (utolsó letöltés: 2018. március 15.)

Pishing. Elérhetőség: http://www.phishing.org/history-of-phishing (utolsó letöltés: 2018. március 15.)

Word Spy. Elérhetőség: https://wordspy.com/index.php (utolsó letöltés: 2018. március 15.)

Szakirodalom

Markus Jakobsson, Steven Myers (2007): Phishing and Countermeasures. John Wiley & Sons, Inc., Hoboken, New Jersey.

7. CSER ORSOLYA: CÉLZOTT TÁMADÁS A PÉNZÜGYI SZEKTOR ELLEN

7.1. A pénz szerepe és biztonsága a védelmi szektor aspektusából

A biztonság (Gazdag Ferenc, 2008.) az egyik legalapvetőbb emberi szükséglet, amely sohasem önmagában, hanem mindig a veszélyhelyzetre történő reagálásként jelenik meg. Egy Magyarország, illetve szövetségesei ellen irányuló, hagyományos fegyverekkel végrehajtott támadás veszélye a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozatban foglaltak szerint elenyésző mértékű. Egy állam belső biztonságát jelenti a politikai, társadalmi, gazdasági rend megóvása, a veszélyek elhárítása, mint például a gazdasági terrorizmus eszköze, a kibertámadás.

Az állam, a gazdaság szereplői, valamint a lakosság részéről elvárás, hogy ezen alapvető létfontosságú, vagy kritikus infrastruktúrák lehető legnagyobb biztonsággal működjenek. A kritikus infrastruktúra elemek terrorcselekményekkel, természeti katasztrófákkal és balesetekkel szembeni védelme érdekében fontos, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve lehetséges mértékben rövid, kivételes és kezelhető legyen.

A biztonság alapfeltétele (Gazdag Ferenc, 2011.) a gazdaság zavartalan működése és a fejlődés feltételeinek biztosítottsága, melynek gazdasági szempontjai:

- gazdasági stabilitás biztosítottsága: hatékony gazdasági szerkezet, biztonságos külgazdasági kapcsolatok, szabad verseny;
- stabil pénzügyi feltételek megteremtése: mérsékelt infláció, rendezhető adósság és hitelállomány, ösztönző kamatrendszer.

A pénzügyi rendszerek biztonságát folyamatosan fenyegetések érik, mint például a csalók és rablók tevékenységei, a pénzhamisítás, valamint ritkábban a katasztrófa- vagy háborús helyzetek.

A pénzügyi válságok (Cser Orsolya, 2012.) témakörének és azok kezelésének szorosan kapcsolódó területe a pénzintézeteknél történő értékmegőrzés. A védelem- és hadigazdaságtan fogalmi rendszere, szemléletmódja alkalmazható egy látszólag távoli területen, mint a bankszféra, amely értékeink védelmében tevékenykedik. A pénzügyi szféra normál menetű, kiegyensúlyozott működését sokféle esemény zavarhatja meg:

- fizikai rablás;
- pilótajáték;
- pénzhamisítás;
- kibertámadás a pénzügyi rendszerek ellen.

A gazdasági terrorizmus egyik eszköze a kibertámadás, valamint az az elleni védelem. Fontos kérdés, mivel a cél mindenekelőtt a pénzügyi válságok kezelése és az azzal kapcsolatos banki feladatok.

A banki biztonság kiemelt jelentőségű, hiszen egy bankrendszert adott esetben kibertámadás érhet. Így szükségszerű, hogy a bankok tekintetében a megfelelően biztonságos környezet biztosítva legyen, ezért a biztonságot be kell építeni az információs rendszerekbe.

A rendkívüli események bekövetkezésének okai lehetnek szándékos vagy óvatlan magatartás, mint

például egy információs rendszereket érő kibertámadás, illetve váratlan események összessége, mint egy természeti csapás. Az adott magatartás vagy esemény következtében az élet és vagyonbiztonság súlyos veszélybe kerül, amely akadályozza, illetve megbénítja a bank normális működését.

A rendkívüli események megelőzése, megakadályozása, a keletkezett hátrány mértékének csökkentése érdekében a helyi rendőri és katonai szervekkel szoros együttműködést kell kialakítani.

A pénzügyi biztonság a védelmi szektorban a hatályos költségvetési törvény funkcionális felosztása szerint a védelem, mint állami működési funkcióhoz (szakfeladat) tartozó HM szervezetek költségvetésének stabilitását jelenti.

Az államháztartás funkcionális kiadásai
(pénzforgalmi szemléletben)

millió forintban

Fő-csoport száma	Cso-port száma	Kormányzati fő funkciók Főcsoport neve Csoport neve	2017. évi előirányzat	2018. évi előirányzat
		ÁLLAMI MŰKÖDÉSI FUNKCIÓK	**3 259 086,1**	**3 720 261,0**
F01		***Általános közösségi szolgáltatások***	***2 174 454,1***	***2 468 049,5***
	F01.a	Törvényhozó és végrehajtó szervek	1 021 376,3	1 249 678,6
	F01.b	Pénzügyi és költségvetési tevékenységek és szolgáltatások	490 811,2	574 464,0
	F01.c	Külügyek	117 489,5	140 785,6
	F01.d	Alapkutatás	127 040,6	123 856,3
	F01.e	Műszaki fejlesztés	7 686,0	10 949,2
	F01.f	Egyéb általános közösségi szolgáltatások	410 050,5	368 315,8
F02		***Védelem***	***312 917,6***	***350 698,0***
F03		***Rendvédelem és közbiztonság***	***771 714,4***	***901 513,5***
	F03.a	Igazságszolgáltatás	145 624,8	167 283,1
	F03.b	Rend- és közbiztonság	451 464,1	537 855,3
	F03.c	Tűzvédelem	81 898,8	83 262,0
	F03.d	Büntetésvégrehajtási igazgatás és működtetés	92 726,7	113 113,1
		JÓLÉTI FUNKCIÓK	**11 816 824,0**	**12 910 262,9**
F04		***Oktatási tevékenységek és szolgáltatások***	***2 182 753,8***	***2 341 578,7***
	F04.a	Iskolai előkészítés és alapfokú oktatás	411 093,0	430 936,3
	F04.b	Középfokú oktatás	219 367,0	223 363,5
	F04.c	Felsőfokú oktatás	589 903,8	596 609,0
	F04.d	Egyéb oktatás	962 390,0	1 090 669,9
F05		***Egészségügy***	***2 661 666,6***	***2 998 273,1***
	F05.a	Kórházi tevékenységek és szolgáltatások	1 874 689,1	2 066 421,9
	F05.b	Háziorvosi és gyermekorvosi szolgálat	135 858,3	151 259,2
	F05.c	Rendelői, orvosi, fogorvosi ellátás	81 579,3	81 377,6
	F05.d	Közegészségügyi tevékenységek és szolgáltatások	43 638,6	40 665,9
	F05.e	Egyéb egészségügy	525 901,3	658 548,5
F06		***Társadalombiztosítási és jólési szolgáltatások***	***5 366 757,9***	***5 953 553,5***
	F06.a	Táppénz, anyasági vagy ideiglenes rokkantsági juttatások	469 165,7	495 787,1
	F06.b	Nyugellátások	3 101 558,1	3 343 295,3
	F06.c	Egyéb társadalombiztosítási ellátások	56 949,1	56 649,0
	F06.d	Munkanélküli ellátások	57 509,5	58 246,6
	F06.e	Családi pótlékok és gyermekeknek járó juttatások	527 018,5	555 210,6
	F06.f	Egyéb szociális támogatások	409 425,0	372 733,2
	F06.g	Szociális és jóléti intézményi szolgáltatások	745 132,0	1 071 631,7
F07		***Lakásügyek, településfejlesztési és közösségi tevékenységek és szolgáltatások***	***626 745,9***	***631 172,1***
F08		***Szórakozási, kulturális, vallási tevékenységek és szolgáltatások***	***978 899,8***	***985 685,5***
	F08.a	Sport és szabadidős tevékenységek és szolgáltatások	242 108,2	237 048,6
	F08.b	Kulturális tevékenységek és szolgáltatások	526 046,9	521 888,6
	F08.c	Műsorszórási és kiadói tevékenységek és szolgáltatások	78 405,9	79 680,7
	F08.d	Hitéleti tevékenységek	52 844,8	51 918,2
	F08.e	Párttevékenységek	2 548,9	8 548,9
	F08.f	Egyéb közösségi és kulturális tevékenységek	76 945,1	86 600,5
		GAZDASÁGI FUNKCIÓK	**4 797 022,9**	**4 758 144,5**
F09		***Tüzelő- és üzemanyag, valamint energiaellátási feladatok***	***115 001,8***	***120 361,7***
F10		***Mező-, erdő-, hal- és vadgazdálkodás***	***374 650,5***	***412 434,3***
F11		***Bányászat és ipar***	***16 926,9***	***14 782,1***
F12		***Közlekedési és távközlési tevékenységek és szolgáltatások***	***1 763 453,5***	***1 774 534,0***
	F12.a	Közúti közlekedési tevékenységek	817 487,2	806 987,5
	F12.b	Vasúti közlekedésügyek és szolgáltatások	386 320,9	450 749,0
	F12.c	Távközlés	40 324,5	60 689,5
	F12.d	Egyéb közlekedés és szállítás	519 320,9	456 108,0
F13		***Egyéb gazdasági tevékenységek és szolgáltatások***	***1 808 971,3***	***1 907 129,2***
	F13.a	Többcélú fejlesztési témák tevékenységei és szolgáltatásai	1 012 697,9	1 171 509,6
	F13.b	Egyéb gazdasági tevékenységek és szolgáltatások	796 273,4	735 619,6
F14		***Környezetvédelem***	***718 008,9***	***528 903,2***
		ÁLLAMADÓSSÁG-KEZELÉS	**1 009 068,7**	**1 044 276,7**
F15		***Államadósság-kezelés, államháztartás***	***1 009 068,7***	***1 044 276,7***
		FUNKCIÓBA NEM SOROLHATÓ TÉTELEK	**481 411,7**	**402 957,3**
F16		***A főcsoportokba nem sorolható tételek***	***481 411,7***	***402 957,3***
		Kiadások összesen:	**21 363 413,4**	**22 835 902,4**
		Bevételek összesen:	**20 177 056,3**	**21 678 352,2**
		Egyenleg:	**-1 186 357,1**	**-1 157 550,2**

1. ábra: Az államháztartás funkcionális kiadásai

Ennek megfelelően Magyarország Kormánya a honvédelmi kiadások és a hosszú távú tervezés feltételeinek megteremtését szolgáló költségvetési források biztosításáról szóló 1273/2016. (VI. 7.) Korm. határozatban kötelezte el magát arra, hogy a Magyar Honvédség jogszabályi és nemzetközi kötelezettségeinek teljesítése érdekében a 2017-2026 költségvetési évekre a GDP részarány évi legalább 0,1 százalékpontos növelésével a támogatási főösszeg 2024-re érje el a GDP legalább 2%-át, és 2025-től legalább az elért szint kerüljön megtartásra.

7.1.1. A védelmi kiadások

Hazánk GPD-arányos védelmi kiadásai (2010-ben 1,2%; 2011-ben 1,06%; 2012-ben 0,81%, 2013-ben 0,72%, 2014-ben 0,65%, 2015-ben 0,6%, végül 2016-ban 0,69% és 2017-ben 0,75%) nagymértékben elmaradtak a környező NATO országok e célra fordított kiadásaitól. Emellett látható a csökkenő tendencia, melyet a korábbi 1046/2012. (II. 29.) Korm. határozatban foglaltak szerint a 2016. költségvetési évtől kezdődően a GDP részarány évi legalább 0,1 százalékpontos növelésével a támogatási főösszeg a 2022. évre eléri a GDP 1,39%-át. Mindez jóval elmarad. A költségvetés az európai NATO tagállamok átlagát közelítve a 1273/2016.(VI. 7.) Korm. határozat 2024. évre tűzte ki célul a 2,0%-os GDP arány elérését. A költségvetési keretszámok tervezése ennek megfelelően áll a védelmi szektor rendelkezésére.

A Honvédelmi Minisztérium mindenkori kiadási előirányzatának fő célja, hogy hazánk önkéntes alapon szervezett, professzionális személyi állománnyal feltöltött honvédséggel képes legyen Magyarország függetlenségét – szövetségi együttműködéssel – megvédeni.

Emellett a NATO és Európai Uniós tagságából eredően a nemzetközi szerepvállalással és a szövetségesi kötelezettségek teljesítésével, az ENSZ és az EBESZ által végrehajtott műveletekben (békefenntartó műveletek) való részvétellel teljes mértékben képessé váljon a nemzetközi biztonság erősítéséhez hozzájárulni; valamint teljesíteni a védelmi felkészülésből adódó feladatokat.

A NATO walesi csúcstalálkozón ismét nagy hangsúlyt kapott az európai NATO-tagállamok védelmi költségvetésének növelése, ami nem csupán a szövetségesi szolidaritás kifejezése és a tehermegosztás megjelenítése, hanem a NATO működőképességének fenntartása szempontjából is kulcsfontosságú. Itt került újból elfogadásra a védelmi kiadások a 2 százalékpontos GDP aránya, melytől hazánk elmarad.

7.1.2. Egy nemzet biztonságának alapvető feltételei

A biztonság (Gazdag Ferenc, 2001.) olyan „közjó” amelyet az állam nemzeti/szövetségi szinten biztosít a polgárainak Megvalósítása szabályozás (szövetségi szinten a szuverenitás meghatározott elemeinek feladásával) útján történik, a végrehajtásban pedig állami (hierarchikus szervezésű), piaci és civil szervezetek egyaránt részt vesznek. A külső biztonság a nemzetközi rendszer tagjai közötti államközi és egyéb kapcsolatok összességét jelenti, vagyis a szövetségi politika, a katonai szövetségek és a nemzetközi szervezetek működésének garanciáját, melyek tekintetében elengedhetetlen, hogy a különböző országok, térségek egységes, korábban egyeztetett gazdaságpolitikát folytassanak. Mára a világgazdaságban számos, a biztonságot fenyegető tényező megjelent, melyek kezelése a kormányok számára elsőrendű.

Ezek a problémák:

- a belső, növekvő társadalmi feszültségek;
- a spekuláció, a pénzügyi szféra elszakadása a reálfolyamatoktól;
- a tőke globalizációja, és ezzel együtt kontrolálhatatlan mozgása;
- a transznacionalista vállalatok hegemóniája;
- az információs forradalom kihívásai.

A történelemben előforduló példák alapján egyértelművé vált a biztonság komplex jellege, globalitása. A biztonság szorosan összefügg a veszély, kihívás vagy fenyegetés fogalmával. A Hadtudományi Lexikon (Szabó József – Gabriel Győző – Horváth Ferenc, 1995.) megfogalmazása szerint: „az egyéneknek, csoportoknak, országoknak, régióknak (szövetségi rendszereknek) a maguk reális képességein, és más hatalmak, nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete (és annak tudati tükröződése), amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak az ellene való eredményes védekezés feltételei...”

Ezek alapján a biztonság (Dr. Hadnagy Imre, 2008.) összetett fogalom és állapot, tartalma a társadalom valamennyi tagjának az életét valamilyen formában érinti, az egyén és a társadalom biztonsága egymástól szétválaszthatatlan, szorosan összefüggnek. A biztonságpolitika új, komplex meghatározása szerint a biztonság elemei a következők:

- Környezeti (ökológiai) elem
- Társadalmi (jogi, szociális) elem
- Politikai (diplomáciai) elem
- Gazdasági elem
- Informatikai elem
- Katonai elem

7.1.3. Nemzeti Biztonsági Stratégia

A biztonság fogalma egyre átfogóbb értelmezést nyer. A folyamatosan változó biztonsági környezetben a kihívások, kockázati tényezők és fenyegetések ma már több síkon – az egyének, közösségek, államok és régiók szintjén, valamint globális szinten – jelennek meg, és az egyének, kormányzati és nem kormányzati szervezetek, valamint transznacionális szereplők széles körét érintik. Mára elengedhetetlenné vált a biztonság politikai, katonai, gazdasági és pénzügyi, társadalmi, ezen belül emberi és kisebbségi jogi, valamint környezeti dimenziójának együttes kezelése.

A Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat az értékek és érdekek számbavétele, valamint a biztonsági környezet elemzése alapján meghatározza azokat a nemzeti célokat, feladatokat és átfogó kormányzati eszközöket, amelyekkel az EU és NATO tag Magyarország a 21. század elejének nemzetközi politikai, biztonsági rendszerben érvényesíteni tudja nemzeti biztonsági érdekeit.

Az új Nemzeti Biztonsági Stratégia (a továbbiakban: NBS) kidolgozását és elfogadását időszerűvé tette az, hogy a legutóbbi, 2004-es hasonló dokumentum elfogadása óta jelentős változások történtek globális téren és hazánk közvetlen biztonsági környezetében, valamint az euro-atlanti integrációs szervezetekben is: életbe lépett az Európai Unió Lisszaboni Szerződése (2009), a NATO pedig új Stratégiai Koncepciót fogadott el (2010). Mindez időszerűvé tette a magyar dokumentum felülvizsgálatát, követve az EU- és NATO-tagállamok gyakorlatát is. Ebben szerepelnek azon biztonsági elemek is, melyek egy pénzügyi krízis esetében – mint például kibertámadás az ország bankrendszere ellen – fontos szempontok annak érdekében, hogy a veszélyhelyzetet megszűntessék.

Az NBS célja, hogy iránymutatást nyújtson a kormányzati szektor számára biztonságpolitikai – azon belül pénzügyi – kérdésekben. Filozófiájában ezért átfogó és összkormányzati megközelítést követ. A 2012. évi Nemzeti Biztonsági Stratégia 30. pontja a pénzügyi biztonságról szól, iránymutatást nyújt a kormányzati szektor számára egy pénzügyi krízis (például a kibertámadás) problémáinak kezeléséről és megszűntetéséről.

A Nemzeti Katonai Stratégia ennek alapján került megfogalmazásra és kiadatásra – kihirdetve a Magyarország Nemzeti Katonai Stratégiájáról szóló 1656/2012. (XII. 20.) Korm. határozattal. Ennek célja, hogy Magyarország Alaptörvényével, a védelmi szféra tevékenységét meghatározó jogszabályokkal, a NATO koncepciójával, továbbá az NBS-ben lefektetett elvek alapján kijelölje azokat a stratégiai szintű célkitűzéseket, irányokat, eszközöket és forrásokat, amelyek révén a Magyar Hon-

védség (a továbbiakban: MH) teljesítheti küldetését.

A megújulás egyik fontos eszköze a Stratégia megalkotása, amely közép- és hosszútávú iránymutatást nyújt az MH számára, valamint meghatározza az ország védelmének és érdekeinek érvényesítését – kijelöli a haderő fenntartásának és alkalmazásának fő elveit, fejlesztési irányait.

Mindezek által meghatározza azokat a célokat és eszközöket – a hozzájuk rendelt költségvetési forrásokkal –, amelyek révén korszerű, rugalmasan és hatékonyan alkalmazható képességekkel, kiegyensúlyozott struktúrával rendelkező haderővé válik.

Azzal, hogy a rendelkezésre álló költségvetési források korlátozottak, elősegíti a hatékonyságra és feladatközpontúságra (feladatfinanszírozás) törekvő új szemléletmód kialakítását. Mindez lehetőséget nyújt az MH képességcsökkenésének megállítása után egy megújult, az erőforrásaival hatékonyan gazdálkodó, szilárd alapokon és jól szervezett haderő létrejöttéhez, mely egy fenntartható fejlődési pályán mozogva, a számára biztosított költségvetési erőforrások növekedésével fokozatosan válik korszerűvé. Emellett a biztonság nem katonai vetületeinek egyre inkább megnő a fontossága, ami ugyanakkor nem jár együtt ezen tényezők szerepkörének csökkenésével.

Hazánk és szövetségeseink ellen irányuló, hagyományos fegyverekkel végrehajtott támadás veszélye nagyon elenyésző mértékű, és középtávon is ezt valószínűsítik. Egy nem hagyományos eszközökkel végrehajtott, céljait tekintve korlátozott támadás valószínűsége is igen alacsony, ugyanakkor teljes mértékben nem zárható ki.

Az Észak-atlanti Szerződéshez való csatlakozásunk következményeként az ország egyéni védelmi képességének fenntartása és fejlesztése mellett fontos a Washingtoni Szerződés szerinti kollektív védelmi képesség fenntartása, fejlesztése is. Hazánk a nemzeti és szövetségi védelmi képességének fenntartásában saját erejére – a nemzetgazdaság erőforrásaira, a Honvédség felkészültségére, valamint az állam-polgároknak a haza védelme iránti hazafias elkötelezettségére és áldozatkészségére –, továbbá a szövetséges államok és fegyveres erőik együttműködésére és segítségnyújtására épít.

Az Észak-atlanti Szerződés 5. cikke, a kollektív védelem Magyarország biztonságának sarokköve. A kollektív védelemhez és biztonsághoz való aktív hozzájárulás Magyarország legfontosabb biztonságpolitikai kötelezettsége.

A lisszaboni NATO csúcson elfogadott stratégiai koncepcióval újabb jelentős lépést tettek afelé, hogy képesek legyenek sikeresen reagálni a 21. század kihívásaira. Az ott megfogalmazott Stratégiai Koncepció kijelöli az irányokat, amelyekkel a Szövetség – a megváltozott biztonsági környezethez igazodva – képes betölteni Washingtoni Szerződésben rögzített szerepét és biztosítani tagországainak védelmét.

Az EU Közös Biztonság- és Védelempolitikája területén új struktúrák, mechanizmusok jöttek létre, amelyek tovább növelhetik az EU biztonságpolitikai szerepét.

Korunk konfliktusainak megelőzése és kezelése globális szemléletet, valamint átfogó megközelítést igényel. A tartós, fenntartható biztonság és stabilitás megköveteli a válságkezelési – beleértve a fejlesztéspolitikai – eszközök átfogó, egymással összhangban lévő használatát, az integrált civil-katonai megközelítést és képességfejlesztést, valamint a nemzetközi szereplők együttműködésének erősítését.

Az ország biztonsága azonban mindenekelőtt közügy, ezért a stratégia egyik feladata, hogy a szakmai körökön túl a mindennapi életben is hasznosítható támpontot nyújtson a hazai biztonságpolitikai gondolkodásban.

Mindezek fontosságát felismerve a NATO Miniszteri Irányelveknek megfelelően azon szakembereket, akiknek a válságkezelésre jó szaktudásuk és képességük van, együtt kell tartani, időnként gyakorlatoztatni, és ezalatt szimulációs döntéseket meghozatalára bíztatni őket. Annak a tudásbázisnak, amely ezen tevékenységeken keresztül az évek során kialakul, adott válság vagy krízishelyzet esetében azonnal alkalmazhatónak kell lennie.

A Nemzeti Biztonsági Stratégiában megfogalmazásra kerülnek mindazon tényezők, melyek a pénzügyi biztonságot meghatározzák az egyes nemzetállamok gazdaságának működése tekintetében:

- pénzügyi tartalék – a krízishelyzetek esetére;
- pénzügyi moratórium – pénzintézetekből történő pénzkivétel korlátozása

- azonnali betét kivétel pánik – például Postabank-botrány (1997. február);
- pénzellátás – bankválság esetén a készpénzellátás korlátozása.

A globális pénzügyi-gazdasági válság példátlan kihívás elé állítja az egész euro-atlanti közösséget. Az elhúzódó és mély válság gyengíti a fejlett országok, köztük hazánk biztonsági intézményrendszerét, a nemzetközi szervezetek és együttműködési keretek kohézióját, és csökkenti a biztonság erősítésére fordítható forrásokat. Mindez megköveteli, hogy a rendelkezésre álló erőforrásokat innovatívan és hatékonyabban összpontosítsuk biztonsági képességeink erősítésére.

Ezen a téren is tovább erősödik a szövetségesi együttműködés, valamint a több nemzeti együttműködésben rejlő lehetőségek tudatosabb kihasználásának jelentősége.

A terrorizmus korunk jelentős globális fenyegetése marad, amely térben és időben eltérő és folyamatosan változó módon jelenik meg, és veszélyezteti szövetségesi rendszerünket és értékrendünket.

Magyarország terrorveszélyeztetettsége alacsony, ugyanakkor külföldi eredetű vagy a külföldi magyar érdekeltségek elleni fenyegetettséggel számolni kell. Emellett külföldi terrorcselekményeknek is lehetnek hazánkat érintő biztonsági és gazdasági következményei.

7.1.4. Kritikus, vagy létfontosságú infrastruktúrák

A modern társadalmak nagymértékben függenek a technikai és virtuális infrastruktúra rendszerektől (energiaellátás, ivóvíz ellátás, informatikai hálózatok stb.), amelyek komplex rendszerét az egymástól való függőségek jellemzik.

Az infrastruktúrák biztonságának növelése ezért elsőrendű kérdéssé vált a fejlett országok biztonságpolitikájában. E rendszerek működési zavarai, illetve egyes elemeinek ideiglenes kiesése, vagy megsemmisülése jelentős kihatással vannak mindennapi életünkre, a gazdaság és a kormányzat hatékony működésére.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI törvény és annak mellékletei kijelölik ezen rendszereket, létesítményeket és elemeket, amelyeket a könnyebben kezelhetőség érdekében a fejezet további részében kritikus infrastruktúraként (KI) említek.

A kritikus vagy létfontosságú infrastruktúrák az általános definíció szerint „létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt következményekkel járna.”

Ezen infrastruktúrák részben az állam, részben a magánszféra tulajdonában vannak, illetve azokat az állam vagy a magánszféra működteti. A létfontosságú infrastruktúrákat kár érheti, működésükben zavar keletkezhet vagy azok meg is semmisülhetnek terrorcselekmény, természeti katasztrófa, hanyagság, baleset, számítógépes hackertevékenység, bűncselekmény vagy rosszhiszemű magatartás következtében.

Az infrastruktúrák biztonságnövelésének fő területei, az egyének, közösségek védelmének és a kritikus infrastruktúrák biztonságának magasabb szintre emelése. Mindhárom területen a veszélyek és fenyegetettségek fizikai, informatikai eredetűek vagy a rendszerek komplexitásból adódnak.

A megoldást az új fenyegetettségek és kockázatok fizikai, informatikai és pszichológiai szintű okainak felderítése, összefüggéseik megértése és kezelése jelenti.

Összességében a Kritikus Infrastruktúrák:

- azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei;
- amelyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése;
- közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat;
- az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI törvény 2. számú mellékletében a nemzeti létfontosságú rendszerelemek kijelölése alapján a pénzügy is egy kritikus infrastruktúra ágazatnak tekintendő.

	A	B
	Ágazat	Alágazat
17	pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
18		bank- és hitelintézeti biztonság
19		készpénzellátás

1. számú táblázat: Nemzeti létfontosságú rendszerelemek (részlet)

A létfontosságú infrastruktúrák több gazdasági ágazatra kiterjednek, többek között a bankügyletekre és pénzügyekre, a szállításra és forgalmazásra, az energiaiparra, a közművekre, az egészségügyre, az élelmiszerellátásra és tájékoztatásra, valamint a kulcsfontosságú állami szolgáltatásokra.

Ezen ágazatok néhány létfontosságú eleme nem tartozik a szigorúan vett „infrastruktúra" fogalmába, de valójában olyan hálózatok vagy ellátási láncok, amelyek valamely alapvető termék vagy szolgáltatás biztosítását támogatják.

A létfontosságú infrastruktúrákat fenyegető katasztrofális terrortámadások lehetősége egyre nő. A létfontosságú infrastruktúrák ipari ellenőrző rendszerei elleni támadás következményei rendkívül eltérőek lehetnek.

Az infrastruktúrák károsodását alapvetően kétféle ok-okozati tényező idézheti elő:

- a spontán fizikai vagy technikai jelleg, amelynek okai az elöregedés/amortizációs, a karbantartás hiánya;
- a kikényszerített jelleg, amelynek lényege a szándékos támadás.

Az infrastruktúrák katasztrofális meghibásodásának egyik típusa, amikor az infrastruktúra egy részének meghibásodása a többi meghibásodásához vezet, ami dominóhatást válthat ki. Ilyen meghibásodás az infrastrukturális ágazatok egymásra gyakorolt szinergikus hatása következtében alakulhat ki.

Ennek egy egyszerű példája lehet a villamosenergia-szolgáltató közüzemek elleni támadás, ahol megszakad a villamosenergia-szolgáltatás, és ezáltal más elektromos készülékek – így a banki rendszerek is – leállhatnak. Az egymást követő események láncolata szintén nagy károkat tud okozni, és a közüzemeken keresztül is a bank-, pénzügyi rendszerek leállását idézheti elő.

A kritikus infrastruktúra elemek terrorcselekményekkel, természeti katasztrófákkal és balesetekkel szembeni védelme érdekében fontos, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve lehetséges mértékben rövid, kivételes és kezelhető legyen. Az infrastruktúrák biztonságának növelése ezért elsőrendű kérdéssé vált a fejlett országok biztonságpolitikájában.

Kritikus infrastruktúráink sérülékenyek és támadhatók. A szakemberek nem látnak olyan határozott lépéseket, amelyek ezen hálózatok – mint például a banki és pénzügyi számítógépes hálózatok – megfelelő, komplex védelmét erősítenék. Mindez azt jelenti, hogy a kritikus infrastruktúrák rendkívül sebezhetőek.

A fejlett hadi- és informatikai kultúrával rendelkező országok a 21. század elejének egyik legkomolyabb kihívásaként kezelik a kritikus információs infrastruktúrák védelmét. A megoldást az új fenyegetettségek és kockázatok fizikai, informatikai és pszichológiai szintű okainak felderítése, összefüggéseik megértése és kezelése jelenti.

7.1.5. A válságok és kezelésük

A mai világban – az országok, nemzetek globalizációja közepette – a biztonság az egyik legalapvetőbb emberi szükséglet, amely sosem önmagában, hanem mindig a vészhelyzetre történő reagálásként jelenik meg. Fontos politikai, társadalmi, gazdasági válságok jellemezték az elmúlt évtizedet. A hidegháború elmúltával a globális katonai szembenállás véget ért, de ettől a világ egyáltalán nem lett biztonságosabb. Összeomlott egy ideológiai rendszer Kelet-Közép Európában, és ezzel együtt az erre épült politikai, gazdasági, társadalmi rend és katonai szövetség. Új biztonsági kihívások jelentek meg, illetve a már meglévő kihívások és kockázatok felerősödtek. Térségünkben a biztonság katonai elemével szemben felerősödtek a politikai, gazdasági és társadalmi feszültségek.

A válság: nincs definiálva (jogszabályilag biztosan nincs), hogy mi a válság. A gazdaságtörténet utólag állapítja meg, hogy milyen típusú és mekkora volt az az esemény, mit az adott időszakban válságnak neveztünk. A válság nem más, mint a társadalom egészében vagy különböző területein kialakuló nagymértékű egyensúlyhiány, amely a társadalom életében zavarokat okoz. Ezek gyógyítására minden országnak meg kell találnia az orvosságot.

A válságot megelőző időszakot az előjelek stádiumának is lehet nevezni, amikor a figyelmeztető jelek megsokasodnak. Gyakran meg lehet határozni azt a fordulópontot, amely után a válság már elkerülhetetlen. Ha ezen ellenlépések nem hatékonyak, a egy olyan krónikus stádium jön el, amikor a válság tovább szélesedik, súlyos veszteségek következnek be, és a megoldásra egyre kevesebb az esély.

Kommunikációs szempontból a válság a nem várt, a normális életbe nem illő változások nagyhatású megnyilvánulása. Olyan helyzetet hoz létre, ami nem engedi meg, hogy a normális üzletmenet újra a korábbi útra térjen vissza. Minden válság sajátos, egyedi, ezért különálló kommunikációs stratégiát igényel. Vannak közös elemek, amit a szakértőknek fel kell ismerni. A válságjelenség 4 összetevője:

- a kiváltó ok: a lőfegyver ravaszához hasonlítható az ok-okozatok láncolatában. Nem várt esemény, amely megváltoztatja az emberek felfogását a válságba került szervezetről. Elindíthat különféle hatásokat, visszahatásokat, érdeklődési és vizsgálódási folyamatot a szervezeten belül és külső partnerekben.
- a fenyegetettség megjelenése: az esemény elindulásával a szakembereknek meg kell határozni a fenyegetettség jellegét, súlyosságát. Emberi élet, vagyontárgyak, maga a természet kerülhet bizonytalan helyzetbe. Gyors, határozott, előre néző, kompromisszumos megoldásokat igényel.
- nem kontrollálható helyzetek kialakulása: zavaró események, amelyek kikerülnek a menedzsment hatásköréből. Kontrollálhatóság gyengül, visszaszorul.
- azonnali figyelem érvényesítésének szükségszerűsége: a válságba került szervezetnek azonnal reagálnia kell, figyelmét koncentráltan kell irányítania.

Egy állam belső biztonsága a politikai, társadalmi és a gazdasági rend megóvását, a veszélyek elhárítását jelenti. A válság koncentrálja az események hatását, felerősíti az országban élő emberek, vagy egy nemzet tagjainak reagálását. A figyelem a válságba került szervezetre koncentrálódik, amelynek változása elkerülhetetlen. A második fejezetben tárgyalt esetben egy ország lakosságának többségét érintheti a szimulált nemzeti (országos) válság, ha terrorizmus által tervezett események megvalósulnak.

Ennek megelőzésére kerülnek megtervezésre a NATO azon gyakorlatai az elmúlt években, amikor szimulációval előidéznek valósnak tűnő helyzeteket, melyek válsághelyzeteket okozhatnak. Amennyiben az ellenlépések nem hatékonyak, a krónikus stádium következik, ahol a válság tovább szélesedik, súlyos veszteségek következnek be, és a megoldásra kevés esély van. Pontosan ennek megelőzésére kerülnek évente megtervezésre a NATO CMX gyakorlatai, amikor szimulációval előidéznek valósnak tűnő helyzeteket, melyek válsághelyzeteket okozhatnak.

Fontos szempont a banki biztonság, melyet adott esetben kibertámadás érhet, ezáltal szükségszerű, hogy a bankok tekintetében a megfelelően biztonságos környezet biztosítva legyen. Ennek érdekében csökkenteni a biztonságot be kell építeni az információs rendszerekbe.

7.1.6. Kibervédelem

A modern hadviselés egyik legfontosabb színtere a kibertér (Haig Zsolt – Várhegyi István, 2008.). Ennek támadása a pénzügyi/ banki rendszerek esetében fontossá tette azt, hogy az informatikai rendszerek a lehető leginkább biztonságos módon kerüljenek kialakításra, a hardver, szoftver és orgver eszközök összehangolt alkalmazásával.

A kibervédelem ennek alapján arra irányul, hogy fenntartsa a saját hálózatos információs rendszereinkben a hozzáférhetőséget az információkhoz, információalapú folyamatokhoz, és biztosítsa ezen rendszerek hatékony használatát békeidőben, válság vagy konfliktus idején egyaránt.

A kiberhadviselés az információs dimenzióban megvalósuló hálózati hadviselést jelenti. Leegyszerűsítve a kritikus információs infrastruktúrák bizalmasságának, sértetlenségének és rendelkezésre állásának befolyásolására irányuló tevékenység informatikai, fizikai és emberi eszközökkel.

A kibertámadás (Tomolya János – Padányi József[2012.]) észlelésének igénye szoros együttműködést és összehangolt cselekvést kíván az információs rendszerek tervezői, gyártói, forgalmazói, adminisztrátorai, felhasználói, valamint a szolgáltatásokat biztosító, jogalkotó és hírszerző szervezetek között.

Az információs rendszereket támadók műveleti sebessége meghaladhatja a humánmegoldásokat tartalmazó észlelési és válaszadási képességeket.

A hatékony kibervédelem érdekében elsődleges fontosságú automatizált módszerekkel felbecsülni az esemény súlyosságát (a rendszer sérülése, kompromittálódás, rosszindulatú program bejutása a rendszerbe) és csökkenteni azok negatív hatásait. A helyreállítás megkezdéséhez és a szükséges válaszlépések megtételéhez a támadások időbeni felderítése alapvető feltétel.

Az információs hadviselés (Haig – Kovács – Munk –Ványa, 2013.) során alkalmazható fenyegetések négy kategóriára bonthatók: „kompromittálás, megtévesztés, szolgáltatás akadályozása/megszakítása, fizikai megsemmisítés. Mind a négy kategória kockázatot jelent azokra az önálló, vagy hálózatba szervezett fegyverekre és támogató rendszerekre (banki rendszerek), amelyek nagymértékben támaszkodnak információs rendszerekre.

A fenyegetés származhat szervezett erőktől (államok) vagy strukturálatlan ellenfelektől (hacker).” A kompromittálásnak többféle formája lehet, így például a technológia illetéktelen megszerzése vagy szoftverhiba, a rendszerbe történő illetéktelen behatolás, rosszindulatú szoftver használata, felderítő szervezet adatgyűjtése vagy egy pszichológiai művelet.

Ahhoz, hogy az automatizált információs rendszereket megvédjük, első lépésben meg kell érteni az ellenük irányuló fenyegetéseket, mint például az adatok és információk kompromittálása, a szolgáltatások részleges vagy teljes akadályozása, rongálása. Ennek legjobb eszköze a képzés és a szoros együttműködés az operátorok és a felhasználók között.

Az előzetes vizsgálatként össze kell gyűjteni a minimális információkat, jelezni kell a várható fegyelmi lépéseket, javaslatot tenni a további vizsgálatra. A kompromittálás utáni veszteségek felbecsülését egy központilag irányított rendszernek kell végeznie, mely egy központi adatbázisból és célirányosan kialakított programokból és projektekből áll.

Az információs rendszerek biztonsági monitorozása a saját hivatalos távközlés lehallgatása, olvasása, másolása vagy rögzítése, amelynek célja anyagot biztosítani az analízishez, amely lehetővé teszi az automatizált banki információs rendszerek biztonsági fokának pontos megállapítását.

Azonban a lehallgatásnak a civil életben igen erős korlátai vannak, annak lehetőségei az alábbiak:

- törvényes bírói engedéllyel (például rendvédelmi szerv nyomozati cselekménye);
- törvénytelenül (például bankbiztonsági szakember lehallgatása csak illegális lehet), amely bűncselekménynek számít.

Ebben az információs környezetben az információs műveletek a fizikai-, az információs- és a tudati dimenzióban érvényesülő, koordinált tevékenységet jelentik, amelyek a szembenálló fél információira, információalapú folyamataira és infokommunikációs rendszereire gyakorolt hatásokkal képesek befolyásolni az ellenfelet. Az információs műveletek célja az információs fölény, uralom és végül a vezetési fölény kivívása.

Az információs műveletek elsődleges fenyegetései: kompromittálás, adatsérülés vagy információs művelet megszakadása, amelyek virtuális térben, vagy a fizikai sérülések (például stuxnet), amelyek fizikai térben történnek. A biztonsági problémák esetében a megelőzés, a gyors reagálás és a károk csökkentése tekinthető kiemelt feladatnak. E feladatok mindegyikénél egyre nagyobb súllyal jelentkezik a számítástechnikai megoldások elterjedt használata. A különböző szempontok szerinti megfogalmazások sokszínűsége bizonyítja az információs műveletek védelme érdekében a széles körű együttműködés szükségességét, a kockázathoz kötött védelmi feladatokat és a minden részletre kiterjedő képzést.

A 2012. évi Nemzeti Biztonsági Stratégia 30. pontja a pénzügyi biztonságról szól, iránymutatást nyújt a kormányzati szektor számára egy pénzügyi krízis (például a kibertámadás) problémáinak kezeléséről és megszűntetéséről.

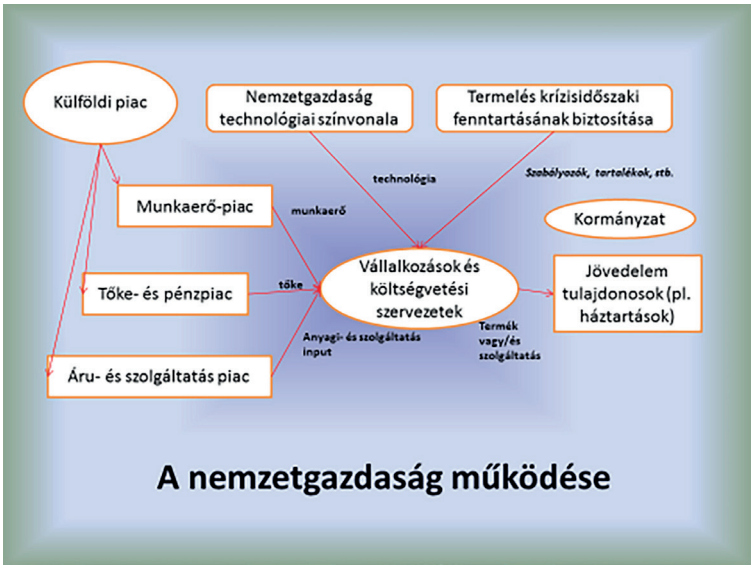
Általánosan elfogadott, hogy egy sikeres kibertámadás legrosszabb esetben is csupán kevés fizikai sérüléssel járna, de a létfontosságú infrastrukturális szolgáltatások szempontjából veszteséget eredményezhet. Például a banki hálózat elleni sikeres kibertámadás miatt az ügyfelek nélkülöznék a banki szolgáltatásokat mindaddig, míg a szakemberek elvégzik a hálózat helyreállítását és javítását.

A kibertér támadása – informatikai vagy más módon – a bankok esetében (Kovács László – Illés Zsolt, 2011.) fontossá tette azt, hogy az informatikai rendszerek a lehető leginkább biztonságos módon kerüljenek kifejlesztésre a szervezeten kívül és belül.

A pénzügyi rendszerek kiemelt szerepet töltenek be, hiszen ezek megfelelő működése nélkül a pénzügyi folyamatok egy része vagy egésze működésképtelenné, de legalábbis jelentősen akadályozottá válik.

7.1.7. Pénzügyi rendszer biztonsága

A makrogazdasági körforgásnak folyamatosan kell működnie ahhoz, hogy a pénzellátás és a számlapénzes tranzakciók, ezáltal a reálfolyamatok (termelés) folytonossága biztosítva legyen. Fő fenyegetés a terrorizmus és kiberbiztonság, napjaink kiemelt biztonsági feladatai.



1. számú ábra: A nemzetgazdaság működése

A pénzügyi szolgáltatási tevékenység csak a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv megléte esetén kezdhető meg, illetve folytatható.

Ennek érdekében vonatkozóan érdemes kidolgozni egy olyan gyakorlati szabályozást – a többféle területen használt Legjobb Gyakorlatok (Best Practises) módszerével -, amely által a pénzügyi szervek (bankszektor) összehangoltan és azonnali reagálással képesek fellépni az őket ért támadások ellen.

Ez a módszer a 2000-es évek elejétől elfogadott a banki szférában. Alapvetéseket és a kialakított legjobban használható módszereket (gyakorlatokat) tartalmazza, amelyeket a szimulált és/vagy élesben bekövetkező problémák, válsághelyzetek megoldására alkalmaztak. Ezeket összegyűjtik, és a véletlenszerű bekövetkezés esetén használják fel. Mindenki banki szerv a saját képére alakíthatja, annak alapján, hogy mik a szervezet sajátosságai.

Emellett a rendkívüli események megelőzése, megakadályozása, a keletkezett hátrány mértékének csökkentése érdekében a helyi rendőri és katonai szervekkel szoros együttműködést kell kialakítani.

7.1.8. Bankbiztonsági tevékenység

Egy bankrendszer biztonságának (Cser Orsolya, 2013.) tekintetében a legfontosabb kritériumok:

- A pénzügyi szolgáltatási tevékenység csak a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv megléte esetén kezdhető meg.
- A pénzügyi intézménynek ki kell alakítania a pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről.
- A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.
- A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, valamint olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére.
- A pénzügyi intézménynek tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább a következőkkel:
    - a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb – a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal;
    - az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. Ezen mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről;

- a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.

A rendkívüli helyzetek kezelésének módjára az alábbiak fogalmazhatóak meg:

1. A pénzintézetnek a mérete, az általa végzett pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenysége jellege, nagyságrendje, összetettsége arányában megbízható irányítási rendszerrel kell rendelkeznie, és ennek keretén belül köteles a felmerülő kockázatok azonosítására, mérésére, kezelésére, nyomon követésére és jelentésére szolgáló hatékony eljárásokat alkalmazni.

2. Emellett írásban rögzített eljárásrendekkel, szabályzatokkal kell rendelkeznie a működési kockázatok mérésére, kezelésére, valamint vészhelyzeti és üzletmenet-folytonossági tervvel a folyamatos működés fenntartása, továbbá a súlyos üzletviteli fennakadásokból következő esetleges veszteségek mérséklése érdekében.

A pénzügyi rendszer biztonságát folyamatosan fenyegetések érik, mint például a katasztrófa és háborús helyzetek, valamint a csalók és rablók tevékenységei. Ezen problémák ellen kell felkészíteni a felsőszintű igazgatást, és azután együttesen fellépni a fenyegetettség megszűntetése és a biztonságos körülmények visszaállítása céljából.

Célszerű a bankrendszerek területén olyan szabályozások általi megoldások létrehozása, amelyek felhasználásával a banki szolgáltatások biztonsági szintje jelentősen növelhető, valamint a felmerülő pénzügyi, gazdasági, nemzetbiztonsági kockázatok nagymértékben csökkenthetők.

A válság (Kiss Petra, 2012.) koncentrálja az események hatását, felerősíti az országban élő emberek, vagy egy nemzet tagjainak reagálását. A figyelem a válságba került szervezetre koncentrálódik, amelynek változása elkerülhetetlen. Jelen esetben egy ország lakosságának többségét érintheti a cikkben szimulált nemzeti (országos) válság, ha terrorizmus által tervezett események megvalósulnak. A válságot megelőző időszakot az előjelek stádiumának is lehet nevezni, amikor a figyelmeztető jelek megsokasodnak. Gyakran meg lehet határozni azt a fordulópontot, amely után a válság már elkerülhetetlen.

A válságkezelés alapvető területei a következők:

- preventív: előrejelzés és kikerülő elhárítás, megelőzés;
- aktív: az észrevehető jelek szerint biztosan bekövetkező válságok növekedésének és terjedésének megakadályozása, visszaszorítása;
- reaktív: a kialakult válságot megszüntető stratégia és intézkedések, azaz válságkezelő politika.

A problémakezelés részekre osztható fel, melyek a következők:

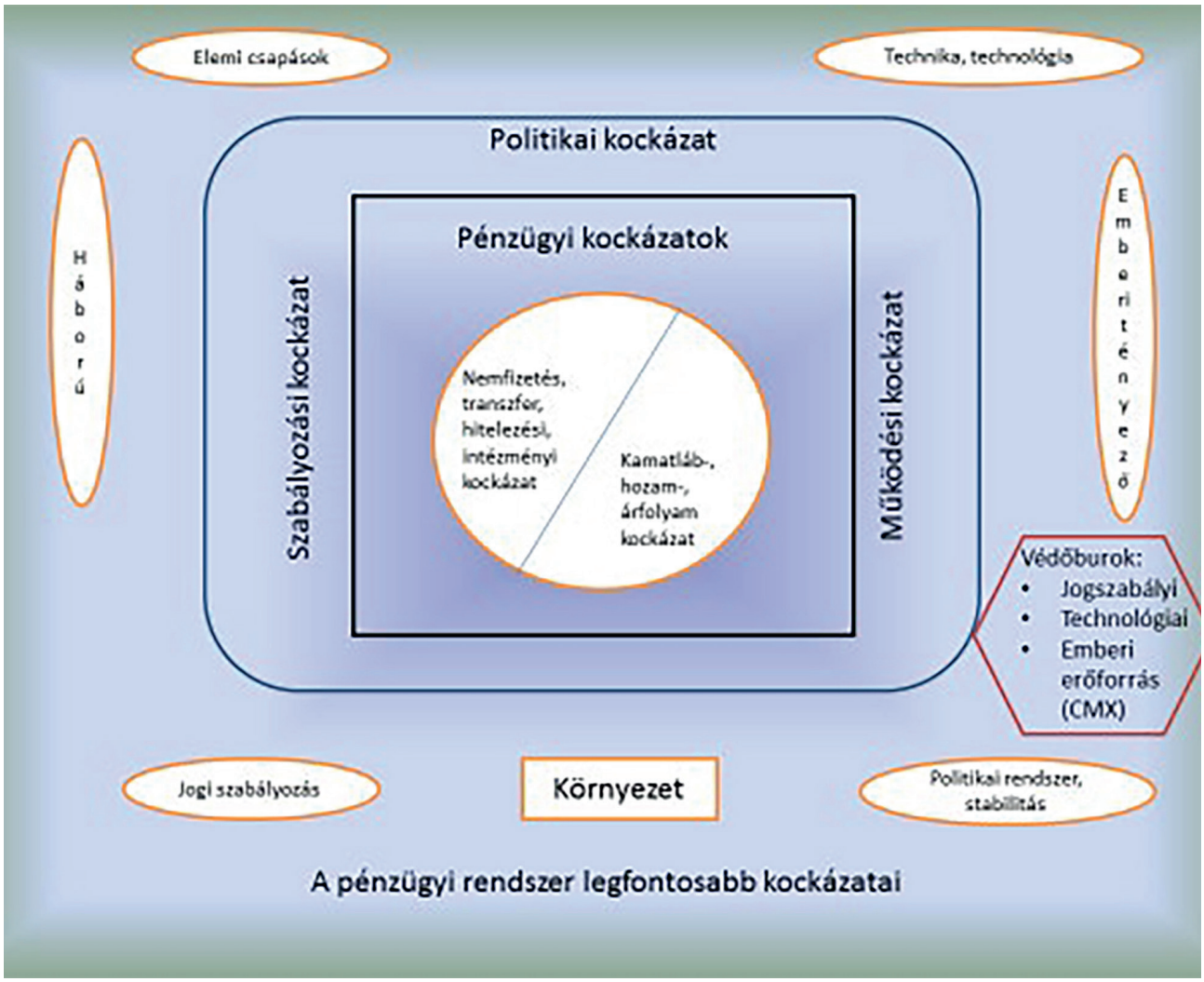
- diagnózis: kudarc- és sikertényezők felismerése;
- helyzetértékelés;
- terápia: operatív intézkedések a problematikus eltérés megszüntetésére.

A rendkívüli események bekövetkezésének okai lehetnek szándékos vagy óvatlan magatartás (belső), illetve váratlan események összessége (külső), mint például egy természeti csapás. Az adott magatartás, esemény következtében az élet és vagyonbiztonság súlyos veszélybe kerül, amely akadályozza, vagy megbénítja a bank normális működését.

A kibertámadás jelentkezhet a fizikai, hardver úton, mint például az eszköz eltulajdonítása, meghibásodásának elősegítése – bankautomatáknál kirobbantása, elvitele, kifosztása – vagy szoftver úton egy elektronikus kibertámadással. A bankautomaták fizikai támadása ellen megvannak a védelmi eszközök, úgymint a szétrobbanó festékkazetta, őrzött helyiség bankkártyás bejutással, fegyveres őr vagy a bankkártya leolvasó rendszerek. A szoftver úton megvalósuló támadással kapcsolatosan azonban bankok szerint nagyon változóak, hogy milyen bankbiztonsági rendszerekkel dolgoznak.

Összességében a bankbiztonsági tevékenység tehát mindazon tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való intézményes gondolkodás, amely a pénzintézet saját

tulajdonú tárgyainak, értékeinek, valamint az alkalmazottak és az ügyfelek biztonságának védelmét szolgálja.

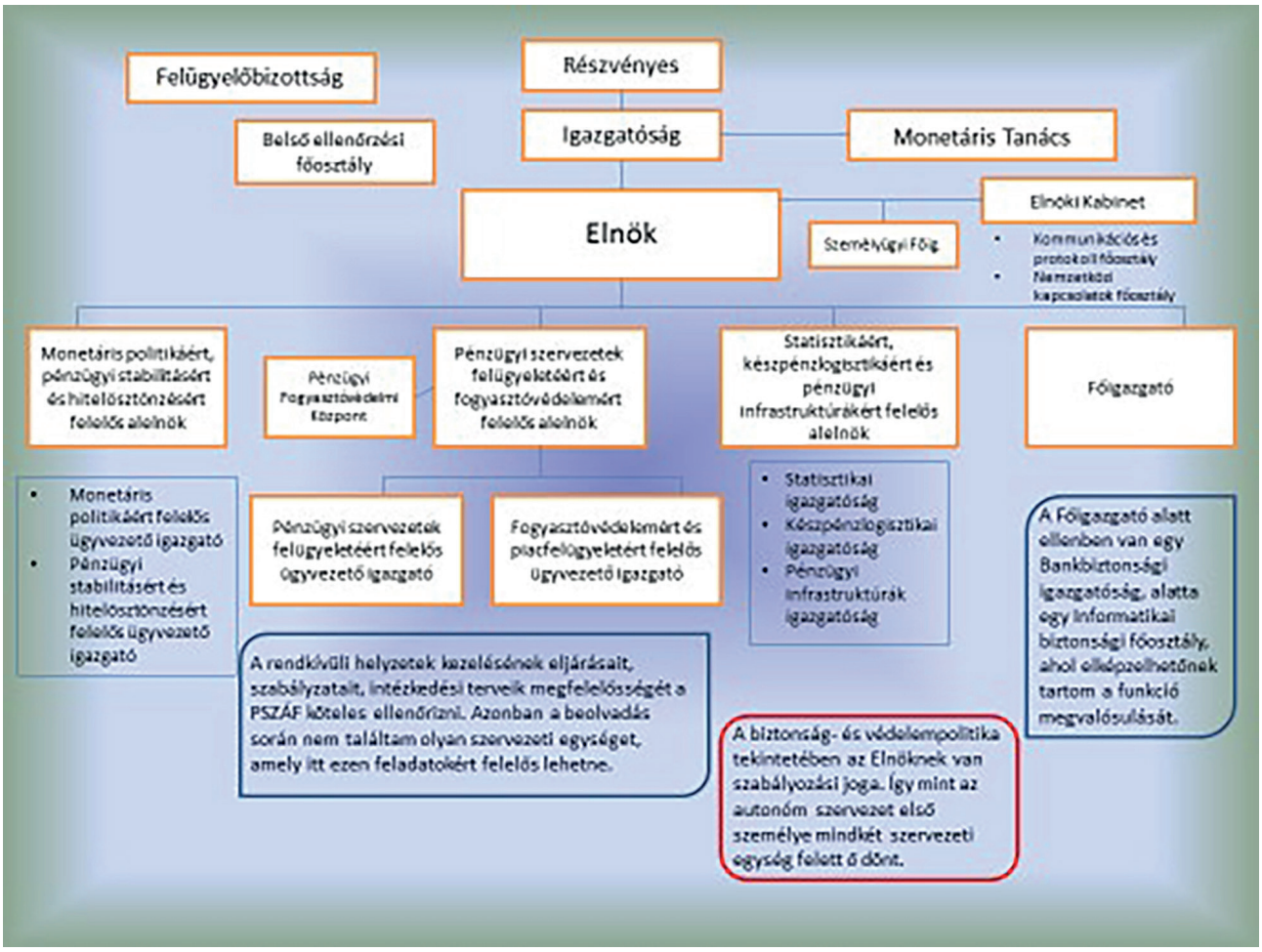


2. számú ábra: A pénzügyi rendszer legfontosabb kockázatai

A pénzügyi szektort, a bankrendszert érintő következtetések, teendők:

- A pénzügyi szolgáltatási tevékenység végzéséhez szükséges egy, a működési kockázatok csökkenését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó intézkedési terv.
- A biztonsági kockázatelemzés eredményei alapján gondoskodni kell az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, valamint a rendszeres biztonsági mentésről és a kritikus folyamatok eseményeit naplózó biztonsági környezetről.
- A rendkívüli helyzetek kezelésének eljárásait, szabályzatait, intézkedési terveik megfelelősségét a PSZÁF beolvadása okán az MNB köteles ellenőrizni, ezért célszerű a bevonása.
- Az MNB alapfeladata a fizetési és elszámolási rendszerek felvigyázása, azok biztonságos és hatékony működése, a pénzforgalom zavartalan lebonyolítása érdekében.
- Összességében az NGM csak a szabályozás elméleti oldaláról érintett, a gyakorlati tennivalók érdekében a PSZÁF, az MNB és a MÁK az illetékes szervek.

A jogalkotó 2013. szeptember 16.-ai döntésével 2013. október 1.-jei hatállyal összevonta a PSZÁF-ot az MNB-vel. Ennek alapján az MNB új szervezetében már megjelennek a pénzügyi biztonság eléréséhez javasolt feladatok.



3. számú ábra: Az MNB új szervezete (2013.)

Magyarország Nemzeti Biztonsági Stratégiájának egyik kulcseleme az ország stabilitásának, gazdasági, pénzügyi rendjének biztosítása. Az Alaptörvény a közpénzekről szóló címben szabályozza az MNB státuszát, feladatait. Az MNB hazánk központi bankja, így felelős a monetáris politikáért, valamint ellátja a pénzügyi közvetítőrendszer felügyeletét.

A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény részletesen meghatározza az MNB jogállását, szervezetét, elsődleges célját, alapvető és egyéb feladatait.

Emellett rögzíti, hogy az MNB elsődleges célja az árstabilitás elérése és fenntartása, valamint ezen elsődleges céljának veszélyeztetése nélkül az MNB támogatja a pénzügyi közvetítőrendszer stabilitásának fenntartását, ellenálló képességének növelését, a gazdasági növekedéshez való fenntartható hozzájárulásának biztosítását és a rendelkezésére álló eszközökkel a Kormány gazdaságpolitikáját.

Magyarország gazdasági és pénzügyi rendszerének stabilitása és ellenálló képessége fontos nemzeti érdek és biztonságpolitikai szempont – elengedhetetlenné vált a biztonság politikai, katonai, gazdasági, pénzügyi és társadalmi dimenziójának együttes kezelése. Egyre inkább előtérbe kerülnek azon biztonságpolitikai kihívások, melyek kezeléséhez átfogó és összehangolt politikai, gazdasági és katonai fellépésre van szükség.

Hazánk elsőszámú biztonsági érdeke az ország gazdasági stabilitásának és fejlődésének biztosítása – a felkészülés arra, hogy térségünkben a legfőbb veszélyforrás a gazdasági, pénzügyi, energiabiztonsági, ellátási és környezeti veszélyeztetettség –, összességében az aszimmetrikus hadviselés elleni védelem a meghatározó. Ennek okán alapvető biztonságpolitikai cél a gazdasági és pénzügyi stabilitás folyamatos erősítése és felügyelete, a makroprudenciális szabályozás (rendszerszintű kockázatok folyamatos monitorozása és minél hatékonyabb kezelése) erősítése, a nemzetgazdaság külső kockázati kitettségének csökkentése, a társadalom jólétének megalapozott, biztonságos és hosszú távú erő-

sítése. A Kormány felkérte a Magyar Nemzeti Bank elnökét, hogy szakterületét érintően működjön együtt az MNB-re vonatkozó honvédelmi intézkedési terv kidolgozásával és bevezetésével összefüggő feladatok végrehajtásában, mindazonáltal az üzletmenet folyamatosságának biztosításában.

Hazánk alapvető biztonsági érdekei közé tartozik az ország gazdasági stabilitásának és fejlődésének biztosítása is. Fel kell készülni arra, hogy térségünkben már nem is annyira a hagyományos fegyverekkel végrehajtott katonai támadás a legfőbb veszélyforrás, hanem a gazdasági, pénzügyi, energiabiztonsági, ellátási és környezeti veszélyeztetettség (összességében az aszimmetrikus hadviselés elemei a meghatározóak). Az instabil régiók, az államok közötti és államokon belüli konfliktusok, a gyenge vagy működésképtelen államok – amelyek így kevéssé képesek korlátok közé szorítani agresszív érdekérvényesítő csoportokat – potenciális veszélyt jelentenek Magyarország számára.

A pénzügyi stabilitás kérdése a 2008-2009-es világgazdasági válság hatására jelentősen felértékelődött. Hazánk sebezhetőségét nagymértékben csökkenti, ha sikeres az adósságcsökkentés, a külföldi kitettség mérséklése, a devizaadósság csökkentése, a gazdasági növekedés feltételeinek megteremtése.

Magyarország biztonságának szilárd gazdasági alapokon kell nyugodnia, amely egyfelől megteremti a hatékony biztonságpolitika erőforrásait, másfelől pedig az ország stabilitásának fokozása révén növeli az ország érdekérvényesítő képességét.

A biztonság nem-katonai vetületeinek egyre inkább megnő a fontossága. Az Alaptörvénnyel összhangban Magyarország Nemzeti Katonai Stratégiája is rögzíti, hogy a honvédelem nemzeti ügy, amelynek két alappillérét a nemzeti önerő és a szövetségesi együttműködés alkotják.

Tekintettel arra, hogy a biztonság összetett és elemei szorosan összefüggnek egymással, a honvédelem ügyét nem lehet a biztonság más területeitől elválasztva, önmagában értelmezni. A biztonsági kihívások kezelése túlnyúlik az egyes intézmények hatáskörén, összehangolt együttműködést kíván meg az állami szereplőktől.

Elsősorban gazdasági és demográfiai változások történtek a világban, amelyek egyes Európán kívüli térségek felértékelődéséhez vezettek, és ezáltal Európa relatív súlyvesztése következett be. A pénzügyi, gazdasági világválság csökkentette az EU kohézióját, így fontosabbá vált a biztonsági struktúrák felülvizsgálata.

A Hvt. egyes rendelkezéseinek végrehajtásáról rendelkező 290/2011. (XII. 22.) Korm. rendelet (Hvr.) 1. § n) pontjában foglalt meghatározás szerint „a védelmi igazgatás a közigazgatás részét képező feladat- és szervezeti rendszer, amely az állam védelmi feladatainak megvalósítására létrehozott, valamint e feladatra kijelölt közigazgatási szervek által végzett végrehajtó, rendelkező tevékenység; magában foglalja a különleges jogrendre történő felkészülést, továbbá az említett időszakok és helyzetek honvédelmi, polgári védelmi, katasztrófavédelmi, védelemgazdasági, lakosság-ellátási feladatainak tervezésére, szervezésére, a feladatok végrehajtására irányuló állami tevékenységek összességét".

A honvédelmi igazgatás a védelmi igazgatás része: feladat- és szervezetrendszer, melynek keretében az ország védelmére létrehozott, az e feladatra kijelölt közigazgatási szervek, és a honvédelemben közreműködő más szervek ellátják a honvédelemre való felkészítésével, az ország védelmével, és a honvédelmi kötelezettségek teljesítésével kapcsolatos feladatokat.

A védelmi igazgatás tervrendszerének bevezetéséről szóló 1061/2014. (II. 18.) Korm. határozat 1. sz. mellékletében meghatározottak szerint a honvédelem, a katasztrófavédelem és a védelemgazdaság sajátos, egymástól funkcionálisan eltérő követelményeire tekintettel megfelelő tervdokumentáció ki-dolgozása indokolt.

A védelmi igazgatási komplex tervrendszer része a különleges jogrendre történő felkészülés, és az ezzel kapcsolatos honvédelmi, polgári védelmi, katasztrófavédelmi, védelemgazdasági, lakosság-ellátási feladatok tervezése, szervezése, a feladatok végrehajtására irányuló tevékenységek összessége.

A komplex védelmi igazgatási terv a mai kor követelményeinek megfelelő, feladatorientált, a központi, területi és helyi sajátosságokat, továbbá a biztonságra hatást gyakorló kihívásokat (kockázatokat és veszélyforrásokat) maximálisan figyelembe vevő, a gyakorlatban jól használható, egymásra

épülő, az együttműködést kiemelten kezelő tervrendszer.

Ez biztosítja a különleges jogrend időszakában, valamint a mindennapi életviszonyokat jelentős mértékben befolyásoló események bekövetkezése esetén is a honvédelemben közreműködő szervek vezetettségét, feladatainak ellátását, így az ország működőképességének fenntartását, szükség esetén a lakosság élet- és vagyonmentését, valamint a lakosság folyamatos ellátását.

Szakmai, tartalmi követelményeit a honvédelmi igazgatási tervre vonatkozóan a honvédelemről, valamint a különleges jogrendben bevezethető intézkedésekről szóló jogszabályok; a veszély-elhárítási tervvel összefüggésben a katasztrófavédelmi jogszabályok; a védelemgazdasági alaptervvel kapcsolatban pedig a nemzetgazdaság védelmi felkészítését szabályozó jogszabályok határozzák meg.

Az MNB feladatainak ellátásához kapcsolódik az MNB – közvetlen és közvetett – kizárólagos tulajdonában álló gazdasági társaságok tevékenysége, amelyre az MNB a honvédelmi típusú különleges jogrend idején is számít. Az MNB megteszi azokat a tulajdonosi joggyakorlás körébe tartozó intézkedéseket, amelyek ezen gazdasági társaságok honvédelmi típusú különleges jogrendi időszakban történő feladat-ellátását elősegítik.

Az MNB honvédelmi igazgatási tárgykörökben részt vesz a honvédelmi igazgatási feladatokban:

- a védelmi tervezés rendszerének kialakítása, működtetése, intézkedési terv elkészítése;
- a nemzetgazdasági erőforrások honvédelmi célú tartalékolása, a gazdaságfelkészítési tervezése;
- az ország területének hadműveleti előkészítéséből adódó feladatok;
- a feladat- és hatáskörébe tartozó különleges jogrendi intézkedések előkészítése:
- a NATO Válságreagálási Rendszerrel összhangban álló, feladat- és hatáskörébe tartozó nemzeti intézkedések, rendszabályok végrehajtása,
- az eseményfigyelő- és jelzőrendszer működtetése;
- a honvédelmi felkészülés irányítási, szervezeti, működési rendszer kialakítása, feltételek biztosítása;
- a szervezetet érintő honvédelmi feladatok gyakorlása, a gyakorlatokon való részvétel tervezése;
- a tárgyévet megelőző év honvédelmi feladatainak végrehajtásáról és az e célra jóváhagyott költségvetési források felhasználásáról szóló beszámolás (november 30.), valamint a honvédelmi felkészítés következő évi feladattervének és a szükséges költségvetési igényeknek összeállítása;
- a jogszabályban vagy kormányhatározatban részére megállapított honvédelmi feladatok elvégzése.

Az Magyar Nemzeti Bank honvédelmi ágazati feladata a védelmi célú tartalékolásnak, mint állami fel-adatnak az egyik nagyon fontos eleme. Ennek biztosítása nagy mennyiségű forrást igényel mindazon képességek elérésénél, amelyek a nemzetgazdaság normál működésének időszakában nem, vagy csak korlátozottan érvényesülő szükségleteken alapszanak.

A finanszírozásnál külön kezelendők a tartalék-készletek fejlesztésével, átstrukturálásával járó – egyedi döntésen alapuló – felhalmozási kiadások és a tartalékolás fenntartásával (az infrastruktúra és a személyzet működtetésével, a készletek nyilvántartásával, ellenőrzésével) járó működési költségek.

Általánosságban az éves költségvetésben a tartalékok készletfejlesztésével, átstrukturálásával kapcsolatos költségeket a védelmi felkészítés központi kiadásai nemzetgazdasági minisztériumi fejezeti előirányzatból kell biztosítani. Ennek felosztásáról külön kormányzati döntést kell hozni – a védelmi felkészítés éves feladattervében meghatározottak szerint. A tartalékolás fenntartási költségeit a felelős tárca költségvetésben célszerű tervezni, illetve amennyiben az adott tartalék jellegéből következően erre lehetőség van, a szükséges forrásokat a tartalékkezelő szervezet gazdálkodási bevételeiből lehet részben vagy egészben fedezni.

Az MNB nagy előnye, hogy nem központi költségvetési szerv, így nem költségvetési forrásból gazdálkodik – ugyanakkor nagy stratégiai szerepe van a pénztartalékok képzésében és annak keze-

lésében. Jelentős saját forrásból gazdálkodóként a honvédelmi ágazati feladatait is sokkal magasabb színvonalon képes a jövőben ellátni, megoldani.

7.2. A NATO CMX gyakorlatainak jelentősége

A Nemzeti Biztonsági Stratégia célja, hogy iránymutatást nyújtson a kormányzati szektor számára biztonságpolitikai kérdésekben. Filozófiájában ezért átfogó és összkormányzati megközelítést követ.

Az ország biztonsága azonban mindenekelőtt közügy, ezért a stratégia egyik feladata, hogy a szakmai körökön túl a mindennapi életben is hasznosítható támpontot nyújtson a hazai biztonságpolitikai gondolkodásban.

Mindezek fontosságát felismerve a NATO Miniszteri Irányelveknek megfelelően azon szakembereket, akiknek a válságkezelésre jó szaktudásuk és képességük van, együtt kell tartani, időnként gyakorlatoztatni, és ezalatt szimulációs döntéseket meghozatalára bíztatni őket.

E célt szolgálják a CMX (Crisis Management Exercise) gyakorlatok, melyeket a Honvédelmi Minisztérium által vezetett szakember gárdának évente el kell végeznie, év közben pedig az adott témakörben történő folyamatos felkészülés jegyében kell telnie a közös munkának.

Annak a tudásbázisnak, amely ezen tevékenységeken keresztül az évek során kialakul, adott válság vagy krízishelyzet esetében azonnal alkalmazhatónak kell lennie.

7.2.1. NATO CMX gyakorlatok

Az átfogó civil-katonai megközelítést nemzeti kormányzati szinten is alkalmazni kell. A nemzeti biztonsági stratégia csak összkormányzati megközelítés, részvétel és felelősség, az intézményi keretek kihívásoknak való megfeleltetése és megfelelő források hozzárendelése esetén lehet hatékony és sikeres. E célt szolgálják a CMX (Crisis Management Exercise) gyakorlatok, melyeket a Honvédelmi Minisztérium által vezetett szakember gárdának évente el kell végeznie, év közben pedig az adott témakörben történő folyamatos felkészülés jegyében kell telnie a közös munkának. A rendkívüli események bekövetkezésének okai lehetnek szándékos vagy óvatlan magatartás (belső), illetve váratlan események összessége (külső), mint például egy természeti csapás. Az adott magatartás, esemény következtében az élet és vagyonbiztonság súlyos veszélybe kerül, amely akadályozza vagy megbénítja a bank normális működését. A rendkívüli események megelőzése, megakadályozása, a keletkezett hátrány mértékének csökkentése érdekében a helyi katonai és rendőri szervekkel szoros együttműködést kell kialakítani. Az első CMX gyakorlatot 1992-ben tartották meg, amelyhez hazánk 1999-ben csatlakozott, melynek témája minden egyes alkalommal különbözik. Egy azonos bennük, hogy egy előre elkészített forgatókönyv szerint szimulálják az eseményeket – felkészülve ezzel a lehetséges éles helyzetekre az eljövendő idők tekintetében.

A NATO szerepvállalásának elemei a következőkben összefoglalhatók:

- NATO-szerepvállalás területen kívüli konfliktusok kezelésében;
- Hagyományos és új típusú szerepvállalás;
- Új típusú biztonsági kihívások (együttes) megjelenése;
- Terrorizmus, kiberbiztonság, proliferáció – napjaink kiemelt biztonsági feladatai;
- Együttműködés más nem nemzetközi szervezetekkel;
- Partnerországok bevonása művelet tervezésébe és végrehajtásába.

7.2.2. Nemzeti Intézkedési Rendszer

Észtország (Dr. Haig Zsolt – Dr. Kovács László, 2010.) kritikus információs infrastruktúráit 2007. április 27-én külső, elosztott túlterheléses (Distributed Denial of Service – DDoS) támadás érte, ame-

lyet tömeges levélküldés (spammelés) és weboldalak megváltoztatása (deface) egészített ki. A főbb célpontok az észt parlament számítógépei, valamint a bankok, minisztériumok, napilapok és elektronikus hírközlő szervezetek voltak. A támadás mind Észtországot, mind pedig a NATO-t felkészületlenül érte, pedig kivitelezéséhez csekély erőforrásokra volt szükség.

Magyarországon (Dr. Kovács László – Dr. Krasznay Csaba, 2010.) ezidáig nem került napvilágra olyan incidens, mely külső támadás eredménye lett volna, de 2009-ben több olyan informatikai hiba is bekövetkezett, amely az adott kritikus információs infrastruktúra működését megakasztotta. Ez emberek tíz- és százezreinek okozott nehézséget, a sajtó kiemelten foglalkozott velük, valamint jelentős presztízsveszteséget jelentett az üzemeltető intézménynek. Hazánknak is van tehát keserű tapasztalata az IT rendszerek leállásának következményeivel kapcsolatban, de a direkt, összehangolt támadások hatása egyelőre elképzelhetetlen.

A pénzügyi rendszerek (Vígvári András, 2009.), a bankügyi tranzakciók működésében hazánkban is egyre hangsúlyosabb szerep jut az elektronikus szolgáltatásoknak. Ezen szolgáltatások biztonságos működése nemzetbiztonsági szempontból kritikus kérdés, hiszen ezek nélkül az ország gazdasági és pénzügyi működése jelentős akadályokba ütközne. A szolgáltatások biztonságát a jogalkotók jogszabályokkal próbálják garantálni, azonban bizonyos területeken jelenleg nincsenek olyan egységes műszaki ajánlások, melyek a szolgáltatások bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit meghatároznák. A nemzetközi trendek és a hazai tapasztalatok is azt mutatják, hogy az elektronikus banki szolgáltatások állandó célpontjai a szervezett bűnözésnek, a hackereknek és más államok hivatalos szerveinek. Tökéletes védelmet nyújtani aránytalanul magas költséget jelentene, azonban az elvárható gondosság elve alapján szükséges a nyilvánosan elérhető szolgáltatásokat biztonságosan kifejleszteni. Ez azt jelenti, hogy a biztonsági gondolkodásnak már az új alkalmazások tervezésénél meg kell jelennie. A banki szolgáltatásokba biztonsági megoldásokat fejleszteni több szinten lehet.

A bankok biztonsági szintje jelentősen növelhető, és így a felmerült nemzetbiztonsági kockázatok nagymértékben csökkenthetők. A válságkezelés és a különleges jogrend kapcsolata fontos tényező tehát annak elérésében, hogy a felmerülő problémák megoldása végrehajtható legyen.

A Tallini események nyomán a válság nem más, mint olyan veszélyhelyzet, amely megoldása a Kormányzati Válságkezelő Bizottság vezetésével számos kormányzati szerv és helyi önkormányzat közötti koordinált cselekvést igényel. Mindez komoly fenyegetést jelent a nemzet biztonságára (ld. NBS), és nem lehet normál eszközökkel kezelni. Ma Magyarországon a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről szóló 278/2011. (XII.20.) Korm. rendeletben korábban már megfogalmazásra került ennek igénye. A már létező válságkezelési alrendszerek és a hozzájuk kapcsolódó képességek ágazati szegmensek szerint megosztottak, az együttműködés sokszor csupán ad hoc jellegű.

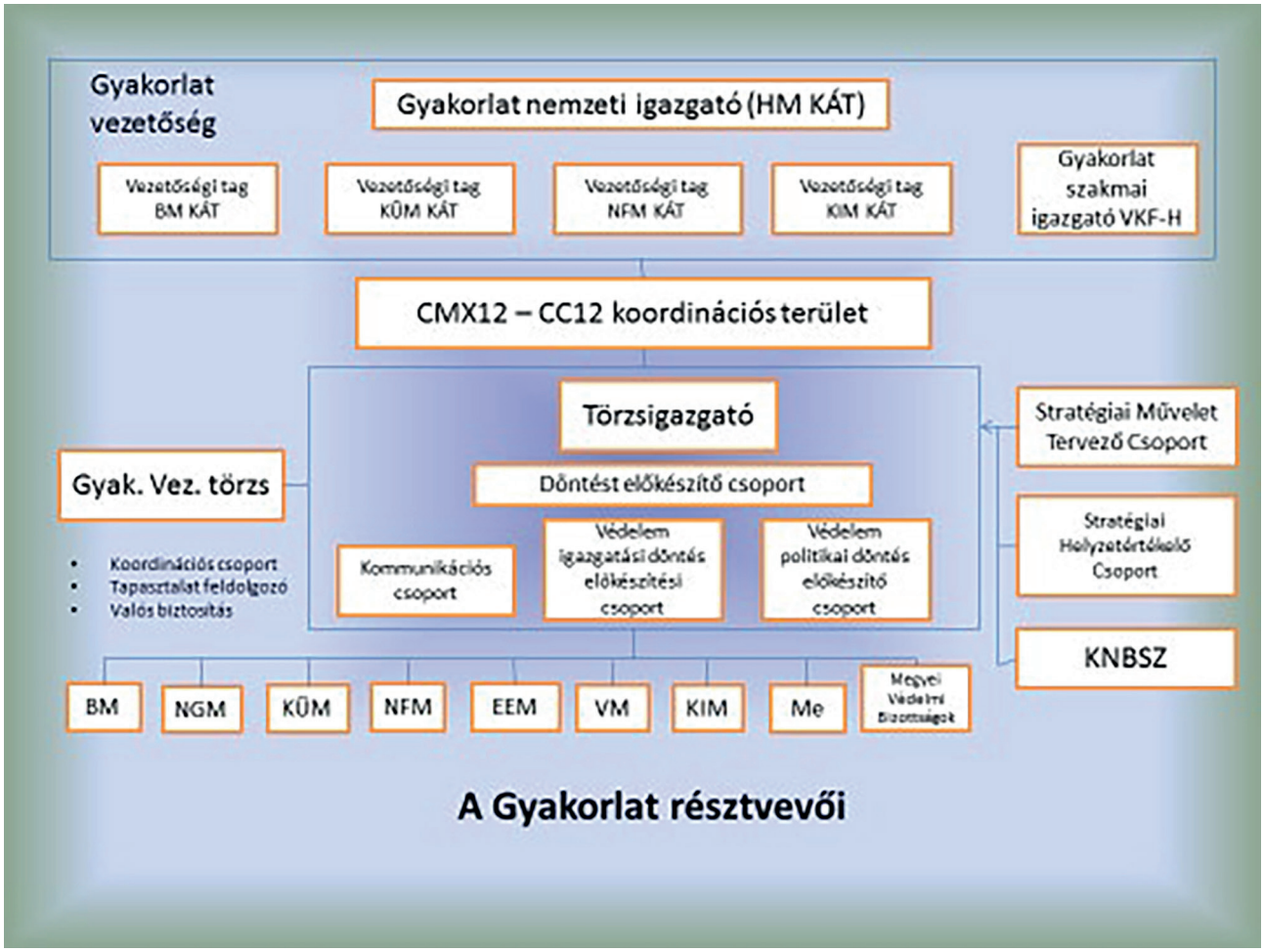
Mindazonáltal szükséges a civil-katonai-rendvédelmi képességek összehangolt alkalmazása a NATO Válságreagálási Rendszerével való összhang miatt is. Ennek eredményeként egy átfogó megközelítés szükséges, amely komplex választ (Dr. Keszely László, 2014.) ad a komplex kihívásokra, a képességeket összehangoltan alkalmazza, megszűnteti a duplikációkat, valamint kohéziót alakít ki a civil-katonai- rendvédelmi együttműködés tekintetében.

7.2.3. A CMX Gyakorlatok általános céljai, tevékenységi körei

A gyakorlat célja a szövetség válságkezelési eljárásainak gyakorlása stratégiai politikai szinten, amelyben a tagországok, a NATO-parancsnokság, a stratégiai parancsnokságok civil és katonai szakemberei vesznek részt. Ezáltal a válságkezelés hazai szakértői és döntéshozói vegyenek részt a NATO konzultációs és döntéshozatali folyamatában, gyakorolják Magyarország polgári-, katonai válságke-

zelési eljárásait. Magyarország számára ez kiváló alkalom a hazai válságkezelési rendszer politikai, katonai döntés előkészítő és döntéshozatali folyamatainak, valamint a NATO-központtal és a tagországokkal való együttműködés gyakorlására.

A CMX a NATO egyik legfontosabb gyakorlata, személyesen a NATO-főtitkár vezeti. A gyakorlat forgatókönyve teljes mértékben fiktív eseményeken alapul és fiktív földrajzi környezetben játszódik: a leírt válsághelyzet a NATO kollektív védelmi feladataira koncentrál a Washingtoni Szerződés 4. és 5. cikkelye szerinti szituációban, beleértve ebbe úgy a tárgyalásos válságrendezést, mint a katonai megoldás lehetőségét is. Ugyanakkor ez egy haderőmozgás nélküli gyakorlat, vagyis csapatok mozgatására nem kerül sor az egy hét során. A gyakorlat végrehajtó állománya a tagországok minisztériumaiból, a NATO Parancsnokság és a Stratégiai Parancsnokságok tagjaiból tevődik össze. Magyarországon a nyolc minisztérium, a négy nemzetbiztonsági szolgálat és a közmédia egyaránt részt vesznek a CMX lebonyolításában.



4. számú ábra: A NATO CMX gyakorlat résztvevői

A hármas tagozódási szint a tevékenység jellegét is megkülönbözteti:

- Legfelsőbb szint: Gyakorlatvezetőség – Kormányzati döntéshozatal
- Középső szint: Központi döntés előkészítés, koordináció, végrehajtás
- Legalsóbb szint: Területi működtetés

A munkacsoportok feladata előkészíteni a kormány döntését arra vonatkozóan, hogy milyen jellegű szakmai és döntéshozói tevékenységre van szükség – a rendelkezésre álló feltételeket, eszközöket figyelembe véve – az elképzelt válsághelyzet leküzdésére. A szerzett tapasztalatok hatékonyabbá, gyorsabbá teszik a stratégiai döntések meghozatalát, ami egy válsághelyzet kezelése és felszámolása során kulcsfontosságú szereppel bír.

A gyakorlat résztvevői a tagországok mellett a szövetség politikai és katonai döntéshozó és döntés-előkészítő, irányító szervezetei: az Észak-atlanti Tanács, a NATO bizottságok és a stratégiai parancsnokságok. A végrehajtás során a résztvevők a NATO válságkezelési eljárásait gyakorolják, amelynek fő célja a jelen kor kihívásai elleni egységes fellépéshez szükséges döntések konszenzus útján történő meghozatala.

A CMX olyan kormányzati szintű törzsvezetési gyakorlat, melyen részt vesznek az érintett minisztériumok képviselői, meghatározott, kijelölt intézményei. A Gyakorlatot a HM Védelmi Igazgatási Főosztálya vezeti. A Gyakorlatban résztvevő további szervek:

- Magyarország Állandó NATO Képviselete;
- Katonai Nemzetbiztonsági Szolgálat;
- Információs Hivatal;
- Alkotmányvédelmi Hivatal;
- Megyei Fővárosi Védelmi Bizottságok Csoportjai;
- BM Országos Katasztrófavédelmi Főigazgatóság;
- Terrorelhárítási Központ;
- Országos Rendőr-főkapitányság;
- Nemzeti Biztonsági Felügyelet;
- Médiaszolgálatatás-támogató és Vagyonkezelő Alap;
- Nemzeti Média és Hírközlési Hatóság;
- PTA Nemzeti Hálózatbiztonsági Központ;
- HungaroControl Zrt.

A hazánkban végrehajtott Gyakorlat végrehajtói az alábbi csoportokat jelentik:

- A Gyakorlatvezetőség feladata a nemzeti döntések meghozatala, a gyakorlat levezetésének irányítása.
- A Koordinációs testület csoportjának tagjai a gyakorlat végrehajtásakor folyamatosan kapcsolatban állnak egymással és szükség szerint személyesen egyeztetnek. A stratégiai fontosságú döntések meghozatalának támogatása érdekében a csoport tagjai minden esetben jelen vannak a CMX gyakorlat vezetőségi ülésein, szükség szerint segítik a Gyakorlatvezetőséget a stratégia szintű döntések meghozatalában.
- A Központi döntés-előkészítő csoport feladata a Gyakorlatvezetőség által meghozandó döntések előkészítése, döntési változatok kidolgozása, nemzeti álláspont előkészítése. A vezető NATO szervek által hozott döntések elemzése, a nemzeti intézkedések jóváhagyásra történő előkészítése.
- A Gyakorlattervezők folyamatosan figyelemmel kísérik a gyakorlat lefolyását a meghatározott célkitűzések megvalósulása érdekében.
- A Végrehajtó csoportok a felkészülési időszakban kiadott anyagokban a kialakult politikai-katonai helyzet tanulmányozzák, elemezik és értékelik. A napi események figyelembevételével javaslatokat dolgoznak ki a lehetséges nemzeti álláspontokra vonatkozóan, majd azokat döntésre előterjesztik a Gyakorlatvezetőség részére.

Hazánk aktív szerepet vállal a gyakorlat tervezésében és megvalósításában. A feladatok végrehajtása, a döntéshozatali folyamatok modellezése a kormányzat aktív bevonásával történik. A következőkben ismertetem azt a NATO CMX gyakorlatot, ahol a banki rendszereket külső támadás érte.

7.2.4. A NATO 2012. évi válságkezelési gyakorlata

A 2012. évi Gyakorlat volt a tizennyolcadik alkalom. A tervezésben (Trautmann Balázs, 2012.) és a végrehajtásban a tagállamok közül Izland kivételével mind a huszonhét tagország részt vett, a NA-

TO-partnerség keretében meghívást kapott Finnország és Svédország, továbbá a Nemzetközi Atomenergiai Ügynökség (IAEA), a Nemzetközi Vöröskereszt (ICRC), illetve most először az Európai Külügyi Szolgálat (EEAS) képviselője. Magyarország a NATO-hoz történő csatlakozása, 1999 óta vesz részt a gyakorlaton. A Gyakorlat tárgya a NATO 2012. évi válságkezelési gyakorlatához (CMX 12), és egyben a Cyber Coalition 2012 elnevezésű kibervédelmi gyakorlatához kapcsolódó nemzeti feladatok végrehajtása volt, melyhez a felhatalmazást a védelmi felkészítés egyes kérdéseiről szóló 1182/2012. (VI. 1.) Korm. határozat adta.

Magyarországon készült olyan tanulmány (Digitális Mohács!), amely számításba veszi, hogy milyen láncreakciót válthat ki egy kritikus információs rendszereket érintő átfogó, informatikai támadásokat is magába foglaló cselekménysorozat, mint például a bankrendszerünk ellen történő kibertámadás – ahogyan azt 2012 novemberében a CMX 2012 gyakorlatban szimulálták.

A gyakorlat forgatókönyve teljes mértékben kitalált eseményeken alapul, elképzelt földrajzi környezetben játszódik: válsághelyzetben fokozódó vegyi, biológiai, nukleáris fenyegetés, a tömegpusztító fegyverek elterjedése, esetenként a NATO stratégiai intézményei ellen végrehajtott nagyfokú kibertámadás történik. A kibertámadás jelentkezhet a fizikai, hardver úton, mint például az eszköz eltulajdonítása, meghibásodásának elősegítése – bankautomatáknál kirobbantása, elvitele, kifosztása – vagy szoftver úton egy elektronikus kibertámadással.

Egy, az információs infrastruktúrákat célzó támadás akár napokig tartó működési zavarokat okozhat az országban. A NATO 2012. évi CMX válságkezelő és egyben kibervédelmi (támadás érte a bankrendszert) gyakorlatának fő célja a jelen kor kihívásai elleni egységes fellépéshez szükséges döntések konszenzusos meghozatala volt:

- NATO-szerződés 5. cikkelyének érvényesítése – a tagországok közösen léptek fel a támadás elhárításáért és a rendszerek helyreállításáért;
- A hazai válságkezelési rendszer döntés-előkészítő és döntéshozatali folyamatainak, valamint a NATO-központtal és a tagországokkal való együttműködés gyakorlása;
- A Gyakorlathoz a 2007-es, Észtország elleni kibertámadást vették mintául (ma már nincsen „valódi" háború kibertámadások nélkül).

A szakemberek felhívják a figyelmet, hogy az ilyen típusú támadásoknál elsősorban a megelőzésre kell törekedni, mivel a más szervezetek által előre tervezett és célzott támadásra szinte lehetetlen felkészülni. A bankbiztonsági tevékenység tehát mindazon tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való intézményes gondolkodás, amely a pénzintézet saját tulajdonú tárgyainak, értékeinek, valamint az alkalmazottak és az ügyfelek biztonságának védelmét szolgálja.

Az 1992 óta a NATO évente megrendezi – hazánk nem minden évben vesz részt – a CMX-gyakorlatot, melynek fő célja, hogy a politikai és a katonai stratégiai irányítás szintjén tesztelni lehessen a NATO érvényben levő eljárásrendjét. Ugyancsak cél a gyakorlat forgatókönyvében szereplő fiktív válsághelyzetek megoldása közbeni gyakoroltatás.

A gyakorlat tényleges csapatmozgatással nem jár, a feladatokat az országok a polgári és katonai vezetési pontokon hajtják végre, valamint onnan tartják a kapcsolatot a NATO brüsszeli központjával, illetve a szövetséges katonai parancsnokságokon részt vevő állománnyal.

Az elmúlt években is sorozatban hajtott végre a NATO – hazánk bevonásával – CMX gyakorlatokat, amelyeknek azonban nem volt pénzügyi biztonságot, banki rendszereket érintő szimulációs mozzanata.

A NATO 2012. évi CMX válságkezelő és egyben kibervédelmi (támadás érte a bankrendszert) gyakorlatának fő célja a jelen kor kihívásai elleni egységes fellépéshez szükséges döntések konszenzus útján történő meghozatala volt:

- NATO-szerződés 5. cikkelyének érvényesítése – a tagországok közösen léptek fel a támadás elhárításáért és a rendszerek helyreállításáért;
- A hazai válságkezelési rendszer döntés-előkészítő és döntéshozatali folyamatainak, valamint a NATO-központtal és a tagországokkal való együttműködés gyakorlása;

• Főszerepben a terrorizmus és kiberbiztonság, mint napjaink kiemelt biztonsági feladatai;
• Potenciális támadások kritikus infrastruktúrák ellen, ebben az esetben a bankszektor;
• A bankok tekintetében biztosítani kell a megfelelően biztonságos környezetet, a biztonságot be kell építeni az információs rendszerekbe.

A szövetségi szintű célkitűzések tervezésben (Fodor Endre, 2012.) között a terrorizmus és proliferáció mellett megjelenő új kihívás, a kibertérből érkező támadások elleni kollektív fellépés gyakorlása volt, amely feladat a gyakorlaton is szerepelt.

CMX 12 gyakorlaton 27 tagország, köztük Magyarország és két partnerország – mintegy 2500 fő – vett részt, akik a tagországok minisztériumaiból, a NATO-parancsnokság tagjaiból és a stratégiai parancsnokságok munkatársaiból tevődött össze. A gyakorlat elképzelt földrajzi környezetben játszódott, menetét a közelmúltban bekövetkezett események és a reális kockázatok felmérése alapján tervezték meg.

Magyarország érdekeltségei a kijelölt sziget és ország vonatkozásában az alábbiak:

- Diplomáciai viszony, de számottevő kapcsolatok nélkül;
- Egyik országnak sincs diplomáciai képviselete Magyarországon.
- Vitatott területeken érdekeltségek, és az ebből fakadó konfliktusok;
- Tevékenység: 50 fő magyar szakértő, olaj- és gáz-feltárások és –kitermelés helyi munkásokkal;
- 15 fős magyar rendőri kontingens;
- Szélsőséges csoportok magyarországi jelenléte (térségbeni menekültekkel);
- Csoportok támogatottsága a szigetről érkezett hallgatók körében;
- Potenciális támadások kritikus infrastruktúrák elleni támadása.

A főbb nemzeti célkitűzések az alábbiakban fogalmazhatóak meg:

• Részvétel a Szövetség tagállamai közötti konzultációs és kollektív döntéshozatali folyamatban, valamint a Szövetség válaszlépéseinek kidolgozásában;
• A hazai válságkezelési rendszer döntés-előkészítő-, és döntéshozatali folyamatainak, a válságkezelési rendszabályok vételének és feldolgozásának gyakoroltatása,
• **Átfogó megközelítés keretében a polgári, rendvédelmi és katonai szervek együttműködésének gyakoroltatása;**
• A nemzeti álláspontok kialakítására irányuló döntés-előkészítési tevékenységek és a vonatkozó döntések meghozatalának gyakoroltatása;
• A válságreagálási rendszabályok bevezetésének előkészítésekor és annak végrehajtása időszakában a minisztériumok és a védelmi igazgatás területi szervei együttes válságkezelő tevékenységének a gyakoroltatása;
• A kiber-védelemben érintett hazai és NATO szervekkel való szoros együttműködés gyakorlása.

A CMX 12 egy olyan belső vezetési gyakorlat, amely a tervezésre és a döntéshozatalra összpontosít. Célja, hogy a résztvevők stratégiai politikai szinten a szövetség válságkezelési eljárásait gyakorolják. A tagországok, a NATO-parancsnokság, a stratégiai parancsnokságok civil és katonai szakemberei vesznek ezen részt. Ellentétben egy „élő gyakorlattal", itt nem történik katonai erők „mozgása". Magyarországon a gyakorlat vezetősége, a végrehajtó és biztosító állomány vesz részt, összesen százhúsz fővel. A CMX 12 gyakorlati célja kettős értelemben vizsgálható, mind a NATO, mind hazánk vonatkozásának tekintetében.

NATO célok:

• A Szövetség tagállamai közötti konzultációs és kollektív döntéshozatali eljárások gyakoroltatása kis intenzitású válságkezelés során. Az új NATO Stratégiai Koncepció, a válságkezelési eljárások tesztelése globális kiber-, terror és ABV fenyegetettség helyzetében.
• A kollektív védelmi képesség demonstrálása a nem hagyományos biztonsági kihívások ellen.

Hazánk céljai:

- Részvétel a NATO konzultációs és döntéshozatali folyamataiban, továbbá Magyarország polgári-, és katonai válságkezelési mechanizmusainak gyakoroltatása a konfliktushoz kapcsolódó, a hazánkat közvetlenül érintő fenyegetések elhárításán keresztül.
- A politikai-, katonai döntés-előkészítő-, és hozatali folyamatok, a válságkezelési rendszabályok vételének és feldolgozásának, valamint a polgári és katonai szervek együttműködésének gyakoroltatása;
- NATO információk feldolgozása, a nemzeti álláspontok kialakítása és megküldése;
- a Magyarországot közvetlenül érintő fenyegetettségek felszámolásának gyakoroltatása;
- a NATO szervek és a nemzetbiztonsági szolgálatok közötti együttműködés gyakoroltatása;
- a NATO Válságreagáló Kézikönyv és a Nemzeti Intézkedések Gyűjteménye együttes használatának gyakorlása;
- a NATO médiaesemények feldolgozása, tájékoztatók kiadása;
- kibervédelmi együttműködés gyakoroltatása a hazai és a NATO szervek között.

A NATO 2012. évi válságkezelési gyakorlatán (CMX 12) a résztvevő civil és katonai szakemberek bebizonyították: Magyarország felkészült arra, hogy gyorsan, hatékonyan kezelje és hárítsa el a válsághelyzeteket a NATO szövetségi kötelékében, melyet az alábbiakban szakembereink is megerősítenek. A szakemberek a 2007-es, Észtország elleni kibertámadást vették mintául. Az ilyen típusú támadásoknál elsősorban a megelőzésre kell törekedni, mivel a más szervezetek által előre tervezett és célzott támadásra szinte lehetetlen felkészülni.

A gyakorlaton egy kibertámadásnál esély nyílt a NATO-szerződés 5. cikkelyének érvényesítésére, vagyis a tagállamok közösen léptek fel a támadás elhárításáért és a rendszerek helyreállításáért. Ilyen a valóságban akkor fordulhat elő, ha például az alapinfrastruktúrát támadják meg informatikai eszközökkel.

A NATO-t alapító washingtoni szerződés 5. cikkelye kimondja: ha valamelyik európai vagy észak-amerikai szövetségest támadás éri, azt valamennyiük elleni támadásnak tekintik.

A gyakorlat tervezésében és a végrehajtásában – Izland kivételével – minden tagállam részt vett, valamint meghívást kaptak a NATO-partnerség keretében Finnország és Svédország, továbbá a Nemzetközi Atomenergiai Ügynökség (IAEA), a Nemzetközi Vöröskereszt (ICRC) és most először az Európai Külügyi Szolgálat (EEAS) képviselői is.

Egy honvédelmi gyakorlat esetén ma már mindenféleképpen kell számolni a kibereseményekkel is, így minden szempont indokolta, hogy a válságkezelési és a kibertámadási NATO-gyakorlaton a lehető legszorosabb együttműködés valósuljon meg. Ez olyannyira sikerült, hogy például amikor a CMX 12 forgatókönyve szerint informatikai támadás érte a honvédelmi gyakorlaton részt vevő tagállamokat, akkor ez a CC 12 gyakorlaton meg is történt és ott „le is játszották" az eseményt, és ennek hatásai már a CMX 12-ben is jelentkeztek.

A CMX 12 gyakorlaton alapvetően olyan események forgatókönyveit játszották végig, amelyek a valós világban is megtörténhetnek. Esetünkben egy, az Indiai-óceánon elhelyezkedő, mesterséges megosztással kialakult két ország közötti konfliktust modelleztek. Az egyik ország a NATO segítségére számíthatott, de a „rossz ország" is számos támogatót vonultatott fel mind a terrorszervezetek, mind pedig a kiberhadviselés területén. A kialakult konfliktus során NATO-tagországokat ért terrortámadási kísérlet (Magyarországon a repülőgép-katasztrófa mellett egy HÉV-szerelvény ellen követtek el robbantásos merényletet), illetve kibertámadás. A következmények elhárításában és a kialakult helyzet kezelésében nemcsak a legmagasabb kormányszinten dolgoztak a szakemberek, hanem – idén először – a megyei védelmi bizottságok is fontos szerepet kaptak.

A Megyei Védelmi Bizottságok (MVB) a területi működtetésért felelősek a veszélyhelyzet beálltakor. Ők azok a szervek, akiknek mindenről tudniuk kell, ami a megyét tekintve fontossággal bír, megyei érdekeltségű. A MVB elnökei kezében van a döntés, így minden információs és egyéb tevékenységbe be kell őket avatni:

- a biztonságot érintő ügyekben eljárnak;
- tájékoztatást nyújtanak a lakosság számára;
- rendészeti feladatokat látnak el például a bankok előtti lázongásokkal szemben;
- a pénzszállítás biztonsági feltételeit megteremtik.

Az MVB a Kormány irányítása alatt működő közigazgatási szerv, valamint a védelmi bizottságok honvédelmi felkészítési és katasztrófavédelmi feladatokat is ellátnak.

Az MVB elnöke a kormánymegbízott, aki a honvédelmi igazgatási feladatok vonatkozásában hatósági jogkört gyakorol, az MVB-k tagjai:

- a megyei közgyűlés elnöke, a fővárosban a főpolgármester;
- a megyei jogú város polgármestere;
- a katonai igazgatás területi szervének vezetője, képviselője;
- a megyei, fővárosi rendőrfőkapitány;
- az egészségügyi államigazgatási szerv képviselője;
- a vízügyi igazgatási szerv képviselője;
- az MVB titkára.

2012. július 6-tól az MVB tagja lett a fővárosi és megyei kormányhivatal főigazgatója is. Az MVB működési költségeinek biztosításához szükséges költségvetési támogatás a kormányhivatalnál jelenik meg.

Az MVB feladata, hogy intézkedjen a honvédelemben közreműködő szervek irányába a honvédelmi feladatok végrehajtásához szükséges intézkedési tervek elkészítésére, továbbá illetékességi területén határozza meg a honvédelemben közreműködő szervek által készítendő terveket és azok tartalmi követelményeit. Az MVB-elnök feladat-végrehajtását közvetlenül támogató szervek a kormányhivatalok és személyi állományuk – szükség esetén, munkaidő-korlátozás nélkül rendkívüli munkavégzésre kötelezhetőek.

Új feladatot jelent az Megyei Védelmi Bizottságok számára, hogy a hivatásos katasztrófavédelmi szerv területi szervének közreműködésével felül kell vizsgálnia a települések polgármesterei által az adott település vonatkozásában lefolytatott kockázatbecslési eljárás eredményeként kialakított katasztrófavédelmi osztályba sorolási javaslatot, és a hivatásos katasztrófavédelmi szerv központi szerve útján jóváhagyásra fel kell terjesztenie a katasztrófák elleni védekezésért felelős miniszterhez. A feladatok teljesítése érdekében, már a felkészülés időszakában elrendelhető a szolgáltatásra kötelezett részére:

- az igénybevételre kijelölt ingatlanok, továbbá ingó dolgok és ezek adataiban történt változások bejelentése, valamint igénybevételre alkalmas állapotban tartása;
- a lakosság alapellátásához szükséges tartalékok és készletek képzése;
- a szolgáltatás teljesítéséhez szükséges előkészületi tevékenység, ideértve a tervezési feladatokat is;
- a bejelentések valódiságának, a szolgáltatások teljesíthetőségének helyszíni ellenőrzése, az ellenőrzés során feltárt hiányosságok megszüntetése;
- a gyakorlatokhoz szükséges ingatlanok és ingó dolgok ideiglenes igénybevétele.

Végül a CMX gyakorlatok szövetségi végrehajtásával kapcsolatban fontos megemlíteni, hogy a tervezés és végrehajtás során a NATO a saját eljárásainak tökéletesítése mellett – a valós válságreagálási műveletek során szerzett tapasztalatok alapján – igyekezett az együttműködők körét szélesíteni, a válságkezelés folyamatába új szervezeteket meghívni. Mindezek szellemében lényeges előrelépésnek tekinthető, hogy a 2012. évi gyakorlat a NATO és az Európai Unió közötti szorosabb együttműködés

jegyében zajlott, és a végrehajtásában a döntések előkészítésében első alkalommal működött közre az Európai Unió Külügyi Szolgálata (European External Affairs Service/ EEAS). Hazánk nagyon jól vizsgázott a szimulációban; a hatóságok, szervezetek kiválóan együtt tudtak működni, viszont az informatikai rendszerek kapacitását növelni kell, és nagyobb figyelmet kell fordítani a rendszereket működtető emberekre – hozzáfűzve –, hogy a gyakorlat eredményeit részletes értékelése után döntenek a további szükséges lépésekről.

2013-ban nem volt hazánkban NATO CMX gyakorlat, de a 2014. évtől ismét részt vettünk ezeken.

CMX 2014: Válságkezelő gyakorlatot tart a NATO

Márciusban kezdődött a NATO CMX 14 (Crisis Management Exercise) válságkezelő gyakorlat, ahol a szövetség tagjai a NATO konzultációs és döntéshozatali folyamatát gyakorolták. A CMX az egyik legfontosabb rendezvény a NATO gyakorlatai között, ezen ugyanis Magyarország polgári-, és katonai válságkezelési mechanizmusait – a hazánkat közvetlenül érintő szimulált fenyegetések elhárításán keresztül – gyakoroltatják. A rendezvényen az Észak-atlanti Szerződés Szervezete polgári és katonai vezető szervei, valamint a tagállamok érintett szervezetei mellett a NATO meghívott és együttműködő partnerei, valamint több megfigyelő állam is részt vettek.

CMX 2015: kibervédelmi szakfeladatokat is gyakoroltak

A CMX 2015 forgatókönyve szerint a gyakorlat eseményei egy válság kialakulása körül bonyolódtak: két olyan ország között alakult ki konfliktus, amelyek nem tagjai a szövetségnek és földrajzilag is távol vannak a NATO-térségtől. A válsághelyzetnek azonban voltak olyan − elsősorban humanitárius és tengeri − következményei, amelyek hatást gyakoroltak a NATO-szövetségesek biztonságára. A forgatókönyv számos, a kibertérben zajló tevékenységet is tartalmazott. Ezek külön kihívást jelentettek az észak-atlanti szervezet civil és katonai vezetésének, s természetesen a híradó-informatikai rendszereket üzemeltető, illetve biztonsági szakterületű állománynak is. A gyakorlat során a kibervédelemmel kapcsolatos események kezelése rávilágított annak fontosságára, hogy a kritikus infrastruktúrák NATO- és nemzeti szinten történő védelme nemcsak a hagyományos értelemben elengedhetetlen feladat, de a kulcsfontosságú rendszerek „kibervédelmi hídfőállásainak" folyamatos biztosítása is megkerülhetetlen része a feladatrendszernek.

A CMX 2015 során a fiktív válsághelyzetek megoldása jó lehetőséget biztosított a kibertérben történő incidensek kezelésének gyakorlására. Fontos tapasztalatként és igényként jelentkezett a kormányzati együttműködő szervezetekkel történő kapcsolattartás színvonalának erősítése, a meglévő Magyar Honvédség-szintű incidenskezelési képesség továbbfejlesztése, illetve az MH Kormányzati Célú Elkülönült Hírközlő Hálózat biztonsági szintjének emeléséhez szükséges feladatok továbbgondolása is.

CMX 2016: NATO éves válságkezelési gyakorlat

A stratégiai válságkezelési gyakorlatban Magyarország is aktívan részt vett 2016-ban, mely a huszadik ilyen esemény volt hazánkban. A CMX gyakorlaton a NATO-szövetséges országok, valamint Finnország és Svédország elsősorban a stratégiai döntéshozatalt gyakorolták. A kitalált földrajzi környezetben játszódó fiktív eseményekre történő reagálás katonai erők és eszközök tényleges mozgásával nem járt.

A gyakorlat kiváló lehetőséget biztosított a kormányzati és szövetségesi döntéshozatali rendszerek tesztelésére, valamint az együttműködés továbbfejlesztésére, melynek célja a NATO válságkezelési eljárásainak gyakorlása stratégiai-politikai szinten, amelyben mind a tagországok, mind a NATO-parancsnokság, mind a stratégiai parancsnokságok civil és katonai szakemberei egyaránt részt vesznek. További cél volt a szövetség tagállamai közötti konzultációs és kollektív döntéshozatali eljárások gyakoroltatása és a szövetséges tagállamok kollektív védelmi képességének demonstrálása a nem

hagyományos biztonsági kihívások ellen. A résztvevők gyakorolták a NATO Válságreagálási Rendszabályok bevezetését, valamint a Nemzeti Intézkedési Rendszer működtetését.

2017: Magyarország a NATO CMX válságkezelési gyakorlatán

A politikai válságkezelési döntéshozatal és a katonai műveletek tervezésének gyakorlása mellett a természeti és ember okozta katasztrófák elleni védekezést is szimulálták a magyar szervek a NATO éves, stratégiai szintű politikai-katonai válságkezelési gyakorlatán, a CMX 17 gyakorlaton. Az immár huszonegyedik alkalommal megtartott eseményen kiemelt figyelmet fordítottak a modern kor egyik legnagyobb kihívásának számító kibertámadások elleni védekezésre.

Magyar részről a való életben is könnyen előforduló helyzeteket szimuláló gyakorlaton: az összes minisztérium mellett a honvédség, a rendőrség, a nemzetbiztonsági szolgálatok, a katasztrófavédelem, a Nemzeti Média és Hírközlési Hatóság, illetve a Médiaszolgáltatás-támogató és Vagyonkezelő Alap szakértőit, valamint a NATO-hoz delegált külképviseleteket is bevonták. A gyakorlat jelentőségét mutatja, hogy azt személyesen Jens Stoltenberg NATO-főtitkár vezette. Hazánkban a 2017. évben is a Honvédelmi Minisztérium közigazgatási államtitkára látta el a nemzeti igazgatói feladatokat, társigazgatókként csatlakoztak hozzá a belügyi, illetve a külgazdasági és külügyi tárca közigazgatási államtitkárai. A helyzetek tekintetében a CMX gyakorlat egyebek mellett napjaink biztonsági kockázatait, a terrorfenyegetettséget, valamint a hibrid hadviselésben rejlő veszélyeket hangsúlyozta.

A NATO 29 tagállamában, illetve Svédországban és Finnországban, a fővárosokban és a NATO-parancsnokságokon egyidejűleg megtartott gyakorlaton valamennyi részt vevő fél összehangoltan dolgozott a fiktív, átfogó megközelítést igénylő krízishelyzetek – például földrengés, terrortámadás, kibertámadás − következményeinek elhárításán. A gyakorlathoz az Európai Unió válságkezelésben érintett központi szervezetei is kapcsolódtak.

7.3. Esettanulmányok

7.3.1. Települések katasztrófavédelmi új besorolása (Szarka Zsolt, 2012.)

A régi besorolás hátrányai (2000–2010):

- merev szabályozás;
- alapvetően honvédelmi kockázatokra épülő besorolás;
- 2010. május-júniusi árvíz;
- vörösiszap katasztrófa;
- katasztrófák számának növekedése;
- összetettebbé vált veszélyforrások.

A 10 év tapasztalatai alapján, a megelőzés előtérbe kerülésével és a jobb közbiztonság megteremtésének igényével – a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról szóló 234/2011. (XI. 10.) Korm. rendelet alapján – az új besorolás a valós veszélyeztetettség alapján kerül meghatározásra, amelyet egy újabb, sokkal rugalmasabb szabályozás útján vezettek be. Települések besorolásának szabályai szerint valamennyi települést be kellett sorolni.

Az eljárás lépései a következők:

1. kockázatazonosítás;
2. kockázatelemzés és értékelés;
3. osztályba sorolás

4. ellenőrzés, visszaellenőrzés.

Kockázatazonosítás folyamata:
- információgyűjtés;
- kockázati tényezők meghatározása;
- veszélyeztető hatások beazonosítása;
- helyi sajátosságok figyelembevétele;
- veszélyek egymásra való hatásának vizsgálata.

Kockázatazonosítás –valamennyi veszélyeztető hatás figyelembevételével:
1. Elemi csapások, természeti eredetű veszélyek:
- árvíz,
- belvíz,
- rendkívüli időjárás,
- földtani veszélyforrások,
- földrengés,
- földcsuszamlás,
- beszakadás,
- talajsüllyedés,
- partfalomlás.

2. Ipari szerencsétlenség, civilizációs eredetű veszélyek:
- a Kat. IV. Fejezetének hatálya alá tartozó üzem,
- más létesítmény (ipari, mezőgazdasági) általi veszélyeztető hatás, veszélyes anyag szabadba kerülésének kockázata,
- távolság nukleáris létesítménytől:
    i. atomerőműtő,
    ii. kutató reaktortól,
- közlekedési útvonalak és csomópontok:
    iii. veszélyes áruk szállítása,
    iv. jelentős forgalom,
- a Kat. IV. Fejezetének hatálya alá nem tartozó, katonai célból üzemeltetett veszélyes anyagokkal foglalkozó üzemek, veszélyes anyagokkal foglalkozó létesítmények.

3. Egyéb eredetű veszélyek:
- felszíni és felszín alatti vizek (elsősorban az ivóvízbázisok) sérülékenysége,
- humánjárvány vagy járványveszély, valamint állatjárvány,
- a riasztási küszöböt elérő mértékű légszennyezettség.

4. Kritikus infrastruktúrákkal kapcsolatos kockázatok:
- a lakosság alapvető ellátását biztosító infrastruktúrák sérülékenysége,
- a közlekedés sérülékenysége,
- a közigazgatás és a lakosság ellátását közvetve biztosító infrastruktúrák sérülékenysége.

Kockázatelemzés és értékelés:
- települési adatok (adatlapok) alapján;
- kockázatazonosítást követően;
- kockázatelemzés és értékelés végrehajtása;
- veszélyeztető hatások következményei;
- bekövetkezés valószínűségének gyakorisága;
- több veszélyeztetettség esetén egymásra gyakorolt hatásuk.

Települések besorolás az alábbiak alapján történik:

- hatás és gyakoriság;
- korrekciós tényező;
- kockázati mátrix (3 osztály);
- legrosszabb forgatókönyv.

Hatás	Bekövetkezési gyakoriság			
	Ritka	Nem gyakori	Gyakori	Nagyon gyakori
Nagyon súlyos	II. osztály	II. osztály	I. osztály	I. osztály
Súlyos	III. osztály	II. osztály	II. osztály	I. osztály
Nem súlyos	III. osztály	III. osztály	II. osztály	II. osztály
Alacsony mértékű	III. osztály	III. osztály	III. osztály	III. osztály

2. számú táblázat: Települések katasztrófavédelmi besorolása

A települések katasztrófavédelmi besorolásáról, valamint a katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII. 29.) BM rendelet módosításáról szóló 61/2012. (XII. 11.) BM rendelet

A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény (a továbbiakban: Kat. tv.) 81. § *d)* pontjában, a 2-5. § tekintetében a 81. § *e)* pontjában kapott felhatalmazás alapján, az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről szóló 212/2010. (VII. 1.) Korm. rendelet 37. § *q)* pontjában meghatározott feladatkörömben eljárva a következőket rendelem el:

1. § Az ország településeinek katasztrófavédelmi besorolását az 1. melléklet határozza meg.

2. § A katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII. 29.) BM rendelet (a továbbiakban: R.) III. fejezete a következő 17/A. alcímmel egészül ki: *„17/A. A polgári védelmi szolgálatra önként jelentkezőkkel kapcsolatos rendelkezések* 26/A. § (1) A polgári védelmi szolgálatra önkéntesen jelentkező személy a rendelkezésre állásának tartalmát és az alkalmazásának feltételeit tartalmazó nyilatkozatát az 1. melléklet szerint teszi meg.

(2) A polgári védelmi szervezetbe történő önkéntes jelentkezéskor

a) határozott időtartamú rendelkezésre állás esetén a polgármester a beosztó határozatban rögzíti, hogy a megjelölt időpontban a beosztás megszűnik,

b) a határozatlan időtartamú rendelkezésre állás esetén az önkéntes írásban kérheti – a lakóhelye szerint illetékes polgármesternek címzett nyilatkozatban – a beosztás megszüntetését.

(3) A polgármester a (2) bekezdés *b)* pontja szerinti kérelem benyújtásától számított 30 napon belül felmenti beosztásából az önkéntest.”

6. § (1) Ez a rendelet 2013. január 1-jén lép hatályba.

A katasztrófavédelem polgári védelmi feladatai fokozatosan alakultak ki a korabeli légoltalmi feladatokból, és váltak a természeti vagy ember okozta katasztrófák megelőzését, és az azokkal szembeni védekezést szolgáló szervezeti, feladat- és intézkedési rendszerré.

A rendszer működése abból az alapelvből indul ki, hogy az állampolgároknak joguk van a biztonságra, de annak megteremtésében nekik maguknak is tevékenyen részt kell venniük.

Ennek jegyében a katasztrófavédelem alapfeladata a lakosságvédelem, tehát az életet és a létfenntar-

táshoz szükséges anyagi javakat veszélyeztető hatások elhárítása, az ennek érdekében szükséges szervezési és felkészítő munka, valamint a mindezt megalapozó tervezés. Munkájukkal hozzájárulnak a közbiztonság hatékonyságának növeléséhez, az emberek életminőségének javításához, valamint a nemzetgazdaság biztonságosabb működéséhez.

Elsődleges cél a hazai települések valós veszélyeztetettségén alapuló rendszeres kockázatértékelése és katasztrófavédelmi osztályba sorolása, a lakosság sebezhetőségére összpontosító veszélyelhárítási tervezés.

A reagálás terén a munka látványosabb része az önkéntes és köteles polgári védelmi szervezetek létrehozása, felszerelése és begyakoroltatása. Ennek során kiemelt szempont, hogy ezek az egységek a veszélyhelyzeti szintet el nem érő feladatokban is képesek legyenek részt venni, hiszen a katasztrófák csak akkor kezelhetők sikeresen, ha az átlagember is felelősséget vállal saját biztonságáért.

A veszélyhelyzetek kezelése során az áldozatok és túlélők jogai mindenekelőtt valók, melyet minden típusú döntéshozatalnál tiszteletben kell tartani.

7.3.2. Pénzügyi innovációk elterjedése hazánkban – a kistelepülések pénzforgalma

Az elmúlt időszakban a digitalizáció (Divéki Éva – Kajdi László, 2015.), a technológia fejlődése jelentős változást eredményezett a gazdaság számos területén. A változások a pénzügyi innovációk megjelenése és elterjedése révén nem hagyták érintetlenül a pénzforgalmat és a pénzügyi infrastruktúrákat sem, jelentős hatást gyakorolva a bankszektorra és annak versenyképességére. Magyarországon a globális tendenciákhoz hasonló folyamatok zajlanak le. A változás forrásai:

- egyrészt a technológia fejlődését és az ügyféligények változását,
- másrészt azokat a szabályozási és szabványosítási fejleményeket, amelyek nagymértékben elősegítik a pénzforgalmi szolgáltatások piacának átalakulását.

A 21. századra az elektronikus pénzforgalmi szolgáltatások elérése és használata a fejlett társadalmakban alapvető igénnyé vált. Az ügyfelek számára a pénzforgalmi szolgáltatások ma már közmű jellegűek, azaz olyan alapvető szükségleteket elégítenek ki, mint a telekommunikációs szolgáltatások, a vezetékes vízszolgáltatás vagy az elektromos energiaellátás. Magyarországon öt háztartásból négy rendelkezik fizetési számlával és kártyával, a munkabérek és nyugdíjak megközelítőleg kétharmada fizetési számlára érkezik. A fizetési számlához és valamilyen fizetési kártyához való hozzáférés már nem csak egy kényelmesebb, elektronikus alternatíva a készpénzzel szemben, hanem a havi jövedelmekhez való hozzájutás eszköze és a mindennapi élethez szükséges alapszolgáltatás. Többek között ennek köszönhető, hogy az ügyfelek a pénzforgalmi szolgáltatók részéről sokszor jelentős díjemelést is eltűrnek, mivel nincs valós lehetőségük az alkalmazkodásra, a pénzügyi rendszerből való kilépésre, vagy a gyors és hatékony szolgáltató váltásra.

Korábban a gazdaság szereplői bankváltás esetén számos problémával kerültek szembe, több akadályba is ütköztek, mivel például egy esetleges hitelfelvétel esetében a pénzügyi intézmény gyakran kötelezővé tette a nála vezetett fizetési számla fenntartását és a legtöbb esetben még a rendszeres jövedelem adott számlára utalását is. Mindezek miatt vált fontossá, hogy a bankváltás könnyen, gyorsan és ügyfélbarát módon valósuljon meg. A pénzforgalmi piac belépési költségei jelentősek. A pénzforgalmi szolgáltatás nyújtásához drága infrastruktúrát kell kiépíteni – fiókhálózat, ügyfélszolgálat, központi informatikai rendszerek, szabályozási előírásoknak való megfelelés stb.–, amelyek jelentős fix költséget indukálva kezdetben méretgazdaságossági hátrányt jelentenek az új belépők számára. Emellett az ügyfeleket nehéz elcsábítani a már piacon lévő többi szereplőtől.

A pénzforgalmi piac hálózatos jellege miatt az innovatív megoldások akkor lesznek sikeresek, ha a felhasználók vagy szolgáltatók száma eléri a megfelelő nagyságrendet. Emiatt sok szereplőnek egyszerre kellene fejlesztenie ahhoz, hogy a szükséges lefedettség biztosított legyen, és a kritikus tömeget elérje.

Mára a technológiai fejlődés által indukált fejlesztési lehetőségek és a hagyományos szereplők által kínált szolgáltatások közötti ellentmondás nagymérvű lett. A gazdaság más szektoraiban lezajlott infokommunikációs forradalom megváltoztatta az ügyféligényeket. A technológiai fejlődés, az ügyféligények átalakulása és a versenyt támogató európai szabályozási és szabványosítási változások hatására a banki jövedelmezőséget védő gátak lassan lebomlanak és a következő tíz évben feltehetően gyökeresen átalakul majd a pénzforgalmi szektor. Ezek a jellemzők globálisan érvényesülnek és alakítják át a piacokat, a változások azonban a magyar piacot sem hagyják érintetlenül. A változás forrásai az alábbiak:

- Technológia fejlődés lépései és hatásuk:
    - a megváltozott ügyféligények kielégítése a hagyományos infrastruktúrák használatával (banki ügyeket valós időben, a nap 24 órájában, az év 365 napján tudják intézni) – elérhetőség, az ügyintézés sebessége;
    - a hagyományos infrastruktúrát használó, arra ráépülő elkerülő megoldások létrejötte – innovatív megoldások: internet, e-kereskedelem, okostelefon, elektronikus pénzalapú rendszerek (PayPal), közösségi oldalak, bankkártyás vásárlás mobiltelefonnal. Fontos, hogy ezekkel a szolgáltatásokkal olyan szereplők (például telefon/számítógép gyártók) lépnek be a pénzforgalmi piacra, amelyeknek nem a fizetések jelentik a fő szolgáltatási területüket, ez csak egy szeletét jelenti a vállalati ökoszisztémájuknak;
    - Központi infrastruktúra megújítása – azonnali fizetési rendszer bevezetése (szükség lehet a jegybankok szerepvállalására a rendszerek fejlesztésének koordinálásában);
    - Új alternatív technológiát használó megoldások létrejötte – virtuális pénzek megjelenése (Bitcoin: „digitális készpénz” vagy „digitális árupénz”, nincs központi kibocsátója, kötött és rugalmatlan a kínálata, ld. arany-pénz)
- A szabályozási, szabványosítási folyamatok és ezek hatása:

Az új Pénzforgalmi irányelv keretében megvalósuló szabályozási változások támogatják az új szereplők piacra lépését, továbbá növelik a versenyt a pénzforgalmi szolgáltatások piacán. Az új Pénzforgalmi irányelv már ezeket az új típusú cégek nyújtotta szolgáltatásokat is a hatálya alá vonja és a szolgáltatások nyújtását engedélyezett és felügyelt pénzforgalmi intézmények számára lehetővé teszi. Így a 2018-tól módosítandó hazai jogszabályok által már Magyarországon is megteremtődik a feltétele az innovatív fizetési szolgáltatásokat kínáló vállalkozások szabályozott keretek közötti piacra lépésének. A Fizetési számla irányelv átültetése révén egyszerűbbé, gyorsabbá válik a bankváltási folyamat, átláthatóbbá válik a pénzforgalmi szolgáltatások árazása, ezzel fokozódik a verseny a pénzforgalmi szolgáltatások piacán.

A jövőben a magyar bankoknak egy sokkal élesebb versenyre kell felkészülniük, és versenyképességüket globálisan is növelni szükséges a technológiai fejlődés révén létrejövő innovatív pénzforgalmi szolgáltatások elterjedése, valamint számos a versenyt ösztönző jogi szabályozás következtében.

Számos manuális beavatkozást igénylő tevékenységet automatizálni kell, és a belső banki folyamatokat is át kell alakítani. Mindezen folyamatok elősegítik, hogy az elektronikus, digitalizált rendszeren keresztül bárki, bárhonnan végezhessen banki műveleteket – így kevésbé válik szükségessé a bankfiókok jelenléte minden kis településen. Az autózás elterjedésével elegendő egy közeli városban elérhető bankfióki jelenlét.

Világszerte megfigyelhető folyamat a fizikai infrastruktúra leépítése-átalakítása, ennek keretében a bankfióki hálózat fokozatos csökkentése mellett például egyre többféle szolgáltatásra alkalmas ATM-ek jelennek meg, és az interneten elintézhető banki ügyek száma is folyamatosan nő. A pénzmosás és terrorizmus finanszírozás elleni szabályok megváltozása lehetővé teszi a távazonosítást, így a távszerződések megkötését is, amely abba az irányba hat, hogy az ügyfélnek még az üzleti kapcsolat létesíté-

sekor sem szükséges személyesen bemennie a bankfiókba. Mindezekkel összefüggésben, világszerte nő a virtuális bankfiókok száma, amelyek széleskörű elterjedése várható Magyarországon is.

Az MNB az innovatív fizetési megoldások hazai elterjedése, valamint a verseny fokozása érdekében az azonnali fizetési rendszer létrehozását aktívan ösztönzi. A hazai pénzforgalmi szolgáltatások terén jelenleg rendkívül korlátozottan figyelhető meg a fejlett technológiák, például a mobilfizetési megoldások alkalmazása. Az MNB célja az azonnali fizetési szolgáltatás létrehozásával a modern informatikai megoldások hasznosítása, ezáltal pedig az innováció támogatása, a pénzforgalmi szolgáltatások fejlesztése és a fizetési piac szereplői közötti verseny ösztönzése.

Minden érintett szereplőnek végre kell hajtania mindazokat a fejlesztéseket, amelyek biztosítják, hogy legkésőbb 2019 második felében elérhetővé váljon az azonnali fizetési szolgáltatás a hazai fogyasztók és vállalkozások számára. Mivel Magyarországon sem a központi infrastruktúra, sem a pénzforgalmi szolgáltatók rendszerei nem képesek megfelelni az alapkoncepcióban meghatározott szabályrendszernek, és ennek megfelelően nem tudják feldolgozni az azonnali fizetési műveleteket, 2017-ben az MNB koordinálásával egy országos pénzügyi infrastruktúra modernizálási projekt indult. Az azonnali fizetéshez kapcsolódó belső fejlesztések végrehajtásával a bankok képesek lesznek megfelelni a 21. századi fogyasztói elvárásoknak, így a folyamatos elérhetőségnek és a fizetési műveletek közel valós idejű lebonyolításának.

A szolgáltatások szintjén a piaci verseny hozhatja el az ügyfelek számára azt az ideális állapotot, amelyben az ügyfelek az általuk elvárt színvonalú, modern pénzforgalmi szolgáltatásokhoz, kedvező feltételek mellett hozzájuthatnak. Az átjárhatóság révén biztosítható, hogy a fogyasztóknak elegendő legyen akár egyetlen fizetési alkalmazásba regisztrálniuk ahhoz, hogy a korszerű, elektronikus fizetési módokat használni tudják.

A piaci szereplők közötti együttműködés több szinten képzelhető el, így az üzleti folyamatok, a pénzforgalmi szolgáltatók fizetési alkalmazásainak és rendszereinek kapcsolódása, valamint az adatbeviteli módok területén egyaránt hasznos lehet a kooperáció.

Következtetések: A sikeres alkalmazkodás öt pontja

1. A működési hatékonyság növelése: a belső munkafolyamatok átalakítása, a manuális beavatkozást igénylő folyamatok automatizálása, széleskörű online ügyintézés biztosítása az ügyfelek számára.

2. Banki infrastruktúra fejlesztése az azonnali fizetési szolgáltatások nyújtása érdekében: az azonnali fizetési rendszer bevezetéséhez kapcsolódó elvárásoknak csak a banki rendszerek fejlesztésével lehet megfelelni. Ugyanakkor ez az infrastruktúra-fejlesztés a magasabb szolgáltatási szintet is támogatja majd, így a folyamatos elérhetőséget vagy a közel valós idejű feldolgozást.

3. Ügyfélbarát árazás alkalmazása: az új pénzforgalmi szolgáltatások felfutását, ezáltal pedig hosszú távon a bevételek növelését biztosíthatja a mérsékelt, ügyfélbarát árazás.

4. Innovációs képesség növelése, így a versenyképesség fokozása és azonnali fizetési szolgáltatások fejlesztése: a pénzforgalmi szolgáltatóknak ki kell fejleszteniük olyan gyors és kényelmes fizetési megoldásokat az ügyfeleik számára, amelyek kihasználják az új azonnali fizetési infrastruktúrában rejlő előnyöket, valamint számos fizetési helyzetben teszik lehetővé az ügyfelek számára előnyös megoldások bevezetését. Ez egyúttal arra is lehetőséget biztosít, hogy felvegyék a versenyt a Fin-tech típusú innovatív szolgáltatókkal.

5. Együttműködés az átjárható szolgáltatások érdekében: a piaci szereplők közötti kooperáció a közös, nyílt piaci szabványok kidolgozásában és alkalmazásában.

7.3.3. A falu

A község Bács-Kiskun megyében, a Duna bal partján helyezkedik el, a kalocsai Sárköz egyik Vajas menti faluja, amely Bajától 25 km-re, Kalocsától 18 km-re található. A település autóval és autóbusszal egyaránt könnyen megközelíthető – érinti az 51. sz. főút, melyet az M9-es autóút és a Szent László híd köt össze a 6. sz. főúttal (M6 autópálya). Természetföldrajzi szempontból a terület a Duna-Tisza közében a Kiskunság déli részéhez tartozik, környéke jellegzetes folyó menti táj.

Bács-Kiskun megye az ország éléskamrájaként máig megőrizte mezőgazdasági jellegét. A falu földje jól termő, iszapos, kiválóan alkalmas földművelésre, ezáltal fő ágazata a paprikatermesztés, de termesztenek itt szőlőt, vöröshagymát és paradicsomot is. A TSZ-ek megjelenésével a ház körüli baromfitenyésztés mellett megindult a nagyüzemi tenyésztés is. Vízi szárnyas telepet és keltetőt építettek. Később a Leneserdőben az erdő- és vadgazdálkodás a Gemenci Erdő- és Vadgazdálkodás kezébe került.

A falu jelenlegi statisztikai adatok alapján az utolsó ismert hivatalosan becsült népessége 3.007 fő (2017 évben). Ha népesség azonos ütemben változna, mint 2015-2017. időszakban (3.21%/év), 2018-ban a becslések szerint a lakossága 3.103 fő lenne. A lakosság nagyobb része a szegény földműves réteg közül került ki. Hiányzott az a módosabb iparos réteg, mely más nagyobb alföldi községekhez hasonló paraszpolgári kultúrát hozott volna létre a maga különböző köreivel. A hatékonyság növelése érdekében ezeket 1961-ben összevonták. Az Egyesült Munkás-Paraszt Tsz 10-15 év alatt egy több lábon álló, jól prosperáló termelőszövetkezetté fejlődött, ami stabil megélhetést teremtett a faluban. A termelőszövetkezet fő profiljává a zöldségtermesztés, ezen belül a fűszerpaprika termesztés és feldolgozás vált. A fűszerpaprika-termesztés egy része a háztáji gazdaságokban folyt. A paprikatermelő és feldolgozó tevékenységet számos további ágazat egészítette ki: baromfi ágazat, terménytároló- és terményszárító ágazat, építőipari ágazat, gépüzem, varroda.

A rendszerváltozás után a jól működő termelőszövetkezet átalakult, majd 2000-ben megszűnt. A korábbi ágazatokból az 1990-es évek elején önálló gazdasági társaságok szerveződtek, melyek a mai napig meghatározó gazdasági szereplői és foglalkoztatói a településnek. A község a mezőgazdasági és terményfeldolgozási hagyományai révén számos prosperáló gazdasági vállalkozással rendelkezik.

Bács-Kiskun megye természeti és civilizációs veszélyeztetettségét vizsgálva megállapítható, hogy ezen a területen a katasztrófák minden típusa és fajtája fellehető, úgymint az elemi csapások, természeti eredetű veszélyek, az ipari szerencsétlenség (Paks), civilizációs eredetű veszélyek, a Kat. IV. Fejezetének hatálya alá tartozó üzemeket veszélyeztető hatások, az egyéb eredetű veszélyek, valamint a kritikus infrastruktúrákkal kapcsolatos kockázatok.

A települések katasztrófavédelmi besorolása alapján jelenleg a falu a II. kategóriába tartozik, ÉS/VAGY:

- atomerőmű által veszélyeztetett, 3-30 km közötti terület (Paks);
- Kat. tv. IV. fejezetének hatálya alá tartozó üzemek által veszélyeztetettek és külső védelmi terv készítésére nem kötelezettek;
- kockázatbecslés alapján II. besorolást kaptak – amelyet a dunai ártér terület határoz meg.

A falu fejlettségéhez mérten elterjedt az e-kereskedelem és az e-bankolás, mivel bankfiók nincs a faluban, csupán egy régebbi időkből megmaradt falusi takarékszövetkezet és posta, valamint egy OTP bank által üzemeltetett automata található a főutcában az iskola előtt – mindkettő az utcán elhelyezett, telepített automata, mindenféle biztonsági védelem nélkül. A banki ügyintézés a helyiek körében a postán vagy a két közeli városban: Kalocsán vagy Baján történik. A posta a városháza utcájában van, amely az 51-es útról a faluba bevezető úton – merőlegesen a főutcára – található. Mivel a község aktív korú lakossága városokba ingázik napi vagy heti rendszerességgel, így többnyire ott bonyolítják pénzügyi tranzakciókat. Azon mezőgazdasági vagy egyéb szolgáltatást végző vállalkozók pedig szintén közeli városokban, leginkább Bajára járnak céges ügyeik intézése céljából. Szerencsére a 21.

században a tudomány és az informatikai eszközök szoftver és hardvert tekintetében való széleskörű fejlődésével, illetve az internet használatával az e-ügyintézésre és az e-banki tranzakciók elvégzésére tevődött rá a hangsúly a fizikai tevékenységekről.

A digitalizáció révén, az infokommunikációs technológiák sikeres alkalmazásával a folyamat jelentősen egyszerűsíthető és gyorsítható, ennek révén pedig a verseny is fokozódik a pénzforgalmi szolgáltatások piacán. Ezáltal egy vidéki faluban, vagy a fővárostól, nagyvárosoktól távolabb eső településen is könnyebbé váltak a banki folyamatok.

A községben lévő kereskedelmi egységek 90%-ában található POS terminállal rendelkező bankterminál – megkönnyítve ezzel a bankkártyás fizetést a vásárlónak. Egyre inkább elterjed a pay-pass-os, azaz bankkártya érintéssel – 5.000 Ft értékhatárig pin kód nélkül – használható fizetési mód. Ez veszélyes lehet egy nagyvárosban a tömegközlekedésben utazók számára, hiszen bizonyára mindannyian hallottunk arról a metódusról, amikor erre specializálódott emberek leolvasókkal szedik le a védtelen utas kártyájáról a pénzösszeget, csupán egy érintéssel. Ez faluhelyen nem veszélyes, főként a nagyobb terek miatt kialakult távolságok miatt, valamint az emberek személyes ismertsége okán (mindenki ismer mindenkit). Ha idegen érkezik az ott lakók közé, akkor jobban odafigyelnek, segítik egymást – egy nagyvárosi közegben ez nem annyira mondaható el. A falu egyik részén nagy rendezvényközpont került kialakításra, amely vonzza a más városokból, falvakból, valamint külföldről is az idelátogató emberek tömegét. Így például a pünkösdi bara bálon (ahogyan a helyiek hívják Rác Pünkösdön) akár meg is duplázódik a falu népessége. Ilyenkor szükséges a fokozottabb védelem a polgári és a hivatásos szervektől.

7.3.4. Az üdülőváros

Balaton parti település a tó déli partján, Siófoktól nyugatra, Budapesttől 136 km távolságra fekszik. Vasúton a Székesfehérvár–Gyékényes vonalon, személygépkocsival és busszal az M7-es autópályán, 7-es vagy 67-úton érhető el. A település a dél-balatoni borvidék részét képezi. Az üdülőváros a Balaton déli partján az 1904-ben megalakult Fürdőegyesület működésének köszönhetően elsők között volt a kulturált fürdőélet megszervezésében. Számos üdülő, villa, panzió épült akkoriban, és a fejlődés a két világháború között is folytatódott. Ekkor épült egyebek mellett a hajókikötő és kezdődött meg a település villamos- és vízhálózatának kiépítése. A századfordulón megindult polgárosodás következtében lassan fellendülő turizmus fogadó helyei közül Budapest, és a gyógyfürdők mellett a Balaton mentén a déli part 10 települése között említik üdülőhelyként. A századforduló és az I. világháború között e 10 településen már 25.000 vendégről szólnak a krónikák.

A gyors növekedés annak volt köszönhető, hogy nem csak az idegenforgalmi szálláshelyek kapacitását növelték meg, hanem a turizmust kiszolgáló létesítményeket is gyarapították a szolgáltatások színvonalának emelésével, továbbá a kommunális létesítmények, utak és parkok létesítésével. Ezt a fejlesztési irányt viszik tovább napjainkban is, hogy a város legjelentősebb bevételi forrásának számító turizmust minél inkább meghonosítsák. Erre vonatkozólag jelenleg komoly marketing munka folyik a turizmus fejlesztéséért, népszerűsítéséért.

A II. világháború utáni években a korábbinál is erőteljesebb ütemű fejlődés következett be, különösen az üdülőépítések vonatkozásában. A településen az 1970-80-as években nagymértékben megindult a belföldi turizmus. Ennek megfelelően a szociál-turizmust kiszolgáló üdülőépületek és táborok épültek. Az 1979. évben egyesítették a szomszédos településsel, így Somogy megye 6. településévé vált az új nevet felvett és városi rangot kapott helység. A két település 1991. október 1-el különvált, és mindkettő megtarthatta városi rangját.

A városban a legnagyobb hagyományokkal rendelkező szociálturisztikai üdültetés a rendszerváltást követően folyamatosan elsorvadt. Ezzel párhuzamosan mind nagyobb teret nyert a magánszálláshelyek kiadása, és a panzió-szerű nyaraltatási forma kialakítása. Ez utóbbit szolgálják az egyre gyarapodó számú utazási irodák szervező munkájukkal. Ma a Balaton déli partjának kedvelt üdülővárosa és keresett fürdőhelye a város.

A város területe 4323 hektár (43.2 km²), utolsó ismert hivatalosan becsült népessége 5.000 fő (2017

évben), ami akkori Magyarország népességének 0.05%-a (Somogy megyének 1.6%-a).

Fontos szempont a lakosság tekintetében az idényszerűség, mivel a nyári hónapokban az üdülő közkedveltsége miatt, akár 6-7-szeresére is duzzad az ott tartózkodó népességszám.

A település az I. besorolási osztályba tartozik, amely az alábbiakat jelenti, ÉS/VAGY:

- atomerőmű 3 km-es és a kutatóreaktor 1 km-es körzetében;
- Kat. tv. IV. fejezetének hatálya alá tartozó üzemek által veszélyeztetettnek és külső védelmi terv készítésére kötelezettek;
- kockázatbecslés alapján I. besorolást kapják;
- veszélyeztetettség együttes hatása alapján.

A védelmi szempontok tekintetében fontos megjegyezni az üdülőváros időszaki veszélyeztetettségét – pontosan a korábban említett üdülő, illetve nyáridőben való népesség megnövekedés okán –, amelyben a Balaton évtizedek óta vonzza a külföldi turistákat is. Ez biztonsági szempontból fokozottabb figyelmet érdemel a pénzügyi tranzakciók (például pénzkivétel, bankkártyahasználat stb.) esetében.

Emellett a strandokon való értékmegőrzés is nagy fontossággal bír, ami miatt a zárt strandon térfigyelő rendszer és párban járkáló fiatal segéd munkaerő támogatja a biztonsági óvintézkedéseket, amelyet alaphelyzetben a pénztárnál bérelhető trezor is megerősít. A városi üdülőövezeti forgatag másik veszélyforrása lehet a vonatállomások körüli terület, amelynek közvetlen közlében bankautomaták is segítik az oda látogató vendégeket. Gyakori helyszíne lehet – főként a késői órákban a támadásoknak, kizsebelésnek. Ha már az esti órákról esett szó, az említett főtér, sétálóutca és rendezvényközpont nagyszabású eseményei, illetve csupán egy könnyű esti nézelődős, vásárolgatós séta során is lopások áldozataivá válhat az ott nyaraló.

A városban banki viszonylatokat tekintve egy OTP bankfiók és 1 Takarék bankfiók található – mindkettő közel a vonatállomáshoz, és egyúttal a városközponthoz is. Emellett 3 OTP bankautomata és 1 Erste bankautomata segíti a bel- és külföldi népek banki ügyleteit. A boltok és a kisebb árusok többsége POS terminállal felszerelt, így többségüknél a kártyás fizetés megengedett. Jó vigyázni még a vendéglátóipari egységek és az éjszakai szórakozóhelyek, bárok esetében a bankkártyás fizetéssel, valamint a Ft érték valós értékének kiszámolásával.

Az azonnaliság, a folyamatos 24 órás működés alapelvárás az üdülő szezonban a kisvárosban lévő ügyfelek részéről, amely a banki működést is folyamatos működés felé tereli a pénzforgalom terén és más banki területeken is – ezáltal itt is. A technológiai fejlődés, a gazdaság más területeihez hasonlóan, az azonnaliság, a folyamatos működés elvárását hozta magával, így az ügyfelek igényei is ilyen irányba változtak.

7.4. Irodalomjegyzék

- Cser Orsolya (2012.): Értékmegőrzés válság idején a pénzintézeteknél, NKE Könyvtár. Elérhetőség: http://193.224.76.4/download/konyvtar/digitgy/publikacio/cser_orsolya01.pdf (utolsó letöltés: 2018. március 1.)
- Cser Orsolya (2013.): Biztonságunk egyik záloga a hatékony civil-katonai együttműködés. Hadtudomány, 2013. 3-4. szám, 104–116. oldal.
- Divéki Éva – Kajdi László (2015.): Digitális átállás a pénzforgalomban – a sikeres banki alkalmazkodás öt pontja. Elérhetőség: https://www.mnb.hu/letoltes/digitalizacio-a-penzforgalomban-mnb-honlapra.pdf (utolsó letöltés: 2018. március 16.)
- Dr. Hadnagy Imre (2008.): A biztonság korszerű értelmezése – avagy a biztonság ma már sokkal bizonytalanabb, mint korábban bármikor. Elérhetőség: www.vedelem.hu/.../135-a-biztonsag-korszeru-ertelmezese-avagy-a-biztonsag-ma.pdf (utolsó letöltés: 2018. január 27.)
- Dr. Haig Zsolt – Dr. Kovács László (2010.): Fenyegetések a cybertérből. (Nemzet és biztonság 2010.) Elérhetőség: http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt

__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf (utolsó letöltés: 2018. január 25.)
- Dr. Keszely László (2014.): A válság és a különleges jogrend kapcsolata, különös tekintettel a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszere. Elérhetőség: http://www.hadijog.hu/wp-content/uploads/2014/03/Keszely-V%C3%A1ls%C3%A1greag%C3%A1l%C3%A1s.pdf (utolsó letöltés: 2018. január 15.)
- Dr. Kovács László – Dr. Krasznay Csaba (2010.): Digitális Mohács – kibertámadási forgatókönyv Magyarország ellen. (Nemzet és biztonság 2010.) Elérhetőség: http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf (utolsó letöltés: 2018. január 12.)
- Fodor Endre (2012.): CMX 12: Tervezés és döntéshozatal. Elérhetőség: http://www.honvedelem.hu/cikk/34831_cmx_12_tervezes_es_donteshozatal (utolsó letöltés: 2017. november 30.)
- Gazdag Ferenc – Tálas Péter (2008.): A biztonság fogalmának határairól. Nemzet és Biztonság 2008. január – Biztonságpolitika, 3–9. oldal, Elérhetőség: www.nemzetesbiztonsag.hu/…/gazdag_ferenc__talas_peter-a_biztonsag_fogalmanak_határairól (utolsó letöltés: 2017. november 25.)
- Gazdag Ferenc (2001.): Biztonságpolitika tankönyv. SVKH, Budapest.
- Gazdag Ferenc (2011.): Biztonsági tanulmányok – biztonságpolitika. ZMNE, Budapest, 37-46. oldal.
- Haig – Kovács – Munk –Ványa (2013.): Az infokommunikációs technológia hatása a hadtudományokra. NKE HH Kar Kari TDT, Budapest, 173. oldal.
- Haig Zsolt – Várhegyi István (2008.): A cybertér és cyberhadviselés értelmezése. Hadtudomány, 2008. 1. szám 1–12. oldal. Elérhetőség: mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (utolsó letöltés: 2018. január 20.)
- Kiss Petra (2012): A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében. Hadtudomány 2012. 3-4. szám, 68–79. oldal.
- Kovács László – Illés Zsolt (2011.): Cyberhadviselés. Hadtudomány, 2011. 1-2. szám, 29–41. oldal
- Szabó József – Gabriel Győző – Horváth Ferenc (1995.): Hadtudományi lexikon. Magyar Hadtudományi Társaság, Magyar Honvédség, Budapest.
- Szarka Zsolt (2012.): Tájékoztató a települések katasztrófavédelmi osztályba sorolásának helyzetéről, tapasztalatairól Elérhetőség: www.katasztrofavedelem.hu/letoltes/filedb/hirek/1137/pv_foferrt_terkepek.pdf (utolsó letöltés: 2018. március 4.)
- Tomolya János – Padányi József (2012.): A terrorizmus jelentette kihívások. Hadtudomány, 2012. 3–4. szám, 34–67. oldal.
- Trautmann Balázs (2012.): CMX 12: 4 nap együttműködés. Elérhetőség: http://www.honvedelem.hu/cikk/34947 (utolsó letöltés: 2017. november 24.)
- Vígvári András (2009.): Pénzügy(rendszer)tan. Akadémiai Kiadó, Budapest.

8. SZABÓ ZSOLT MIHÁLY: CÉLZOTT TÁMADÁS A KÖZIGAZGATÁSI SZEKTOR ELLEN

8.1. Célzott támadás a közigazgatási szektor ellen

Napjainkban az állam, annak minden szervezete valamint polgára kiszolgáltatottá vált a többszörösen összetett elektronikus információs rendszereknek Magyarország kiberterében, amelyek nélkül az állami működés, különböző szolgáltatások (e-közigazgatás) biztosítása és igénybevétele megvalósíthatatlanná válik. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket – egyértelműen – védeni kell, különös tekintettel arra, hogy azok működése során felhasznált és keletkező információk, továbbá az azokban kezelt adatok jelentős vagyont képviselnek. Az informatikai eszközök használata mára teljesen hétköznapivá vált az állami szervezeteknél. Ahhoz, hogy ezen eszközök használatában megbízhassunk az informatikai biztonság kérdéseire is oda kell figyelnünk.

Az informatikai rendszerekkel szembeni fenyegetések többsége az internetről érkezik. Több nemzetközi kutatás, mint például az ESET 2017 és a Symantec 2017 jelentései arra is rámutatnak, hogy az adatszivárgásra visszavezethető leggyakoribb és legköltségesebb károkat nem a külső támadók, hanem a munkavállalók okozzák a szervezeteknek. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) rendelkezik a nemzeti vagyon részét képező elektronikus adatvagyon biztonságának és védelmének szabályairól. A védelemhez számos feltételt szab a törvény, amelynek egyik fontos eleme a felhasználók biztonságtudatossági képzése. Az Ibtv. végrehajtási rendelete a 41/2015. (VII. 15.) BM rendelet (BMr.) ezt a feltételt a szervezetek által meghozandó védelmi intézkedések között érvényesíti úgy, hogy „az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára”, mely képzésnek nem csak a belépéskor kell megtörténnie, hanem az ismeretek felfrissítése és aktualizálása érdekében rendszeresen (célszerűen évente) meg kell tartani.

Az előbbiek alapján indokolt az állami szervezetek vezetőinek és munkavállalóinak biztonságtudatosságának fokozása és naprakész információval való ellátása, továbbá felkészítése a veszélyhelyzetek felismerésére. A fejezetek témájához kapcsolódó elméleti hátér áttekintése után az információvédelemi vezetőkkel készített személyes interjúk segítségével bemutatjuk a lehetséges veszélyforrásokat és elkerülésükre való felkészülés lehetőségeit.

Az információ biztonsága, a hivatalok, cégek és magánszemélyek adatainak védelme egyre inkább központi kérdéssé válik. Az adatok véletlen vagy szándékos kompromittálódása, sérülése, ellopása vagy rossz szándékú manipulálása komoly erkölcsi károkat okoz az érintett szereplőknek, elvesztik jó hírnevüket, megrendül a bizalom a szolgáltatásukban. E mellett sokszor további anyagi, kártérítési és büntetőjogi következményei is lehetnek az adatok helytelen kezelésének (Ibtv. és GDPR megfelelőség). A nemzetközi és hazai adatok azt mutatják, hogy az adatvesztés, adat-kompromittálódás legtöbbször emberi tényezőkre vezethető vissza – a munkatársak odafigyelésével, képzésével, a szabályok betartásával sok esetben megelőzhető lett volna az incidens.

Vezetői interjú:
dr. Bencsik Balázs
Nemzeti Kibervédelmi Intézet (NKI)
vezetője

Kérdés: Hogyan épül fel az NKI?
Válasz: Az 1. ábra alapján az NKI három szakmai területből áll: a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület; a Kormányzati Eseménykezelő Központ (GovCERT) a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó incidenskezelési szakterület; és a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási-, és sérülékenység-vizsgálati szakterület.

	GovCERT	NEIH
Mit?	**technikai** támogatás és vizsgálat	**jogszabályi megfelelőség** támogatás és ellenőrzés
Mikor?	incidens esetén vagy **igény szerint**	a tervezőasztaltól **folyamatosan**
Hogyan?	incidenskoordináció, tájékoztatás, tudatosítás, oktatás, sérülékenységvizsgálat, gyakorlatok, …	megfelelőségvizsgálat, állásfoglalások, ajánlások, fejlesztések IT biztonsági kontrollja, …

1. sz. ábra: A Nemzeti Kibervédelmi Intézet szakmai területei

Kérdés: A NEIH milyen feladatokat lát el?
Válasz: A NEIH az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. Amennyiben valamely szervezet a hatósággal nem működik együtt, úgy – költségvetési szerv esetében – a hatóságnak joga van kirendelni úgynevezett információbiztonsági felügyelőt, míg nem költségvetési szerv esetén bírság kiszabására is lehetősége van. A hatóság ellenőrző funkciója erőteljes támogató funkcióval is bír, ugyanis jogosult a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában véleményezni és ellenőrizni az információbiztonsági követelmények megtartását. Az információtechnológiai fejlesztések elektronikus információbiztonsága szempontjából kiemelt fontosságú, hogy a vonatkozó előírások a rendszerek teljes életciklusa alatt következetesen és maradéktalanul megvalósításra kerüljenek és a fejlesztések eredményeként önmagukban is teljes, továbbá a meglévő rendszerekhez funkcionálisan és biztonsági aspektusból is harmonikusan és költséghatékonyan illeszkedő rendszerelemek, rendszerek épüljenek ki.
Kérdés: A Kormányzati Eseménykezelő Központ milyen feladatokat lát el?
Válasz: A GovCERT alapvető rendeltetése az állami és önkormányzati szervek informatikai biztonsági támogatása, amely egyrészt megelőző jelleggel, úgynevezett sérülékenység menedzsment formájában a szoftver-sérülékenységek és információbiztonsági fenyegetések nyomon követésére, valamint a fenyegetés kiváltotta biztonsági esemény megelőzése érdekében az érintett IT rendszerek üzemeltetőinek tájékoztatására fókuszál. Ezen túlmenően pedig reaktív jelleggel, úgynevezett incidenskezelési tevékenységet lát el, amely a védett szerveknél bekövetkező biztonsági események

(incidensek) kivizsgálására és – több állami szervet érintően – a kezelésük koordinációjára irányul.
Kérdés: Az NKI milyen biztonságtudatosító tevékenységet segít elő?
Válasz: A kibervédelem legolcsóbb és leghatékonyabb módja a biztonságtudatos használat. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne a megfelelő szinten kialakítható. Az NKI önmagában nem képes biztosítani a magyar kibertér védelmét, azonban szakmai tudásával hozzájárul ahhoz, hogy az egyes elektronikus információs rendszerek üzemeltetői megszerezzék és alkalmazzák a rendszereik védelméhez szükséges ismereteket. Ez a tevékenység a tudatosítás, amely számos formában megjelenhet, mint például szakmai anyagok és útmutatók készítése, közvetlenül kifejtett oktatási vagy képzési tevékenység, a kiberbiztonság hangsúlyának növelése a médiában stb. A tudatosító tevékenység számos réteget céloz, ezek közt elsősorban kell említeni a döntéshozókat (szervezeti vezetőket, akik a rendszerek védelméért felelősek), az üzemeltetőket (akik ellátják a rendszerek működtetését, és akiktől elvárható a védelmi intézkedések megtétele), és a felhasználókat, akiket pedig meg kell tanítani az internet és az információs technológiák biztonságos használatára, a saját és a rájuk bízott adatok felelős és szakszerű kezelésére. Az IT biztonság közérthetően az alábbi linkről szabadon letölthető: http://njszt.hu/de/it-biztonsag-kozerthetoen.

8.2. Informatikai rendszerek ellen indítható célzott támadás lehetséges fajtái

Biztonság alatt azt az állapotot értjük, amelyben a szervezet számára fontos tevékenységek zavartalanul végezhetők. A támadások célja alapvetően az adat, melyet különböző rendszerelemek vesznek körül, és melyeket folyamatok kezelnek. A kiber fenyegetettségek a rendszerelemek meghatározott láncán keresztül az adatokat és azokat kezelő folyamatokat veszélyeztetik (Szabó, 2017b). Az Ibtv. írja elő, hogy az állami szervek informatikai rendszerének képesnek kell lennie a szervezet működése szempontjából meghatározó hardver- és szoftvereszközök kritikus biztonsági eseményeinek megfigyelésére és naplózására, illetve ezen események automatizált kezelésére (Szádeczky, 2014). Egy állami szervezet informatikai rendszerének és biztonsági menedzsmentjének kialakításakor a fenti követelményeken túl fontos, hogy a biztonsági rendszerben egyszerűen legyen leképezhető és ellenőrizhető a szervezet biztonságpolitikájának megvalósítása (Michelberger-Lábodi, 2012). A biztonsági menedzsmentnek legyen szerves része a hálózat-, felhasználó-, szoftver-, tűzfalmenedzsment, a levelező rendszer tartalomszűrése, vírusvédelme és egyéb más informatikai rendszerek (Tihanyi-Varga-Frész, 2014). Az információbiztonság három alapvető követelmény (bizalmasság, sértetlenség, rendelkezésre állás) együttes teljesülése esetén valósítható meg. Ez a három követelmény az információkkal kapcsolatos (Muha-Krasznay, 2014). Ha ezek a követelmények nem teljesülnek, elveszhet, sérülhet az IT rendszer, illetve az általa kezelt adatok:

- bizalmassága: az információt más is megismerheti, mint aki jogosult;
- sértetlensége: az információ átadása során megváltozhat;
- rendelkezésre állásának funkcionalitása: az információ kellő időben nem hozzáférhető.

Célzott támadások (Targeted Attacks) már a 2000-es évek elején is léteztek, sőt néhány esetben Magyarországon is megjelentek. Az egyik ilyen hazai esetről szóló esettanulmány (SaveAs, 1999) szerint 2001-ben egy magyarországi intézmény – mely mintegy 200 számítógéppel rendelkezik – vált célzott támadás áldozatává. A tanulságos történet szerint a vezetés a rendszergazda elbocsátását követően néhány hónappal vette észre, hogy kezdik sorozatosan elveszteni a tendereket. Megbíztak egy informatikai biztonsággal foglalkozó vállalkozást a szervezet átvilágítására, melynek során a számítógépeket is szúrópróbaszerűen megvizsgálták. Miután a második olyan számítógépet is megtalálták, amelyen egy sehova nem köthető kis programot találtak, a vizsgálatot kiterjesztették a szervezet valamennyi számítógépére. Összesen 11 számítógépen került elő ez a kis program, valamennyi a szervezet működéséhez szükséges legfontosabb pontokon volt, beleértve a vezetők hordozható számítógépeit is. A

kis program elemzése során kiderült, hogy az alkalmas arra, hogy információkat küldjön a szervezeten kívülre, másik számítógépre telepedjen. Mintegy 16 különböző módszerrel rendelkezett a külső kommunikáció érdekében, a kapcsolatot pedig számtalan úgynevezett proxy szerveren keresztül valósította meg, ami meggátolta a támadó kilétének az azonosítását (Leitold, 2014, 9–10. old.).

Az APT-k (Advanced Persistent Threat – magas szintű, folyamatos fenyegetést jelentő támadások) a 2010-es évek elején világosan bebizonyították, hogy képesek a hagyományos védelmi technológiák mellett is rendszerekbe behatolni és ott hosszú ideig észrevétlenül maradni, valamint gondoskodni értékes információknak a szervezeten kívülre történő küldéséről, azok eltulajdonításáról. Az APT-k működésük során (lásd 1. melléklet) több különböző támadási lehetőség módszereit egyesítik, úgymint a Social Engineering módszereket a felhasználók átverésére, vírusterjedési módszereket újabb számítógépek felderítésére és megfertőzésére, illetve hálózati kommunikációs módszereket a kártékony kód távirányítására és az adatok kijuttatására (Leitold, 2014, 0. old.). A 2. melléklet összefoglalja célzott támadások kihívásaira a lehetséges védelmi intézkedéseket, melyek az egyéni megoldások és a központosított védelmi technológiák együttes alkalmazását javasolják a hatékony védelemi kialakításokhoz (Trend Micro, 2014).

Az elmúlt években a célzott támadások folyamatosan növekvő tendenciát mutatnak és ez alól az idei, 2018-as év sem lesz kivétel. Az APTNotes, a GitHub (https://github.com/kbandla/APTnotes) által létrehozott és karbantartott adatbank 2008 óta gyűjtött publikált jelentéseket a célzott támadásokról. Az adatbank szerint az ilyen jellegű támadások az elmúlt pár évben megsokszorozódtak, 2010-től 2014-ig összesen 53 ismert támadást azonosítottak, és ezek mellett valószínűleg nagyon sok volt a még felfedezetlen kísérlet is. Az adatok alapján 2015 augusztusában összesen 291 célzott kampányt gyűjtöttek össze a vállalatok, az intézetek és a kormányok ellen. Ezek közül 72-őt megfigyeltek 2015-ben, több mint kétszerese az előző év hasonló időszakában, és hasonló mennyiségű volt a 2014 második felében tapasztaltnál. A területek alapján legfőbb azt láthatjuk, hogy jellemzően a pénzügyi és az üzleti szféra áll leginkább a célkeresztben, de időnként politikai motivációk is tetten érhetőek, vagy legalábbis gyaníthatók. Emellett aggasztó lehet, hogy folyamatosan növekszik az egészségügyi adatok elleni támadások száma is. Napjainkban az informatikai támadások jelentős része az alkalmazási szinten tapasztalható. Az alsóbb rétegeken olyan kifinomult védelmi megoldások érhetők el, melyek hatékonyan – de nem feltétlenül teljes körűen – védenek a támadások ellen. Az alkalmazások közül is előszeretettel a weben keresztül elérhető szolgáltatások állnak a célkeresztben. Ez még általában az egyes portálmotorokat érinti, de már rendelkezésre állnak olyan letölthető eszközök, melyek kimondottan a web service-ek sebezhetőségeinek felderítésére lettek kifejlesztve. A közigazgatási SOA architektúra, és a rajta elérhető web service-ek ezért olyan támadásoknak vannak kitéve, melyekre a Közigazgatási Informatikai Bizottság (KIB) ajánlásai nem hívják fel külön a figyelmet. A centralizált magyar e-közigazgatási rendszer lényegesen jobb lehetőségekkel kecsegtet az informatikai biztonság területén. A kiadott közigazgatási ajánlások megfelelő alapot jelentenek, de folyamatos fejlesztésük, és főleg kikényszerítésük nélkül az e-közigazgatási rendszerek veszélyeztetve vannak (Krasznay, 2009).

Vezetői interjú:
Dr. Muha Lajos
Magyar Államkincstár
informatikai biztonsági vezető

Kérdés: Milyen támadási trendek várhatóak a 2018-as évben?
Válasz: Az informatikai biztonsági szakértő elmondta, hogy az elektronikus információs rendszereket érő támadások egyre szofisztikáltabbá váltak és nehéz védekezni ellenük. A zsarolóvírus kampányok egyre kiterjedtebbek lesznek. A támadásokra nincs általános orvosság. Legnagyobb gondot az adat-

vesztés okozhat egy szervezet számára. A problémák kezelésére az incidenskezelés komolyan vétele adhat megoldást. A védelmi intézkedések és a megelőzés elősegítheti az informatikai rendszerek védelmét.
Kérdés: Milyen veszélyeket rejt az e-közigazgatás?
Válasz: Az e-közigazgatás a közszféra kapcsolatrendszerének tudás alapú átalakítását és racionalizált, szolgáltató jellegű újraszervezését jelenti, az infokommunikációs technológiai alkalmazások közműszerű használata révén. Modern és hatékony közigazgatás nem képzelhető el széleskörűen elérhető elektronikus szolgáltatások, és azokat rendszeresen és örömmel használó ügyfelek nélkül. Az e-közigazgatás minden résztvevő költségeit csökkenti és versenyképességét növeli, így bevezetése társadalmi és nemzetgazdasági szinten is egyértelmű előnyöket jelent. Ahhoz azonban, hogy ezek a fejlesztések az állam, illetve a felhasználók oldalán tényleges megtakarításokat eredményezzenek, az e-közigazgatás valamennyi sikerkritériumának teljesülnie kell: az infrastruktúra és a szolgáltatások rendelkezésre állása mellett szükség van felkészült és motivált emberekre a közigazgatásban, illetve nyitott és tájékozott felhasználókra a lakosság és a vállalkozások körében. A web alapú alkalmazások, melyeket a felhasználók online érnek el számtalan biztonsági kockázatot rejtenek, melyekre fel kell készülni és a védelmi intézkedéseket meg kell tenni.
Kérdés: Milyen védelmi megoldások ajánlottak?
Válasz: Az állami szervezetek informatikai rendszereinek biztonsági kérdései, nagyban hasonlítanak más informatikai rendszerek biztonsági problematikáira, ugyanakkor a fentebb említett tényezők különleges eljárásokat, speciális eszközöket és megoldásokat követelnek meg. A tervezés minden esetben meglehetősen intézmény specifikus, az adott intézmény szerkezetét, adottságait messzemenően figyelembe kell venni: tények és körülmények ismerete nélkül nem képzelhető el megfelelően biztonságos informatikai rendszer. Az intézmény valamennyi dolgozójának és külső munkatársának az információ biztonságra vonatkozó irányelveket, az informatikai rendszerek alkalmazására vonatkozó szabályokat ismerniük és alkalmazniuk kell. A Közigazgatási Informatikai Bizottság (KIB) 25. számú ajánlása és kapcsolódó egyéb ajánlások letölthetőek: https://ugyintezes.magyarorszag.hu/dokumentumok/.

8.3. A közigazgatás, mint kritikus infrastruktúra

A kritikus infrastruktúra védelme (KIV) a mai kor kihívása, amely a globális terrorizmus terjedésével került a figyelem fókuszába világszerte. A kritikusnak minősített infrastruktúrák azok, amelyeknek köszönhetően tud alapvetően működni egy társadalom, egy gazdaság. A védelem különösen fontos ma, az úgynevezett negyedik generációs (4GW) vagy aszimmetrikus hadviselés korában, amikor információs hadviselési eszközökkel szinte bármely érdekcsoport tudja érdekeit érvényesíteni, nála jóval nagyobb ellenfelével – tipikusan nemzetállamokkal – szemben. Ezen támadások fő célpontjai a kritikus infrastruktúrák (KI), különösen a kritikus információs infrastruktúrák (KII) (Muha, 2007).

Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK tanácsi irányelvet (irányelv) tagállami kötelezettségünk átültetni a hazai jogrendszerbe (Rajnai-Fregan, 2016). Ezen jogharmonizációs kötelezettség mentén tagállami szinten meg kell hozni azokat az intézkedéseket, amelyek beültetik az irányelvet a magyar jogrendszerbe (Haig-Kovács-Ványa, 2012). A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 1§. f) pontja szerint létfontosságú rendszerelemnek azt kell tekinteni, mely „a meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna”. A kritikus infra-

struktúra azonosításánál a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról iránymutatásait is figyelembe kell venni (Répás-Dalicsek, 2015). A Kormányrendelet alapján létfontosságú információs rendszer és létesítmény: a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek. Továbbá kockázatelemzést kell végezni, mely a rendelet értelmezésében: fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából (Szabó, 2017a). Egy lehetséges eljárás lehet a CRAMM (CCTA Risk Analysis and Management Method) alapú módszertan, amelyet a Közigazgatási Informatikai Bizottság (KIB) 25. számú ajánlása is említ, és az egyik legelfogadottabb metodológia napjainkban (Muha, 2008). Ez a módszer leírja a számítástechnikai rendszerek sebezhető pontjait, és javaslatokat tesz ellenintézkedésekre (Szabó, 2018c).

Vezetői interjú
Prof. Dr. Rajnai Zoltán
Óbudai Egyetem Biztonságtudományi
Doktori Iskola vezetője
Magyarország kiberkoordinátora

Kérdés: Mi a kritikus infrastruktúra?
Válasz: A Belügyminisztérium alá tartozó Országos Katasztrófavédelmi Főigazgatóság honlapján található meg a kritikus infrastruktúra általános fogalma, azaz: egy országon belül a lakosság szellemi és tárgyi életfeltételeit megteremtő, a gazdaság működését elősegítő vagy lehetővé tévő azon szervezetek, létesítmények, létesítményrendszerek, hálózatok összessége vagy ezek részei, amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire negatív hatással jár. Az előzőek alapján meghatározható a kritikus infrastruktúra egy lehetséges hazai definíciója: egymással összekapcsolódó, interaktív (egymástól kölcsönös függésben lévő) infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózata, melyek az ország működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű biztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.
Kérdés: A közigazgatás, mint kritikus infrastruktúra?
Válasz: Kritikus infrastruktúra-elemek segítségével tartja nyilván állampolgárai adatait az állam, ezek igénybevételével működik a közigazgatás (nem csak az e-közigazgatás), és ezek segítségével nyújt az állam (nem csak e-kormányzati) szolgáltatásokat. Ezek védelme tehát jórészt állami feladat, a védelem megszervezése pedig kifejezetten az. Állami feladat már csak azért is, mivel az állam maga is ezekre az infrastruktúrákra támaszkodik. Egy ilyen kritikus infrastruktúra-elem bármilyen okból történő kiesése pedig gyakorlatilag káoszba, anarchiába tudja sodorni az adott nemzetállamot. Ezért a feladatok pontos végrehajtására, a védelem folyamatos fenntartására kell az államnak koncentrálnia.
Kérdés: Miért fontos az információbiztonsági képzés?
Válasz: Úgy gondolom, a hazai hivatalos szereplők kiberbiztonsága megfelelően jó: gondolok itt például a tavalyi WannaCry zsarolóvírus világméretű terjedésére, amely százötven állam százötvenezer informatikai rendszerét támadta meg, de Magyarországon a kormányzati, önkormányzati és államigazgatási oldalon nem sikerült bejutniuk a támadóknak. A GovCERT olyan támogatást tudott adni a hozzáfordulóknak – és itt cégekről is beszélünk –, amellyel sikeresen hárították el a károkozási kísérleteket. Természetesen becsúszhatnak hibák az események után, de, ha a hozzáértők mindig idejében elvégzik a szükséges és folyton frissített biztonsági protokollokat, akkor minimálisra lehet szorítani a betörés veszélyét. Viszont el kell mondani, hogy az államigazgatásból, azon belül

különösen a kistérségi régiókból jelenleg közel kétezer információbiztonsági szakember hiányzik. A hazai felsőoktatás elkezdett kidolgozni egy rendszert, így hamarosan megoldás születhet a problémára. Meg kell még említeni az Európai Hálózatbiztonsági Ügynökség (ENISA) 2012 óta minden év októberében nemzetközi kampányt szervez kiberbiztonsági hónap témában (European Cyber Security Month – ECSM). Az ECSM célja a kiberbiztonsági tudatosság növelése, valamint a kibertérben megjelenő fenyegetések széles körben történő megismertetése. A kiberbiztonsági hónap keretében képzéseket, tudatosító előadásokat tartanak az Európai Uniós tagországok intézményei, ezek koordinálását az ENISA ügynökség végzi. A kampányhoz Magyarország is csatlakozott. A kampánnyal összefüggő feladatokat, valamint az érintett nemzeti és uniós felekkel való kapcsolattartást és egyeztetést a Nemzeti Kibervédelmi Intézet (NKI) látja el. Az NKI célja, hogy az információbiztonsággal foglalkozó kormányzati és nem kormányzati cégeket, egyetemeket, iskolákat, szervezeteket bevonja a kampányba, és ezen együttműködés keretében minél szélesebb réteget sikerüljön megszólítani a kiberhónap során. Ez a kampány egyedülálló lehetőséget nyújt a köz- és magánszféra szereplőinek együttműködésére irányuló kezdeményezések megindítására. Európai kiberbiztonsági hónapról és az NKI megbízásából elkészült letölthető IT biztonságot érintő tematikus tájékoztatók megtalálhatóak: https://kiberhonap.hu/kampanyrol.

8.4. Elkerülhető-e a „digitális mohács”?

VÍZIÓ: „A kiberdzsihádot az al-Kaida támadásával indítanák, amihez képest a Világkereskedelmi Központ lerombolása gyerekjátéknak tűnik majd. Dollármilliárdos vagyonokat semmisítünk meg, megbénítjuk az internetet, amelytől annyira függ a nyugat; árvizeket indítunk, leállítunk és megsemmisítünk erőműveket; atomerőműveket is. Sok repülőgép lezuhan. Millió és millió számítógép egyszerre és mindenkorra tönkremegy, azok is, amelyeken a nyugdíjak adatai vannak. Hatalmas mennyiségű kulcsfontosságú adat vész majd el.” (2011. március 15. kedd: Mark Russinovich – Zero Day)

VALÓSÁG: „Már 74 ország intézményeit érinti a pénteken indult zsarolóvírusos támadáshullám, ami a brit egészségügyi rendszer összeomlásával kezdődött. Rossz kezekbe kerülve pusztított csak igazán az amerikai titkosszolgálat (NSA) által kifejlesztett szoftveres kártevő, amely már 99 országban bénított meg számítógépeket. Az érintett felhasználók száma gyorsan nő, egy zsarolóvírus van a háttérben. A WannaCry és más, hasonló neveken támadó rosszindulatú program 300 dollárért cserébe szabadítja fel a blokkolt számítógépet. Egy külföldi portál értesülései szerint magyar érintettség is van, a Telenornál pénteken kikapcsoltatták a dolgozók számítógépeit. Az eddigi hírek szerint a pár napja útjára indult világméretű kibertámadás (WannaCry zsarolóvírus) több mint 230.000 számítógépet fertőzött meg 150 országban, itthon is óráról órára bővül az érintettek száma. Az eddigiektől eltérően a mostani kártevő már önmagától is képes terjedni. Egy új trend megjelenése látható, ez a Ransomware of Things (RoT), ami azt jelenti, hogy a kiberbűnözők feltörik eszközeinket, majd váltságdíjat követelnek az eszközök blokkolásának feloldásáért. Az előrejelzések alapján további fenyegetések várhatók és még indokoltabb az elektronikus információs rendszereink védelmének megerősítése.” (2017. május 12. péntek: Gigászi kibertámadás)

Hazánk is számos olyan infrastruktúrával rendelkezik, amelyek a mindennapi életben – a gazdaságtól kezdve a politikán át a mindennapi emberek életéig – nélkülözhetetlenek. Kritikus információs infrastruktúráink mindenhol megtalálhatóak. Csak néhány példa: villamosenergia-rendszer irányítása, banki és pénzügyi számítógépes hálózatok, vezetékes és mobil kommunikáció, egészségügyi informatikai rendszerek. Az nem újdonság ma már senki számára, hogy ezek a rendszerek (is) sérülékenyek, támadhatóak. Ugyanakkor nem látunk olyan határozott lépéseket, amelyek ezek komplex védelmére irányulnának. Gyakran mondogatjuk: nekünk egy Mohács kell, hogy felfogjuk, valóban veszélyben vagyunk! Ha ez a Mohács az információs infrastruktúrák területén jelentkezik, akkor bekövetkezhet egy „Digitális Mohács”, azaz egy olyan informatikai-információs katasztrófa, amelyek

következményei mindannyiunkat el fognak érni (Kovács-Krasznay, 2010, 1. old.).

Az alábbi Kevin D. Mitnick legendás hacker szavai is felhívják a figyelmet arra, hogy a támadásokkal szembeni védekezés legfontosabb eleme azoknak a képzése, akik használják, adminisztrálják, üzemeltetik és felelősek az elektronikus információs rendszerekért és létfontosságú információs rendszerelemekért.

„Vállalatok dollármilliókat költhetnek tűzfalakra, titkosításra és biztonságos hozzáférést biztosító eszközökre, de mindez kidobott pénz, mivel egyik intézkedés sem foglalkozik a leggyengébb láncszemével a biztonsági láncnak: ez pedig az ember, aki használja, adminisztrálja, üzemelteti és felelős ezen rendszerekért, amin védett információk találhatóak."

Vezetői interjú:
Dr. Krasznay Csaba
Nemzeti Közszolgálati Egyetem
Kiberbiztonsági Akadémia programigazgató

Kérdés: Mi a célja „Digitális Mohács" tanulmánynak?
Válasz: A tanulmány azokat a rendszereket kívánja bemutatni, amelyek a leginkább támadhatóak hazánkban, és a leginkább sérülékenyek egy összehangolt információs támadás esetén. A cél az, hogy felhívjuk a figyelmet arra, hogy hazánk is komoly veszélyben van, amelyet nem lehet túldimenzionálni.
Kérdés: Mi a célja „Digitális Mohács" 2.0 tanulmánynak?
Válasz: Életünk, legyen szó politikáról, gazdaságról vagy éppen kultúráról, nagyban függ azoktól az információs rendszerektől, amelyek sokszor láthatatlanul vannak jelen mindennapjainkban. Ugyanakkor egy-egy informatikai vagy kommunikációs rendszer kiesése, részleges vagy teljes működésképtelensége azonnal ráirányítja a figyelmet ezekre az infrastruktúrákra. 2009-ben „Digitális Mohács" címmel egy elképzelt forgatókönyvet vázoltunk fel annak bizonyítására, hogy szándékos támadások sorozatával valóban lehetséges-e komoly károkozás egy olyan, viszonylag fejlett infrastruktúrával rendelkező ország esetében, mint hazánk. Az azóta eltelt időben egy sor kormányzati lépés és számos jogszabály született, amelyek infrastruktúráink védelmének jogi és szervezeti alapjait hivatottak megteremteni. Ezért itt az idő, hogy megvizsgáljuk, ma mi a véleményük a szakembereknek, elegendők-e az eddigi lépések a védelem megteremtése érdekében. Így egy új forgatókönyvet vázoltunk fel, amelynek egyes lépéseit a szakemberek elé tártuk, és megkérdeztük, mit tennének az adott támadások esetén.
Kérdés: Elkerülhető-e egy kibertámadás Magyarország ellen?
Válasz: Mindezeknek megfelelően olyan – az elmúlt években már számos alkalommal elhangzott, de sajnos továbbra is érvényes – általános, a védelmet növelő, de eltérő módszereket kell hangsúlyoznunk, mint például az információbiztonsági tudatosság növelése, amelyet az egyébként szintén fejleszteni szükséges kibervédelmi szervezetek feladatául is kell szabni. További védelmi megoldást kell jelenteniük – függetlenül a gazdaságossági megfontolásoktól – az alternatív, vészhelyzetben is működő infrastruktúráknak, vagy legalábbis ezek egyes elemei kiépítésének, fenntartásának. Mindezeken túl továbbra is hangsúlyoznunk kell a koordinált, centralizált védelem eszközrendszerének erősítésére tett megoldásokat. Ezt igazolja az az eredményünk, mely szerint a felvázolt forgatókönyvben szereplő támadások intenzitásával növekszik a szakemberek igénye a központi (állami) incidenskezelésre, mely során a különböző támadások kezelésében a szakma a Nemzeti Kibervédelmi Intézet szerepét kiemelt jelentőségűnek látja. Ugyanakkor a szervezetrendszer erősítése megköveteli, hogy a közigazgatás, a piaci szereplők, valamint az akadémiai szféra a már megkezdett – a kiberteret és az ott elvárt biztonságot fő kérdésként tárgyaló – párbeszéde folytatódjék.
Kérdés: Miért fontos a kiberbiztonsági képzés?

Válasz: A kiberbiztonság fontosságát mutatja, hogy napi szinten jelennek meg sajtóhírek hackertámadásokról a hazai és a nemzetközi sajtóban, így a kibervédelem kérdése egyre égetőbbé válik a nemzetállamok számára. Az elmúlt években a magyar kormány is számos erőfeszítést tett ezen a területen, ennek egyik fontos része a kiberbiztonsághoz kapcsolódó gyakorlatok szervezése, melynek felelőse a Nemzeti Kibervédelmi Intézet. A 2018. január 18-án megtartott egynapos kibervédelmi gyakorlat, melyen több állami és nem állami partner is részt vett. Az esemény célja a kommunikációs csatornák és a sajtóval való kapcsolattartás tesztelésén túl a kibertérből érkező incidensek elemzésének gyakorlása volt. A gyakorlat elsődleges célja az volt, hogy egy komplex, incidenskezelési és technikai szempontból is érdekes és tanulságos, célzott jellegű hacktivista támadás szimulálásán keresztül a résztvevők begyakorolják saját eljárásrendjüket – kiemelten az incidenskezelés vonatkozásában –, valamint teszteljék meglévő kommunikációs csatornáikat és a sajtóval való kapcsolattartást egyaránt. Ez utóbbi érdekében egy zárt hírportál is elkészítésre került, ahol folyamatosan frissültek a sajtóhírek (valós napi hírek között „rejtettük„ el a gyakorlathoz kapcsolódó cikkeket) a gyakorlat napján, valamint minden intézmény kapott írásos, illetve telefonos sajtómegkeresést is. Továbbá meg kell említeni, hogy az információbiztonsági képzések és a továbbképzések szervezése elsősorban a Nemzeti Közszolgálati Egyetem (NKE) feladata. A 2013-ban megszülető információbiztonsági törvény alapján kezdődött meg a szervezeti vezetők, szakértők, közreműködők és dolgozók képzése, az NKE-n eddig már mintegy 150-en végezték el sikeresen a kurzusokat. A 2017. márciustól működő Kiberbiztonsági Akadémia feladata, hogy az NKE egyes karainak, kutatóintézeteinek, műhelyeinek már meglévő erőforrásait összehangolják, a kiberbiztonsági kutatásokat, szakembereket támogassák. Képzési programokat kezdeményeznek, szerveznek, kiberbiztonsági gyakorlatokat is terveznek. Az akadémia célja, hogy a közszolgálat, a rendvédelem és a honvédelem területén is katalizátorként működjön a kiberbiztonsági képzésben. Az Elektronikus információbiztonsági vezető szakirányú továbbképzési szakhoz kapcsolódó tananyagok letölthetőek: https://vtkk.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/tananyagok.

8.5. Mellékletek

1. melléklet: Célzott támadások anatómiája

	Lépés	Tevékenység
1.	Intelligens felderítés (Intelligence Gathering)	Az első lépés során a támadó elsősorban nyilvános forrásból információkat gyűjt a leendő áldozatról, általában, mint szervezetről, illetve az ott dolgozó munkatársakról. Az információk összegyűjtésével, a szervezet és alkalmazottainak a felderítésével előkészítheti az egyedi, testreszabott támadást.
2.	Bejutás (Point of Entry)	Egy támadás során a támadó a kártékony kódjának bejuttatására több módszer közül is választhat. A lehetőségeket azonban két lényeges csoportba oszthatjuk: egyrészt azokra a bejutási formákra, melyek nem igényelnek felhasználói interaktivitást, illetve azokra, amelyeknek szükségük van a felhasználó beavatkozására.
3.	C&C kommunikáció (Command and Control (C&C) Communication)	Amennyiben a támadó sikeresen bejuttatta a kiszemelt környezetbe a kártékony kódját, a következő lépés során a támadó irányítása alá vonja a megtámadott eszközöket. Ennek érdekében egy saját C&C szerver állít fel, melyen keresztül a megtámadott számítógépeket irányíthatja: parancsokat adhat, állományokat tölthet le és fel.
4.	„Oldalazó mozgás" (Lateral Movement and Persistence)	A bejutás és a sikeres kapcsolatfelvételt követően a támadás következő lépésében a helyi hálózaton belüli további számítógépek és eszközök felderítése, majd az azokba történő behatolás következik. Ennek a célja, hogy további hozzáférési adatokat szerezzen meg, növelje a privilégium szintet, illetve, hogy biztosítsa a hálózat folyamatos felügyeletének a lehetőségét.

5.	Értekes adatok, információk felderítése (Asset/Data Discovery)	A belső hálózaton történő terjedés során a támadó célja nem egyszerűen más számítógépek és eszközök felderítése, hanem ezeken az eszközökön tárolt értékes adatok és információk elérését biztosító szerverek és szolgáltatások azonosítása is.
6.	Adatok kiszívárogtatása (Data Exfiltration)	Miután az érzékeny adatokat, információkat a támadó azonosította, az adatokat általában először egy olyan belső számítógépre juttatja el, ahol egy elsődleges elemzés, válogatás és tömörítés történik, majd az így összeállított információk kijuttatása egy külső szerverre, amelyet a támadó közvetlenül elér.

2. melléklet: Célzott támadások kihívásaira a védelmi intézkedések lehetőségei

	Kihívás	Védelmi intézkedések
1.	Láthatóság (Visibility)	A hálózati forgalomfigyelés a legtöbb biztonsági elemző és szakértő által javasolt proaktív kockázatkezelési stratégia alapja.
2.	Érzékelés (Detection)	Célzott támadások felderítése a sandbox szimuláció és a fenyegetés-észlelési szabályok alkalmazásával.
3.	Kockázatértékelés (Risk Assessment)	Automatizált helyi fenyegetéselemzés és a releváns teljes szervezeti fenyegetéselemzés együttes alkalmazása.
4.	Megelőzés (Prevention)	Egyéni védelmi megoldások alkalmazása.
5.	Kármentesítési (Remediation)	A mélyreható fenyegetésprofilok segítenek az elszigetelési és kármentesítési lépéseknek, és lehetővé teszik a speciális eszközök és a SIEM vagy más naplóelemzési módszerek optimális használatát a támadás teljes terjedelmének meghatározásához és a támadás részletes igazságügyi elemzéséhez.

8.6. Irodalomjegyzék

- Budai, B. (2009): Az e-közigazgatás elmélete. Akadémiai Kiadó, Budapest, 1–474. oldal.
- ESET (2017): Trends 2017: Security Held Ransom. Elérhetőség: https://www.welivesecurity.com/wp-content/uploads/2016/12/ESET-Trends-2017-security-held-ransom.pdf (utolsó letöltés: 2018. január 7.)
- Haig, Zs. – Kovács, L. – Ványa, L. (szerk.) (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák: tanulmány. Budapest: Nemzeti Közszolgálati Egyetem, 2012. 1–298. oldal.
- Katasztrófavédelmi Oktatási Központ (2013): Létfontosságú Rendszerek és Létesítmények Védelme. Elérhetőség: http://kok.katasztrofavedelem.hu/letoltes/document/document_218.pdf (utolsó letöltés: 2018. január 10.)
- Kovács L. – Krasznay, Cs. (2010): Digitális Mohács Kibertámadási Forgatókönyv Magyarország Ellen. Elérhetőség: http://m.ludita.uni-nke.hu/repozitorium/handle/11410/1013 (utolsó letöltés: 2018. február 17.)
- Kovács L. – Krasznay, Cs. (2017): Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. Elérhetőség: http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf (utolsó letöltés: 2018. február 20.)
- Krasznay, Cs. (2009): Web service fenyegetések e-közigazgatási környezetben, Nemzeti Információs Infrastruktúra Fejlesztési Intézet (NIIFI), Budapest, 2009. 1–12. oldal.
- Leitold, F. (2014): Biztonsági Technológiák Alkalmazása. Budapest: NKE Vezető- és Továbbképzési Intézet. 1–41. oldal.

- Michelberger, P. – Lábodi, Cs. (2012): Vállalati információbiztonság szervezése. In Nagy Imre Zoltán (szerk.), Vállalkozásfejlesztés a XXI. században II. Tanulmánykötet, Óbudai Egyetem. 241–302. oldal.
- Muha, L. (2007): A Magyar Köztársaság információs infrastruktúráinak védelme. Doktori (PhD) értekezés. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem. 1–127. oldal.
- Muha, L. (szerk.) (2008): Informatikai Biztonság Irányításának Vizsgálata (IBIV) Budapest: Miniszterelnöki Hivatal (MEH), 2008. 324. oldal. (Közigazgatási Informatikai Bizottság ajánlásai; 25.) 1–3., Magyar Informatikai Biztonsági Ajánlások. Elérhetőség: https://ugyintezes.magyarorszag.hu/dokumentumok/kib25mibik.pdf (utolsó letöltés: 2018. január 26.)
- Muha, L. – Krasznay, Cs. (2014): Az elektronikus információs rendszerek biztonságának menedzselése. Budapest: NKE Vezető- és Továbbképzési Intézet. 1–120. oldal.
- Rajnai, Z. – Fregan, B. (2016): Kritikus infrastruktúrák védelme. In: Bitay Enikő (szerk.) A XXI. FMTÜ előadásai: Proceedings of the XXI-th International Scientific Conference of Young Engineers. 2016. 349–352. oldal.
- Répás, S. – Dalicsek, I. (2015): Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében. Budapest: A NKE állam- és közigazgatás-tudományi szakmai folyóirata 2015. 4. 22–33. oldal.
- SaveAs Kft. (1999): Esettanulmány egy felfedezett poloska programról. 1–18. oldal.
- Symantec (2017): Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders. Elérhetőség: http://www.symantec.com/content/de/de/about/downloads/press/WP_Organizational_Security_and_the_InsiderThreat_Malicious_Negligent_and_Well-Meaning_FINAL.pdf (utolsó letöltés: 2018. január 7.)
- Szabó, Zs. M. (2017a): A nyugdíjfolyósítás információbiztonsági és informatikai biztonsági kérdései. In: Bitay Enikő (szerk.) A XXII. FMTÜ előadásai: Proceedings of the XXII-th International Scientific Conference of Young Engineers. 2017. 363–366. oldal.
- Szabó, Zs. M. (2017b): A nyugdíjfolyósítás kiberbiztonsági kérdései. In: Ács K. – Bódog F. – Mechler M. – Mészáros O. – Pónusz R. (szerk.) VI. IDK2017. Pécs: Tanulmánykötet 507–517. oldal.
- Szabó, Zs. M. (2018c): A nyugdíjfolyósítás mint kritikus infrastruktúra. In: Bitay Enikő (szerk.) A XXIII. FMTÜ előadásai: Proceedings of the XXIII-rd International Scientific Conference of Young Engineers. 2018. 215–218. oldal. Budapest: NKE Vezető- és Továbbképzési Intézet. 1–68. oldal.
- Trend Micro (2014): The Custom Defense Against Targeted Attacks, A Trend Micro White Paper. Elérhetőség: https://www.trendmicro.de/cloud-content/us/pdfs/business/white-papers/wp_custom-defense-against-targeted-attacks.pdf (utolsó letöltés: 2018. január 8.)

9. GYARAKI RÉKA: BELSŐ MUNKATÁRSAK JELENTETTE KOCKÁZATOK A CÉLZOTT INFORMATIKAI TÁMADÁSOKBAN

9.1. Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban

Ahogyan egy szállóigévé vált mondás tartja: „A leggyengébb láncszem mindig az ember". Még akkor is tartja magát ez a nézet, amikor a XXI. században egyre nagyobb szerep jut az informatikának és az informatikai eszközöknek, amelyek segítségével a kommunikáció, az ügyintézés, a közszférában a különböző szolgáltatások elérése, a vásárlás, az áruk kifizetése stb. lényegesen egyszerűbbé vált.

Ugyanakkor annyira megszoktuk ezek jelenlétét és használatát, természetesen kezeljük önmagunk jelenlétét a virtuális térben, hogy elfelejtkezünk arról, hogy odafigyeljünk a fokozott biztonságra, adataink megvédésére.

A köz-és magánszféra azért, hogy hatékonyabban tudjon működni, igyekszik egyre több és jobb minőségű IT eszközt beszerezni, valamint adataik védelme érdekében szerencsére törekszenek egyre nagyobb hangsúlyt fektetni az informatika biztonságra és a fizikai védelemre is.

Sajnos ez azonban legtöbbször nem elegendő, amikor a munkavállalók a biztonsági előírásokat szándékosan vagy gondatlanságból megszegik, amikor tetteik következményeit látják vagy nem látják előre, de kiteszik magukat és munkaadójukat (beleértve azok informatikai rendszereit) támadásnak, vagy épp saját maguk követik el a támdást.

9.1.1. Mit értünk kockázat alatt?

A kockázat tulajdonképpen „a fenyegetettség mértéke, amely […] egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye"[183].

A célzott informatikai támadások esetében a legnagyobb kockázatot az azt használó és felhasználó személyek jelentik akár a fizikai-, akár a pszichológiai támadás során, vagy amikor bármilyen természeti csapás miatt sérülnek meg az informatikai eszközök, esetleg az információs rendszerek, hiszen abban is szerepet játszhat az emberi hanyagság, a hozzá nem értés.

A kibertámadások célja a rombolás, pénzszerzés, az informatikai rendszer hozzáférhetetlenné tétele, a rendszerben tárolt adatok megszerzése, megismerése, nyilvánossá tétele, esetleg megváltoztatása, az üzleti partnerek vagy elbocsátott vagy a meg nem fizetett, elégedetlen munkatársak bosszúja, figyelemfelkeltés, politikai véleménynyilvánítás stb.

A felsorolt célok célpontjai úgy az üzleti élet is (kisebb vagy nagyobb vállalatok, cégek, non-profit szervezetek – továbbiakban szervezetekként), mint a kormányzati szervek, a kritikus infrastruktúrák, de ugyanúgy a magánszemélyek számítógépei, informatikai eszközei és az azokon tárolt adatok és információk is lehetnek.

A kibertámadásokért nemcsak az eszköz és a rendszer tehető felelőssé, hanem az azt kezelő, használó, alkalmazó személyek és munkatársak is.

Gyors említésként a támadások miatt felelőssé tehető – motivációként megjelenő – általánosságban tehát az emberi mulasztás, a hanyagság, a szakértelem hiánya, a bosszú, figyelemfelkeltés, de bizonyos esetekben politikai vagy vallási motiváció is.

---

[183] Muha Lajos, Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése, NKE, Budapest.

9.1.2. A kibertámadások során leggyakrabban használt rosszindulatú programok:

- Vírusok
- Kémszoftverek
- Spam vagy kéretlen levelek
- Keyloggerek
- Kéretlen reklám programok
- Botnetek
- Trójai vírusok
- Adathalászat (Phising)
- Férgek
- Kevert fenyegetések

Ezen fenyegetések célja lehet többek között adat és/vagy pénzszerzés, a másik fél/felek számítógépes hálózatainak működésképtelenné tétele, esetleg a konkurens cégek, vállalatok, üzleti ellenfelek információinak, pénzügyi- és befektetésre vonatkozó terveinek megismerése, azok kiszolgáltatása másik fél részére vagy üzleti partnerei előtt történő ellehetetlenítése.

9.1.3. Adatok, információk

A XXI. században, az információs társadalomban az információ értéke magasabb az arany értékénél. Különösen szívesen árulják, adják és veszik ezeket az internet sötét oldalaként aposztrofált Dark Weben.

Az értékesítendő adatok megszerzése illegális forrásból történik, ami köszönhető a nem megfelelően kezelt adatoknak, jelszavaknak és a gyenge védelmi rendszereknek.

A 2013. évi L. törvény alapján *az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.*[184]

Az adatvédelem fogalma: *a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.*[185]

A munkavégzés során keletkezett adatok között (is) különbség tehető aszerint, hogy:

- Tartalmaz-e személyes adatot? A 2011.évi CXII. törvény[186] szerint személyes adatnak minősül „*az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés”*[187]

- Tartalmaz-e különleges adatot: *a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat,*[188]

- Az adat a 2009. évi CLV. törvény (a minősített adatok védelméről szóló törvény Mavtv.) hatálya alá tartozik-e és ha igen, milyen minősítési szinten van

184 2013. évi L. törvény 1.§ (1) bekezdés Értelmező rendelkezések.
185 Lásd: https://www.naih.hu/adatvedelmi-szotar.html (letöltve: 2018. március 01.)
186 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (röviden Infotv.).
187 Infotv. 3.§ (2) pontja.
188 Infotv. 3.§ (3) pontja.

A felsorolt adatokkal kapcsolatban annak készítésére, tárolására, megismerésére, hozzáférhetővé tételére, megsemmisítésére vonatkozóan eltérő szabályok vonatkoznak, ugyanakkor illetéktelenek számára azok megismerésével kapcsolatban más-más érdek fűződik, valamint a vonatkozó szabályok be nem tartására eltérő büntetőjogi vonatkozások vannak[189].

A fent említett felsorolás alapján a támadások rejtette veszélyek:

Vírusok

A támadó kártékony programmal próbálja megfertőzni a rendszert, amelyet akár egy kéretlen levélben vagy félrement levélként, annak csatolmányába továbbít. A felhasználók sokszor még a legnagyobb körültekintés ellenére is megnyithatnak egy vírust tartalmazó fájlt, amely akár azonnal vagy akár bizonyos idő után okoz kárt, amellyel az informatikai eszközön található dokumentumok, de lehet, hogy a vállalat rendszere válik használhatatlanná, esetlegesen a tárolt adatok, információk jogosulatlanok számára hozzáférhetővé.

Sokszor a munkavállalók saját kényelmük érdekében az általuk használt irodai eszközökre telepítik azokat a programokat (Skype, Viber, Facebook stb) amelyeket otthon is alkalmaznak és megnyitva hagyják a folyamatos virtuális térben történő aktivitásuk érdekében. Ezzel lehetőséget teremtenek – persze sok egyéb, így jelszavuk ellesése mellett – arra, hogy vírus vagy trójai program kerüljön az eszközre vagy az irodai rendszerbe.

Férgek

A számítógépes férgek olyan kártevők, amelyek a hálózatok hibáit, vagy hiányos biztonsági beállításait használják ki és ezáltal sokszorosítják önmagukat. Sok esetben a számítógép memóriáját vagy a rendszer kapacitását csökkenti, vagy biztonsági szempontból olyan backdoort nyit meg, amelynek segítségével a válallatok, a közszféra információbiztonságát veszélyeztetik.

Kéretlen reklámlevelek

Bár a kéretlen levelek nem mindig jelentenek kockázatot, ugyanakkor vezethetik a felhasználót olyan weboldalra, amely illegális, hamis termékeket árul, valamint a gyanútlan felhasználó kiadhatja azokat az adatait, amelyekkel a későbbiekben visszaélhetnek.

Adathalászat (Phising)

Az adathalászat leginkább a magánszférában okoz felbecsülhetetlen anyagi károkat, de a közszférában is informatikai rendszerek terjedésével egyre gyakoribb támadási forma. Az adathalászok a weboldalak segítségével, megtévesztéssel, jogtalan behatolással szerzik meg a felhasználók adatait, jelszavait stb, azért, hogy azokkal a későbbiekben vissza tudjanak élni.

Gyakori megjelenési formája, hogy a felhasználót saját bankjának nevében keresik meg e-mailben, amelyben akár adatokat, belépési jelszót, kódot kérnek vagy elirányítják egy, a bank honlapjához megszólalásig hasonló oldalra, ahol az ügyfél gyanútlanul megadja a kért információkat, amelyekkel aztán megkárosítják.

Az adathalászattal együtt említhető a keylogger vagy leütésnaplózás, amelyhez egy trójai programmal a felhasználó nevét és jelszavát szerzik meg, úgy, hogy a trójai naplózza a leütéseket.

[189] A büntetőjogi szabályozással kapcsolatban a fejezet végén térek ki részletesen.

9.1.4. Munkaviszonnyal kapcsolatos kockázatok

A belső munkatársakkal kapcsolatban először is a vonatkozó jogszabályok, majd azt követően az információvédelemmel és információbiztonsággal és információvédelemmel kapcsolatos regulációk ismertetése történik.

A munkaviszonnyal kapcsolatos kockázatok közül beszélhetünk:

- Belső policyt megsértő eseményekről
- A törvényi rendelkezéseket megsértő események, amelyeknek munkajogi, polgárjogi és büntetőjogi következményei lehetnek
- Adatvédelmi szabályok megsértéséről

A kockázatokkal kapcsolatban külön kell szólni a jogszabályok és azok alapján megalkotott belső szabályokról mind a munkavállaló mind pedig a munkáltató (a főnök, vezető) tekintetében, hiszen a kötelezettségek, felelősségek vonatkozásában is eltérés van.

Munkavállaló

A munkavállaló fogalmát a 2012. évi I törvény, a Munka Törvénykönyve (továbbiakban Mt.) határozza meg. Így munkavállalónak tekinthető az a természetes személy, aki munkaszerződés alapján munkát végez. Így minden 16. életévet betöltött személy, aki jogviszony formájában, díjazás fejében elvégzi a munkát.

9.1.5. A munkavállalók által jelentett kockázatok

A munkavállalók – vagyis a munkaviszonnyal kapcsolatos – jelentett kockázatok többek között a belső policyt megsértő események. Azaz, amikor a munkáltató a belső szabályzatában előír olyan kötelezettségeket, amelyek a munkavállalóra kötelezőek, de azok nem kerülnek betartásra. Ezek a proaktív biztonsági előírások

Ilyen kötelezettség például a „céges" e-mail fiókok kezelésével vagy a kimenő és beérkező elektronikus levelek törlésével, tárolásával kapcsolatos előírások.

Ugyanennyire fontos a már említett, úgynevezett „clean desk policy", azaz a „tiszta asztal policy". Ez egy olyan biztonságpolitikai előírás, amelynek betartása, vagyis az íróasztalon a jogosulatlan hozzáférés és információszerzés stb. miatt szükséges bevezetni.

Az egyik általános problémát jelent a felhasználónevek és jelszavak hanyag kezelése, amelyről a későbbiekben részletesen szó lesz, de ugyanilyen kockázati tényező a közösségi oldalak nem megfelelő alkalmazása, a biztonsági előírások be nem tartása vagy vállalati szinten azok hiánya.

9.1.6. Munkavállaló felelőssége

A célzott informatikai támadások esetében a munkavállaló felelőssége nem zárható ki, sem a szándékos, sem pedig a súlyos gondatlanságból okozott károkozás esetében. A munkavállaló felelősségének kérdésével kapcsolatban többek között a Munkatörvénykönyve, valamint egyes esetekben a munkavállalóra vonatkozó speciális ágazati törvények (így a kormánytisztviselő esetében a 2010. évi LVIII. törvény, közalkalmazottakra az 1992. évi XXXIII. törvény, a hivatásos jogviszonyban álló személyekre a 2012. évi CCV. törvény,[190] a rendvédelmi feladatokat ellátó személyekről a 2015. évi XLII. törvény[191] stb.) irányadó rendelkezéseiket kell alapul venni, azaz a munkaviszonyból származó

[190] A honvédek jogállásáról szóló törvény.

[191] A rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati viszonyáról (Hszt.).

kötelezettségének megszegésével okozott kárt köteles megtéríteni, ha nem úgy járt el, ahogy az az adott helyzetben általában elvárható. Ugyanakkor a kárt a munkáltatónak kell bizonyítani.[192]

Szándékos károkozásról (azaz, amikor a célzott támadást belső munkavállaló) akkor beszélünk, amikor a kár bekövetkezését a munkavállaló egyértelműen kívánta (szándékosan telepítette a vírust az informatikai eszközre) vagy pedig abba belenyugodott (a rendszergazda azért, hogy pénzt spóroljon, nem jogtiszta szoftvert telepített fel a munkavállalók eszközeire).

A magán-és közszférában dolgozó munkavállalók felelősek a személyes használatukban lévő számítástechnikai eszközökért, ezért ezek használatát a munkavégzésre és belső- valamint ügyfelekkel történő kommunikációra célszerű használni. A belső szabályozásnál fontos, hogy az eszközök védelméről (azok megvásárlása, a licencek megszerzése, folyamatos frissítése stb.) a munkaadó feladata, a munkavállaló kötelezettsége, hogy a vírusírtó, a tűzfal védelmet nem kapcsolhatja ki.

9.1.7. Jellemzően felmerülő problémák

1. Jelszavak ellesése (observing passwords attack)

A felhasználónevek és jelszavak ellesése a belső policy, a clear desk és az Informatikai Biztonsági Szabályzat (IBSZ) megsértésének következménye lehet. Ebben az esetben a jelszavak megszerzése nem jelszófeltöréssel történik, hanem amikor a felhasználó (jogosult) a belépéshez szükséges kódokat látható helyen tárolja, ami lehetőséget teremt arra, hogy azt bárki – így kolléga is megismerje –, vagy amikor a jelszó beírását egy másik személy például személyesen, illetve kamerán keresztül látja. Jelszó ellesésére alkalmasak azonban az olyan szoftverek is, amelyek rögzítik a billentyűzet leütését is. (Ebben az esetben leginkább a rendszergazda felelőssége merül fel.)

Amennyiben a jelszó és a felhasználónév jogosulatlanul megszerzik, úgy a belső rendszerhez vagy levelezéshez történő hozzáférés lehetséges.

2. Rossz vagy gyenge jelszavak vagy azok tárolása

Az Informatikai Biztonsági Szabályzatok és ezzel a rendszerek úgy vannak beállítva, hogy a jelszó legalább 8 karakter legyen, tartalmazzon nagy- és kisbetűket és számot. Ugyanakkor annak megadásakor a felhasználó már nem figyel, hogy az ne legyen hozzá köthető, sem a kollégák, sem egy kívülálló számára.

Leggyakoribb problémák:

- Amennyiben számot is tartalmaz, úgy azt mindig a jelszó végére szokták tenni, ami általában – ha havonta kell változtatni – az adott hónap, valamelyik családtag születési hónapja vagy napja, vagy családi esemény (például házasságkötés vagy évforduló hónapja vagy napja).
- A betűkből álló jelszó esetében szintén a könnyen megjegyezhetőségre törekszenek, így családtag neve, háziállat neve vagy esetleg a felhasználó saját családi- vagy keresztneve.
- Amennyiben jelszógeneráló programot használnak, akkor engedik, hogy a generált jelszót a rendszer megjegyezze vagy egy erre rendszeresített füzetbe feljegyzik, netalántán egy papírfecnire vagy post it-re felírják, és a számítógép közelében (fiókban, íróasztalon) vagy a monitorra felragasztva tárolják.

3. Adathordozók nem megfelelő kezelése

Ma már munkavégzés során külsőadathordozók (így pendrive, DVD stb.) használata csökken a sérülékenysége miatt. Ugyanakkor a tiltások ellenére a munkavállalók számára mindig is csábító tény,

[192] 2012. évi I. törvény a Munka Törvénykönyvéről (Mt.) 179.§ (1) bekezdés.

hogy a magáncélra (így akár tanuláshoz vagy hozzátartozó számára) olcsóbb a munkahelyen történő fénymásolás, nyomtatás, mint otthon vagy az ezzel foglalkozó vállalkozásoknál. Ehhez gyakori, hogy saját vagy nem ellenőrzött forrásból és védelem nélküli adathordozókra mentve, azt a munkahelyi eszközök igénybevételével nyomtatják ki, amivel nemcsak bűncselekményt valósítanak meg (Btk. 372.§ sikkasztás tényállása, hiszen sajátjaként rendelkezik a nyomtatóval és a papírral), hanem- amennyiben kijátsza azt, hogy külső adathordozó nem csatlakoztatható a számítógéphez, még a vállalat informatikai rendszerét is veszélynek teheti ki.

Mit is értünk adathordozó alatt? Minden olyan anyagi eszköz, mely alkalmas adatok megőrzésére, tárolására. Az Európai Parlament és a Tanács 2002/65/EK irányelve[193] szerint, amely már *tartós adathordozóként* nevesít: „*olyan eszköz, amely lehetővé teszi a fogyasztó számára a személyesen neki címzett adatoknak a jövőben is hozzáférhető módon és az adat céljának megfelelő ideig történő tárolását, valamint a tárolt adatok változatlan formában történő megjelenítését”.* Így adathordozó a pendrive, a DVD, CD, SSD kártya, amely alkalmas kisebb vagy nagyobb adatok tárolására. Ezeken a hordozókon tárolt adatok többek között lehetnek magánszemélyhez kapcsolódó – így videó- és hangfájlok, fényképek és a személyes adatok körébe tartozó információk is[194].

A fent említett problémán kívül további kockázatot rejthet az úgynevezett „Home office[195]” sajátos értelmezése, amikor saját számítógépére vagy adathordozójára mindenfajta védelem nélkül menti le a dokumentumokat, hogy azt az irodán kívül, otthon elkészítse.

Mivel a természetes személyek által használt adathordozókon előfordulhat, hogy olyan adatok, információk is találhatóak, amelyek tartalmazhatnak személyes-, különleges-, netalántán minősített adatokat, amelynek védelme akár nemzetbiztonsági vagy bűnüldözési érdekeket sérthet vagy veszélyeztethet[196], így azok illetéktelen számára történő megismerése, hozzáférhetővé tétele- annak fényében, hogy például a minősített adatok tárolásával kapcsolatos szabályokat is megszegte- büntetőjogi felelősségre vonás is felmerül.

4. Eszközök, adatok selejtezése, megsemmisítése

A technika fejlődésének és eszközökre történő pályázati lehetőségeknek köszönhetően – főleg a magánszektorban – igyekeznek a legmodernebb IT eszközöket beszerezni, így az elavultnak minősített számítógépeket, informatikai eszközöket értékesítik, leselejtezik vagy ingyen továbbadják. Gyakori hiba ugyanakkor, hogy a rajtuk lévő adatokat, dokumentumokat nem vagy nem megfelelően törlik, így azok a későbbiekben visszanyerhetőek.

Ugyanez a probléma a kukába dobott adathordozókkal – DVD, CD, elrontott nyomtatványok, roszszul sikerült fénymásolás miatt feleslegessé vált dokumentumok, feljegyzések, számlák, jelszavak stb – esetében is. A hanyagság (negligentia[197]) miatt, vagyis nem iratmegsemmisítővel vagy egyéb végleges törlésre alkalmas lehetőség nélkül, válnak megismerhetővé a kényes iratok.

---

193 a fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról (forrás: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32002L0065) letöltve: 2018. március 12.

194 Személyes adatnak minősül.

195 Home Office: amikor valaki az irodai munkáját nem a munkahelyén, a cég irodájában végzi el, hanem **otthonról dolgozik**, a saját lakásában lévő íróasztalon, számítógépen, az elkészült produktumokat, feladatokat pedig valahogy bemutatja, dokumentálja feletteseinek. (letöltve:https://www.cvonline.hu/blog/2017/karriertanacsok/ismerd-meg-a-home-office-t-munka-otthonrol/15072 ,2018.03.20)

196 https://www.telegraph.co.uk/news/2017/10/29/heathrow-investigates-queens-security-details-found-usb-drive/letöltve: 2018. március 12.

197 Negligentia vagy hanyag gondatlanság: az elkövető nem látja előre magatartásának lehetséges következményeit, mert elmulasztja a tőle elvárható körültekintést.

5. Pszichológiai befolyásolás

A pszichológiai befolyásolás egyik legismertebb elnevezése a social engineering. A támadások leggyakrabban megvalósuló formái:

- tett láb: a támadó jelentéktelennek tűnő kérésekkel fordul az Megfélemlítés: a munkavállókat telefonon vagy elektronikus levélen keresztül magasrangú, befolyásos személynek kiadva, vagy épp a vezetőség nevében szereznek meg adatokat, információkat
- Segítségkérés: az egyik emberi tulajdonságot kihasználva – a segítségnyújtás kérése elesett, bajbajutott emberként- keresik meg a munkavállalót, hogy segítséget kérjenek (például elfelejtett vagy lejárt jelszó miatt, vagy kártyás beléptető helyeken mind a két kéz tele és emiatt nem tudja a saját belépőjét elővéve engedteti be magát a támadó) és kicsalják a belépéshez szükséges kódokat vagy információkat.
- Ajtóba alkalmazotthoz, majd, amikor elnyeri annak bizalmát, azzal visszaél.

Pszichológiai visszaélés még, amikor a felhasználók által kedvelt közösségi oldalakat tanulmányoznak. Sok ember a közösségi oldalakon nárcisztikusabban viselkedik, szívesen osztja meg az általa látogatott szórakozóhelyeket, érdeklődési köröket, hobbikat. Amennyiben a social media fiókjukhoz tartozó adatvédelmi beállításuk nem jó vagy nem megfelelő, úgy rengeteg személyes információt osztanak meg magukról és ezzel megnő a visszaélés lehetősége.

Az ismerősség mint pszichológiai fogalom azt jelenti, hogy azokkal a személyekkel szemben, akiket már többször látnak, bizalmasabbakká válnak, még akkor is, ha nem tudják a nevüket, és semmit nem tudnak róluk.

A támadó a felelőtlen munkavállalókkal (de sima internethasználók esetében is igaz) a világháló segítségével, mintegy ráhangolódásként, tájékozódik a személyről, a közvetlen családi és baráti társaságról és akár közvetlenül, akár közvetetten olyan információk birtokába kerülhet, amelyek alkalmasak lesznek a jelszavak megismerésére, kikövetkeztetésére.

6. Közösségi oldalak felelőtlen használata

Egyre kedveltebbek a közösségi- és társkereső oldalak, amelyen rég nem látott osztálytársakat, ismerősöket lehet újra megtalálni, hasonló gondolkodású emberekhez, közösségekhez lehet virtuálisan csatlakozni. Alkalmasak arra, hogy a felhasználó az éppen végzett tevékenységéről fotókat osszon meg másokkal. Az egyik legkedveltebbek az ilyen oldalakon azok az alkalmazások, amelyek segítségével egy felhasználó hollywoody sztár vagy bankrabló, esetleg jövőutazóként látja viszont magát, vagy a születési időpontjából „jósoltat" magának. Ezen alkalmazások segítségével pedig épp a saját adataikat adják ki, persze legtöbb esetben nem is tudják, hogy visszaélést követhetnek el azokkal.

Gyakran előfordul, hogy épp a munkahelyi számítógépről készítenek egy viccesnek szánt képet, amelyen jól kivehető az épp végzett munka vagy a monitorra ragasztott jelszó stb.

7. Irodai pletyka

Az emberek társas és szociális igényéből fakadóan az információmegosztást tekintik a legfontosabbnak mind helyi lakó, mind pedig munkahelyi szinten. Erre vonatkozóan szabályozást sem belső szabályozási sem jogszabályozási szinten nem lehetséges. A pletykával okozott kár – akár jószándékból, akár rosszindulatból történik, akár van valós alapja, hírértéke akár nincs – mindenki számára káros lehet, ráadásul olyan információkat tartalmazhat, amelyekre akár a pszichológiai manipulációt, akár zsarolást alapozni lehet.

9.1.8. Adatkezelés

Az adatkezeléssel kapcsolatos szabályok betartása illetve azok megszegése is kockázatot jelenthet kibertámadások esetén.

2018. május 25-án életbe lép az Európai Unió adatvédelmi rendelete, a GDPR[198], amely következtében a hazai adatvédelemmel kapcsolatos jogi szabályok is módosulnak.

Az egyik ilyen kiemelt kockázatokkal kezelésével kapcsolatos újítás a Rendelet alapján:

- Ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat.
- Ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett.
- Ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra, egészségügyi adatokra vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkozik.
- Ha személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából.[199]

Titoktartás megszegése

Egyes munkaviszonyokban, illetve bizonyos adatbázisokhoz, minősített adatokhoz történő hozzáférés, hivatásos szolgálati jogviszonyban tudomásra jutott tények, üzleti titkok, egészségügyi adatokra vonatkozó információk vonatkozásában a munkavállalókat köti a titoktartás. Ezek lehetnek törvényi szabályokon alapulók, hivatásokhoz kapcsolódó vagy munkaviszonyból, vállalkozói szerződésből, kutatások során a tudomásra jutottak, amelyek megszegése súlyosan veszélyeztetheti munkaadó (vállalkozás) gazdasági, üzleti érdekeit, presztizsét, bizonyos esetekben a know-how-t is.

A titoktartás esetében írásbeli (jog)nyilatkozat tehető, amelyben rögzítik a titoktartásra jogosultak személyét, annak időbeli hatályát, valamint megszegésének büntetőjogi, polgárjogi és egyéb jogszabályba ütköző rendelkezéseit a felek saját kezű aláírásukkal látják el.

A munkaviszonnyal összefüggésben megszerzett információk megsértése, nyilvánosságra kerülése vagy hozzáférhetővé tételével enyhébb esetben azonnali felmondással vagy büntetőjogi következményekkel járhat.

A munkavállaló a titoktartás megszegését elkövetheti:

- Bosszúból, amely akár az előléptetése vagy fizetésemelése elmaradása miatt, vagy épp fegyelmi eljáráskövetkeztébe szándékosan (dolus directus vagy dolus eventualis) történhet.
- A megszűnt munkaviszony miatt, gondatlanul sértheti meg a titoktartási kötelezettségét. A kilépő munkavállaló a korábban megismert információk tekintetében nem veszi tekintetben, hogy azokról a későbbiekben sem beszélhet.
- Jogtalan anyagi ellenszolgáltatás miatt, a kötelezettségek ellenére konkurens cégnek vagy államnak a tudomására jutott és kért információkat „eladja", amely büntetőjogi felelősségre vonással jár[200].

[198] GDPR: General Data Protection- az Európai Unió új Általános Adatvédelmi Rendelete

[199] GDPR (75)

[200] A büntetőjogi vonatkozások a fejezet végén kerülnek részletezésre

9.1.9. Rendszergazda

Ha a munkavállalókról szó volt, akkor szükséges a rendszergazdáról, mint a vállalatban vagy hivatalban az informatikai eszközökkel és rendszerekkel foglalkozó, azt felügyelő személyről is szót ejteni, hiszen jogállásukat tekintve ők is a munkavállalók köréhez tartoznak, ugyanakkor amíg a „sima" munkavállaló tekintetében nem elvárás, hogy a rábízott rendszert kezelje és felügyelje, a működéshez szükséges szoftvert telepítse, frissítse. Sokkal inkább már annak inkább megelégednek azzal a munkáltatók, ha az alkalmazott a felügyeletére bízott eszközt, rendszert az IBSZ-nek megfelelően tudja kezelni, annak biztonsága, a szoftverek telepítése, frissítése, karbantartása, a zavarok elhárítása, adatok mentése már a rendszergazda feladata.

Az állami, valamint a vállalati szektorban is munkavállalóként alkalmaznak rendszergazdát, akinek elsődleges feladata, hogy a munkaviszonyának vagy megbízási szerződésének keretei között, az abban rögzített feladatokat elvégezze.

A rendszergazdák általános feladata nagy vonalakban:

Általános rendszergazdai feladatok: telepített szoftverek átvizsgálása, rendszernaplók, víruskeresési naplók, ha van egyéb naplók vizsgálata, kábelek ellenőrzése, az eszközök megfelelő működésének ellenőrzése. Az általános feladatok mellett végeznek szoftveres rendszergazdai feladatokat (így a szoftverek telepítése, beállítása, biztonsági mentések készítése, frissítések letöltése, a rendszerek átvizsgálása során tapasztalt hibák ellenőrzése, javítása, a munkatársak igényeinek figyelemmel kísérése, biztonsági beállítások folyamatos felülvizsgálata és szükség esetén korrigálásuk)

A rendszergazdák hardverekkel kapcsolatos feladatai az általános átvizsgálás során észlelt hardver hibák garanciális javíttatása, hatáskörébe tartozó eszközök garanciális ügyeinek intézése, megelőző lépések megtétele, új eszközök vásárlásához javaslatok megtétele, azok üzembe helyezése, telepítése és kipróbálása, hálózattal kapcsolatos feladatok (hálózat kiépítése, üzemeltetése), szerverek telepítése, üzemeltetése, munkaállomások és más hálózatban részt vevő egységek telepítése és üzemeltetése, hálózati szabályok kialakítása és betartatása.

Az említett rendszergazdai feladatok elvégzése is rejt kockázatokat magában, amennyiben azokat megszegi, az általa telepített szoftverek nem legális forrásból származik- akár a vállalat kiadásainak csökkentése miatt, akár szándékosan, saját zsebre dolgozva- nem ellenőrzött helyről szerzi be a működéshez szükséges szoftvert, ami miatt azok frissítése, a hibák kiküszöbölése sem lehetséges, így ezzel anyagi kárt okozhat vagy pedig a tárolt információk sérülhetnek, hozzáférhetővé válnak.

A rendszergazda további feladatai:

- A rendszergazda feladata a hálózat és a hálózatban részt vevő egységek biztonságának megoldása, felügyelete, javaslatok megtétele a biztonsági hiányosságok pótlására. Különös tekintettel az alábbiakra:
- eszközök elektromos biztonsága, például szünetmentes áramellátás, túlfeszültség védelem,
- üzemképesség és állag megóvása, így külső és belső portalanítás, tisztítás,
- adattárolás biztonsága, adatmentések megoldása,
- vírusvédelem, kémprogram védelem,
- hálózati biztonsági szabályok létrehozása, tűzfal üzemeltetése,
- hálózati jogosultságok létrehozása,
- levelezés biztosítása, levélszemét szűrése,
- saját szerver esetén levélszemét-szűrés,
- nincs saját szervere a cégnek: a szolgáltatást biztosító cég feladatkörébe tartozik. A rendszergazda feladata a kapcsolattartásra korlátozódik.
- A levélszemét-szűrés a fentieken túl több lépcsőben is megoldható feladat, így speciális szűrő szoftverek vásárlásával házon belül is kezelhető. Ez esetben a rendszergazda feladata.

A GDPR, az új Általános Adatvédelmi Rendelet értelmében a munkavállalónak bármilyen cégen belüli adatszivárgást, adatvédelmi incidenst 72 órán belül jelentenie kell. Az adatvédelmi incidensek megelőzésével a rendszergazdának alábbi feladatai vannak:

- biztonsági házirend megismertetése a felhasználókkal,
- informatikai szabályzat – ha van – megismertetése a felhasználókkal,
- szoftvernyilvántartás vezetése és időnként a cég vezetésének tájékoztatása.
- licencek lejáratáról tájékoztatás előre,
- tervezett karbantartásokról előre figyelmeztetés,
- várható meghibásodásokról tájékoztatás,
- általános feladatok elvégzéséről és eredményükről időnkénti beszámolás,
- az informatikai szabályokban történt változásokról a felhasználók tájékoztatása.

Az incidens figyelése, észlelése és jelentése elsősorban a rendszergazdát terheli, mivel a legnagyobb szakértelemmel, az adott vállalat informatikai rendszereivel, hálózatával kapcsolatban ő van a legjobban tisztában. Amennyiben ezt elmulasztja, illetve nem működik együtt a NAIH-hal, úgy a vállalatot bírság terheli, amelyet aztán vétkességének foka miatt részben vagy egészben megtéríteni köteles.

9.1.10. Informatikai Biztonsági Szabályzat

Az Informatikai Biztonsági Szabályzat (röviden IBSZ) elkészítése kötelező minden szervezet (állami, önkormányzati valamint egyéb, ezek alá nem tartozó szervezet, vállalkozás) számára. Minden, informatikai rendszert, hálózatot üzemeltető, használó és ezen adatokat kezelők számára, a rendszereik és adataik védelme érdekében létre kell hozni és elérhetővé kell tenni IBSZ-t, amely a szervezetekben dolgozó személlyel ismertetni kell, azt elérhetővé téve.

A szabályzat célja, hogy a belső policyben meghatározott elvek és célok alapján meghatározza a működési rendet.

Az információ bármilyen formában is legyen olyan jelentőséggel bíró érték, amely nemcsak az emberek életének privát szféráját befolyásolja, hanem a gazdasági fejlődés mértékére és irányára is, tehát óvni kell. A biztonságtudatos szervezetben a biztonsági kultúra jelen van, amely azt jelenti, hogy a munkavállalók ismerik jogaikat és kötelezettségeiket, érvényesítik azokat, a biztonság tudatos magatartású munkavállalók nem csak felismerik a biztonsági elvárástól eltérő viselkedés veszélyét, hanem azt is, hogy a veszélyben mi a teendő és mi nem. A biztonsági incidensek prevenciójában a fizikai biztonság (például a géptermek külső és belső helyiségeinek biztonsági zárral felszerelése, a gépteremben belépés-kilépés szabályozása).

A felelősség jogi kategória, az információs rendszerek és hálózatok biztonságának alapkövetelménye.

Mit is jelent a biztonság az elektronikus információs rendszerek vonatkozásában? A kérdésre leginkább akkor keresik a választ, amikor az információbiztonsági esemény – mintegy nem kívánt, vagy nem várt egyedi esemény az elektronikus információs rendszerben, vagy egy előzőleg ismeretlen helyzet – bekövetkezik, és ennek hatására a rendszer által hordozott információ bizalmassága, sérthetetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása eltűnik, vagy ellehetetlenül.

Az információbiztonsági esemény által érintett szervezet – a kár enyhítése és elhárítása mellett – hangsúlyt fektet a belső leszabályozottságát tekintve, az esemény bekövetkezéséért felelős humánerőforrás felderítésére, a felelősségi szankció alkalmazására.

Az információs rendszerek elleni megnövekedett és egyre összetettebb támadásokra a szervezet felső vezetésének komolyan szembe kell néznie, a szervezetre irányuló potenciális támadás súlyosságát vélelmeznie kell és azt a tényt, hogy a tényleges támadás csak idő kérdése. A biztonsági incidensek lehetnek véletlen események, illetve szándékos vagy gondatlan emberi cselekmények eredményei.

Ezért a vezetésnek előre gondolkozva, konkrét támadás hiányában kell meghatároznia mindazokat a célokat, az ezek megvalósításának irányelveit, és a feladatok végrehajtását végző szakemberek

(esetleg szervezetet) biztosítását, amelyek eredményesen biztosítják az elvárt biztonsági szintet. Az eredmény elérhető, ha az információbiztonságot különböző biztonsági intézkedések életbe léptetésével vagy valamely szabvány adaptálásával teremtik meg, de a szervezet célkitűzéseinek elérését szolgálja a szervezetirányítási gyakorlatok alkalmazása. Az információbiztonsági funkció tehát minden szervezet belső irányítási és kontroll rendszerének része kell, hogy legyen.

Az információbiztonság irányítását és menedzselését a szervezetek céljainak elérése érdekében, a kockázatokkal arányban levő módon, a rendkívüli biztonsági eseményeket megelőzve, feltárva, helyesbítve kell végezni.

Az információbiztonság irányítása feltételezi, hogy egy olyan irányítási rendszert kell kialakítani az információbiztonság területén, amely összhangban van a szervezet céljával, feladataival, a szervezetet veszélyeztető tényezőkkel és a biztonságra fordítható erőforrásokkal. A szervezetben az információs rendszereket veszélyeztető kockázatokat a jogszabályokban előírt és a szervezet vezetője által elfogadott szinten kell tartani. Az információbiztonsági programot kell kidolgozni, amelynek megvalósítása legyen összhangban az információbiztonsági stratégiával. Ezáltal is az információbiztonsági rendkívüli esemény kezelése és a következményeinek a helyreállítása a szervezet által megtervezett módon történik a károk csökkentése érdekében.

Az incidensek megelőzésében logikai védelem a humán kockázat mértékét csökkenti.

Az Ibtv. rendelkezése szerint a logikai védelem az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem. A logikai védelem eszközrendszere alkalmas az incidensek megelőzésében a humán kockázat mértékének csökkentéséhez (minimalizálásához).

A humán kockázat és logikai védelem összefüggéseire példák:

- Az informatikai rendszerhez való hozzáférés kezelésében azt az alapelvet kell érvényesíteni, hogy a tárolt adatokhoz csak az illetékes személyek férjenek hozzá. Ennek módja a bejelentkezési azonosítók használata, amely a biztonsági szintre tekintettel digitális kártya vagy biometrikus azonosítás is lehet. Az azonosítók használatával szabályozható, hogy ki milyen szinten jogosult az adatok hozzáféréséhez. Az adatbevitel során – a négy szem elvére tekintettel – az azonos állomány bevitele és ellenőrzése más-más munkavállaló által történjen.
- Az adatrögzítés folyamatának valamennyi egységét érintő belső utasítás, kezelési utasítás, műszaki leírások stb. készítése, ezek betartásának ellenőrzése az információbiztonságáért felelős vezető vagy dolgozó feladata.
- A szervezet megfelelő biztonsági kontroll rendszerének kialakításában és működtetésében az olyan személyiségű munkavállaló „értékes”, aki feladatát előírásszerűen végzi és egy esetleges biztonsági esemény esetén gyorsan és hatékonyan reagál.

9.1.11. A Szabályzat céljaként meghatározandó rendelkezések:

Az informatikai biztonsági szabályzat elkészítésének célja, hogy az elektronikus információs rendszerek használata, alkalmazása során biztosítsa az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozását. A dokumentum szabályozási körében meghatározásra kerülnek a rendszer biztonságos üzemeltetésének alapvető feltételei, az ellenőrizhető informatikai környezet kialakításának feltételei, figyelemmel a használattal és üzemeltetéssel összefüggő jogszabályok, egyéb normák rendelkezéseire.

A szabályzat további célja, hogy rendelkezéseivel elősegíti és támogatja, hogy a szervezetben az információs és kommunikációs eszközök használata a jogszabályoknak, egyéb jogi normáknak megfelelően biztonságosan történhessen, ezáltal a szervezet tulajdonában és használatában lévő információ vagyon sérthetetlensége, bizalmassága és rendelkezésre állása garantálható legyen.

Célja még a belső szabályzatnak, hogy a szervezet kijelölt szervezeti egysége vagy informatikai

felelős (rendszergazda) útján gondoskodik az üzemeltetésről azzal a céllal, hogy az informatikai (és kommunikációs) hálózat az információ áramlását, valamint az informatikai kommunikációs szolgáltatásokat biztosíthassa a szervezetben.

A szabályzat a továbbiakban még meghatározza a célok teljesüléséhez, a rendszerekre és azokkal kapcsolatos tevékenységekre vonatkozó adminisztratív, fizikai és logikai követelmények teljesítésével összefüggő feladatokat, folyamatokat és felelősségeket.

A szabályzat személyi hatálya a szervezet informatikai rendszerének szolgáltatását igénybevevő felhasználókra és rendszergazdákra terjed ki. A felhasználók körének részletes felsorolása (a szervezetnél betöltött munkakörök, egyéb jogviszony alapján (állandó vagy eseti jelleggel, szerződés alapján) az adott szervezet informatikai szolgáltatását igénybevevők meghatározása, akik különböző jogosultsággal és kötelezettséggel rendelkeznek.

A tárgyi hatálya alá tartozó fizikai, infrastruktúrális eszközök, adatok, szoftverek teljes körének, folyamatoknak stb. meghatározása, figyelemmel arra, hogy a minősített adatok védelmére vonatkozó rendelkezések külön szabályzat kerülnek meghatározásra.

A Szabályzatban mindazoknak a jogszabályoknak a felsorolása, amelyekkel összhangban van kialakítva a belső szabályozás és kötelező alkalmazásuk. A felsorolás a közszférát érintő.

a) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.),

b) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.),

c) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet,

d) a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény,

e) a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet,

f) az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet,

g) a minősített adat védelméről szóló 2009. évi CLV. törvény.

A szabályozásnál figyelembe veendő szabványok felsorolása:

A szabályzat alkalmazásában egyes értelmező rendelkezések felsorolása (például:)

1. Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik;[201]

2. Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi;[202]

3. Adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;[203]

[201] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[202] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[203] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

4. Adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;[204]
5. Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;[205]
6. Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;[206]
7. Adatvédelem: a személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások.[207]
8. Adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.[208]
9. Auditálás: Az előírások, elvárások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés.[209]
10. Banktitok: Minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.[210]
11. Bizalmasság: Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.[211]
12. Biztonsági esemény: Olyan nemkívánt vagy nemvárt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.[212]
13. Biztonsági esemény kezelése: Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység. [213]

---

204 Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
205 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
206 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
207 2001. évi XXXV. törvény az elektronikus aláírásról
208 Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
209 Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
210 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról
211 Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.
212 Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
213 Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény

14. Biztonsági osztály: Az elektronikus információs rendszer védelmének elvárt erőssége.[214]
15. Biztonsági osztályba sorolás: Az elektronikus információs rendszer védelme elvárt erősségének meghatározása a kockázatok alapján.[215]
16. Biztonsági szint: A szervezet felkészültsége (érettsége) a biztonsági feladatok kezelésére.[216]
17. Biztonsági szintbe sorolás: A szervezet felkészültségének (érettségének) meghatározása a biztonsági feladatok kezelésére.[217]
18. bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
19. Elektronikus aláírás: Az informatikai rendszerben kezelt adathoz csatolt, rejtjelzéssel előállított jelsorozat, amelyet az adat hitelességének és sértetlenségének bizonyítására használható.[218]
20. Elektronikus dokumentum: Olyan elektronikus eszköz útján értelmezhető adat, mely elektronikus aláírással van ellátva.[219]
21. Elektronikus információs rendszer: Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.[220]
22. Elektronikus információs rendszer biztonsága: A rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme a rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[221]
23. **Életciklus**: Az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam.[222]
24. Elosztott szolgáltatásmegtagadás (DDoS): Olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatásigénnyel túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet.[223]
25. Felhasználó: Egy adott elektronikus információs rendszert igénybe vevők köre.[224]
26. Fenyegetés: Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemeinek védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát. Ang.: Threat.[225]
27. Hitelesség: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan

[214] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[215] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[216] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[217] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[218] 2001. évi XXXV. törvény az elektronikus aláírásról
[219] 2001. évi XXXV. törvény az elektronikus aláírásról
[220] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.
[221] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.
[222] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[223] 2001. évi XXXV. törvény az elektronikus aláírásról
[224] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[225] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény

vagy bizonyíthatóan az elvárt forrásból származik.[226]
28. Kiberbűnözés: Az elektronikus információs rendszerek biztonsága ellen irányuló vagy azok felhasználásával elkövetett bűncselekmények összefoglaló megnevezése;
29. Kiberhadviselés (kiberműveletek): A kibertér képességek alkalmazása, ahol az elsődleges cél katonai eredmények vagy hatások elérése a kibertérben vagy azon keresztül.[227]
30. Kibertér: Egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszereket és beágyazott processzorokat, vezérlőket.[228]
31. Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;[229]
32. Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;[230]
33. Kritikus információs infrastruktúrák (létfontosságú információs rendszerelemek): Azok az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikusinfrastruktúra-elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése a kritikus infrastruktúrákat vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené.[231]
34. Rendelkezésre állás: Az az elektronikus információs rendszer vagy annak elemének tulajdonsága, amely arra vonatkozik, hogy az (ideértve az abban vagy az által kezelt adatot is) a szükséges időben és időtartamban használható.[232]
35. Sértetlenség: Az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.[233]
36. Sérülékenység: Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.[234]
37. Sérülékenységvizsgálat: Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.[235]

---

226 2001. évi XXXV. törvény az elektronikus aláírásról
227 Joint Publication 3-0, Joint Operations, USA
228 Joint Publication 1-02, Dictionary of Military and Associated Terms, Department of Defense, USA, 2010/2013
229 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
230 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
231 Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 2007
232 Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
233 Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.
234 Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
235 Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény

38. Teljes körű védelem: Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.[236]
39. **Üzemeltető**: Az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező szervezet, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős.[237]
40. Vírus: Olyan programtörzs, amely a megfertőzött program alkalmazása során másolja, esetleg kis mértékben változtatja (mutálja) önmagát. Valamilyen beépített feltétel bekövetkezésekor többnyire romboló, néha csak figyelmeztető vagy „tréfás" hatású kódja is elindul. Többnyire komoly károkat okoznak, adatot törölnek, formázzák a merevlemezt, vagy az adatállományokat küldik szét e-mailben.[238]
41. Zárt célú elektronikus információs rendszer: Jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer.[239]
42. Zárt védelem: Az összes releváns fenyegetést figyelembe vevő védelem.[240]

Alapelvek meghatározása körében annak rögzítése, hogy a szervezetben az informatikai rendszerekkel, infokommunikációs eszközökkel és adathordozókkal kapcsolatos fejlesztői, üzemeltetői, biztonsági, továbbá felhasználói tevékenység olyanképpen szükséges megtervezni és végrehajtani, a továbbá fejlesztési, üzemeltetési és védelmi előírásokat meghatározni és dokumentálni, hogy azok garantálják az információbiztonság szükséges és elégséges szintjét. Az Ibtv. 5. §-a alapján az elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

A szervezetben kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni. Mindezeknek a tevékenységeket úgy kell szabályozni, hogy a tevékenységek megtervezéséért és végrehajtásáért való felelősséget minden esetben meg lehessen állapítani.

Az informatikai biztonsági szabályzat átfogóan és keretjelleggel határozza meg az információbiztonsági szempontból legfontosabb kérdéseket és területeket a szervezetben, a jogszabályi előírásoknak, egyéb követelményeknek megfelelően. A szervezet az információ biztonság érdekében további szabályzatok, belső utasításokban meghatározott szabályok, folyamatok leírásának készítését határozhatja el, például:

- informatikai kockázatkezelési szabályzat (a kockázatok és vagyonelemek azonosításának szabályai, fenyegetettség és védelmi intézkedések meghatározása, hatások és következmények azonosítása stb.,
- a szervezet biztonsági osztályba sorolására vonatkozó elvek meghatározása biztonsági események kezelésére, incidenskezelésre vonatkozó szabályok,
- gépterem használati szabályok,
- jogosultsági és hozzáférési szabályok,
- informatikai folyamatleírás, amely az alkalmazók körét, az alkalmazással érintett rendszer, szolgáltatás megnevezését, az adott munkafolyamat és alkalmazandó eljárás rendjét tartalmazza.

[236] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[237] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[238] 2001. évi XXXV. törvény az elektronikus aláírásról
[239] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény
[240] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.

A szabályzatban egyértelműen kell meghatározni az informatikai biztonságért felelős szervezeti rendszer valamennyi részvevőjét (a szervezetben elfoglalt munkakörének megnevezésével) és a hozzárendelt biztonsági feladattal.

A szervezet vezetője felelős az szervezet informatikai/és informatikai biztonsági tevékenységének jogszerűségéért, a személyi és tárgyi feltételek biztosításáért, gondoskodik a szabályozás szerinti és ellenőrzés által a jogszabályokban előírt információ biztonsággal kapcsolatos tevékenységek végrehajtásáról, dönt informatikai biztonsági kérdésekben, ellátja a szervezet informatikai biztonsági szakmai irányítási és felügyeleti feladatait, gondoskodik a szabályzat aktualitásáról és oktatásról stb.

Az informatikai szervezeti egység vezetője felelős a rendszer működtetéséért. E körben gondoskodik a szervezet informatikai rendszere és a tárolt, kezelt adatok zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosításához szükséges intézkedések előkészítéséről, az intézkedések megvalósításáról, ellenőrzésről köteles gondoskodni. Felelős a szervezet által üzemeltetett informatikai rendszer jogszerű és szakszerű működéséért/működtetéséért, a rendszerre vonatkozó informatikai és információ biztonsági előírások teljesítéséért, kezdeményezi a szervezet informatikai és információ biztonsági érdekeinek érvényesítése javaslatot tesz a rendszer fejlesztésére, módosítására, ellátja a rendszer használatához szükséges jogosultságok kezelésével kapcsolatos feladatokat, ellenőrzéseket tervez és végrehajt. Informatikai biztonság megsértése esetén vizsgálatot folytat le és javaslatot tesz intézkedések megtételére.

A szervezet feladatellátása és informatikai szolgáltatási tevékenysége szükségessé teheti, hogy a szervezet elektronikus információs rendszer biztonságát – akár önálló státuszban –kijelölt felelős személy lássa el. Ebben az esetben ez a kijelölt felel a szervezet elektronikus információs rendszerének védelméhez kapcsolódó feladat ellátásáért, tehát gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való megfelelőségének megteremtéséről és fenntartásáról, elvégzi vagy irányítja a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek tervezését, szervezését, koordinálását és ellenőrzését. A rendszerbiztonság megteremtéséhez előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot, előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és biztonsági szintbe történő besorolását.

A Szabályzat, a vonatkozó jogszabályok, belső szabályzatok be nem tartása, valamint az informatikai biztonság veszélyeztetése, megsértése esetén a felhasználóval szemben fegyelmi, illetve büntetőjogi felelősségre vonásnak lehet helye.

A szabályzatban rendelkezni kell a személyi biztonsági követelményekről. A jogtalan hozzáférés, információvesztés és rongálás elkerülése érdekében a „tisztaasztal, tisztaképernyő”[241] szabály alkalmazása elengedhetetlen, tehát az aktuális feladathoz csak a legszükségesebb anyagokat kell az asztalon hozzáférhetően, a képernyőn láthatóan tartani. Munkaidőn túl az iratokat az íróasztalokon nem lehet tárolni, el kell zárni azokat. Kiemelt figyelmet kell fordítani és messzemenően be kell tartani az információk/adatok minősítésére vonatkozó előírásokat. Az aktuálisan nem használt számítógépet ki kell kapcsolni vagy jelszóvédetten zárolni.

A szervezetnek menedzsmentjének külön figyelmet kell fordítania az információbiztonsági képzésre, továbbképzésre, amelynek nemcsak a munkahelyre belépő és a biztonsági szabályzattal megismerkedő munkavállaló vonatkozásában van jelentősége, hanem az információbiztonsági tudatosság növelése érdekében a biztonsági események bekövetkezésének lehetőségére tekintettel, a munkavállalók időszakosan visszatérő, folyamatos képzéséről is gondoskodni kell (például jogszabály változás, külső-belső biztonsági események feldolgozása).

Magyarországon az állami és önkormányzati szervek adatok, és ezeket tartalmazó dokumentumok sokaságát kezelik, amelyek részben nem nyilvános, vagy fokozottan védett minősített adatok, részben pedig bárki által korlátlanul megismerhető közérdekű adatok, információk. Az adatok természetes személyre, az adott szervezet vagy más szervezet működésére vonatkoznak, mindezek kezelését, gyűjtését, továbbítását jogszabályok határozzák meg.

241 Clear desk

A hazai adatvédelmi szabályozás, alapjait az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény szabályozza. A jogi szabályozással biztosított védelem fontos az állam irányító, szabályozó és ellenőrző szerepének növekedése, az informatikai szolgáltatások körének bővítése miatt, amellyel a célhoz kötött adatgyűjtés és kezelés számszerűségében is emelkedett.

A személyes adatok bizonyos köre különleges adatnak minősül és fokozott védelem alatt áll, ezeknek az adatoknak a sérülése a magánszférát különösen komolyan érinti (például a bűnügyi személyes adat, egészségügyi állapotra vonatkozó adatok). A létfontosságú infrastruktúra védelmére vonatkozó jogszabályok 2008-2013 között léptek hatályba. A jogi szabályozások olyan létfontosságú fizikai és információs-technológiai berendezések és – hálózatok, szolgáltatások és eszközök védelmét érintik, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a kormányok hatékony működése szempontjából.

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. Korm. határozata rögzíti Magyarország kibertérre vonatkozó értékrendjét, jövőképét és céljait, és a dinamikusan változó kibertér igényeihez és a változás által generált feladatokhoz alkalmazkodni képes kormányzati struktúra kiépítését.

A stratégia gyakorlati megvalósulásának biztosítéka a 2013 áprilisában elfogadott, az állami és önkormányzati rendszerek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv), amely meghatározza a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága alapfeltételei megteremtéséhez szükséges intézményrendszert.

A nemzeti vagyon részét képező nemzeti adatvagyon, az ezeket kezelő információs rendszerek, rendszerelemek biztonsága kiemelt jelentőségű. Az elektronikus információs rendszer biztonsága az elektronikus informatikai rendszer olyan állapota, amelyben az információs rendszerekben kezelt adatok és információk bizalmassága, sérthetetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Az Ibtv. alkalmazásában egy elektronikus információs rendszernek kell tekinteni adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét.

Az Ibtv. hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában – azaz az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartamban -, meg kell valósítani és biztosítani kell

a. az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
b. az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása

zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

Az elektronikus információs rendszernek az előzőek feltételeknek megfelelő védelme körében a szervezetnek

- logikai (az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem),
- fizikai (a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem) és
- adminisztratív (a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás

védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

a. a megelőzést és a korai figyelmeztetést,
b. az észlelést,
c. a reagálást,
d. a biztonsági események kezelését.

Az adminisztratív védelmi intézkedés eszköze az adott szervezetben az Ibtv. szerinti intézményrendszer egyes elemeinek működését/működtetését, személyi felelősségi rendszerének feltételeit tartalmazó informatikai biztonsági szabályzat elkészítése.

Az Ibtv. meghatározza a hatálya alá tartozó szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségeket a feladat meghatározása és személyi felelősség szerint:

A szervezet vezetője köteles:

a. meghatározni a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadni az informatikai biztonsági szabályzatot,
b. biztosítani az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
c. jóváhagyja a biztonsági osztályba sorolást, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért,
d. biztosítani a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
e. kinevezni vagy megbízni az elektronikus információs rendszer biztonságáért felelős személyt,
f. gondoskodni az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
g. rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződni arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
h. gondoskodni az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
i. gondoskodni biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
j. ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, köteles gondoskodni arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
k. ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodni arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
l. felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
m. megtenni az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

Az előzőekben meghatározott feladatokért a szervezet vezetője az i) és j) pontokban meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.

Amennyiben a feltételek teljesítése jogszabály által kijelölt központosított szolgáltató igénybevételével történik, a jogszabály által kijelölt központosított szolgáltató közreműködik a szervezet és az elektronikus információs rendszer biztonságáért felelős személy feladatai ellátásában a jogkörébe tartozó tevékenységek tekintetében.

A két szervezet közötti feladatmegosztást kétoldalú szolgáltatási szerződések biztosítják, amelyek a központi szolgáltató felett felügyeletet gyakorló miniszter vagy megbízottja ellenjegyzésével lépnek hatályba.

Az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében, valamint a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülése vonatkozásában a szervezeti szintű informatikai biztonsági szabályok kidolgozása abban az esetben is a szervezet vezetőjének felelőssége, ha a jogszabály által kijelölt központosított elektronikus és hírközlési szolgáltatót vesz igénybe.

A nemzetbiztonsági védelem alá eső állami szervek esetében az elektronikus információs rendszer biztonságáért felelős személy kinevezése tekintetében a kormányzati eseménykezelő központ előzetes véleményezési jogot gyakorol.

A szervezet vezetője köteles együttműködni a hatósággal, ennek során:

a. az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,
b. a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,
c. az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére.

Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért.

Ennek körében:

a. gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b. elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
c. előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
d. előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
e. véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
f. kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.
g. feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.
h. Az elektronikus információs rendszer biztonságáért felelős személy e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az Ibtv.-ben meghatározott követelmények teljesülését:

a. a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,
b. ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők

Ibtv. hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

Az a) és b) pontokban meghatározottak esetében az elektronikus információs rendszer biztonságá-

ért felelős személynek az Ibtv. szerinti feladatai és felelőssége más személyre nem átruházható.

Az elektronikus információs rendszer biztonságáért felelős személy jogosult az előzőek szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel, amelyet a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja. Nem kell a feladatellátás szerinti képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.

Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

Informatikai/információs biztonsági szabályzatról általában

A szabályzat céljaként határozható meg az informatikai rendszer alkalmazása során az adatvédelem elveinek biztosítása, az adatbiztonság követelményeinek érvényesülése, a jogosulatlan hozzáférés, az adatok megváltoztatásának és jogosulatlan nyilvánosságra hozatalának megakadályozása, mindezek megvalósulásának érdekében az informatikai rendszer biztonságos üzemeltetésének alapvető szabályai, az ellenőrizhető informatikai környezet kialakításához szükséges feltételek, a használathoz és üzemeltetéshez kapcsolódó magas szintű szabályok, az alapvető biztonsági normákat és követelmények.

A szabályzat személyi hatálya alá tartozó az adott szervezet informatikai rendszerét és (amennyiben a lehetőség biztosított a szervezet részéről) a szolgáltatásait használó felhasználók és rendszergazdák.

A szabályzat tárgyi hatálya kiterjed a védelmet élvező elektronikus adatok teljes körére, fellelhetőségük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül, a szervezet tulajdonában, illetve az általa bérelt valamennyi informatikai berendezésre, valamint az informatikai eszközök műszaki dokumentációira, az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési), a rendszer- és felhasználói programokra, az adatok felhasználására vonatkozó utasításokra az adathordozók tárolására, felhasználására.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembe helyezésen keresztül az üzemeltetésig.

9.1.12. Biztonsági kultúráról:

Az információs rendszerek és hálózatok biztonságára vonatkozóan az OECD (Organisation for Economic Cooperation and Development – Gazdasági Együttműködési és Fejlesztési Szervezet) a biztonsági kultúra sikeres megvalósítása érdekében útmutatót[242] adott ki.[243] Az útmutatóban megfogalmazott kilenc alapelv a felhasználókra, a vezetőkre, és a szervezet szintjére egyaránt eredményesen alkalmazhatóak, annak figyelembevételével, hogy a különböző szinteken, az egyéni felelősség mértéke eltérő.

[242] Guidelines for the Security of Information Systems and Networks, OECD 2002.

[243] Közérthetően nem csak az IT biztonságról. Információ és IT biztonság kultúra fejlesztése a közigazgatásban KIFÜ Budapest, 2013 szerző: Horváth Gergely Krisztián CISA CISM

A biztonsági kultúra megvalósításának alapelvei:

1. Tudatosítás elve: meg kell értenünk és tudatosítanunk, hogy az információs rendszerek és hálózatok hasznát csak úgy élvezhetjük, veszélyeiket csak kerülhetjük el, ha a biztonsági kockázatok tudatában használjuk őket.
2. Felelősség elve: a felhasználók, az üzemeltetők, a fejlesztők és a tulajdonosok is felelősek az információs rendszerek és hálózatok biztonságáért. A rendszerek biztonsága függ a velük összeköttetésben lévő helyi és globális rendszerek biztonságától. Ahhoz, hogy a biztonságot fenn tudjuk tartani, minden érintettnek tudatában kell lennie saját felelősségével, és ezt számon kell tudni rajta kérni.
3. Válaszintézkedések elve: az érintetteknek kellő időben, egymással együttműködve kell a váratlan biztonsági eseményeket megelőzni, észlelni, illetve az ezekre vonatkozó megfelelő válaszintézkedéseket megtenni.
4. Etikai elv: az érintetteknek tiszteletben kell tartaniuk mások jogos érdekeit.
5. Demokrácia elv: Az információs rendszerek és hálózatok biztonságát megvalósító megoldásoknak a demokratikus társadalmak alapvető értékeivel összeférhetőnek kell lenniük.
6. Kockázatfelmérés elve: A biztonság tervezése és megvalósítása során a releváns lényeges kockázatokat fel kell mérni.
7. Biztonságtervezés és végrehajtás elve: Az érintetteknek a biztonságot az információs rendszerek és hálózatok kialakítása során lényeges szempontként kell kezelni, és megvalósítani.
8. Biztonságmenedzsment elve: Az érintetteknek minden szempontra kiterjedő módon kell a biztonságmenedzsment feladatokat végezniük.
9. Újraértékelés elve: Az érintetteknek az információs rendszerek és hálózatok biztonságát felül kell vizsgálniuk és újra kell értékelniük. A biztonsági irányelvekben, gyakorlatokban, intézkedésekben és eljárásokban szükséges módosításokat el kell végezniük.

9.1.13. Munkáltató

A munkavállalói oldal, az IBSZ ismertetése után elengedhetetlen a munkáltató, mint kockázati tényező bemutatása.

A munkáltató kötelessége, hogy a munkavállalónak biztonságos munkakörnyezetet biztosítson, ne veszélyeztesse annak egészségét, valamint a munkavégzéshez szükséges eszközöket és feltételeket nyújtsa.

A munkáltató, mint kockázat, hasonló a munkavállalói kockázatokhoz.

A munkáltató felelőssége, hogy a tudomására jutott személyes adatokat, különleges adatokat illetéktelen számára ne tegye hozzáférhetővé. A biztonságra vonatkozó utasításai egyértelműek legyenek mindenki számára, mivel objektív felelősséggel tartozik a munkavállaló által a munkahelyére bevitt tárgyakért és eszközökért, kivéve, ha azok bevitelét és használatát a belső policy egyértelműen tiltja vagy korlátozza. Ebben az esetben csak a szándékos károkozás miatt felelhet a munkavállaló, amennyiben a kárt ő maga okozza.

Ugyanolyan kockázatot rejt, ha a munkavállaló anyagi helyzetére hivatkozva az informatikai rendszert nem frissítteti, az ahhoz szükséges feltételeket nem biztosítja, valamint gondatlanságából fakadóan a cége hibájából válnak hozzáférhetővé az általuk kezelt adatok.

9.1.14. Biztonsági intézkedések szakaszai:

Preventív vagy megelőző intézkedés

Amikor egy szervezet meghatározott időközönként a megelőző intézkedés keretein belül feltérképezi az általuk használt informatikai rendszerek sebezhetőségét, sérülékenységét, ezzel meghatározza a külső és belső „hiányosságokat", gyenge pontokat és lehetséges javaslatokat, intézkedéseket tesz az esetleges támadások megelőzésére és elhárítására.

Proaktív biztonsági intézkedés

Proaktív intézkedésről akkor beszélünk, amikor egy szervezet védelmi rendszere képes valós idejű reakcióra a szervezetet érő támadás esetén. A proaktív magatartás tulajdonképpen egy megelőzésre törekvő magatartás, a reaktív magatartás helyett. Ebbe a típusba tartozik, amikor az előző, azaz a preventív szakaszban- talált sérülékenységek javítását.

Reaktív biztonsági intézkedés

A szervezetet ért támadásra, incidensre a védelmi rendszer később reagál, azaz egy követő magatartást jelent. Ebben az esetben az adott szervezetet ért támadás miatt már nagy eséllyel a bekövetkezett kár valamint a meg nem tett védelmi intézkedések költségei megfizetésre kell, hogy kerüljenek.

A támadói/elkövetői oldal tekintetében figyelembe kell venni, hogy jelenleg az adat és információ az egyik legnagyobb érték, amely lehetőséget ad az egymással szembenálló felek (igaz ez a magánszférára és az államiszférára is) stratégiájának, pozíciójának megismerésére, azok kihasználására és az azokkal történő visszaélésre, helyzeti előny létesítésére.

Az alább felsorolt tényezők az adat-és információgyűjtéssel kapcsolatban ugyanakkor nemcsak a legálisan megszerezhetőekre érthető, hanem az támadások során alkalmazott eszközökre és módszerekre is:

- A szükséges információk mennyisége és minősége
- Az igényelt információk mennyisége és minősége
- A külső és belső források lehetőségei
- A rendelkezésre álló idő
- Az információs rendszer kiépítettsége, lehetőségei, hatékonysága
- A technikai lehetőségek
- A humán erőforrások

9.1.15. Büntetőjogi vonatkozások

Ahogyan a fentebb leírtakból kiolvasható, a belső munkatársak jelentette kockázatok esetében nemcsak munkajogi és polgárjogi felelősségről, hanem büntetőjogi megítélése is van a munkavégzés során bekövetkező és a vállalatok, állami szektorban lévő informatikai rendszerek, az azokban tárolt adatok megsértésének, amennyiben azok a munkatársak szándékosan cselekményei vagy gondatlansága, hanyagsága miatt következik be.

9.1.16.Személyes adattal visszaélés

A 2012. évi C. törvény, a Büntető Törvénykönyv 219. § (1) bekezdése alapján: „*Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva*

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy

b) az adatok biztonságát szolgáló intézkedést elmulasztja,

(2) [...]büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.

(3) [...] ha a személyes adattal visszaélést különleges adatra követik el.

(4) [...] ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.”

A tényállás keretdiszpozíció, amelyet a 2011. évi CXII. törvény, az Infotv. tölti ki tartalommal. Célzatos bűncselekmény, amelynél az elkövető a jogellenes magatartásának célja az anyagi haszonszerzés vagy a jelentős érdeksérelem.

Amennyiben valaki, aki a személyes vagy közérdekű adattal kapcsolatban a törvényben rögzített feltételek ellenére azt jogosulatlanul vagy céltól eltérően kezeli, szándékos cselekményével elköveti a bűncselekményt.

A (2) bekezdés esetében az említett Infotv. megfelelő rendelkezéseit kell elővenni. Eszerint[244] az adatbiztonság követelményeinek érdekében, azokat megfelelően védeni kell a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés, megsemmisítés, véletlen megsemmisülés, sérülés és az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.[245]

A tényállás további részében az érintett felé a tájékozatási kötelezettségének nem tesz eleget és ezzel másoknak érdeksérelmet okoz. Ez utóbbi az Infotv.-ben meghatározott adatkezeléssel kapcsolatos értesítési kötelezettségének megszegése (legyen az szándékos vagy gondatlan) megalapozhatja a deliktum elkövetésének gyanúját.

Közérdekű adattal visszaélés

Btk. 220. § (1) Aki a közérdekű adatok nyilvánosságáról szóló törvényi rendelkezések megszegésével

a) közérdekű adatot az adatigénylő elől eltitkol, vagy azt követően, hogy a bíróság jogerősen a közérdekű adat közlésére kötelezte, tájékoztatási kötelezettségének nem tesz eleget,

b) közérdekű adatot hozzáférhetetlenné tesz vagy meghamisít, illetve

c) hamis vagy hamisított közérdekű adatot hozzáférhetővé vagy közzé tesz....

(2)....., ha a közérdekű adattal visszaélést jogtalan haszonszerzés végett követik el.

Az Alaptörvényünk VI. Cikk (2) bekezdése alapján mindenkinek joga van a közérdekű adatok megismeréséhez és terjesztéséhez. Ennek érvényesülését szintén az Infotv. biztosítja.

A közérdekből nyilvános adat a közfeladatot ellátó szerv feladat-és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízatása, az azzal összefüggő egyéb személyes adata...[246]

A bűncselekmény elkövetési magatartásai:

- Eltitkolás.
- Tájékoztatási kötelezettségének nem tesz eleget.
- Hozzáférhetetlenné tesz.
- Meghamisít.
- Hamis vagy hamisított közérdekű adatot hozzáférhetővé tesz vagy közzé tesz.

[244] Infotv. 7.§

[245] Infotv. 7.§ (3) bekezdés

[246] Infotv. 26.§ (2) bekezdés

A bűncselekmény alanya bárki lehet.

Minősített adattal visszaélés

Btk. 265. § (1) Aki minősített adatot

a) jogosulatlanul megszerez vagy felhasznál,

b) jogosulatlan személy részére hozzáférhetővé, vagy jogosult személy részére hozzáférhetetlenné tesz,

minősített adattal visszaélést követ el.

(2) A büntetés

a) ...., ha korlátozott terjesztésű,

b) ....., ha bizalmas,

c) ....., ha titkos,

d) ....., ha szigorúan titkos

minősítésű adatra követik el a bűncselekményt.

(3) Az a minősített adat felhasználására törvény alapján jogosult személy, aki a minősített adattal visszaélést korlátozott terjesztésű, bizalmas, titkos vagy szigorúan titkos minősítésű adatra követi el,

(4) Aki a (2) bekezdés c)-d) pontjaiban meghatározott minősített adattal visszaélésre irányuló előkészületet követ el, az ott tett megkülönböztetés szerint ....,

(5) Az a minősített adat felhasználására törvény alapján jogosult személy, aki a (2) bekezdés c)-d) pontjaiban meghatározott minősített adattal visszaélésre irányuló előkészületet követ el, az ott tett megkülönböztetés szerint ....

(6) Az a minősített adat felhasználására törvény alapján jogosult személy, aki a bűncselekményt gondatlanságból követi el, a (2) bekezdésben meghatározott megkülönböztetés szerint .....

***266. §** (1) A büntetőjogi védelem a minősítés kezdeményezésétől számított harminc napig kiterjed arra az adatra is, amelynek a minősítését kezdeményezték, de a bűncselekmény elkövetésekor a minősítési eljárást még nem fejezték be, és erről az elkövető tudomással bír.*

(2) Minősített adattal visszaélés miatt büntetőeljárásnak csak a minősített adat védelméről szóló törvényben az adott adatfajta minősítésére jogosult szerv vagy személy feljelentése alapján van helye.

A minősített adatok tekintetében a legnagyobb kockázatot nemcsak az adatok megsértése, hanem mind nemzetbiztonsági, bűnüldözési és nemzetgazdasági érdekek, azokkal összefüggő személyek védelme is jelenti. A minősített adatok tekintetében annak megismerésére nem mindenki jogosult. A jogosultak köre a Mavtv.-ben meghatározott személyek részére, valamint betekintési engedély birtokában lehetséges.

A minősített adatok megsértésének elkövetési magatartása: az irat jogosulatlan személy által történő megszerzése, felhasználása, hozzáférhetővé tétele vagy jogosult személy számára hozzáférhetetlenné tétele.

Az elkövető személye tekintetében: bárki lehet, aki akár foglalkozása, működése során (mert a vállalat telephelybiztonsági tanúsítvánnyal (TBT) és személybiztonsági tanúsítvánnyal (SZBT)is rendelkezik)minősített adatot kezelhet, előállíthat, vagy az a személy is elkövetheti, aki bár sem munkavégzése, sem egyéb okból kifolyólag sem kezel ilyen adatot, de valamilyen úton (például az utcán talál minősített iratot zárt borítékban és azt felbontja, annak tartalmát a kezelési utasítás ellenére megismeri) átmenetileg magánál tartja vagy megszerezi.

A minősített iratok sokszor tartalmazhatnak olyan személyekre vagy eseményekre vonatkozó konkrétumokat, esetleg adott személy bűncselekménynek elkövetésére vonatkozó tényeket, amely a már említett irodai pletyka során az adatot kezelő személy megoszt olyan közvetlen munkatársakkal vagy személyekkel, amellyel kimeríti a törvényi tényállást.

A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény

Btk. 267. § (1) Aki a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatot az adatkezelő részére hozzáférhetetlenné teszi, ha más bűncselekmény nem valósul meg, ...

(2) ....., ha a bűncselekmény jelentős érdeksérelmet okoz.

A büntető törvénykönyvünk bünteti a nemzeti adatvagyon körébe tartozó adat hozzáférhetetlenné tételét, amennyiben azt az adat kezelője számára teszi hozzáférhetetlenné. Ugyanakkor – mivel ez egy szubszidiárius tényállás – így annak elkövetése csak akkor valósul meg, ha az elkövetési magatartás nem valósít meg másik bűncselekményt.

A nemzeti adatvagyon fogalmát a nemzeti adatvagyon védelméről szóló 2010. évi CLVII. törvény határozza meg, amely szerint a „közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége."[247]

A Fehér Könyvben a fogalmi megközelítés ugyanakkor elkülöníti a közszférát és a magánszférát.

Az állami szférával kapcsolatban megkülönbözteti az állami szervek és vállalatok, valamint az önkormányzati szervek és vállalatok révén létrejövő adatokat, így a különböző nyilvántartásokat, jogi- és szervezeti normákat, gyűjteményeket stb.[248]

A belső munkatársak jelentett kockázatokat, mivel sokszor az emberi jellemből fakadóan, lehet gyenge, és lehet erősen befolyásoló tényező, de a rendszeres tudatosítás, képzések és nem utolsósorban megfelelően védett rendszerek, hálózatok és Szabályzat megalkotásával, kialakításával a támadások enyhíthetők, időben felismerhetőek, elháríthatóakká válhatnak.

9.2. Irodalomjegyzék

- Guidelines for the Security of Information Systems and Networks, OECD 2002.
- Horváth Gergely Krisztián (2013): Közérthetően nem csak az IT biztonságról. Információ és IT biztonság kultúra fejlesztése a közigazgatásban, KIFÜ, Budapest.
- Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, 137. oldal.
- Muha Lajos (2007): A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezése, ZMNE, Budapest.
- Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése, NKE, Budapest.
- Joint Publication 1-02, Dictionary of Military and Associated Terms, Department of Defense, USA, 2010/2013., Elérhetőség: https://www.telegraph.co.uk/news/2017/10/29/heathrow-investigates-queens-security-details-found-usb-drive/ (utolsó letöltés: 2018. március 12.)

Felhasznált jogszabályok

- 2009. évi CLV. törvény a minősített adatok védelméről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2012. évi C. törvény Büntető Törvénykönyv
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- A fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32002L0065 (utolsó letöltés: 2018. március 12.)

[247] 2010. évi CLVII. törvény 1.§ 1.) pontja

[248] Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér Könyvhöz (Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete Budapest, 2016. július)

10. TIKOS ANITA: INFORMÁCIÓMEGOSZTÁS SZERVEZETEK ÉS ÁLLAMOK KÖZÖTT CÉLZOTT KIBERBIZTONSÁGI INCIDENSEK ESETÉN

10.1. Együttműködés fontossága az információbiztonságban

A digitalizáció és a technika gyors fejlődésének köszönhetően, mára minden területen a digitális technika és a kibertér térnyerése vált megfigyelhetővé. A kibertér a munkavégzésünk a mindennapi életünk elengedhetetlen részévé vált, valamint gazdaságunk is jelentősen függ tőle.

Tagadhatatlan, hogy a kibertér számos új lehetőséget kínál számunkra, valamint megkönnyíti a munkavégzésünket és mindennapjainkat egyaránt, de mindeközben számos fenyegetés és veszély is rejtőzik a kibertérben. Ezen fenyegetések elkerülése, illetve kezelése egy folyamatosan fennálló és folyton új kihívásokat magába foglaló feladat, mellyel számos különböző szervezet küzd nap mint nap.

A kibertérben jelentkező fenyegetések és kihívások megelőzésével, kezelésével és a megfelelő válasz lépések kidolgozásával már hosszú évek óta foglalkoznak a nemzetek, valamint a kibertér határon átnyúló természete miatt a nemzetközi szervezetek és különböző nemzetközi közösségek egyaránt.

A kibertérben jelentkező kihívásokra való felkészülés érdekében az országok és a nemzetközi szervezetek egyaránt a szakosított szervezetek (CSIRT-ek és információbiztonsági hatóságok) létrehozását, kiberbiztonsági stratégiák megfogalmazását, jogszabályi háttér (információbiztonsági követelmények, sérülékenység vizsgálatra vonatkozó előírások, eseménykezelés és incidens bejelentés szabályai, bűntetőjogi vonatkozások stb.) kialakítását, valamint a tudatosítás és az együttműködés fontosságát emelik ki, tűzik ki célul.

A kiberbiztonsági fenyegetések vagy incidensek bekövetkezése kapcsán mindenkinek az operatív szintű szakosított szervezetek (CERT, CSIRT, Kiberbiztonsági központ stb.) jutnak eszébe, melyet kifejezetten az incidensek kezelésére lettek létrehozva. De egy fenyegetés vagy incidens a technikai elhárításon túl számos egyéb feladatot jelenthet az incidens részleteitől függően, például:

- ha az incidens során adatok is sérültek, vagy adatokat loptak el, akkor az adatvédelmi
- hatóság bevonása szükséges;
- ha az incidens során bűncselekmény történt, akkor a bűnüldöző hatóságok bevonása szükséges;
- ha az incidens jelentős média visszhangot kapott, vagy olyan nagy méretű volt, hogy azt az álampolgárok/ügyfelek felé kommunikálni szükséges akkor a szakterület sajtó osztályának bevonása is szükséges;
- ha az incidens több szervezetet is érint, akkor az érintett szervezetek közötti együttműködés, információmegosztás is fontos szerepet kap.

A kibertér határon átnyúló természete miatt a kibervédelmi incidensek sokszor több országot is érintenek, így nemzetközi együttműködést igényel a gyors és hatékony kezelésük. Ennek megfelelően számos különböző bilaterális, regionális, uniós és egyéb nemzetközi együttműködések alakultak ki az évek során.

A határon átnyúló, több országot érintő incidensek az információmegosztó és incidenskezelési feladatokon túl nemzetközi jogi, sőt akár diplomáciai vagy politikai kérdéseket is felvethetnek, ezzel pedig tovább növelik az együttműködési fórumok, lehetőségek és eszközök tárházát.

Jelen tananyag célja, hogy feltárja, hogy milyen intézkedéseket fogalmaztak meg célokat tűztek ki az egyes nemzetközi szervezetek, közösségek, valamint, hogy egy célzott támadás esetén milyen együttműködésre, információ megosztásra esetleg közös fellépésre van lehetőség a nemzetközi szervezetek illetve a különböző bilaterális vagy multilaterális együttműködések keretében.

Az Európai Unió, az Észak-atlanti Szerződés Szervezete (NATO), az Egyesült Nemzetek Szervezete (ENSZ), az Európai Biztonsági és Együttműködési Szervezet (EBESZ) sőt még az Nemzetközi Távközlési Egyesület (ITU) is foglalkozik a kiberbiztonság kérdéskörével. Mindegyik nemzetközi szervezet fontosnak tartja az együttműködést, a bizalom kialakítását, a megelőző tevékenységek bevezetését, a tudatosítást. A nemzetközi szervezetek figyelembe veszik egymás rendelkezéseit és együttműködési mechanizmusait, sőt előfordul az is, hogy azokat tovább gondolva, kiegészítve fogalmaznak meg további célkitűzéseket, intézkedéseket a saját fórumaik, munkacsoportjaik keretében.

Egyes szervezetek csak iránymutatásokat fogalmaznak meg, jó gyakorlatokat gyűjtenek, esetleg tanulmánykötetbe foglalják azokat, míg más nemzetközi szervezetek közös stratégiát fogalmaznak meg, jogi erővel rendelkező intézkedéseket, szabályozásokat hoznak létre.

10.2. Főbb fenyegetési trendek 2017. Évre vonatkozóan

Napjainkban egyre több féle fenyegetést figyelhetünk meg a kibertérben, szinte mindennaposá váltak a kibertámadásokról, kiberbűnüldözésről illetve a kiberháborúról szóló hírek.

Az ENISA 2017. évről szóló áttekintő fenyegetettségi összefoglalója a tizenöt leggyakoribb fenyegetést sorol fel a 2016. év és a 2017. év tapasztalatai, statisztikái alapján.

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

1. ábra: ENISA fenyegetettségi ábrája 2016-2017-re vonatkozóan[249]

[249] ENISA (2018): ENISA Threat Landscape Report 2017 15 Top Cyber-Threats and Trends 9. oldal. Elérhetőség: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

Az ENISA adatai alapján egyértelműen azonosítani tudjuk az aktuális támadási és fenyegetési trendeket. A malware támadás/fertőzés mindkét évben az első helyen szerepelt, a Webes alapú támadások szintén változatlanul a második leggyakoribb támadásnak tekinthetőek, de a ransomware 2016-hoz képest egy szinttel előrébb került a nyolcadik helyről.

Az ENISA átfogó riportjában nem szerepel a tizenöt leggyakoribb támadások, fenyegetések között a célzott támadás, de ez sajnos nem jelenti azt, hogy ne jelentenének nagy fenyegetést napjainkban.

Egy másik, a Kaspersky Lab által a 2017. évre vonatkozó IT Biztonsági Kockázatok felmérés eredményei között már kiemelten szerepel a célzott támadások növekedési trendje, miszerint a felmérésben részt vett ipari vállalatok 28%-a esett áldozatául célzott támadásnak 2017 folyamán.

Megvan a magyarázata annak is, hogy nem mindegyik éves beszámolóban, elemzésben jelenik meg a célzott támadás kiemelve, elkülönítve.

Az ENISA elemzése nem jeleníti meg külön a célzott támadásokat, méghozzá azért, mert a célzott támadásokat az ábrán szereplő fenyegetésekkel/támadások felhasználásával lehet kivitelezni, így az ENISA csak magát a módszert, fenyegetést jeleníti meg az ábrán. Viszont a riport magyarázatában az egyes fenyegetéseknél kitér arra, hogy azt célzott támadások során is alkalmazták, például a ransomware esetén, kémkedés esetén vagy az úgynevezett „spear-phishing" azaz a célzott adathalász-támadások esetén.

Az ENISA összefoglaló elemzés kiemeli, hogy 2016 és 2017 folyamán jelentősen megnőtt a választások során tapasztalt célzott támadás a vizsgált országok körében.

10.2.1. Mit nevezünk célzott támadásnak?

A fenti példák után felmerül a kérdés, hogy pontosan mi számít célzott támadásnak.

Célzott támadásnak (angol terminológiával: targeted attack) nevezzük azon fenyegetést/ támadást, amelyet a támadó kifejezetten egy adott célpont (adott cég, személy vagy szervezet) megtámadására irányul, haszonszerzés (adat vagy információ lopás), károkozás vagy egyéb okokból. Különböző eszközökkel lehet célzott támadásokat végrehajtani.

A 2017-es helyzetelemzések alapján továbbra is jelentős a célzott támadások száma a pénzügyi szektor szervezetei ellen, a kormányzati szervezetek ellen a választások esetén a nemzeti választási rendszerek ellen, valamint egyre növekvő trendet figyelhetünk meg az ipari szereplők elleni célzott támadások vonatkozásában.

A 2010-ben készült Digitális Mohács[250] tanulmány, valamint a 2017-ben megjelent Digitális Mohács 2.0[251] tanulmány is arra hívja fel a figyelmet, hogy milyen komoly veszélyt és milyen volumenű károkat tud okozni egy szándékos, előre kitervelt (tulajdonképpen célzott) támadássorozat, illetve, hogy meg kell tennünk a lehetséges óvintézkedéseket, létre kell hoznunk a szükséges szabályozásokat, együttműködéseket.

[250] Kovács László – Krasznay Csaba (2010): Digitális Mohács Egy kibertámadási forgatókönyv Magyarország ellen, Nemzet és Biztonság. Elérhetőség: http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

[251] Kovács László – Krasznay Csaba (2017): Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság. Elérhetőség: http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf

10.3. Operatív szintű kiberbiztonsági együttműködések

Aránylag korán, már a nyolcvanas években egyértelművé vált, hogy szükség van különböző szakosított szervezetek, intézmények létrehozására, illetve azok együttműködésére a kibertérben megjelenő fenyegetések és incidensek kezelésére.

Az első ilyen szakosított szervezet egy eseménykezelő központ (CERT) volt, melyet 1988-ban Pittsburgben hoztak létre a Morris nevű féregtámadást követően a Carnegie Mellon Egyetemen. Ennek mintájára számos eseménykezelő központ (Továbbiakban CSIRT) jött lére világszerte (kormányzati, szektorális, szervezeten belüli stb.).

Az eseménykezelő központok szolgáltatás portfóliójuk (fő szolgáltatási csoportok: megelőző szolgáltatások, válaszintézkedést nyújtó szolgáltatások és biztonsági minőségirányítás) kiterjedésük, felhatalmazásuk (szektorális, nemzeti, kormányzati vagy egy adott cég belső CERT-je) szempontjából különböző típusúak lehetnek, ám ezen részletek ismertetése nem tartozik jelen tananyaghoz.

Minden CSIRT szolgáltatásai, fő feladatai közé tartozik a reaktív szolgáltatások csoportja, tehát a hozzá bejelentett incidensek kezelése, elemzése, valamint a válaszintézkedések koordinálása. Az információbiztonsági események, illetve a célzott támadások esetében pedig pont ezek a legfontosabb CSIRT szolgáltatások, melyeket szeretne igénybe venni az incidensben érintett szervezet.

Az államhatárokat nem ismerő globális kibertérben egyre kifinomultabb és kiterjedtebb incidensek jelentek, meg melyre már nem lehetett izoláltan egyetlen szervezeten belül megtalálni a gyors, hatékony és megfelelő választ.

Ennek a helyzetnek a felismeréseként jöttek létre különböző CSIRT együttműködések, közösségek.

10.3.1. Bilaterális CSIRT együttműködés

A CSIRT-ek egy adott incidens kapcsán felvehetik a kapcsolatot egy másik az incidensben érintett ország CSIRT-jével, és ilyen módon bilaterális keretek között is megvalósulhat együttműködés a támadás, az incidens elhárítására.

A tapasztalatok szerint a bilaterális kapcsolatok esetiek, nem olyan tartósak abban az esetben, ha csak egy adott incidens vagy sérülékenység estén vették fel a CSIRT-ek egymással a kapcsolatot. A közösségekben való együttműködés a közös tevékenységek, rendszeres találkozók, riport készítés, gyakorlatokban való részvétel kvázi életben tartja a kialakult együttműködést és kapcsolatot, mely előnyt jelenthet a későbbiekben egy mindkét felet érintő jelentősebb incidens vagy támadás mielőbbi kezelése és elhárítása során.

10.3.2. CSIRT közösségek

A különböző együttműködési modellek között létrejöttek különböző kiterjedésű és tagságú nemzetközi CSIRT közösségek is. Elsőként 1990-ben a mára már globális nemzetközi közösségnek számító Forum of Incident Response and Security Teams (FIRST) jött létre, majd 2004-ben az Interet Watch and Warning Network (IWWN), 2000-ben az Európai CSIRT-ek együttműködését megcélzó Trusted Introducer (TI) közösség, majd pedig a 2016-ban megjelent NIS irányelv létrehozta az Európai Unió CSIRT közösségét a CSIRT-ek hálózatát.

A CSIRT közösségek tagjai megosztják egymással a bevált gyakorlataikat, megvitatják az adott időszakban tapasztalt főbb sérülékenységeket, illetve együttműködnek egy határon átnyúló incidens kezelésében és kivizsgálásában.

A CSIRT közösségen belül előre meghatározott eljárásrend szerint működnek együtt a CSIRT-ek, illetve általában egy zárt közösségi felületen vagy levelező listán történik a közösségen belüli kom-

munikáció és információmegosztás.

A CSIRT közösségek szinte kivétel nélkül különböző tagsági feltételeket szabnak meg, amiből következik az is, hogy ha a közösségnek nem vagyunk a tagjai, akkor nem férünk hozzá a kommunikációs és információ megosztó csatornákhoz, ez pedig hátrányt lehet a CSIT-nek a mindennapi munka során, de főként egy átfogó, több országon átívelő összefüggő támadás sorozat elhárításakor szükséges együttműködés és információ áramlás megvalósítása során.

10.3.3. Regionális CSIRT együttműködés

Létrejöttek regionális szintű CSIRT együttműködések is, például a 2013-ban alapított Visegrádi Négyek és Ausztria CSIRT-jeinek és információbiztonsági hatóságainak együttműködésének biztosításáért felelős Közép Európai Kiberbiztonsági Platform (CECSP).

A regionális együttműködések esetében is a nagyobb CSIRT közösségeknél alkalmazott kommunikációs és eljárásrendi szabályok szoktak érvényesülni. A regionális együttműködések esetleges előnye a földrajzi közelségből és a közösség kisebb méretéből adódhat, mert ennek köszönhetően még szorosabb együttműködésre és alaposabb részletesebb és aktívabb információmegosztásra van lehetőség.

10.3.4. CSIRT-ek egyéb szervezetekkel történő együttműködési lehetőségei

Fontos még kiemelni, hogy a CSIRT-ek egy incidens esetén más szervekkel például. bűnüldöző hatóságokkal, Adatvédelmi Hatósággal, Diplomáciai képviselővel, politikai vagy szabályozói szereplőkkel is együtt kell, hogy működjenek.

A felsorolt együttműködési formákat és szabályait a későbbiekben a nemzetközi szervezetek által megfogalmazott kiberbiztonsági célkitűzések és intézkedések során fogjuk részletesen megismerni.

10.3.5. Információ megosztó és elemző központok

Fontos előtte még kiemelni, hogy napjainkban már egyre több úgynevezett információ megosztó és elemző központ jön létre (ISAC), mely nemzeti vagy nemzetközi szinten szektorspecifikusan egy platformra hozza a szabályozó szerveket (minisztérium) szolgáltatókat, felelős hatóságokat és CSIRT-eket is, mely lehetővé teszi a terület komplex átgondolását vagy akár egy incidensből adódó jogi, technikai, politikai kérdések alapos megvitatását.

10.4. Európa Tanács

2001. november 23-án, Budapesten huszonhat európai és négy tengeren túli ország (Amerikai Egyesült Államok, Kanada, Japán és Dél-Afrika) írta alá az Európa Tanács által kidolgozott Számítástechnikai Bűnözésről szóló Egyezményt (más néven: Budapest Egyezményt). A Budapest Egyezmény az egyik első olyan dokumentum, mely nemzetközi szinten fogalmaz meg és koordinál közös lépéseket az internet és az informatika világában. Az egyezmény célja a társadalom védelme a számítástechnikai bűnözéssel szemben a nemzetközi politikai együttműködés keretein belül.

Az egyezmény fontos mérföldkőnek számít, mert a számítógépes bűnözéssel kapcsolatos eljárásjogi és nemzetközi bűntetőjogi kérdéseket komplexen kezeli, illetve a számítógépes környezetben használt főbb fogalmakat (számítástechnikai rendszer, számítás technikai adat és szolgáltató, forga-

lomra vonatkozó adat) definiálja, egységesti a nemzetközi területen. Az egyezmény meghatározza a jogtalan belépés, adat sérthetetlensége elleni cselekmény, kifürkészés, eszközökkel való visszaélés, számítástechnikai csalás és hamisítás tényállásokat, valamint a gyermekpornográfiával kapcsolatos bűncselekmények eseteit.

Az egyezmény 23. cikkében foglaltak szerint, az aláíró országok széles körben együttműködnek a számítógépes rendszerekkel és adatokkal kapcsolatos bűncselekményekkel kapcsolatos nyomozások és eljárások során, illetve az ezekre vonatkozó elektronikus bizonyítékok összegyűjtése céljából.

Az egyezmény rendelkezései szerint az aláíró országok között már hatályban lépő kiadatás szerződések innentől kiterjednek a cikkben szereplő bűncselekményekre is, továbbá az aláíró felek széles körben nyújtanak egymásnak jogsegélyt a számítástechnikai rendszerek elleni bűncselekményekre irányuló eljárások és nyomozások során.

Az egyezmény rendelkezik a nyomozás során szerzett információk megosztásának szabályairól, tehát már 2001-ben is kiemelt figyelmet fordítottak az országok az információmegosztás, információcsere jelentőségére a kibertérben végzett tevékenységek vonatkozásában.

10.5. Egyesült Nemzetek Szervezete

A kétezres évek elején az Egyesült Nemzetek Szervezete (ENSZ) is felismerte az információs és távközlési technológiák jelentőségét a nemzetközi biztonság vonatkozásában, így ezt a kérdést is a napirendjére tűzte.

2012. július 5-én az ENSZ Emberi Jogi Tanácsa és Közgyűlése határozatot fogadott el az emberi jogok előmozdításáról és védelméről az interneten. A dokumentumban a Közgyűlés felhívja a figyelmet arra, hogy a gyors technológiai fejlődés és a távközlési eszközök elterjedése miatt egyre fontosabbá válik, hogy az emberi jogok, főként a véleménynyilvánítás szabadsága megfelelően érvényesüljön az internet világában.

A határozat kimondja, hogy online felületeken ugyanazokat a jogokat kell biztosítani az embereknek, amit az offline világban. Ezt az elvet kiemelten fontos érvényesíteni a véleménynyilvánítás szabadságának biztosítása vonatkozásában. Ezen szabadságjogok országhatároktól függetlenül bármely médiumon keresztül érvényesítendők, összhangban a Polgári és politikai jogok nemzetközi egyezségokmány 19. cikkével.

A határozatában a Közgyűlés úgy határoz, hogy folytatja annak a vizsgálatát, hogy hogyan lehet az emberi jogok védelmét biztosítani és élvezni az interneten és az egyéb technológiák alkalmazása során, valamint, hogy hogyan lehet az internet megfelelő eszköze a fejlődésnek és az alapvető jogok gyakorlásának.

Az ENSZ Közgyűlés a 2003. december 8-i 58/32-es számú határozatában létre hozott egy kormányzati szakértői csoportot, mely a nemzetközi biztonság összefüggésében az információs és távközlési technológiák területén tapasztalható fejleményeket vitatja meg. A munkacsoport munkájában az első évben tizenöt ország vett részt.

A munkacsoport feladata, hogy tanulmányt készítsen a globális távközlési és infokommunikációs rendszerek megerősítésének nemzetközi lehetőségeiről. Az elmúlt évek során összesen négy tanulmányt, riportot adott ki a kormányzati szakértői munkacsoport.

A kormányzati munkacsoport 2005-ben fogalmazta meg az első beszámolóját, mely mindössze a munkacsoport létrejöttének célját, feladatát, a munkacsoport összetételét és működését tartalmazta.

A 2010. évi beszámolóban a munkacsoport az infokommunikációs technológiákra vonatkozó fenyegetéseket nevezi a 21. század fő kihívásának. Ezek a fenyegetések akár a nemzeti és nemzetközi biztonságban is komoly károkat okozhatnak. A helyzetelemzés során kiemeli a bűnözés kialakulását a kibertérben, valamint azt, hogy az államok megkezdték az ICT technológia felhasználását és fejlesztését hadviselés és politikai célok alkalmazására egyaránt. Célkitűzésként azonosította a létező

normák alkalmazását az információs technológiára vonatkozóan, illetve új normák megfogalmazását, kapacitás építést, nemzetközi együttműködések kialakítását, bizalom növelését és a veszélyeket csökkentő intézkedések megfogalmazását.

A 2013. évi jelentésben a munkacsoport kiemelte, hogy a kibertében alkalmazandó a nemzetközi jog, főként az ENSZ Alapokmánya. Fontos célként fogalmazta meg a munkacsoport a kockázatok csökkentését a béke és stabilitás fenntartásának érdekében. Feladatként fogalmazza meg az együttműködés kialakítását nemzetközi szinten, a nemzetközi jog és normák alkalmazásának értelmezését a kibertérben, valamint a felelős állami viselkedés körül határolását. A munkacsoport szerint ebben az ENSZ-nek kellene a vezető szerepet vállalnia. A magán szféra és a civil társadalom együttműködésbe való bevonását is feladatként definiálja a jelentés.

Kína, az Orosz Föderáció, Tádzsikisztán és Üzbegisztán közösen készített egy nemzetközi magatartás kódexet az információbiztonságra vonatkozóan, melyet 2011-ben nyújtottak be a munkacsoportnak. A magatartási kódex bevezetője kitér arra, hogy a tudományos és technikai fejlesztések katonai és polgári alkalmazásra egyaránt felhasználhatóak. Elismeri, hogy meg kell akadályozni, hogy az információs és kommunikációs technológiákat olyan célokra használják fel, amely a nemzetközi stabilitás és biztonság fenntartásával ellentétes, valamint hátrányosan befolyásolhatják az államokon belüli infrastruktúrák integritását, biztonságát. Kiemeli, hogy az országok fokozott együttműködése szükséges az információs technológia bűnügyi felhasználása elleni küzdelemben.

A magatartási kódexhez bárki csatlakozhat önkéntes alapon. A kódex célja, hogy azonosítsa az országok jogait és kötelezettségeit az információs térben, megfogalmazza az államok felelősségteljes és konstruktív viselkedését, javítsa az államok közötti együttműködést a közös fenyegetések és támadások esetében. A kódex egy lehetséges eszköz annak biztosítására, hogy az államok az információs és kommunikációs technológiákat kizárólag az emberek jólétét szolgáló társadalmi fejlődésre és a nemzetközi stabilitás és biztonság fenntartásra alkalmazzák.

A kódex tizenegy pontban fogalmazza meg az államok által betartandó szabályokat a kibertérben:

- Tiszteletben tartják az államok szuverenitását, integritását és politikai függetlenségét, az emberi jogokat és az alapvető szabadságjogokat valamint az országok történelmi kulturális és társadalmi rendszereinek sokféleségét.
- Nem használják az információs és kommunikációs technológiát, beleértve a hálózatokat is semmilyen ellenséges vagy agresszív tevékenységre, melyek fenyegetést jelentenének a nemzetközi békére és biztonságra vagy az információs fegyverek növekedésére,
- Az információs és kommunikációs technológiákat alkalmazó bűnözői és terrorista tevékenységek elleni küzdelemben együttműködnek, valamint megfékezik az olyan információk terjesztését melyek ösztönzik a terrorizmust vagy a szélsőségeket.
- Törekednek az információs és kommunikációs technológiai termékek és szolgáltatások ellátási láncának biztonságának biztosítására, annak érdekében, hogy megakadályozzák, hogy más államok használják az ő erőforrásaikat, kritikus infrastruktúráikat, alapvető technológiájukat, független ellenőrzést végezzenek az információs és kommunikációs technológiák vonatkozásában.
- Megerősíti az országok kötelezettségeit és jogait, hogy a releváns törvények és szabályozások alapján megvédjék a támadásoktól és szabotázstól az online információs teréket és a kritikus információs infrastruktúráikat.
- Teljes körűen tiszteletben tartják az információs térben fennálló jogokat és szabadságokat, beleértve a nemzeti jogszabályoknak és előírásoknak való megfelelés előfeltételeiről szóló információk megszerzésére és terjesztésére vonatkozó jogokat és szabadságot.
- Népszerűsíteni kell a multilaterális, transzparens és demokratikus internet irányítás létrehozását, annak érdekében, hogy biztosítsuk az erőforrások igazságos eloszlását, és hogy megkönnyítsük a hozzáférést mindenki számára.
- információs és kommunikációs területen történő együttműködést kell működtetni a privát szektorral, azért, hogy megértsék a szerepüket és felelősségüket az információbiztonságban

Ez jelentősen hozzájárulhat az információbiztonság kultúrájának megteremtéséhez.
- A fejlődő országokat támogatják az információbiztonság kapacitásépítés érdekében és a digitális szakadék megszüntetése érdekében tett erőfeszítésekben
- A kétoldalú, regionális és nemzetközi együttműködéseket megerősítik, az ENSZ szerepét népszerűsítik a nemzetközi kiberbiztonsági normák kialakításában, a nemzetközi viták békés rendezésében továbbá fokozzák a nemzetközi szervezetek közötti együttműködést.
- Jelen kódex alkalmazásából eredő viták békés úton történő rendezése, tartózkodnak fenyegetés vagy erő alkalmazásától,

A 2015. évi beszámolójában[252] a munkacsoport a 2013. évi beszámolóban azonosított célok és feladatok kerülnek részletes kifejtésre, megfogalmazásra.

A beszámolóban a munkacsoport kiemeli, hogy az információst technológiák használata az államok jövőbeli konfliktusaiban egyre valószínűbbé válik. A rosszindulatú nem állami szereplők sokfélesége, a rosszindulatú események gyorsasága egyaránt növelik a lehetséges veszélyeket. Az államok közötti eltérő kiberbiztonsági felkészültségi szintek növelhetik a sebezhetőséget egy összekapcsolt világban.

Az országok felelős viselkedésére vonatkozó normák, szabályok és elvek esetében a munkacsoport megállapította, hogy új normaként kerüljön meghatározásra, hogy incidens esetén az érintett országoknak meg kell vizsgálniuk az összes releváns információt, beleértve az incidens nagyobb összefüggéseit

Fontos, hogy az államok nem engedhetik, hogy a területeiket nemzetközileg jogellenes IKT cselekményekhez használják fel. Az államoknak meg kell fontolniuk, hogy hogyan a legjobb együttműködniük az információ megosztás érdekében, hogyan segíthetik egymást az IKT technológiát használó bűnözők és terroristák elleni vádemelésben.

A bevezetendő új szabályok és normák között kiemelte, hogy államok nem folytathatnak vagy támogathatnak olyan IKT tevékenységet mely ellentétes a nemzetközi jogi kötelezettségeikkel, valamint, hogy meg kell gondolniuk, hogy az információ cserét és az együttműködést hogyan lehet a leghatékonyabban kivitelezni abból a célból, hogy a IKT termék bűncselekményre való felhasználását megakadályozzák a terroristákat pedig le tudják tartóztatni.

Az országoknak meg kell tenniük a szükséges intézkedéseket (az 58/199 számú Közgyűlési határozatot), hogy megvédjék a kritikus infrastruktúráikat az IKT támadásoktól.

Olyan intézkedéseket kell hozni, amely elősegíti az ellátási lánc integritását, annak érdekében, hogy a végfelhasználók biztosak lehessenek az IKT eszközeik biztonságában.

A bizalom építés témakörében javasolta a munkacsoport, hogy jelöljenek ki kapcsolattartó pontokat technikai és stratégiai szinten egyaránt, ezzel is segítve a kialakuló nemzetközi együttműködést A regionális, bilaterális és nemzetközi egyeztetések segítenek az országok közötti bizalom kialakulásában, mely megalapozhatja a későbbi szakmai egyeztetések és együttműködések létrejöttét.

A munkacsoport javasolja összegyűjteni az országok vonatkozó szakpolitikai nemzeti jogszabályait, célkitűzéseit, valamint a különböző szintű együttműködések kialakítására és működtetésére vonatkozó mechanizmusok meghatározását.

Javasolja továbbá az országoknak, hogy hozzanak létre nemzeti eseménykezelő csoportokat, valamint támogassa azokat a sérülékenységi információ megosztásban, együttműködések kialakításában, koordinált incidens kezelési tapasztalatokban, kiberbiztonsági gyakorlatok szervezésében stb.

[252] A/70/174 UN. Elérhetőség: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement

10.6. Európai Biztonsági és Együttműködési Szervezet

Az Európai Biztonsági és Együttműködési Szervezet (EBESZ) a világ egyik legnagyobb nemzetközi biztonsági szervezete, melynek munkájában összesen 57 résztvevő állam működik együtt Európa, Észak-Amerika, valamint Közép Ázsia térségéből.

Felismerve az infokommunikáció elterjedésének jelentőségét, az internet szabályozásának fontosságát és a biztonsági dimenzió érzékenységét ezen kérdésekben, 2012 április 29-én az EBESZ Állandó Tanácsa a 1039. számú döntése alapján létrehozta a kiberügyekkel foglalkozó informális munkacsoport (IWG), melynek feladata, hogy kidolgozza (12 darab) az úgynevezett kiber bizalomépítő intézkedéseket. Az intézkedések célja, hogy a résztvevő országok között csökkentsék az információs és kommunikációs technológiák használatából eredő konfliktusokat.

2013 december 13-án az EBESZ Állandó Tanácsának PC.DEC/1106 számú döntése útján elfogadta a munkacsoport által megfogalmazott tizenegy kiberbiztonsági bizalomerősítő intézkedést (CBM), melyet az elmúlt évek folyamán további három intézkedéssel kiegészített a munkacsoport.

Jelenleg összesen tizenhat bizalomépítő intézkedéssel rendelkezik az EBESZ a kiberbiztonság területén:

- CBM1: A részt vevő országok önkéntesen megosztják egymással a nemzeti álláspontjukat a nemzeti és transznacionális fenyegetések különböző aspektusairól.
- CBM2: A részt vevő országok önként elősegítik a kompetens nemzeti szervezeteik közötti együttműködést és információcserét az információs és kommunikációs technológiák biztonsága és alkalmazása vonatkozásában.
- CBM3: A részt vevő országok konzultációkat tartanak annak érdekében, hogy csökkentsék az esetlegesen az ICT használata kapcsán felmerülő félreértésből adódó politikai vagy katonai feszültségek lehetőségét. Célként fogalmazza meg még a nemzeti és nemzetközi kritikus ICT infrastruktúrák védelmét és integritásának megőrzését.
- CMB4: A résztvevő országok önként megosztják, hogy milyen intézkedéseket hoztak a nyílt, interoperábilis, biztonságos és megbízható Internet biztosítása érdekében.
- CMB5: A részt vevő országok az EBESZ-t egy olyan platformnak tekintik mely, alkalmas a párbeszédek lefolytatására, a jó gyakorlatok megosztására, valamint az információs és kommunikációs technológiák biztonságára vonatkozó kapacitás építés témakörének és az egyes támadásokra vonatkozó hatékony válaszlépések megvitatására, megosztására. Az EBESZ ezen területen tovább szeretné fejleszteni a szerepét.
- CBM6: A részt vevő országok olyan modern és hatékony nemzeti szabályozásokat hoznak létre, amely lehetővé teszi a kompetens hatóságok közötti kétoldalú együttműködések megvalósítást a hatékony, gyors, információ csere érdekében. Fontos cél, a bűnüldöző szervek együttműködésének a biztosítása az információs és kommunikációs technológiák terrorista vagy bűnözői célokra történő felhasználása elleni hatékony fellépés érdekében. A létező bűnüldözési csatornákat tiszteletben tartva azt nem duplikálva szeretné ezt a célt végrehajtani.
- CMB7: A részt vevő országok önként megosztják a kiberbiztonsági szervezeti felépítésüket, nemzeti stratégiájukat, politikáikat és programjaikat (például PPP együttműködés)
- CMB8: A részt vevő országok kijelölnek egy kapcsolattartó pontot, annak érdekében, hogy elősegítsék a hatékony kommunikációt és együttműködést az információs és kommunikációs technológiák biztonságára vonatkozóan. Az országok megosztják a nemzeti szervezeti struktúra egyes elemeihez tartozó kapcsolattartási adatokat, hogy egy esetleges incidens esetén a megfelelő kompetens szervezetek és szakemberek tudjanak együttműködni, megvitatni a felmerülő kérdéseket. A kapcsolattartási adatokat évente frissíteni kell.
- CMB9: A közös terminológia hiányából adódó félreértések elkerülése miatt a részt vevő országok készítenek egy listát az IKT biztonságára vonatkozó terminológiákról, magyaráza-

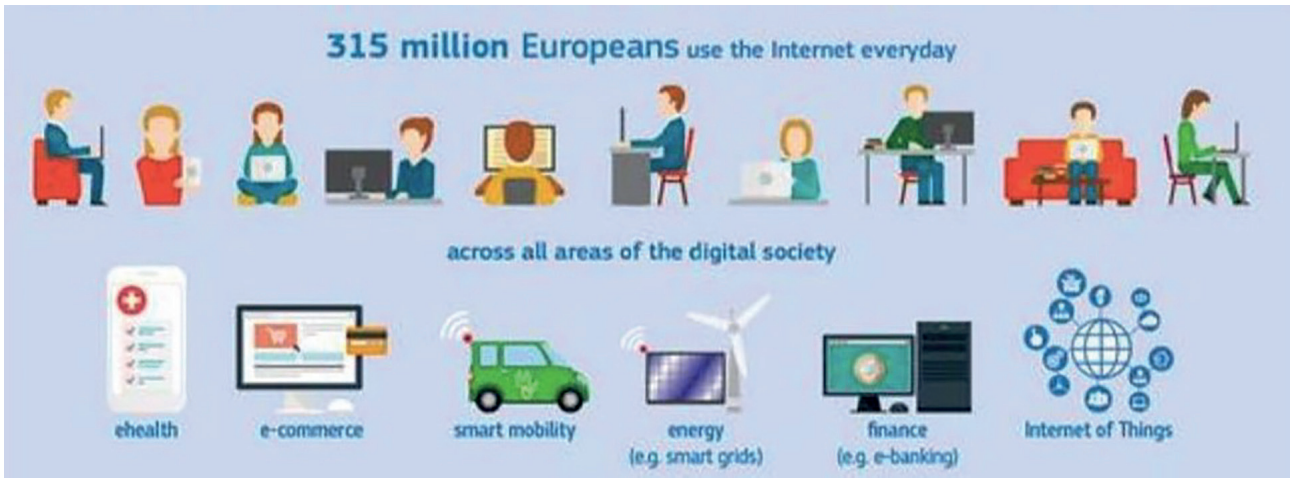
tokkal és definíciókkal ellátva. A hosszú távú cél egy konszenzuson alapuló közös szószedet létrehozása.
- CBM10: A részt vevő országok az EBESZ platformok (többek között az EBESZ Kommunikációs Hálózaton) és mechanizmusok felhasználásával folytatnak eszmecserét az OSCE döntésekről, a CBM-ekről.
- CBM11: A részt vevő országok, kijelölt tagállami szakértők szintjén évente legalább három alkalommal találkoznak a kiberügyekkel foglalkozó informális munkacsoport (IWG) keretein belül annak érdekében, hogy megvitassák a bizalomerősítő intézkedések megvalósítását, valamint továbbfejlesztésének lehetőségét, szükségességét.
- CBM12: A részt vevő országok támogatják az információ megosztást és elősegítik az államok közötti információ cserét workshopok, szemináriumok, kerekasztal-beszélgetések stb. keretein belül regionális és kistérségi szinten egyaránt. Ezen egyeztetések célja, hogy azonosítani tudjanak olyan mechanizmusokat és eljárásokat, amelyek az IKT használatából eredő veszélyek csökkenését eredményezhetik, például elősegítik az IKT békés használatának biztosítását. Ezen eseményekre a magán szektor, az akadémia és a civil társadalom képviselőit is meg lehet hívni.
- CBM: 13: A részt vevő országok elősegítik, hogy a tisztségviselőik és szakértőik védett és engedélyezett csatornákon keresztül kommunikáljanak. Az EBESZ Állandó Tanácsának 1039. számú döntésében szereplő kommunikációs csatornák használatát nem zárja ki ez az intézkedés.
- CBM 14: A részt vevő országok népszerűsítik a köz és magánszféra közötti együttműködéseket (PPP) valamint megosztják egymással az IKT használatából eredő gyakori biztonsági kihívásokra adható válaszlépések, jó gyakorlataikat, mely alapján mechanizmusokat hozhatnak létre.
- CBM 15: A részt vevő országok elősegítik a regionális és kistérségi együttműködés kiépítését (akár még részt is vesznek az együttműködésben) a kritikus infrastruktúrák biztonságáért felelős hatságok között, annak érdekében, hogy megvitassák a nemzeti és határokon átnyúló IKT hálózatokból adódó lehetőségeket és kihívásokat. Az együttműködés kiterjedhet a támadásokról szóló információ megosztásra, jó gyakorlatok megosztására, közös válaszlépések kidolgozására, tudatosításra egyaránt.
- CBM 16: A részt vevő államok ösztönzik a sérülékenységekre vonatkozó felelős információmegosztást, hiszen minden IKT biztonságot érintő tájékoztatás és kommunikáció elősegíti az OSCE régió szintű együttműködését. Az információmegosztás vonatkozásában a CBM8 végrehajtásával a részt vevő államok pontosan azonosítják a kommunikációért, együttműködését, információ megosztásért felelős kapcsolattartó személyt/ személyeket.

Az EBESZ kiberügyekkel foglalkozó informális munkacsoportja 2017 szeptember 7-én a megtartotta az EBESZ kiber bizalomerősítő intézkedések (CBM) megvalósítására vonatkozó kiberbiztonsági válság-szimulációs (table top) gyakorlatot. A gyakorlat során a részt vevő országok a felvázolt információbiztonsági incidensek és támadások során ismertették saját nemzeti szabályaiknak megfelelő eljárásrendjüket, valamint megvitatták, hogy az EBESZ keretein belül, a bizalom építő intézkedések alapján milyen nemzetközi együttműködésre, fellépésre lenne szükség vagy lehetőség.

Az EBESZ bizalomépítő intézkedései nem tekinthetők kötelező erejű, konkrét intézkedéseket előíró szabályozásnak. A részt vevő országoknak az intézkedések mentén lehetősége nyílik megismerni más államok főbb kiberbiztonsági célkitűzéseiket, kiberbiztonsági stratégiáit, szervezeti felépítését, jogszabályi rendelkezéseit stb. A 8. intézkedésben a kapcsolattartó kijelölése az egyik legkonkrétabbnak és egy kiberbiztonsági incidens esetén a legfontosabbnak tekinthető intézkedése.

10.7. Európai Unió

Az Európai Unió már korán azonosította a kibertér növekvő jelentőségét, sőt felismerte, hogy az elmúlt években a kibertér digitális technológiák és az európai gazdaság gerincévé vált, hiszen közel 15 millió európai használja az internetet munkája, szabadideje vagy hivatalos ügyek elintézése során.



2. ábra: a kibertér mára a digitális technológiák és az európai gazdaság gerincévé vált[253]

Kezdetekben csak politikai célkitűzéseket, közleményeket és valós intézkedést még nem megfogalmazó dokumentumok elfogadása volt a jellemző.

Az EU kiberbiztonságra vonatkozó legfőbb célkitűzései:

- Kiberbiztonsági képességek és együttműködés növelése
- Az EU-t erős szereplővé tegyük a kiberbiztonság terén
- Beágyazzuk a kiberbiztonságot a kiberbiztonsági politikák közé

A kibertér témakörét 2001-ben elsőként a Bizottság vetette fel a „Hálózat- és információbiztonság: javaslat egy európai politikai megközelítésre" című közleményében, melyben felhívta a figyelmet a hálózat- és információbiztonság egyre növekvő jelentőségére.

Az első konkrét kiberbiztonsági intézkedésnek az Európai Hálózat- és Információbiztonsági Ügynökség (Továbbiakban: ENISA) létrehozását tekintjük 2004-ben.

Ezt követte 2006-ban a biztonságos információs társadalomra irányuló stratégia elfogadása, amelynek célja az európai hálózat- és információbiztonsági kultúra kialakítása volt. A Bizottság ezenkívül 2009. március 30-án közleményt fogadott el a kritikus informatikai infrastruktúrák védelméről (CIIP), melynek középpontjában Európa hálózati zavarokkal szembeni védelmének a biztonság javításával történő biztosítása állt.

A Tanács 2009. december 18-án állásfoglalást fogadott el „a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről". A bizalomról és a biztonságról szóló szakaszában az európai digitális menetrend hangsúlyozta, hogy valamennyi érdekelt félnek össze kell fognia, és a megelőzésre, a felkészültségre és a tudatosításra, valamint a hatékony és összehangolt biztonsági mechanizmusok kidolgozására összpontosító, átfogó erőfeszítés.

A következő mérföldkőnek az EU intézményeinek támogatására létrehozott a hálózatbiztonsági vészhelyzeteket elhárító, állandó csoport, más néven a CERT-EU létrehozása tekinthető 2012 szeptemberében.

---

253 Az SWD(2017) 500 final számú dokumentum mely az ENISA rendelet felülvizsgálatára vonatkozó hatástanulmány. Elérhetőség: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0500&from=EN

Az Európai unió kiberbiztonsági politika kialakulás következő jelentős lépésének az EU kiberbiztonsági stratégiájának elfogadását tekintjük 2013-ban. A stratégia öt fő prioritást fogalmaz meg a kiberbiztonság terén:

- kiber ellenálló képesség növelése
- Kiberbűnözés csökkentése
- kibervédelmi (cyberdefence) politika és képességek kialakítása
- ipari és technológiai források kialakítása
- koherens nemzetközi kibertér politika létrehozása az EU-ban.

A kibertér biztonságának megteremtése érdekében számos kiberbűnözés elleni célkitűzést fogalmazott meg, intézkedést és szakosított szervezeteket hozott létre az Európai Unió.

Mindenképp ki kell emelni a 2015. évi Európai Biztonság Stratégiát, melynek az egyik legfőbb célkitűzése a kiberbűnözés elleni harcra irányult. A stratégia alapján a kiberbűnözés elleni harc legfőbb elemei:

- a kiberbűnözés elleni küzdelem növelése,
- a bűnügyi nyomozás akadályainak felülvizsgálata a kiberbűnözés esetén,
- a létező kiberbiztonsági szakpolitikák végrehajtása a gyermekek szexuális kizsákmányolása elleni küzdelem, valamint az információs rendszerek elleni támadások vonatkozásában.

Számos jelentős intézkedés és jogalkotási aktus született az elmúlt évek során a kiberbűnözés elleni harc témakörében ide értve a gyermekek online kizsákmnyolása elleni irányelvet (2011) is.

Jelen témakör esetében viszont a 2013. augusztus 12-i az információs rendszerek elleni támadásokról szóló irányelv rendelkezései a kiemelendőek.

Az irányelv alapvető célja a számítástechnikai bűnözés elleni küzdelem, az információbiztonság előmozdítása a megerősített nemzeti jogszabályok, a szigorúbb büntetőjogi szankciók és az illetékes hatóságok közötti hatékony együttműködés révén.

Az irányelv megfogalmazza, hogy az igazságügyi és bűnüldöző hatóságok között fokozottabb nemzetközi együttműködésre van szükség, melynek érdekében létre kell hozni minden tagállamnak egy operatív nemzeti kapcsolattartó pontot, igénybe kell venni a hét minden napján 24 órában rendelkezésre álló kapcsolattartó pontok hálózatát; valamint a sürgős segítségkérésekre 8 órán belül reagálni kell.

Az európai kiberbűnüldözési együttműködés tekintetében fontos előrelépés volt, amikor 2013-ban az Europol (amely szervezet a súlyos nemzetközi bűncselekmények és a terrorizmus elleni fellépésben nyújt segítséget a tagállamoknak) létre hozta az Európai Számítógépes Bűnüldözési Központot (EC3) annak érdekében, hogy megerősítse a kiberbűnözésre adott európai válaszokat.

10.7.1. Hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv

A 2013-ban elfogadott kiberbiztonsági stratégiának és a 2016-ban elfogadott Hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelvnek (Továbbiakban: NIS irányelv) a célja, hogy a tagállamok azonos minimum képességekkel, jogszabályi alapokkal és szakosított intézményekkel rendelkezzenek a kiberbiztonság terén.

Az irányelv esetében érdemes kiemelni, hogy a határon átnyúló incidensek kérdéskörének leszabályozását tűzte ki célul

A NIS irányelv egyik kiemelendő intézkedése, hogy létrehozza a CSIRT-ek hálózatát, a tagállamok nemzeti eseménykezelőközpontjaiból és a CERT-EU-ból álló közösséget, melynek fő célkitűzése a bizalom erősítése és a kommunikáció és információcsere elősegítése a tagállamok között, a gyors operatív együttműködés előmozdítása valamint a határon átnyúló incidensek esetén történő összehangolt, hatékony és gyors technikai együttműködés, információmegosztás megvalósítása.

A CSIRT-ek hálózatának feladatai:

- az incidensben érintett tagállam CSIRT-jének kérésére megosztja és megvitatja az adott eseményre és kockázatokra vonatkozó nem érzékeny információkat,
- lehetőség esetén koordinált választ ad a biztonsági eseményre,
- megvitatja a CSIRT -ek felkészültségét és képességeit kérésükre
- megvitatja az operatív együttműködés lehetséges és hatékony formáit (korai előrejelzés, események kategóriái, kölcsönös segítség nyújtás és a koordináció lehetősége) a határon átnyúló incidensek esetén.

Az irányelv a CSIRT-ek hálózatán túl egy stratégiai szintű együttműködési mechanizmust is létrehozott, mégpedig a tagállamok illetékes információbiztonsági hatóságainak a munkacsoportját, az Együttműködési Csoportot.

Ezen csoport fő feladata az irányelv átültetésének monitorozása, bizalomépítés, valamint az információ csere megkönnyítése. Az Együttműködési Csoportnak az incidensek megelőzésében, a bevált gyakorlatok megosztásában, valamint a megfelelő szabályok kidolgozásában van jelentős szerepe.

Egy bekövetkezett jelentősebb, határon átnyúló incidens esetén, a tapasztalatok megvitatásában, a riasztások és ajánlások népszerűsítésében tud aktív szerepet vállalni.

Az irányelv rendelkezéseinek megfelelően minden tagállam kijelöl egy hálózati és információs rendszerek biztonságáért felelős úgynevezett nemzeti egyedüli kapcsolattartó pontot (Single Point of Contact- továbbiakban (SPOC)) a nemzeti illetékes hatóságok közül. A nemzeti kapcsolattartó pont feladata, hogy elősegítse a nemzeti és közösségi szintű együttműködést a NIS irányelv hatálya alá eső hatóságok és CSIRT-ek között.

Kiemelt szerepet játszik a kapcsolattartó pont a határon átnyúló incidensek vonatkozásában, hiszen, ha egy incidens két vagy több tagállamot érint (vagy akár ennek a gyanúja is felmerül) akkor a nemzeti kapcsolattartó pont feladata, hogy tájékoztassa az érintett tagállamok kapcsolattartó pontjait az incidensről és a rendelkezésére álló információkról. Ezt követően már lehetősége nyílik a tagállamoknak közösen fellépni az támadással szemben az incidens kezelése érdekében. A közös fellépések alatt a technikai segítségnyújtáson túl azonos tartalmú riasztás kidolgozására vagy akár nyilvánosság tájékoztatására is van lehetőség.

10.7.2. Kiberbiztonsági csomag

2017. szeptember 19-én az Európai Bizottság bemutatta az ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése című stratégiát és annak mellékleteit képező szakpolitikai javaslatait.

Ahogy fentebb láthattuk az elmúlt évek során számos szakterület foglalkozik az EU a kiberbiztonsági kérdéskör (bűnüldözés, igazságszolgáltatás, hálózat és információbiztonság, gyermekvédelem, diplomácia stb.) egyes szegmenseivel, de ezek az intézkedések alapvetően egymástól elkülönülten, egymástól függetlenül jöttek létre.

A 2017. évi kiberbiztonsági csomag megfogalmazása során a Bizottság azonosította a szakpolitikák elszigetelődését, ezért a csomag megfogalmazásakor az volt a Bizottság célja, hogy a különböző munkafolyamatokat összefogja, a megfogalmazott célkitűzések és intézkedések össze kapcsolódhassanak, egységes folyamatot alkothassanak.

Emellett a Bizottság a stratégiában célként fogalmazza meg az ágazatspecifikus kiberbiztonsági stratégiák és szabályozások kidolgozását (a meglévő uniós célok, eljárások stb. figyelembevételével) az olyan jelentős szektorokban, mint a pénzügy, közlekedés vagy energetika.

A stratégia három fő célkitűzés köré csoportosítva fogalmazta meg a céljait, javasolt intézkedéseit:

- az Unió kibertámadásokkal **szembeni ellenálló képességének kiépítése,**
- **uniós kibertámadás-elhárítás létrehozása,**
- **a kiberbiztonsági nemzetközi együttműködés erősítése.**

10.7.2.1. Az Unió kibertámadásokkal szembeni ellenálló képességének kiépítése

Ezen célkitűzés keretében a stratégia előirányozza az uniós kiberbiztonsági tanúsítási keretrendszer kidolgozását, mely biztosítaná a termékekbe beépített magasabb fokú ellenálló képesség megvalósítását és a piaci szintű bizalom kialakulását.

A stratégia célja az ENISA Ügynökség mandátumának megújítása és felelősségi körének további területekre történő kiterjesztése, annak érdekében, hogy hatékonyan be tudja tölteni a szerepét az EU kibertámadásokkal szembeni ellenálló képességének és válaszreakciójának erősítésében.

Az ellenálló képesség növelése érdekében kiemeli a stratégia, hogy elengedhetetlen a NIS irányelv mielőbbi teljes körű végrehajtása.

Témánk szempontjából az egyik legfontosabb tervezett intézkedés a gyors vészhelyzeti reagálás útján elérendő ellenálló képesség kialakítása, a már meglévő uniós válságkezelési mechanizmusok kiberspecifikus intézkedésekkel és szervezetekkel történő kiegészítése útján.

A kiberbiztonsági incidensek a gazdasági életre és az emberek mindennapi életére jelentős hatást gyakorolnak, ezért megvizsgálja az EU a Kiberbiztonsági Vészhelyzet-elártási Alap létrehozását, más területen már meglévő válságmechanizmusok mintájára. Az alap lehetővé tenné a tagállamoknak, hogy uniós szintű segítséget kérjenek egy adott incidens vonatkozásában. Az alap tehát konkrét vészhelyzeti válaszlépéseket tudna finanszírozni ˙(például berendezések cseréje, válaszeszközök bevezetése).

10.7.2.2. Uniós kibertámadás-elhárítás létrehozása

Olyan hatékony támadáselhártás és intézkedési keret megfogalmazását jelenti, mely visszatartó erővel bírhat a leendő kiberbűnözők és támadók számára.

Fontos feladat a kiberbűnözők felderítése, nyomon követhetősége, valamint a bűntető eljárás alá vonása. Kulcsfontosságú a leleplezés és a bűncselekmény elkövetéséért járó büntetés kiszabása.

A kibertámadásokat azonnal ki kell vizsgálni, bűntető eljárást kell indítani az elkövető ellen, továbbá meg kell tenni a szükség esetén az arányos és megfelelő politikai és diplomáciai lépéseket is.

Egy jelentős nemzetközi és védelmi vonatkozású válság esetében a lehetséges reakciókat a Tanács munkacsoportja által előkészítve fel kell terjeszteni a Főképviselőnek.

A rossz szándékú szereplők azonosítására van lehetőség már a digitális technológia világában a digitális nyomok segítségével. A digitális nyomok felderítési lehetőségének érdekében bővítenünk kell a technológiai képességeinket. Ebben a feladatban az Europolnak kell központi szerepet játszania, mint a tagállamok szakértői központja az online nyomozás és a kiberkriminalisztika terén.

A Bűnüldözés fokozására 2018-ban a Bizottság javaslatot fog benyújtani az elektronikus bizonyítékokhoz határokon átnyúló hozzáférés elősegítése érdekében. A gyakorlati megvalósulását pedig finanszírozási hozzájárulással tervezi elősegíteni az Bizottság

A Bizottság vizsgálatai szerint megfelelő bűnüldözés másik akadálya az, hogy minden tagállam más kriminalisztikai eljárásokat használ az elektronikus bizonyítékok kiberbűnözéssel kapcsolatos vizsgálatai során. Ezt közös kriminalisztikai szabványok kidolgozásával javasolja orvosolni a stratégia alapján.

A „sötét web” (dark net vagy dark web) komoly fenyegetést jelent unió szerte, hiszen újabb lehetőségeket teremt a bűnözők számára, hogy könnyedén és lelepleződés nélkül jussanak kábítószerekhez, fegyverekhez, illetve a kiberbűnözés során használható eszközökhöz (például rossz szándékú számítógépes eszközök, feltörésre szolgáló programokhoz).

Az Europol feladata a dark webbel kapcsolatos vizsgálatok elősegítése, fenyegetések értékelése, a joghatóság megállapítása. A stratégában megfogalmazottak szerint a nagy kockázatú eseteket előnyben kell részesíteni, illetve vezető szerepet kell vállalnia az EU-nak a nemzetközi fellépés összehangolásában.

Másik kiemelt egyre növekvő kiberbűnözési terület a hitelkártya adatok és egyéb elektronikus fizetési eszközök illetéktelen, csalárd felhasználása. Ennek felszámolása érdekében a Bizottság javaslatot fogalmaz meg a támadás-elhárítás előmozdítására a nem készpénzes fizetőeszközökkel összefüggő csalás és hamistás elleni küzdelemre vonatkozóan.

A kiberdiplomáciai eszköztár fogalmaz meg a közös kül- és biztonságpolitika keretébe tartozó lehetséges intézkedéseket (akár korlátozó intézkedéseket is). Fontos kiemelni, hogy ezen intézkedések az arányos reagálás alapelvét figyelembe véve fogalmaznak meg különböző szintű intézkedési lehetőségeket.

Az eszköztár jelentősen hozzájárul, a potenciális támadók megatartásának befolyásolásához, ami többször megjelenő kiemelt célja a stratégiának.

10.7.2.3. A kiberbiztonsági nemzetközi együttműködés erősítése

A kibertérre vonatkozó nemzetközi együttműködés jelentőségét tökéletesen demonstrálják a stratégia nemzetközi kiberbiztonsági célkitűzései

A támadások és fenyegetése globális jellegét tekintve kiemelt fontosságú az unión belüli egységes fellépésen és együttműködésen túl a partnerség kialakítása a harmadik országokkal a kibertámadások megelőzése és elhárítása érdekében.

Ennek megfelelően az EU számára fontos célkitűzés az EU külkapcsolatainak kiépítése kiberbiztonság területén, valamint a bilaterális, regionális és multilaterális együttműködéseken belül a kibertérben való stabilitás elősegítő illetve a konfliktus megelőzését megcélzó intézkedési keret kidolgozása. Ennek megvalósításaként folytatódnak az úgynevezett kiberpárbeszédek a harmadik országokkal (USA-val, Kínával és Indiával már folytatott kiber párbeszédet az EKSZ az elmúlt évek folyamán).

A stratégia más nemzetközi szervezetek állásfoglalásának megfelelően kijelenti, hogy a nemzetközi jognak kell érvényesülnie a kibertérben is, továbbá az EU elfogadja az ENSZ munkacsoportja által megfogalmazott önkéntes normákat, célokat és szabályokat.

A stratégia célként fogalmazza meg a harmadik országok kiberbiztonsági kapacitásépítésének támogatását, mely globálisan emelheti a kiberbiztonsági szintet és ellenálló képességet, így pedig az Unió kiberbiztonsági szintjére is kedvező hatást gyakorol majd a harmadik országokban elért fejlődés.

Ennek a tevékenységnek a fejlesztése és kiterjesztése céljából a stratégia előírja, hogy létre kell hozni egy úgynevezett „célzott uniós kiberkapacitás-éptő hálózatot", mely egybefogja az EU-n belül az összes olyan szervezetet és képességet, amely ezen tevékenységben együttműködik.

A legutolsó nemzetközi intézkedési területe a stratégiának az EU-NATO együttműködés megerősítésé.

2016 július 8-án közös közleményt adott ki az EU és a NATO a kiberbiztonság, a hibrid fenyegetések és a védelem területén létrehozandó együttműködésre vonatkozóan.

A stratégia célja ezen együttműködés elmélyítése, a kibervédelmi szabványok és követelmények terén az átjárhatóság megvalósítása, közös gyakorlatok szervezése, valamint a párhuzamos és összehangolt gyakorlatok szervezése.

A nemzetközi együttműködés kidolgozása fontos célkitűzés az EU számára, így az Európai Külügyi Szolgálat (EKSZ), a Bizottság és a Tagállamok párbeszédet folytatnak nemzetközi partnerekkel és nemzetközi szervezetekkel (mint például az Európa Tanács, OECD, EBESZ, NATO és ENSZ) egy lehetséges globális nemzetközi megközelítés létrehozása érdekében.

Kiemelendő, hogy már megkezdődtek az egyeztetések és a kommunikáció Braziliával, Kínával, Indiával, Japánnal, Koreával valamint az USA-val a kiberszakpolitikáról, valamint az információs és kommunikációs technológiák biztonságáról.

10.7.3. Kiberdiplomáciai eszköztár

Az Európai Unió a CSIRT-ek technikai együttműködésén túl további együttműködési mechanizmusok létrehozását és alkalmazását is szorgalmazza egy támadás vagy incidens esetén, mégpedig a rossz szándékú kiber tevékenységekkel szembeni közös uniós intézkedések, vagy más néven a kiberdiplomáciai eszköztár alkalmazását.

A kiberdiplomáciai eszköztár szükségessége viszonylag korán, már 2015-ben is az uniós döntéshozók napirendjére került.

2015 február 10-én az Általános Ügyek Tanácsa kiberdiplomáciáról szóló tanácsi következtetéseket fogadott el, melyben az Európai Unió Tanácsa elismeri, hogy a kibertér számos lehetőséget nyújt a közös kül- és biztonságpolitika és egyéb politikák számára, ugyanakkor aggályait is kifejezte amiatt, hogy a kibertér lehetőségeit rossz szándékú tevékenységekre is használhatják állami és nem állami szereplők egyaránt.

A tanácsi következtetésekben ismét megerősítésre kerül az EU állásfoglalása, miszerint a kibertérben is implementálni kell azon normákat és elveket melyek az offile környezetben alkalmazandók, mint például a gyermekek jogai, emberi jogok és az alapvető szabadság elve vagy a polgári és politikai jogok.

Figyelembe kell venni az egyéb nemzetközi fórumok és szervezetek munkáját és döntéseit a kibertérre vonatkozóan, így velük együttműködve kell kialakítani a kibertérre vonatkozó szabályokat.

Ki kell dolgozni egy olyan közös és átfogó, globális kiberdiplomáciai megközelítést, amely:

- védi az emberi jogokat,
- demokrácián, az emberi jogokon a véleménynyilvánítás szabadságán, az információhoz való hozzáférés jogán valamint, a magánélethez való jogon alapul,
- előmozdítja a nemek közötti egyenlőséget figyelembe vevő kiberpolitikát,
- diplomáciai és jogi eszközök segítségével hozzájárul a kiberbiztonsági fenyegetések mérsékléséhez, a konfliktusok megelőzéséhez,
- elősegíti a felelősség megosztást és az együttműködést a köz és magánszektor között.

Az Európai Unió Tanácsa a tanácsi következtetésekben felszólítja a tagállamokat, hogy aktívan járuljanak hozzá a nemzetközi emberi jogi kötelezettségeknek az érvényesítéséhez a kibertérben, valamint védjék meg a kibertében megvalósult bűnözés áldozatait hatékony vizsgálattal és bűntető eljárások kidolgozásával.

Kiemeli azt a célkitűzést, hogy a hatályos nemzetközi jog kerüljön alkalmazásra a kibertérben történő események kezelése és minősítése során. Üdvözli és figyelembe veszi az ENSZ és az EBESZ keretében végzett munkát és intézkedéseket, valamint Ösztönzi az Unió tagállamait, hogy járuljanak hozzá a nemzetközi jog kibertérre vonatkozó globális értelmezésének és a felelősségteljes állami magatartási normák kialakításához.

Mindemellett kiemeli, hogy a digitális technológia az uniós belső piac gazdasági növekedésének jelentős részét biztosítja, így egy olyan alaposan és körültekintően szabályozott környezetet kell létre hozni, mely biztosítja a biztonságot és kiszámíthatóságot, de továbbra is lehetővé teszi a gazdasági növekedést.

A tanácsi következtetések másik fontos célkitűzése, hogy a kibertérben lévő megnövekedett szervezett bűnözés és egyéb jogellenes cselekmények ellen fel kell lépnie a tagállamoknak az emberi jogi normákkal, valamint a kölcsönös jogsegélyről szóló nemzetközi megállapodásokkal összhangban.

Végül ösztönzi a tagállamokat, hogy alakítsanak ki aktív nemzetközi párbeszédet a hatékony szakpolitikai koordináció létrehozása, illetve a párhuzamos munkavégzés elkerülése céljából.

A 2015-ben született tanácsi következtetésekben megfogalmazott célkitűzések végrehajtása érdekében 2017 júniusában a Tanács elfogadta a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések kereteiről szóló tanácsi következtetéseket.

A tanácsi következtetés megerősíti, hogy egyetért az ENSZ kormányzati szakértő csoportjának

2015. évi jelentésében megfogalmazott célokkal, valamint elkötelezett az EBESZ által kidolgozott regionális bizalomépítő rendelkezések kialakításában és végrehajtásában.

Nyomatékosítja, hogy a megfogalmazott közös kiberdiplomáciai intézkedések nem csak állami szereplők esetében alkalmazható. Kijelenti, hogy a közös kül- és biztonságpolitikai területen meghatározott intézkedések is alkalmazhatóak a rossz szándékú kibertevékenységekkel szembeni közös uniós fellépés eszközeként.

A 2017. évi tanácsi következtetésekben megfogalmazott lehetséges intézkedések alkalmazási feltételeinek és részéleteinek kidolgozására felszólítja az EU a tagállamokat az Európai Külügyi Szolgálatot (EKSZ) és a Bizottságot az alábbi elvek mentén:

- „Védeni kell az EU, az uniós tagállamok és az uniós polgárok sértetlenségét és biztonságát,
- figyelembe kell venni az érintett állammal fennálló uniós külkapcsolatok tágabb összefüggéseit,
- biztosítani kell a KKBP-célkitűzések elérését, az Európai Unióról szóló szerződésben foglaltakkal és az e célkitűzések elérése érdekébenmeghatározott megfelelő eljárásokkal összhangban,
- az intézkedéseknek a tagállamok által közösen kialakított helyzetismereten kell alapulniuk és meg kell felelniük az adott helyzet támasztotta igényeknek,
- az intézkedéseknek arányosnak kell lenniük a kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival,
- tiszteletben kell tartani az alkalmazandó nemzetközi jogot és nem szabad alapvető jogokat és szabadságokat sérteni.”

A 2015. évi kiberdiplomáciai eszköztárhoz képest az lehet a benyomásunk, hogy nem sok új dolgot fogalmazott meg a 2017-ben elfogadott eszköztár. Ez csak részben igaz, mert a hiányérzetünk abból adódik, hogy a megfogalmazott lehetséges intézkedések listáját nem tette elérhetővé az Európai Unió, de a publikusan elérhető tanácsi következtetésekbe leírt állásfoglalás alapján, miszerint a nemzetközi jog szabályai alkalmazandók, nagyjából körül tudjuk határolni a lehetséges elemeit az eszköztárnak:

A nemzetközi jog számos vitarendezési lehetőséget fogalmaz meg (az egyetlen szigorú tilalom alá eső tevékenység az erőszak alkalmazása) a diplomáciai eszközöktől, a nemzetközi bírósági eszközökön, a gazdasági eszközökön át egészen a katonai eszközökig.

A nemzetközi jog alapján a legfőbb klasszikus diplomáciai vitarendezési eszközök a közvetlen tárgyalás, a jószolgálat, a közvetítés, a kivizsgálás és egyeztetések, állásfoglalás vagy akár a demarché (diplomáciai jegyzék, állásfoglalás) lehetnek. Ide tartozik még az a lehetőség is, hogy a vita rendezésének céljából lehet a nemzetközi szervezetekhez is fordulni.

Napjainkban is előfordul, hogy valamely ország él a felsorolt eszközök valamelyikével.

A leggyakrabban a legenyhébbnek tekinthető két vagy többoldalú (a kérdésben érintett feleknek megfelelően) egyeztetéseken igyekeznek a tagállamok konszenzusra, megoldásra jutni. Arra is egyre több példát láthatunk (nem kifejezetten kiberbiztonságot érintő viták kapcsán), hogy a tagállamok visszahívják az adott országba kihelyezett diplomatáikat, illetve még durvább esetben kitiltják az országból a vitás fél diplomatáit.

A demarche megfogalmazása kapcsán valószínűleg az Amerkiai Egyesült Államok tartja a rekordot, ugyanis 2012-2013 között a pénzügyi szervezeteket ért DDoS támadáshoz kötődően összesen 20 diplomáciai demarce-ot adtak át különböző országoknak.

Fontos még egyszer kiemelni, azt a szempontot, hogy rossz szándékú kibertevékenység esetén a tevékenységgel egyenértékű/azonos súlyú válaszlépést kell kiválasztania az Unió döntéshozóinak. Ezért ki kell dolgozni egy minden szempontot magába foglaló döntési mechanizmus vagy szabályrendszert, ami alapján a tagállamok vagy az EU megtalálja a megfelelő és arányos válaszlépést.

10.7.4. Nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálás

A 2017. évi kiberbiztonsági stratégiában foglalt céloknak és intézkedéseknek megfelelően a Bizottság bemutatta a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálás című javaslatát, ajánlását 2017. szeptember 13-án.

A javaslat egy új, az eddigi kiberbiztonsági vonatkozású anyagokban nem használt terminológiát vezet át a biztonságpolitika területéről (a nagyszabású, határokon átnyúló kiberbiztonsági események és válsághelyzet), valamint arra vonatkozóan fogalmaz meg szabályokat, intézkedési és eljárási javaslatokat.

A nagyszabású, határokon átnyúló kiberbiztonsági esemény és válsághelyzet a definíció szerint, olyan kiberbiztonsági események „melyek következtében olyan kiterjedt zavar keletkezik, amellyel az érintett tagállam saját maga nem képes megbirkózni, illetve amelyek két vagy több tagállamot vagy uniós intézményt érintenek, és technikai vagy politikai szempontból olyan szerteágazó és jelentős hatásuk van, hogy kellő időben történő szakpolitikai koordinációt és uniós szintű politikai fellépést tesznek szükségessé."[254]

A bizottsági javaslat szerint az egész Unióra kiterjedő, a definíciónak megfelelő nagyszabású kiberbiztonsági válsághelyzetek elhárítása számos uniós valamint EU-n belüli szervezet együttműködésének a lehetőségét megteremti, vagy legalább felveti, de a válsághelyzet reagálás politikai szintű korordinációját minden esetben a Tanács végzi.

A válságkezelés a biztonságpolitika egy már nagyon kiforrott, kidolgozott területe, így természetesen az EU már rendelkezik úgynevezett politikai szintű integrált válságelhártási intézkedésekkel (Továbbiakban: IPCR). Jelen javaslat célja körül határolni, hogy a fent említett intézkedések és mechanizmusok felhasználásával, hogyan lehetne a tagállami kiberbiztonsági szervezetek képességeit, valamint a tagállamok között létrejött uniós együttműködési mechanizmusokat a lehető leghatékonyabban és gyorsan felhasználni egy kiber válsághelyzet elhárítása során.

Az Európai Bizottság kiemeli a javaslatában, hogy a kiberbiztonsági események vagy válsághelyzetek esetében figyelembe kell venni, hogy más ágazatok is érintettek lehetnek a benne, vagy esetleg más ágazatok válságaival valamilyen összefüggésben lehet a kiberválság.

Ennek megfelelően felhívja a figyelmet arra, hogy olyan intézkedéseket kell hozni a válság kezelése érdekében, melyek az informatikai és nem informatikai (fizikai világ) hatásokat is enyhítik, kezelik.

A javaslat a válságkezelési ciklus (megelőzés, felkészültség, reagálás, helyreálltás) egyetlen elemével a reagálással foglalkozik, és arra vonatkozóan fogalmaz meg intézkedéseket, együttműködési mechanizmusokat.

Egy esetleges kiberbiztonsági válságkezelés lehetséges szereplői:

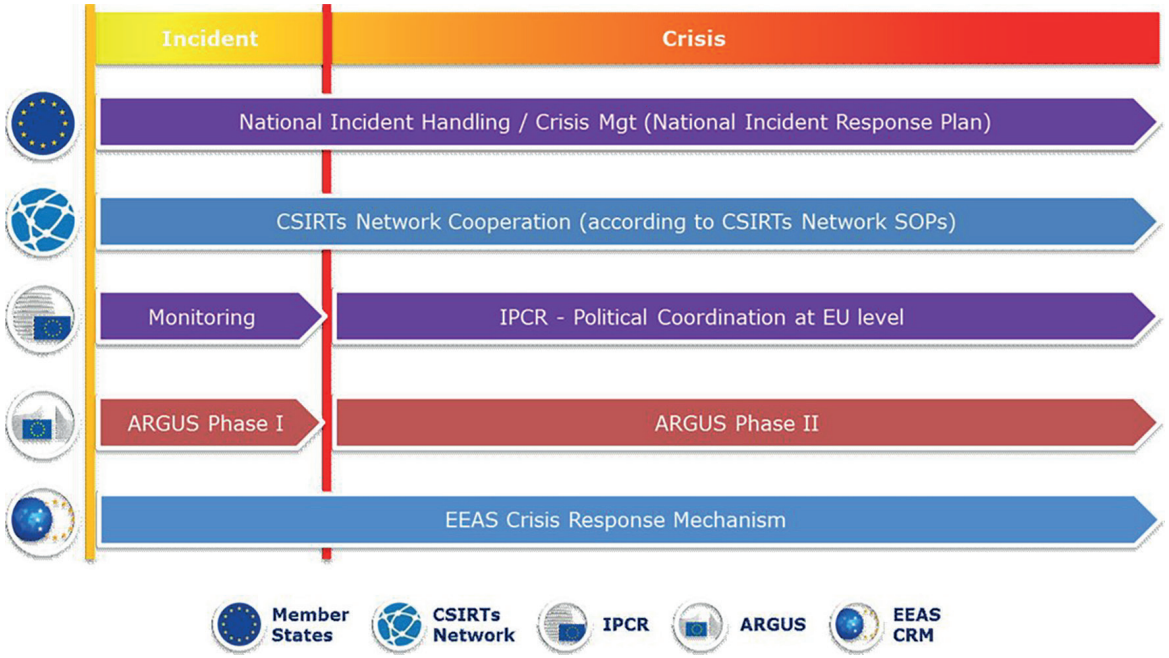
- tagállamok CSIRT-jei,
- tagállamok illetékes hatóságai vagy a NIS irányelv rendelkezései szerint kijelölt egyedüli kapcsolattartó pontok,
- CSIRT-ek hálózata,
- ENISA,
- Az uniós intézmények, szervek és ügynökségek CERT-je (Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU),
- Europolon belül működő Számtástechnikai Bűnözés elleni Európai Központ (EC3),
- Európai Bizottság Vészhelyzet reagálási koordinációs Központja,
- Az Európai Külügyi Szolgálaton belül az Európai Unió Helyzetelemző Központja (INTCEN),
- Európai Unió Katonai Törzsének Hírszerzési osztálya (EUMS INT),
- Európai Unió Katonai Törzsének Helyzetelemző Központja (SITROOM).

[254] Bizottság ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról, 1. oldal.

A válsághelyzetre való reagálás lépéseinek és módozatainak kidolgozása, vagy kiválasztása során négy fontos alapelvet kell figyelembe venni:

1. Arányosság,
2. Szubszidiaritás,
3. komplementaritás,
4. az információk bizalmas kezelése.

A szubszidiaritás és arányosság elvének megfelelően fontos, hogy egy válsághelyzetre való reagálás során is vegyük figyelembe, hogy elsődlegesen a tagállamok felelőssége az eseményekre való reagálás, valamint, hogy alkalmazzuk azon együttműködési mechanizmusokat is, melyek a válsághelyzetnek nem tekinthető incidens esetén alkalmazandók.



3. ábra: Kiberbiztonsági válsághelyzetnek tekinthető eseményekre való reagálás szintjei uniós szinten[255]

Tehát ahogy az arányosság elve megköveteli és a fenti ábra is mutatja, egy európai kiberbiztonsági válság esetén az uniós válságkezelési mechanizmusok aktiválása mellett fontos, hogy alkalmazzuk a már létező nemzeti képességeket, illetve az egyéb uniós együttműködési formákat, mint például a CSIRT-ek hálózatát.

A javaslat kiemeli, hogy a nagyszabású kiberbiztonsági eseményekre való közösségi szintű reagálás hatékonysága a technikai, operatív és politikai együttműködés együttes hatékonyságától függ.

10.7.4.1. Technikai szintű együttműködés

Egy incidens észlelése esetén az első és legfontosabb feladat az esemény kezelése (elemzés, elszigetelés, valamint javasolt intézkedések az esemény elhárítása érdekében) valamint az események nyomon követése, felügyelete, kockázatelemzés.

Ezt a technikai szintű feladatot a tagállamok CSIRT-jei látják el, közösségi szinten pedig az együttműködésüket biztostó fórum és felület a CSIRT-ek Hálózata.

Közösségi szinten ebben, a technikai feladatban az ENISA (főként a CSIRT-ek hálózatának titkárságaként), a CERT-EU valamint szükség esetén az Europol EC3 kaphat szerepet.

[255] Forrás: A Bizottság ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetre való összehangolt reagálásról 11. oldal

Az Európai Bizottság vonatkozásában az Európai Polgári Védelem és Humanitárius Segítségnyújtási Műveletek Főigazgatóságán belül található ERCC nevű szervezeti egység napi 24 órában tart operatív szolgálatot, a válságkezelés folyamatába ezen szervezet is bevonásra kerület.

A fent említett szervezeteken túl még a kiberbiztonsági válságban érintett szektor uniós ügynökségének (például közlekedés) bevonása merülhet fel, valamint az EKSZ részéről a helyzetelemző vagy egyéb az esemény okán szükséges földrajzilag kijelölt vagy tematikus szolgálata.

10.7.4.2. A szereplők együttműködésének módja

A javaslat szerint az ENISA rendszeresen elkészíti a kiberbiztonsági eseményekről és fenyegetésekről szóló uniós kiberbiztonsági jelentést, a fent említett tagállami és uniós szervek által megosztott információk alapján. Ez a jelentés a közösen kialakított közösségi helyzetismeret létrehozásának fontos eleme lesz majd.

Súlyos biztonsági esemény esetén a CSIRT-ek hálózatának elnöke az ENISA -val közösen készti el a kiberbiztonsági eseményről az uniós szintű helyzetértékelést. Ezt az értékelést az elnökséget ellátó tagállam CSIRT-je megküldi a Bizottságnak és a Főképviselőnek.

A CERT-EU technikai szintű jelentéseket készít, melyet benyújt a CSIRT-ek Hálózatának, valamint szükség esetén az ARGUS-nak,[256] Az Europol/EC3 munkatársai kriminalisztikai elemzéseket végeznek az ENISA támogatásával. Az eredményeit pedig a CSIRT-ek Hálózatával megosztja.

AZ EKSZ esetében a hibrid fenyegetésekkel foglalkozó uniós információs és elemző csoport kapcsolódik be a technikai elemzés folyamatába.

A tagállamok CSIRT-jei egymással szorosan együttműködnek, információt cserlének, elemzéseket osztanak meg, valamint az esemény észlelését követő 24 órában megküldik az ENISA részére a rendelkezésükre álló információkat. Ez már a válsághelyzet reagálás elemének tekintendő.

A CSIRT-ek hálózatának eljárásrendjében foglaltak szerint működnek együtt a tagállamok az esemény okainak és a szükséges elhárító vagy enyhítő intézkedések azonosításában. Az ENISA a felhatalmazása szerint, szakértelmével támogatja a CSIRT-ek technikai tevékenységét és kommunikációjukat.

A tagállamok CSIRT-jei az ENISA-val és a Bizottsággal együttműködve koordinálják a reagálás technikai aspektusait.

Az EKSZ SIAC[257] részéről a hibrid fenyegetésekkel foglalkozó elemző csoport megkezdi az adatgyűjtést a bizonyítékok esetében.

Az incidens megfelelő kommunikációja és a nyilvános tájékoztatás elengedhetetlen része a válsághelyzetre való reagálásnak.

A CSIRT-ek riasztásokat és útmutató, tanácsadó dokumentumokat késztenek, melyet a közösségek és a nyilvánosság számára is elérhetővé tesznek. Az ENISA segíti a CSIRT-ek hálózatának közleményeinek az elkésztését, valamint összehangolja a nyilvános tájékoztatást a Bizottság szóvivői szolgálatával.

Szükség esetén az ENISA a közlemény és figyelem felkeltő anyagok készítése során egyeztet az Europollal is, valamint ha a válsághelyzetnek van külpolitikát vagy közös biztonság és védelempolitikát érintő dimenziója, akkor a nyilvános tájékoztató tevékenységekről az EKSZ-szel is egyeztetnie kell.

10.7.4.3. Az operatív szintű együttműködés

Az operatív szintű együttműködés célja a politikai döntéshozatal előkésztése, szükség esetén a kiber-

256

257

biztonsági válsághelyzet koordinálása, a válsághelyzetet előidéző esemény(ek) következményeinek és hatásainak értékelése közösségi szinten, esetleg enyhítő intézkedések megfogalmazása.

Az operatív szintű együttműködés során is a közös helyzetismerettel kezdődik a válságkezelési folyamat, mely keretében a politikai helyzetről szóló jelentések, elemzések készülnek el elsőként.

A Bizottság területileg érintett szolgálata vagy az EKSZ az ENISA, a CSIRT hálózat, az INTCEN, az Europol valamint az EUSM INT hozzájárulásával elkészíti az Uniós szintű integrált helyzetismereti és -elemzési jelentést. A jelentés tartalmaz fenyegetettség elemzést, kockázat értékelést, valamint nem technikai aspektusokat és hatásokat egyaránt.

Az Európai Unió Tanácsának a kiberpolitikai kérdésekkel foglalkozó horizontális munkacsoportja előkészti az Állandó Képviselők Bizottságának (COREPER) valamint a Politikai és Biztonsági Bizottságnak a válsághelyzetről szóló ülését.

Ebben a szakaszban van lehetőség az IPCR aktiválására, mely tulajdonképpen egy kerekasztal találkozót jelent, amit az elnökség hív össze a tagállamok, uniós intézmények, szervezetek, harmadik országok, sőt akár egyéb nemzetközi szervezetek érdekelt feleinek bevonásával.

Fennáll a lehetőség az ARGUS és a SIAC (az EKSZ válságelhárítási mechanizmusa) aktiválására is, melyek szintén a részletes, sok forrásból származó alapos elemzés és értékelés létrejöttét segíthetik elő.

A helyzetelemzés eredményétől függően különböző módon lehet reagálni egy adott válságra. Az egyik lehetőség a NIS irányelv szerinti egyetlen kapcsolattartó pontok közötti határon átnyúló együttműködés megvalósítása, a javasolt technikai intézkedések végrehajtása, a technikai kapacitások koordinálása. Ezen intézkedések végrehajtása és koordinálása megvalósulhat a CSIRT-ek Hálózatának keretein belül is a hálózat eljárásrendjének megfelelően. Minden esetben meg kell vizsgálni az érintett harmadik felekkel való együttműködés szükségét is.

Végül meg kell állapodni, hogy szükséges e nyilvános közlemény az eseményről, és ha igen, akkor milyen tartalommal. Ha az eseménynek külpolitikát vagy közös biztonság és védelempolitikát érintő dimenziója is van, akkor a nyilvános tájékoztató tevékenységekről az EKSZ-vel is egyeztetni kell.

10.7.4.4. Stratégiai szintű együttműködés

A stratégiai és politikai szintű együttműködési szakasz tulajdonképpen tekinthető a felvázolt együttműködés végpontjának vagy tetőpontjának. Ezen a szinten történik a válsághelyzet összes vonatkozásának stratégiai és politikai kezelése.

Ennek megfelelően elsődleges célja az együttműködésnek ezen a szinten a válsághelyzet Unió működésére gyakorolt hatásainak meghatározása, valamint további válságkezelési mechanizmusok vagy eszközök aktiválásának szükségéről való döntés.

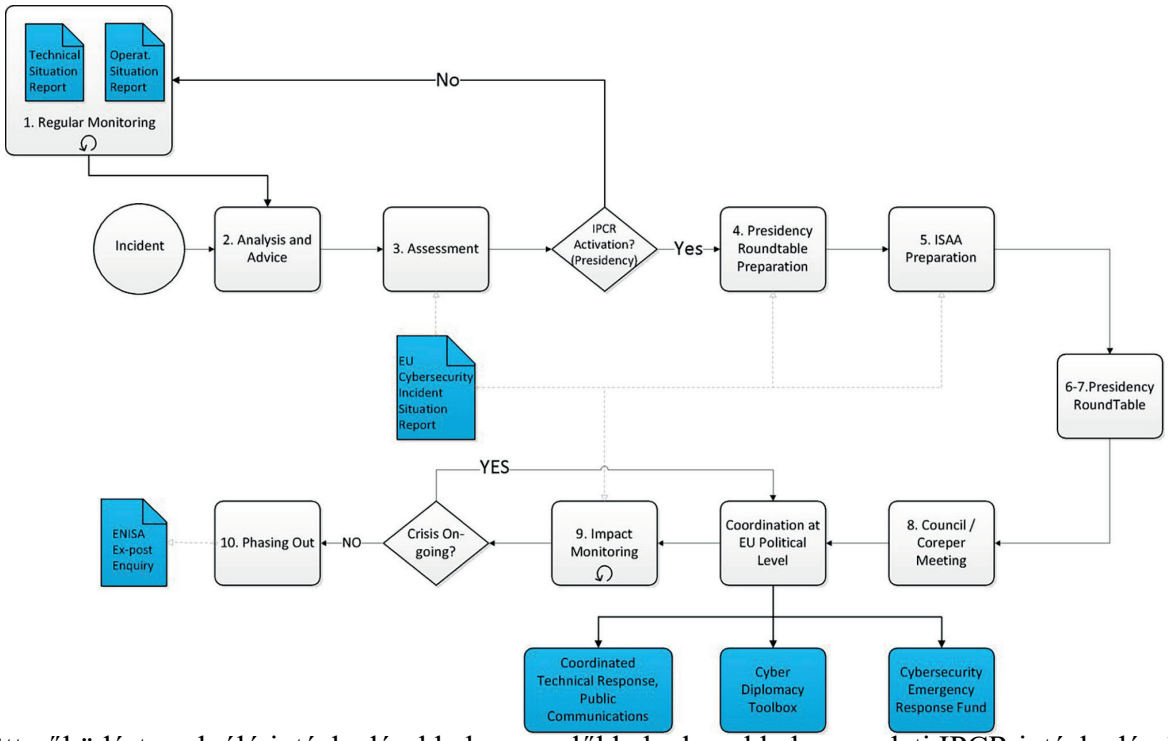
Ezen válságkezelési folyamatban is van lehetőség a kiberdiplomáciai eszköztárban megfogalmazott intézkedések közül a megfelelő intézkedés kiválasztása és végrehajtása. A Bizottság vészhelyzeti támogatást tud nyújtani az érintett tagállamoknak a Kiberbiztonsági Vészhelyzet-elhárítási alapból (miután ez az alap létrejött, mert jelenleg ez csak a kibercsomaghoz tartozó stratégia egyik eleme, célkitűzése).

A stratégiai szinten történik a nemzetközi szervezetekkel való együttműködés és koordináció egyaránt.

10.7.4.5. IPCR folyamat vagy intézkedések

A nagyszabású kiberbiztonsági eseményekre való reagálás technikai, operatív és politikai együttműködési szintek bemutatása során többször felmerült az úgynevezett IPCR intézkedések aktiválása.

Az IPCR intézkedéseket az elnökség barátai csoport dolgozta ki 2015-ben az unió politikai szintű integrált válságelhártási folyamatának pontosítása érdekében. Annak érdekében, hogy ezen intézkedések megfelelően és hatékonyan legyenek alkalmazhatóak a kiberbiztonsági válságok esetében is, a Bizottság kiegészítette már létező kifejezetten kiberbiztonsági



együttműködést szolgáló intézkedésekkel, szereplőkkel, elemekkel az eredeti IPCR intézkedéseket.

2.ábra: IPCR folyamat kiberbiztonsággal kapcsolatos elemekkel kiegészítve[258]

A második ábrán az IPCR folyamat ábrázolását láthatjuk, kiegészítve a kifejezetten kiberbiztonsági elemekkel/intézkedésekkel, melyek kék színnel vannak megkülönböztetve a folyamat eredeti elemeitől.

A folyamatban felvázolt összes intézkedés alkalmazása nem kötelező minden esetben, hanem az adott helyzettől, eseménytől, válságtól függ. Kiemelendő, hogy ebben az esetben már egy teljesebb folyamatról beszélhetünk, akár a teljes válságkezelési életciklust megvalósíthatjuk nem csak a konkrét esemény kezelését/elhárítását.

Az ábrán láthat elemeknek megfelelően összesen tíz lépésből áll az IPCR folyamat.

Az első lépés a rendszeres ágazati nyomon követés, mely során jelentések és riasztások segítik a Tanács elnökségét egy esetleges válsághelyzet kialakulásának lehetőségéről.

A kiberbiztonság szakpolitikai területén jelenleg nincs ilyen a kiberbiztonsági eseményekről szóló rendszeres jelentés vagy riasztás. A kibercsomag viszont már előre vetíti, előírja, hogy az ENISA a nyilvánosan hozzáférhető információk alapján és az uniós partnereitől kapott információk alapján rendszeres uniós szintű technikai kiberbiztonsági helyzetjelentést készítsen.

A hibrid fenyegetések vonatkozásában pedig a SIAC hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoportjának kell kiberbiztonsági operatív helyzetjelentést késztenie.

A második lépés az elemzés és tanácsadás, mely már az incidens észlelését követő szakaszban alkalmazandó. Ezen szakaszban a rendelkezésre álló információk (riasztások, helyzetjelentések stb.) alapján a bizottsági szolgálat, az EKSZ, és a Tanács folyamatosan tájékoztatják egymást a fejleményekről, annak érdekében, hogy szükség esetén tanácsot tudjanak adni a Tanács elnökségének a szükséges uniós közös válságmechanizmusok aktiválására vonatkozóan.

A tervek szerint ebbe a folyamatba is több szereplőt kell bevonni (például: CSIRT-ek Hálózata, EKSZ munkacsoportja), mint az eredeti eljárás szerint.

A harmadik lépés az uniós politikai szintű integrált válságkezelési intézkedések aktiválásának szük-

[258] A Bizottság ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetre való összehangolt reagálásról 12. oldal

ségességének felmérése, azaz el kell dönteni, hogy szükséges-e valamilyen politikai koordináció, információcsere vagy döntéshozatal uniós szinten az adott eseményre. Ebben a szakaszban az elnökségnek már lehetősége van az informális kerekasztal összehívására.

A kiberbiztonsági aspektusokra való specializálás ebben a pontban azt jelenti, hogy a kerekasztal- találkozó résztvevői körét ki kell egészíteni a horizontális tanácsi munkacsoporttal, a nemzeti illetékes hatóságokkal, CSIRT-ekkel, valamint a Bizottság és az EKSZ szakterületi munkatársaival.

A Bizottság, az EKSZ és a Tanács főtitkársága közösen dönthet arról, hogy szükséges-e egy válsághelyzeti weboldal létrehozása.

A negyedik lépés az információgyűjtés és információcsere mint intézkedés.

Ebben az esetben létrehozzák az IPCR webes felületén a válsághelyzeti weboldalt, mely lehetővé teszi az elemzésekhez, politikai megbeszélések előkésztéséhez szükséges információk megosztást.

Az ötödik lépés az integrált helyzetismereti és elemzési jelentések megfogalmazása, melyet a Bizottság kezdeményez. Ezen jelentések a politikai szint számára készülnek, céljuk, hogy elősegítsék a helyzet stratégiai áttekintését. Minden esetben külön meg kell határozni a jelentés, elemzés konkrét fókuszterületeit, annak érdekében, hogy alkalmas legyen a politikai koordináció vagy döntéshozatal támogatására. A tervek szerint a kiberbiztonsági válságkezelés során ebbe a munkába bekapcsolódik a CSIRT-ek hálózata, a tagállamok kiberbiztonsági hatóságai, az Europol/EC3, a SITROOM, és a CERT-EU.

A hatodik lépés az elnökség által összehívott informális kerekasztal előkésztése, mely alatt az esemény idejét, napirendjét, résztvevőit és lehetséges/elvárt eredményeit is meghatározzák. Ezt az elnökség a Tanács Főtitkárságával együtt határozza meg.

A hetedik lépés már maga a kerekasztal, ahol a helyzet áttekintésén túl a COREPER és a Tanács elé terjesztendő javaslatok, intézkedések, témák kerülnek megvitatásra. Ez esetben annyi változás észlelhető az eredeti folyamathoz képest, hogy a kiberbiztonsági kérdések esetén a tanács kiberpolitikai kérdésekért felelős horizontális munkacsoportja készítse fel a COREPERT és a PBB-t egyaránt.

A nyolcadik lépés már maga a COREPER-en történő döntéshozatal vagy koordináció. Ez az a szakasz és döntéshozatali fórum, ahol a reagálási tevékenységek koordinálásáról, a rendkívüli intézkedések szükségességéről, illetve politikai nyilatkozatokról születnek meg a végső döntések.

A kilencedik lépés a hatások nyomon követése, melynek során a politikai döntések hatásáról és a válsághelyzet alakulásáról tájékoztatást nyújt az integrált helyzetismeretét és -elemzésért felelős szervezet.

A folyamat zárásaként a tizedik lépés folyamán el kell dönteni, hogy szükséges-e továbbra is fenntartani a válságelhárítási intézkedéseket. Az elnökség dönthet az intézkedések mértékének csökkentéséről, fenntartásáról vagy akár a megszüntetéséről is.

A Bizottság javaslata szerint az ENISA felhatalmazást kaphatna az esemény utólagos műszaki kivizsgálásának elvégzésére, vagy az abban való közreműködésre.

10.8. Célzott támadás esetén alkalmazható együttműködési és kommunikációs mechanizmusok összefoglalása

Az államok és a nemzetközi szervezetek is nagyjából az ezredforduló magasságában kezdtek foglalkozni a kibertérben megjelenő fenyegetések kérdéskörével.

Ebben a viszonylag rövid időszakban sok különböző együttműködési és kommunikációs mechanizmus fogalmazódott meg a döntéshozókban. Ezért felmerülhet bennünk a kérdés, hogy a sok különböző féle megközelítés, eljárás és együttműködési mechanizmus közül melyek alkalmazhatóak egy célzott támadás esetén, hiszen egyik sem vonatkozott kifejezetten a célzott támadásokra, minden megközelítés, szabályozás, alapelv, irányelv más-más terminológiát alkalmazott.

Ahogy a számtalan példa is mutatta fentebb, nem lehet egyértelműen kijelölni egyetlen együtt-

működési, kommunikációs vagy válságkezelési mechanizmust sem, hiszen nagyban függ az adott támadás részleteitől, specifikumaitól. A nemzetközi szervezetek és szabályozások által használt fogalmakban és terminológiákba bele érthető a célzott támadás is.

Természetesen nem szabad elfelejteni azt sem, hogy a sok önkéntesen alkalmazható és választható elvek és mechanizmusok mellett vannak olyan szabályok is melyek kötelező erejűek és nem választhatjuk ki szabadon, hogy alkalmazzuk-e egy adott esemény kapcsán.

Az áttekintett összes politikai, jogi, diplomáciai és technikai megközelítés alapján egyértelműen kijelenthető, hogy a támadás észlelését követően mindenképpen nagyon fontos az incidens (az észlelésnél még nincs pontos információnk az incidens természetéről, ezért még csak incidensnek vagy eseménynek nevezhetjük) mielőbbi kezelése, az informatikai rendszer vagy szolgáltatás mielőbbi vissza állítása, valamint az esemény alapos minden részletre kiterjedő elemzése, kivizsgálása. Ehhez a folyamathoz a legtöbb esetben már javasolt egy CSIRT bevonása, hiszen a szaktudásával támogatni tudja az elemzést.

Az incidens elemzése, vizsgálata során ki kell vizsgálni, hogy mekkora kárt okozott az incidens, történt-e adatvesztés vagy sérülés, határon átnyúló incidensről van-e szó (ha igen akkor mely országok érintettek benne), mi okozta az incidenst stb. Ezen vizsgálat során derülhet fény arra is, hogy célzott támadással állunk szemben.

A nemzeti szintű együttműködés és információ megosztás esetében támadásról és részleteiről nemzeti szinten értesíteni kell a szektorért felelős CSIRT-et, bűncselekményre utaló jelek esetén a Bűnüldöző hatóságot (Nemzeti Nyomozó Iroda), valamint személyes adatok integritása vagy bizalmassága sérülése esetén a Nemzeti Adatvédelmi és Információszabadság Hatóságot (NAIH) is.

Ez esetben a CSIRT és a többi hatóság együttműködik az incidens kivizsgálásában, egymásnak átadják a releváns információkat. A CSIRT az incidens kezelésén túl segítséget nyújthat a szükséges válaszintézkedések kiválasztásában, biztonsági tanácsadással, tudatosító tevékenységgel.

A nemzetközi információ megosztási és együttműködési lehetőségek vonatkozásában számos lehetőség áll rendelkezésünkre a célzott kiberbiztonsági incidensre vonatkozó információ megosztására.

A CSIRT-ek különböző együttműködésének keretében történő információ megosztásnak több féle célja lehet:

- figyelmeztetés, tájékoztatás nyújtása,
- technikai segítség kérése az incidens kezelése vagy elemzése során,
- az incidensnek nem egyetlen célpontja volt és célunk a többi támadással megcélzott szervezet vagy személy figyelmeztetése.

Fontos kiemelni, hogy a NIS irányelv által megfogalmazott szabályok kötelező erejűek, tehát a hatálya alá eső szektorok határon átnyúló incidenseiről minden esetben tájékoztatást kell adni a CSIRT-ek hálózatának, valamint fel kell venni a kapcsolatot az incidensben érintett további tagállamok kapcsolattartó pontjaival a Nemzeti Kibervédelmi Intézetnek mint a magyar kapcsolattartó pontnak.

A NIS szerinti együttműködési mechanizmus alapján itt lehetőség van megmaradni annál, hogy egyszerűen csak tájékoztatjuk az érintett felet a támadásról vagy esetleg együttműködve közösen kezeljük, elemezzük az incidenst, keressük a lehetséges támadót.

Abban az esetben, ha olyan országok is érintettek a támadásban, melyek nem uniós tagállamok, így nem tagjai az európai uniós közösségeknek, akkor egyéb nemzetközi vagy regionális CSIRT közösségek keretében tudjuk felvenni az adott ország CSIRT-jével a kapcsolatot.

Az ENSZ ugyan fontos alapelveket és célokat fektetett le az információ megosztás, együttműködés, valamint az államok felelős viselkedése kapcsán, de a jelenlegi tapasztalatok szerint ezen platform leginkább az incidens után a tapasztalatok megosztására, a probléma elvi megvitatására nyújt lehetőséget. Az EBESZ keretein belül már nagyobb lehetőségek mutatkoznak célzott támadás esetén alkalmazható együttműködésre, kommunikációra. A nyolcadik bizalomerősítő célkitűzés keretében létrehozott kapcsolattartó pontoknak fontos szerepe lehet egy incidens gyors megosztásában, valamint egy esetleges válaszintézkedés, segítség megvalósításban.

Az EBESZ és az ENSZ is megfelelő diplomáciai fórum abban az esetben, ha a célzott kiberbiztonsági incidenssel kapcsolatosan felmerül valamilyen vitás helyzet vagy egyet nem értés valamely tagállammal, és vitarendezési fórumként szeretnénk a szervezetet felhasználni.

Európai Uniós szinten az együttműködés formák és lehetséges intézkedések vonatkozásában nagyon sok lehetőség áll a rendelkezésünkre. Abban az esetben, ha az információ megosztás és az egyeztetések már nem bizonyulnak elégségesnek ahhoz, hogy egy tagállam együttműködjön velünk a támadás elhárításában, akkor például a kiberdiplomáciai eszköztár biztosít számos olyan diplomáciai és politikai szintű válaszlépést, mellyel elgondolkodásra, akár még együttműködésre is tudjuk sarkallni. A komolyabb nagy kiterjedésű már a válsághelyzet irányába haladó incidensek/támadások esetében pedig rövidesen lehetőség nyílik a biztonságpolitikai válságkezelési eljárás elemeinek alkalmazására.

Mára már lehetőségünk van arra, hogy megválasszuk, hogy milyen közösségben, milyen keretek között szeretnénk együttműködni. Az együttműködés során lehetőségünk van segítséget kérni (akár technikai akár diplomáciai), megosztani tapasztalatainkat, a tapasztalatok alapján új intézkedések, szabályok stb. kidolgozásának kezdeményezésére, az incidens okán kialakult vitáink félreértéseink rendezésére (egyeztetés vagy valamilyen politikai vagy diplomáciai eszköz által), de akár egy váratlan kiberválság közös kezelésére is.

Bármely típusú fórumot választjuk az együttműködéshez és az információmegosztáshoz, nagyon fontos mindig a megfelelő és arányos intézkedések kiválasztására, a nemzetközi jog és fő alapelvek betartására kell törekedünk.

10.9. Irodalomjegyzék

ENISA (2018): ENISA Threat Landscape Report 2017 15 Top Cyber-Threats and Trends. Elérhetőség: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (utolsó letöltés: 2018. március 28.)

Kovács László – Krasznay Csaba (2010): Digitális Mohács Egy kibertámadási forgatókönyv Magyarország ellen, Nemzet és Biztonság. Elérhetőség: http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf (utolsó letöltés: 2018. március 30.)

Kovács László – Krasznay Csaba (2017): Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság. Elérhetőség: http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf (utolsó letöltés: 2018. március 30.)

Kovács Péter (2011) Nemzetközi Közjog Osiris Kiadó, Budapest.

Bruhács János (2014): Nemzetközi jog I., Dialóg Campus Kiadó – Nordex Kft., Budapest.

Európai Hálózat- és Információbiztonsági Ügynökség (2006.): CERT Cooperation and its further relevant facilitation by relevant stakeholders, Athén. Elérhetőség: www.enisa.europa.eu/publications/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders (utolsó letöltés: 2018. április 2.)

A/70/174 UN: ENSZ kormányzati szakértői csoport 2015. évi beszámolója. Elérhetőség: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement (utolsó letöltés: 2018. március 30.)

A/68/98 UN: ENSZ kormányzati szakértői csoport 2013. évi beszámolója. Elérhetőség: http://undocs.org/A/68/98 (utolsó letöltés: 2018. március 30.)

A/65/201 UN: ENSZ kormányzati szakértői csoport 2010. évi beszámolója. Elérhetőség: http://undocs.org/A/65/201 (utolsó letöltés: 2018. március 30.)

A/60/202 UN: ENSZ kormányzati szakértői csoport 2005. évi beszámolója Elérhetőség: http://undocs.org/A/60/202 (utolsó letöltés: 2018. március 30.)

11. JOGSZABÁLYTÁR

11.1. Magyar jogszabályok

- 2001. évi XXXV. törvény az elektronikus aláírásról

Elérhetőség: https://mkogy.jogtar.hu/?page=show&docid=a0100035.TV (utolsó letöltés: 2018. március 30.)

- 2003. évi C. törvény az elektronikus hírközlésről

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV (utolsó letöltés: 2018. március 30.)

- 2009. évi CLV. törvény a minősített adat védelméről

Elérhetőség: http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131 (utolsó letöltés: 2018. március 30.)

- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1000157.tv (utolsó letöltés: 2018. március 30.)

- 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

Elérhetőség: https://net.jogtar.hu/jogszabaly?docid=A1100128.TV (utolsó letöltés: 2018. március 30.)

- 2011. évi CXII. törvény információs önrendelkezési jogról és az információszabadságról

Elérhetőség: http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945 (utolsó letöltés: 2018. március 30.)

- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv (utolsó letöltés: 2018. március 30.)

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Elérhetőség: http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158 (utolsó letöltés: 2018. március 30.)

- 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól

Elérhetőség: https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV (utolsó letöltés: 2018. március 30.)

- 2015. évi CXLIII. törvény a közbeszerzésekről

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500143.TV (utolsó letöltés: 2018. március 30.)

- 2016. évi CL. törvény az általános közigazgatási rendtartásról

Elérhetőség: https://net.jogtar.hu/jogszabaly?docid=A1600150.TV (utolsó letöltés: 2018. március 30.)

- 86/1997. (V. 28.) Korm. rendelet a Magyar Köztársaság Kormánya és a Németországi Szövetségi

Köztársaság Kormánya között Budapesten, 1989. december 18-án aláírt légiközlekedési egyezmény kihirdetéséről
Elérhetőség: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99700086.KOR (utolsó letöltés: 2018. március 30.)
• 168/2004. (V. 25.) Korm. rendelet a központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről
Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400168.KOR (utolsó letöltés: 2018. március 30.)
• 83/2012. (IV. 21.) Korm. rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról
Elérhetőség: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200083.KOR&txtreferer=A1500042.BM (utolsó letöltés: 2018. március 30.)
• 85/2012. (IV. 21.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól
Elérhetőség: http://njt.hu/cgi_bin/njt_doc.cgi?docid=148205.295314 (utolsó letöltés: 2018. március 30.)
• 84/2012. (IV. 21.) Korm. rendelet az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.kor (utolsó letöltés: 2018. március 30.)
• 65/2013 (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300065.kor (utolsó letöltés: 2018. március 30.)
• 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásairól
Elérhetőség: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300301.KOR&txtreferer=A1300050.TV (utolsó letöltés: 2018. március 30.)
• 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről
Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300484.kor (utolsó letöltés: 2018. március 30.)
• 535/2013. (XII. 30.) Korm. rendelet a pénzügyi intézmények, a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről
Elérhetőség: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300535.KOR&txtreferer=A1300235.TV (utolsó letöltés: 2018. március 30.)
• 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
Elérhetőség: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf (utolsó letöltés: 2018. március 30.)
• 60/2014. (III. 6.) Korm. rendelet a támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról
Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1400060.kor (utolsó letöltés: 2018. március 30.)
• 1631/2014. (XI. 6.) Korm. határozat a Digitális Nemzet Fejlesztési Program" megvalósításáról
Elérhetőség: http://net.jogtar.hu/jogszabaly?docid=A14H1631.KOR&getdoc=1 (utolsó letöltés: 2018. március 30.)
• 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500185.kor (utolsó letöltés: 2018. március 30.)

- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor (utolsó letöltés: 2018. március 30.)

- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR (utolsó letöltés: 2018. március 30.)

- 1052/2015. (II. 16.) Korm. határozat a Közigazgatás- és Közszolgáltatás-fejlesztési Stratégiával kapcsolatos feladatokról

Elérhetőség: https://net.jogtar.hu/getpdf?docid=A15H1052.KOR&targetdate=fffffff4&printTitle=1052/2015.+%28II.+16.%29+Korm.+hat%C3%A1rozat&referer=http%3A//net.jogtar.hu/jr/gen/hjegy_doc.cgi%3Fdocid%3D00000001.TXT (utolsó letöltés: 2018. március 30.)

- 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról

Elérhetőség: https://net.jogtar.hu/jogszabaly?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (utolsó letöltés: 2018. március 30.)

- 157/2016. (VI. 13.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet módosításáról

Elérhetőség: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600157.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (utolsó letöltés: 2018. március 30.)

- 228/2016. (VII. 29.) Korm. rendelet az állami szervek informatikai fejlesztéseinek koordinációjáról

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1600228.kor (utolsó letöltés: 2018. március 30.)

- 1488/2016. (IX. 2.) Korm. határozat a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról

Elérhetőség: https://net.jogtar.hu/jogszabaly?docid=A16H1488.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (utolsó letöltés: 2018. március 30.)

- 1536/2016. (X. 13.) Korm. határozat a köznevelési, a szakképzési, a felsőoktatási és a felnőttképzési rendszer digitális átalakításáról és Magyarország Digitális Oktatási Stratégiájáról

Elérhetőség: https://net.jogtar.hu/jogszabaly?docid=A16H1536.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (utolsó letöltés: 2018. március 30.)

- 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia 2016. évi monitoring jelentéséről, a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről

Elérhetőség: https://net.jogtar.hu/jogszabaly?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (utolsó letöltés: 2018. március 30.)

- 23/2013. (XI. 6.) MNB rendelet a jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank alapvető feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről

Elérhetőség: https://www.mnb.hu/letoltes/23-2013-xi-6-mnbrendelet.pdf (utolsó letöltés: 2018. március 30.)

- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információ-

biztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

Elérhetőség: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300026.KIM (utolsó letöltés: 2018. március 30.)

- 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről

Elérhetőség: http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/9.pdf (utolsó letöltés: 2018. március 30.)

- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm (utolsó letöltés: 2018. március 30.)

- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

Elérhetőség: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm (utolsó letöltés: 2018. március 30.)

11.2. Európai uniós jogi aktusok

- Számítástechnikai bűnözésről szóló Egyezmény (2001)

Elérhetőség: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa405 (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10) az Európai Hálózat és Információbiztonsági Ügynökség létrehozásáról

Elérhetőség: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről

Elérhetőség: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013R0526&from=HU (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

Elérhetőség: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament és a Tanács rendelet tervezete az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról

Elérhetőség: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52017PC0477R%2801%29 (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

Elérhetőség: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hír-

közlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről
Elérhetőség: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament és a Tanács 2013. augusztus 12-i 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

Elérhetőség: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33193&from=EN (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

Elérhetőség: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU (utolsó letöltés: 2018. március 30.)

- Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér

Elérhetőség: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=HU (utolsó letöltés: 2018. március 30.)

- Közös Közlsemény az Európai Parlamentnek és A Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése vonatkozásában

Elérhetőség: http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN (utolsó letöltés: 2018. március 30.)

- Az ENSZ Közgyűlés a 2003. december 8-i 58/32-es számú határozata

Elérhetőség: https://undocs.org/A/RES/58/32 (utolsó letöltés: 2018. március 30.)

- Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé" című dokumentumról (2011/2284(INI))

Elérhetőség: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012IP0237&qid=1521197299768&from=HU (utolsó letöltés: 2018. március 30.)

- A Tanács következtetései a kiberdiplomáciáról (2015)

Elérhetőség: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf (utolsó letöltés: 2018. március 30.)

- A Bizottság 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról

Elérhetőség: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.HUN&toc=OJ:L:2017:239:TOC (utolsó letöltés: 2018. március 30.)

- A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (2017):

Elérhetőség: http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf (utolsó letöltés: 2018. március 30.)

11.3. Külföldi jogi aktusok

- Az EBESZ Állandó Tanácsának PC.DEC/1039 számú döntése:

Elérhetőség: https://www.osce.org/pc/90169?download=true (utolsó letöltés: 2018. március 30.)

- Az EBESZ bizalomépítő intézkedései: PC.DEC/1106

Elérhetőség: https://www.osce.org/pc/109168 (utolsó letöltés: 2018. március 30.)

12. FOGALOMTÁR

- **Adat**: Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas, számos megjelenési formát vehet fel (például alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása. [1]
- **Adatalany**: Bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet. [2]
- **Adatbiztonság***:* Az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében. [2]
- **Adathalászat**: Más néven phishing, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül, – például e-mailben, azonnali üzenetben, vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. [3]
- **Adatfeldolgozás**: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől). [2]
- **Adatfeldolgozó***:* Az a személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi. [2]
- **Adathordozó***:* Minden olyan anyagi eszköz, mely alkalmas adatok megőrzésére, tárolására. Az Európai Parlament és a Tanács 2002/65/EK irányelve szerint, amely már tartós adathordozóként nevesít: olyan eszköz, amely lehetővé teszi a fogyasztó számára a személyesen neki címzett adatoknak a jövőben is hozzáférhető módon és az adat céljának megfelelő ideig történő tárolását, valamint a tárolt adatok változatlan formában történő megjelenítését". Így adathordozó a pendrive, a DVD, CD, SSD kártya, amely alkalmas kisebb vagy nagyobb mennyiségű adat tárolására. [4]
- **Adatkezelés***:* Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése. [2]
- **Adatkezelő***:* Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja,

vagy az általa megbízott adatfeldolgozóval végrehajtatja. [2]
• **Adatvédelem***:* A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások.[5]
• **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens. [2]
• **Adattal rendelkezés:** A birtokban tartás, az adat alapján további adat készítése, az adat másolása, sokszorosítása, a betekintés engedélyezése, a feldolgozás és felhasználás, a minősítés (biztonsági osztályba sorolás) felülvizsgálata, a minősítés (biztonsági osztályba sorolás) felülbírálata, a nyilvánosságra hozatal, titoktartási kötelezettség alóli felmentés, megismerési engedély kiadása. [5]

- **Adminisztratív védelem**: A védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás. [5]
- **Advanced persistent threat (APT)**: Magas szintű, tartós vagy más néven (és az anyagban is használt) célzott támadás olyan titkos és folyamatos számítógépes hackerfolyamatok sorozatát jelenti, amelyeket gyakran meghatározott személy, személyek vagy szervezet ellen követnek el. Az APT általában magánszervezetek, államok vagy mindkettő ellen irányul, és üzleti vagy politikai motívumok vezérlik az elkövetőket, a cél általában információszerzés, de előfordult már olyan támadás is, melynek célja a szabotázs volt. [6]
- **Android**: Linux kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve. [7]
- **Auditor**: Valamilyen szempontrendszernek, előírásnak, elvárásnak való megfelelést ellenőrző személy. [8]
  • **Authentikáció**: Az authentikáció az a folyamat, amelynek során ellenőrizzük a felhasználó identitását és azt, hogy hozzáférhet-e a rendszerhez. A felhasználók azonosításakor az alábbi négy lehetőség közül választhatunk: tudás (valami, amit csak a felhasználó tud), tulajdon vagy birtok (valami, ami csak a felhasználónál van), tulajdonság (a felhasználóra jellemző egyedi biológiai tulajdonság). [9]
- **Automatizált informatikai biztonsági vizsgálat**: Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre. [10]
- **Backdoor („hátsóajtó) program:** A felhasználók számára általában nem látható elem, amelyet a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nem csak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként). [11]
- **Bankbiztonsági tevékenység**: Mindazon tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való intézményes gondolkodás, amely a pénzintézet saját tulajdonú tárgyainak, értékeinek, valamint az alkalmazottak és az ügyfelek biztonságának védelmét szolgálja. [12]
- **Banktitok:** Minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel

kötött szerződéseire vonatkozik. [5]

- **Belső adatvédelmi felelős**: Az adatkezelő/adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó azon munkavállaló, aki az adatvédelmi szabályok betartásáért, a személyes adatok védelméért a szervezet nevében felelős. [2]
- **Betörés detektáló eszköz:** Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e, vagy sem. Fajtái a minta alapú betörés detektáló eszközök (signatura-based IDS) és a viselkedést vizsgáló betörés detektáló eszközök (behavior-based IDS). Intrusion Detecting Systems (rövidítve: IDS). [13]
- **Big Data**: A cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és ügyfelek számára. [14]
- **Biometrikus azonosítás**: Olyan eszközök és eljárások összessége, amely a személyek mérhető testi tulajdonságait használják fel valamilyen technika segítségével azonosításra vagy a személyazonosság megállapítására. Az azonosítás szempontjából a legalkalmasabb adatok, illetve eljárások: a DNS-minta, ujjnyomatok, retinaképek, hangelemzés, íriszdiagnosztika, tenyér vénamintáinak azonosítása, gépelési minta alapú azonosítás. [15]
- **Bitcoin**: Egy virtuális fizető eszköz, amely titkosított csatornán keresztül teszi lehetővé a fizetést. Ennél fogva különösen népszerű az illegális cselekmények finanszírozásában, legyen szó kábítószer-, fegyverkereskedelemről vagy akár terrorizmus finanszírozásról. A legelső és legismertebb kriptovaluta, 2009-ben került kibocsátásra egy Satoshi Nakamoto álnéven ismert ember által. [16]
- **Bizalmasság elve***:* Az elektronikus információs rendszer azon tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról csak az arra jogosult és csak a jogosultság szintje szerint férhet az adathoz és használhatja fel. [1]
- **Biztonság:** A biztonságot olyan állapotnak tekinthetjük, amelyben kizárható, vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak a veszéllyel szembeni eredményes védekezés feltételei. [5]
- **Biztonsági esemény***:* Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. [5]
- **Biztonsági esemény kezelése***:* Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység. [5]
- **Biztonsági osztály***:* Az elektronikus információs rendszer védelmének elvárt erőssége. [5]
- **Biztonsági osztályba sorolás***:* A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása. [5]
- **Biztonsági szint***:* A szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonsági szintbe sorolás***:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonságtudatosság**: A felhasználó azon magatartása, amikor betartja az információbiztonsági szabályokat, megérti az információbiztonságban betöltött szerepét és figyel az őt esetlegesen érintő fenyegetésekre. [8]
- **Biztonságtudatossági kampány**: Olyan pár napig, hétig vagy hónapig tartó akciósorozat, melynek célja a biztonságtudatosság fejlesztése, fokozása, az ismeretek naprakészen tartása. [8]

- **Biztonságtudatossági oktatás**: Olyan képzés, melynek célja a biztonságtudatossági ismeretek átadása, a biztonságtudatosság fejlesztése. [8]
- **Biztonságtudatossági program**: Olyan, általában egész évet felölelő akciósorozat, melynek célja a biztonságtudatosság fejlesztése, fokozása, az ismeretek naprakészen tartása. [8]
- **Biztonságtudatossági tréning**: Olyan gyakorlatias képzés, melynek célja a biztonságtudatossági ismeretek elmélyítése, begyakorlása. [8]
- **Black-hat hacker:** Ide tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba. Sok black-hat válik később white-hat hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon white-hat hackerként, hogy előtte soha nem próbált betörni egy számítógépbe sem. Így a határ inkább etikus és etikátlan hackerre osztható. [17]
- **Bot-hálózat**: A botnet olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást. Ezeket egész egyszerűen csak „botoknak”, vagy zombi gépeknek hívjuk. A ilyen számítógépeket többnyire valamilyen malware-rel fertőzik meg azért, hogy a távolból is irányítani lehessen őket. A „bot” kifejezés a „robot” szóból ered és csakúgy, mint a robotok, a szoftveres botok is lehetnek jók és rosszak is. Amikor a számítógépünk egy botnet része, akkor rendszerint malware-rel van megfertőzve. A bot ilyenkor vagy egy távoli szerverrel létesít kapcsolatot, vagy egész egyszerűen csak más, közeli botokkal lép kapcsolatba, majd ezt követően várja az utasításokat a hálózat irányítójától. Mindez pedig lehetővé teszi a támadó számára, hogy egyszerre több számítógép irányításával valósíthassa meg az általában nem túl „nemes” céljait. [18]
- **Call center**: Egy vállalaton belüli – vagy kiszervezett – funkció, amelynek segítségével a szervezet nagyszámú telefonhívást képes hatékonyan kezelni. Magát azt a technikai eszközt, speciális telefonközpont-számítógép-szoftver rendszert is call centernek nevezzük, ami ezt a funkciót ellátja. [19]
- **Célszemély**: Olyan felhasználó, akit a támadó kiszemel egy potenciális támadás végrehajtásához és megpróbál megtéveszteni. [8]
- **Célzott támadások** (Targeted Attacks): Célzott támadásoknak nevezzük az olyan fenyegetéseket, melyeket a támadók kifejezetten egy adott célpont (személy vagy szervezet) ellen használnak. Egy számítógépes vírushoz képest a fenyegetés „megalkotója” ebben az esetben nem arra törekszik, hogy a kártékony kód minél jobban elterjedjen, hanem arra, hogy a kiszemelt célpont eszközére, eszközeire bejusson. [13]
- **Célhoz kötött adatkezelés**: Személyes adat kizárólag előre meghatározott célból kezelhető, valamely jog gyakorlása vagy kötelezettség teljesítése érdekében. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és – ha az adatkezelés céljára tekintettel szükséges – naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. [20]
- **Chipkártya**: A mikroprocesszoros chipkártya jelenleg a legkorszerűbb elektronikus adathordozó kártya. Maga a chipkártya elnevezés széles termékskálát jelöl. Ide tartozik minden olyan bankkártya méretű (az ISO 7810 szabvány szerint) műanyag kártya, amely beépített mikrochipet tartalmaz, ugyanakkor paramétertől függően számos típust lehet megkülönböztetni. A két alapvető csoport az „unintelligens” memóriakártya és az intelligens mikroprocesszoros kártya. [21]
- **CIA**: Az elektronikus információs rendszer védelmének alapvető céljának, a bizalmasság (angolul: confidentiality), a sértetlenség (angolul: integrity) és a rendelkezésre állás (angolul: availability) védelmi hármasának jelölése. [5]
  • **CMX gyakorlat (Crisis Management Exercise)**: A CMX a NATO egyik legfontosabb gyakorlata, személyesen a NATO-főtitkár vezeti. A gyakorlat forgatókönyve teljes mértékben fiktív eseményeken alapul és fiktív földrajzi környezetben játszódik: a leírt válsághelyzet a NATO

kollektív védelmi feladataira koncentrál a Washingtoni Szerződés 4. és 5. cikkelye szerinti szituációban, beleértve ebbe úgy a tárgyalásos válságrendezést, mint a katonai megoldás lehetőségét is. Olyan gyakorlatok, melyeket a Honvédelmi Minisztérium által vezetett szakember gárdának évente el kell végeznie. Kormányzati szintű törzsvezetési gyakorlat, melyen részt vesznek az érintett minisztériumok képviselői, illetve meghatározott, kijelölt intézményei. A Gyakorlatot a HM Védelmi Hivatala vezeti. A gyakorlat célja a szövetség válságkezelési eljárásainak gyakorlása stratégiai politikai szinten, amelyben a tagországok, a NATO-parancsnokság, a stratégiai parancsnokságok civil és katonai szakemberei vesznek részt. Ezáltal a válságkezelés hazai szakértői és döntéshozói vegyenek részt a NATO konzultációs és döntéshozatali folyamatában, gyakorolják Magyarország polgári-, katonai válságkezelési eljárásait. [12]

- **Cloud computing**: („számítástechnikai felhő”, „felhő alapú informatika”): A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (például Gmail) vagy az online tárhelyek (például Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni. [2]
- **Content-injection phishing**: Olyan módszert jelent, amikor rossz szándékú tartalmat helyez el a támadó egy legitim oldal kódjában. Ez a tartalom legtöbbször átirányítja a látogatót egy, a támadó által előkészített weboldalra, kártékony kódot telepít a felhasználó számítógépére, vagy a felhasználó által a módosított weboldalon bevitt adatokat azonnal továbbítja a támadó számára. [22]
- **Cookie-k („sütik”)**: Rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (például egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (például egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Az Európai Bizottság irányelvei alapján cookie-kat (kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek) csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni. A cookie-k ugyanis számos adatvédelmi aggályt vetnek fel, például a segítségükkel nyomon követhetőek a felhasználó böngészési szokásai. [2]
  •**Cookie poisoning**: Más néven sütimérgezés, amely a weblapok működését segítő dinamikus tartalmak, cookie-k, módosítását és azok a webszervernek történő eljuttatását jelenti. A manipulálás különféle módokon lehetséges. [23]
- **Covering tracks**: Az IT támadások egyik lépése, amely a nyomok eltüntetéséről szól. Ez egy célzott támadásnál kiemelt jelentőséggel bírhat, hiszen a támadó még kevesebb információt szeretne magáról hagyni ezekben az esetekben, mint máskor. A profi támadó addig tevékenykedik, amíg el tudja úgy fedni, tüntetni a tevékenysége által okozott nyomokat, hogy arra ne, vagy csak nagyon későn jöjjenek rá. [23]

- **Crime as a Service**: Szolgáltatásszerű bűnözés.
- **Crack**: A programok védelmének „feltörése”, kijátszása. A crack eredeti jelentése: valami keménynek (például dióhéjnak) az összeroppantása, feltörése. [5]
- **Cracker**: Az informatikai rendszerbe informatikai eszközöket használva, direkt rombolási céllal betörő személy. [5]
- **Cryptoloot**: Kriptobányász, amely az áldozat CPU vagy GPU teljesítményét, valamint elérhető erőforrásait használja crypto-bányászatra, tranzakciókat rendelve a blockchainhez, így szabadítva fel új valutát. [16]
- **Dark Web (Dark Net)**: A Deep Web része, ahol alapvetően illegális cselekmények folynak.
- **Data theft**: Az adatlopó kódok előre meghatározott információkat keresnek az áldozat gépén és azokat küldik el az adathalászoknak/támadóknak. Ilyen információk lehetnek például a jelszavak, licenszkulcsok, aktiváló kódok, email-ek, bankkártya adatok, személyes adatok, illetve bármilyen, keresőszavaknak vagy keresőkifejezéseknek megfelelő tartalom. Ez a fajta támadás a vállalati kémkedés legkedveltebb eszköze, mert azok az érzékeny információk, melyek egy jól védett szerveren tárolódnak, a legtöbb esetben megtalálhatóak a kliens gépeken is valamilyen formában. A kliens gépek védelme pedig általában alacsonyabb szintű, mint a szerverek védelme. [22]
- **Domain Name System (DNS):** Azaz a tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott tartománynevekhez (doménekhez) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le”, „oldja fel”, melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton. [22]
- **DNS szerver**: A DNS-kiszolgáló egy olyan szolgáltató oldali szerver, amely az internetes címek fordításáért felelős. Ezen szerver segítségével tudunk az interneten keresztül weboldalakon böngészni, e-maileket küldeni és fogadni. [22]
- **Dumpster diving**: Magyarul hulladék-átvizsgálásnak, „kuka-búvárkodásnak” nevezetett technika, mely során a támadó átvizsgálja a célszemély szemetesét. A hulladékban a támadó rengeteg olyan dolgot találhat, amely segítséget nyújthat egy esetleges támadás előkészítéséhez és végrehajtásához. [8]
- **Elektronikus információbiztonság**: Távközlési és informatikai, valamint egyéb elektronikus rendszerekben és a támogató infrastruktúrákban alkalmazott rendszabályok összessége, amelyek védelmet nyújtanak az elektronikusan előállított, feldolgozott, tárolt, továbbított és megjelenített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen. [3]
- **Elektronikus információs rendszer**: Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. [5]
- **Elektronikus információs rendszer biztonsága**: Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [5]
- **Elosztott szolgáltatás megtagadásos támadás***:* Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elér-

hetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]

- **Emberi tényező**: Humán faktor. Ide érthető minden emberi erőforrás, felhasználó, legyen akár magánszemély vagy munkavállaló. [8]
- **Enumeration**: Az IT támadásik egyik lépése, mely alatt a támadó kiszűri a hasznos információkat a korábbi lépésekből és mélyebb vizsgálatok útján el tud jutni a rejtett információkhoz, a felhasználónevekhez, a felhasználói csoportok, alkalmazások, használt protokollok, bannerek listájához. E lépés alatt történik általában a jelszavak megszerzése is.[23]
- **Escalation of privilege**: A felhasználói jogosultságok kiterjesztését foglalja magában. A cél, hogy a korábbi támadások segítségével a támadó minél magasabb szintű hozzáféréssel és jogosultággal rendelkezzen a cél rendszerben, hogy ott a valódi tevékenységet később el tudja végezni. [23]
- **Észlelés***:* A biztonsági esemény bekövetkezésének felismerése. [5]
- **Felhasználó***:* Egy adott elektronikus információs rendszert igénybe vevők köre.[5]
- **Fenyegetés***:* Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát. [5]
- **Firmware**: Közvetlenül a hardvereszközzel egybeépített ROM, PROM vagy EPROM memóriamodulban tárolt szoftver, amelynek feladata az eszköz működtetése, illetve az ahhoz szükséges alapvető be/kimeneti rutinok biztosítása. [24]
- **Fizikai védelem**: A fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem. [5]
- **Fizikai biztonság**: Fizikai biztonság körébe soroljuk az információrendszert működtető eszközrendszerek, például a számítógépek, tárolók, hálózati eszközök fizikai védelmét. A fizikai védelem eszközei többek között a beléptető rendszerek, a lopásgátló eszközök, rácsok vagy biztonsági ajtók. [9]
- **Folytonos védelem**: Az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [1]
- **Forráskód analízis**: A program forráskódjában, statikus eszközökkel, a kód futtatása nélkül keres biztonsági réseket. [13]
- **GDPR**: A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, más néven általános adatvédelmi rendelet (General Data Protection Regulation). A GDPR közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó. Ennél fogva minden tagállamban ez a rendelet lesz a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekintetében, attól eltérni csak akkor lehet, ha azt maga a GDPR megengedi. A rendeletet 2018. május 25-től kell alkalmazni.
- **Google Hacking**: Olyan információgyűjtési technika, melynek során a támadó a Google kereső operátorait használja a minél pontosabb, kifinomultabb találatok érdekében. [8]
- **Hacker**: Az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő személy. A tömegkommunikációban helytelenül minden számítógépes bűnözőre használják. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. [5]
- **Hacktivizmus**: Olyan cselekedet, amelyben a támadók számítógép hálózatokba hatolnak be, és az ott megszerzett adatokat közzéteszik, hogy így hívják fel a figyelmet az általuk képviselt célokra. Fogalmilag bár nem azonos, mégis számos közös pont van a kiberterrorizmussal. Mindkettőre jellemző, elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadások, amelyek célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Hatásuk bár elenyésző, ugyanis nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges

lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport. [25]

- **Hálózat**: Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége. [5]
- **Hardver**: Az információs rendszerek (talán) legegyértelműbb eleme, mely magában foglal minden olyan eszközt, vagy részelemet, mely az információ feldolgozásában, továbbításában, tárolásában részt vesz. Az okos eszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, melyek ideiglenesen, vagy állandó módon csatlakoztathatok az eszközhöz. [19]
- **Hardver/szoftver token**: A token egy jellemzően PIN-kóddal védett kódgenerátor, amely lehet hardveres vagy szoftveres alapon működő. A token egy egyszer felhasználható (előre meghatározott ideig érvényes) jelszót vagy kódsorozatot ad meg, ami biztonsági kódként szolgál az adott rendszerbe történő bejelentkezéshez, vagy egyéb művelet elvégzéséhez. [19]
- **Hitelesség**: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [5]
- **Hoax**: Olyan e-mail, ami valamilyen új – általában fiktív – vírus terjedésére figyelmeztet, és a fertőzés megakadályozása érdekében egy vagy több fájl törlésére ösztönöz (ezek azonban a rendszer működéséhez szükséges, de kevésbé ismert állományok). Az e-mail tovább küldésére is buzdít, hogy a levéláradat – lánc-levél – szűkkeresztmetszetet generáljon a hálózaton. [5]
- **Host file poisoning**: Amikor egy felhasználó el akar érni egy weboldalt (például www.penzintezet.hu) és a böngésző címsorába begépeli az URL címet, akkor a beírt címet a számítógépnek át kell fordítania numerikus karakterekké, azaz a domain nevet IP címmé kell átalakítania. Alapértelmezetten ez egy DNS (Domain Name System) lekérdezéssel történik. Annak érdekben, hogy ezt ne kelljen minden egyes alkalommal elvégeznie a számítógépnek, a már egyszer meglátogatott domain nevekhez tartozó IP címeket több operációs rendszer is úgynevezett host file-okban tárolja. Ha ennek a file-nak a tartalma módosításra kerül, akkor a felhasználó által megadott www.penzintezet.hu domain helyett a támadó által kívánt IP címen található oldalt fogja betölteni a böngésző. Ezen az oldalon általában egy megtévesztő másolata jelenik meg az eredeti oldalnak, így a felhasználó gyanútlanul megadhatja az eredeti oldalhoz tartozó belépési adatait, melyek így a támadóhoz kerülnek. [22]
- **HunCERT**: Az MTA SZTAKI keretén belül a működik a HunCERT csoport, amely az Internet Szolgáltatók Tanácsának (a továbbiakban: ISZT) támogatásával végzi a munkáját. Feladata, hogy az ISZT tagszervezeteinél (tehát a nem állami szereplőknél) előforduló hálózati incidensek felderítésénél, elemzésénél és kezelésénél segítséget nyújtsanak az ügyfeleknek és a tagszervezeteknek. További célja a biztonsági tudatosság növelése. Ez utóbbi tevékenység elsősorban nem a hivatásszerűen számítástechnikával foglalkozókat célozza meg, hanem az ISZT tagok nagyszámú felhasználóinak kíván olyan információt nyújtani, amely képessé teszi őket az Internet használatával együtt járó kockázatok minél teljesebb megértésére és a sikeres védekezésre. [13]
- **Hybrid felhasználó és jogosultságkezelési működés**: Olyan szervezeti működés, ahol a felhasználó és jogosultságkezelés több módszerrel támogatott egyidőben. Ezalatt értjük az Identity management rendszerrel támogatott és vezérelt, szerepkörösített rendszerek és a saját felhasználó és jogosultságkezelő funkciót alkalmazó rendszerek egyidejű működését. [19]
- **Illetéktelen személy**: Valamely tevékenység végzésére nem jogosult személy. Az informatikai biztonság esetében tipikusan az objektumba, az informatikai rendszerbe történő belépésre, adatkezelésre nem jogosult személy. [5]
- **Információ**: Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti. [1]
- **Információbiztonság***:* Olyan tevékenység vagy állapot, amely középpontjában: a bizalmasság,

a sértetlenség és rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (például alfabetikus, numerikus, grafikus, képi forma) és milyen adathordozón jelenik meg. [26]

- **Információgyűjtés (footprinting)**: Az informatikai biztonsági terminológiában a felderítést, megfigyelést foglalja magába és általában egy megelőző lépése a támadásoknak. A felderítés célja annak feltárása, hogy az információs rendszerben melyek azok a sérülékeny elemek, amelyek önállóan vagy összességében egy sikeres támadás kivitelezéséhez vezetnetnek. A felderítés, megfigyelése az információs rendszernek – a sikeres támadás érdekében – észlelés nélkül akár hónapokon, sőt éveken keresztül is folyhat, a felderítés valódi időbenisége, a támadás pontos kezdete célzott kivizsgálás és megfelelő bizonyítékok hiányában jól nem meghatározható. [27]
- **Információvédelem***:* Összetettsége miatt a definíciós meghatározás helyett, azokat a tevékenységeket rögzítjük, amelyekkel maga a védelmi tevékenyég leírható. Ide sorolható az információt hordozó entitások (személyek és eszközök) védelme, azaz az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelme, az irat- és dokumentumvédelem, valamint a személyi védelem is. Az információvédelem célja – hasonlóan az adatvédelemhez – a jogosulatlan hozzáférés, módosítás vagy megsemmisítés elleni védelem és az információk folyamatos rendelkezésre állásának biztosítása. Az információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelme. [5]
- **Informatikai biztonság**: Egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ez azt jelenti, hogy egy, az összes fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelmi rendszer. [5]
- **Informatikai biztonságpolitika**: A biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására. [5]
- **Informatikai biztonsági stratégia**: Az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere. [5]
- **IntCERT**: Az Információs Hivatal a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelése feladatának ellátására a szervezeti keretén belül működő eseménykezelő központot (IntCERT) működtet. [13]
- **Internet of Things (Iot)**: A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra, és azok internetszerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, „mérni”, és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő, vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek. [28]
- **iOS**: Az Apple Inc. mobil operációs rendszere, amelyet iPhone, iPod touch és iPad készülékekre fejlesztenek.
- **Katonai Nemzetbiztonsági Szolgálat Kibervédelmi Központja**: A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelését végző szerv.
- **Keylogger**: Más néven keystroke logger, olyan billentyűzet naplózásra alkalmas program, amely a felhasználó által begépelt karaktereket, illetve a képernyő tartalmát naplózza, majd eltárolja azt. [8]
- **Kémprogramok** (**spyware**): A rendszerbe jutva a háttérből figyelik a rendszerben lezajló eseményeket, melyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [11]
- **Kézi vagy manuális informatikai biztonsági vizsgálat**: Olyan biztonsági vizsgálati eljárás,

mely során az érintett szervezet informatikai rendszerének sérülékenységei a vizsgálatot végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával kerülnek feltérképezésre. [13]

- **Kiberbiztonság**: A kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez. [1]
- **Kibervédelem**: A kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését. [1]
- **Kiberbűnözés***:* **Célja az informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, amelyek rendkívül adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ezen a területen meglevő lehetőségeket**
- **Kiberhadviselés***:* Az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még inkább a konvencionális hadviselés támogatására. [12]
- **Kiberkémkedés***:* Az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést értünk. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület. [29]
- **Kihívás:** Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége, amelyek eredői hátrányosan befolyásolják a belső és külső stabilitást és kihatással lehetnek egy adott régió hatalmi viszonyaira. [30]
- **Kockázat***:* A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye. Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek megvalósulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. [5]
- **Kockázatazonosítás**: Célja, azon helyzetek, lehetőségek, események felismerése, melyek a kitűzött céloknak való megfelelést befolyásolhatják. Az azonosítás, a lehetőségek felmérésén túl magában kell, hogy foglalja mindazokat a tényezőket, melyek a kockázat kialakulásának környezetét jelentik. Ebben ki kell térni azokra a folyamatokra, szabályozókra, technikai eszközökre, emberekre, rendszerekre, hardver és szoftver tényezőkre stb. melyek relevánsak a kockázat és környezet megértésének szempontjából.
- **Kockázatelemzés**: Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése. [5]
- **Kockázatértékelés**: Választ kaphatunk olyan kérdésekre mint: Kell-e kezelni egy kockázatot? Ha igen, milyen sorrendben? Megkezdhető-e egy adott beruházás, folyamat a jelenlegi paraméterekkel? A különböző lehetséges megoldások közül melyiket kell választani? A különböző besorolások, értékelése értelmezésére a legtöbb esetben nem két (elfogadható, nem elfogadható) hanem három, (elfogadható, feltételekkel elfogadható, nem elfogadható) kategóriát célszerű létrehozni. [5]
- **Kockázatkezelés**: Az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása. [5]
- **Kockázattal arányos védelem**: Az elektronikus információs rendszer olyan védelme, amelynek során – egy kellően nagy időintervallumban – a védelem költségei arányosak a fenyegetések által okozható károk értékével. [5]
- **Közigazgatás**: Azon szervezetek összessége, amelyek közhatalmat gyakorolva, az állam vagy az önkormányzat nevében közfeladatokat látnak el és jogszabályokat hajtanak végre. A helyi köz-

ügyekben az önkormányzati igazgatás, az országos jelentőségű ügyekben a központi közigazgatás jár el.

- **Közérdekű adat**: Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat. [20]
- **Kormányzati Eseménykezelő Központ (GovCERT)**: A GovCERT alapvető rendeltetése az állami és önkormányzati szervek informatikai biztonsági támogatása, amely egyrészt megelőző jelleggel, úgynevezett sérülékenység menedzsment formájában a szoftver-sérülékenységek és információbiztonsági fenyegetések nyomon követésére, valamint a fenyegetés kiváltotta biztonsági esemény megelőzése érdekében az érintett IT rendszerek üzemeltetőinek tájékoztatására fókuszál. Ezen túlmenően pedig reaktív jelleggel, úgynevezett incidenskezelési tevékenységet lát el, amely a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és – több állami szervet érintően – a kezelésük koordinációjára irányul. [31]
- **Közösségi média**: Social Media vagy szociális média. Olyan tartalommegosztó felület, melyet bárki szerkeszthet. Ide sorolhatóak a közösségi oldalak (például Facebook, LinkedIn stb.), kép- és videómegosztó portálok (például Instagram, YouTube stb.), blogok, fórumok. [8]
- **Közreműködő**: Az üzemeltető, adatkezelő, adatfeldolgozó és ezen fogalmak alá tartozó személyi és szervezeti kör az Ibtv. szerint az elektronikus információbiztonság szervezeti érvényesülését illetően közreműködőnek minősül. Az adatfeldolgozón, az adatkezelőn és az üzemeltetőn túl közreműködőnek tekinti továbbá az Ibtv. az elektronikus információs rendszer létrehozásában, auditálásában, karbantartásában vagy javításában, továbbá tervezésében, fejlesztésében, vizsgálatában, kockázatelemzésében és kockázatkezelésében részt vevők körét. [2]
- **Kritikus információk**: Azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük, hatékony tervezéséhez és végrehajtásához. [13]
- **Kritikus sérülékenység**: Kritikusnak tekinthető az a sérülékenység, amely a bizalmasságot, sértetlenséget vagy rendelkezésre állást nagymértékben sérti, illetőleg a sérülékenység távolról, könnyedén vagy hitelesítés nélkül kihasználható, tehát valós és komoly veszélyt jelent a rendszerre és az abban tárolt adatokra. [13]
- **Kriptográfia**: Mindazoknak az eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek információnak illetéktelenek előli elrejtését hivatottak megvalósítani. Rejtjelzés, titkosítás. [5]
- **Kriptovaluta:** Olyan digitális eszköz, mely csereeszközként vagy manapság fizetőeszközként is funkcionál. Kriptográfiát (titkosítást) használ a tranzakciók biztonságossága érdekében. A kriptovaluták a digitális valuták egy részhalmazát képviselik, de besorolhatók az alternatív valuták vagy a virtuális valuták csoportjába is. [5]
- **Különleges adat**: Faji eredetre, nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, az érdek-képviseleti szervezeti tagságra, világnézeti vagy vallási meggyőződésre, illetve a szexuális életre vonatkozó személyes adat, továbbá e kategóriába sorolható még az egészségügyi állapotra, a kóros szenvedélyre vonatkozó, és a bűnügyi személyes adat is. [20]
- **Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK)**: A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. CLXVI. törvény alapján 2018 végéig a kijelölt létfontosságú létesítmények elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelését

– az állami és önkormányzati szervek kivételével – a BM Országos Katasztrófavédelmi Főigazgatóság által működtetett LRLIBEK látta el. [13]

- **Létfontosságú információs rendszerelem**: Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené. [1]
- **Létfontosságú rendszerelem**: Létfontosságú rendszerelemnek tekinthetők azok a rendszerek, illetve rendszerelemek, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, (például az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális szolgáltatások biztosításához) és amelynek kiesése jelentős következménnyel járna. [32]
- **Logikai biztonság**: A logikai biztonság körébe tartoznak a vírusok, a rosszindulatú kódok, az adathalászattal kapcsolatos támadások, az ilyen típusú támadások elleni védekezés, a vírusok, a hekker támadások, az adatlopás, az illetéktelen hozzáférés és módosítás, illetve az illetéktelen közzététel. [9]
- **Logikai védelem**: Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem. [5]
- **Logikai bomba**: Olyan program vagy programrészlet, amely logikailag (funkcionálisan) nem várt hatást fejt ki. Jelentkezése váratlan, hatása pusztító – innen a bomba kifejezés. [5]
- **Malware**: Az angol malicious software (kártékony szoftver, káros szoftver, rosszindulatú szoftver) összevonásából kialakított mozaikszó. Rosszindulatú szoftvernek tekinthetők azok a szoftverek, amelyek célja nem az információs rendszer működésének biztosítása és fenntartása, hanem bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek végzése. Ezen rosszindulatú szoftverek segítségével a támadó könnyedén zavart okozhat a célszemély számára, például túlterhelheti, működésében akadályozhatja, valamint akár működésképtelenné teheti a felhasználó bármely infokommunikációs eszközét. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program. [11]
- **Man-in-the-middle támadás:** A támadás során a támadó beékelődik a felhasználó és az általa elérni kívánt szerver közé. Ez a beékelődés azt jelenti, hogy a kliens által közölt adatokat a támadó szervere fogadja és továbbítja a legitim szerver felé, majd az onnan érkező válaszokat, mint kliens fogadja és továbbítja a felhasználó felé. Annak érdekében, hogy ez megtörténhessen, a támadónak már komoly előkészületeket kellett tennie, hiszen biztosítania kellett, hogy a kliens az eredeti szerver helyett először a támadóhoz csatlakozzon. Erre megoldás lehet a már fentebb részletezett DNS-spoofing vagy a kliens proxy beállításainak módosítása. Normál HTTP alapú oldalak esetében a felhasználó sok esetben nem is veheti észre, hogy nem direkt az általa meglátogatott weboldal kiszolgáló szerverével kommunikál. Ha sikeresen beékelődött a támadó, akkor minden információ, amit a kliens és a weboldal között áramlik, átfolyik a phisher szerverén így az érzékeny információk megszerezhetővé válnak. [22]
- **Megelőzés**: A fenyegetés által okozható hatás bekövetkezésének elkerülése. [5]
- **Megszemélyesítés**: Olyan támadási technika, melynek során a támadó egy valós személy személyazonosságát veszi fel, annak engedélye nélkül. [8]
- **Megtévesztés**: Olyan támadási technika, melynek során a támadó egy fiktív személynek adja ki magát egy támadás végrehajtása során. [8]
- **Metasploit Framework**: A Metasploit a világ legelterjedtebb penetrációs tesztszoftvere, mely segítségével megtámadhatjuk a saját rendszerünket úgy, ahogy egy hacker tenné, így kiderít-

hetjük, hol vannak sötét foltok a védelemben. Lehetőséget biztosít arra, hogy a szakértők megismerkedhessenek az exploitokkal és tesztelhessék saját rendszereik védelmét. De ugyanúgy a támadóknak is megnyitja a lehetőséget arra, hogy ezeket a biztonsági hibákat számítógépek megfertőzésére kihasználhassák. [33]

- **Mimikatz**: Egy szabad forrású program, ami a memóriában található jelszavakat és jelszó hasheket gyűjti ki, ezeket a kezdeti fertőzés után a lokális hálózaton belüli továbbterjedéshez szokták használni a célzott támadások során. Ezen felül a kifejezetten romboló céllal alkalmazott NotPetya használta a lokális hálózaton belüli autonóm terjedéshez. [33]
- **Minősített adat**: A minősített adat (korábbi elnevezése: államtitok vagy szolgálati titok) olyan minősítéssel védhető közérdek körébe tartozó információ, amelyről megfelelő eljárásban megállapította a minősítésre jogszabályban felhatalmazott személy, hogy az adat érvényességi időn belüli nyilvánosságra hozatala, illetéktelen személy részére hozzáférhetővé tétele veszélyezteti Magyarország biztonságát. „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása, nyilvánosságra hozatala bűncselekmény. [5]
- **Munkavállaló**: Fogalmát a 2012. évi I törvény, a Munka Törvénykönyve határozza meg. Ez alapján munkavállalónak tekinthető az a természetes személy, aki munkaszerződés alapján munkát végez. Így minden 16. életévet betöltött személy, aki jogviszony formájában, díjazás fejében elvégzi a munkát.
- **NAIH**: Nemzeti Adatvédelmi és Információszabadság Hatóság: az Infotv. által 2012. január 1-jével létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.
- **NEIH**: Nemzeti Elektronikus Információbiztonsági Hatóság, amely az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. A hatóság egyik legfontosabb feladatként elbírálja az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását, valamint ellenőrzi az elektronikus információs rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését. A rendelkezésre álló információk alapján kockázatelemzést végez és az éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést. Ezen túlmenően a hatóság elrendeli az ellenőrzés során feltárt, vagy más módon tudomására jutott biztonsági rések elhárítását, és ellenőrzi a helyreállító intézkedés eredményességét. [13]
- **Nemzeti Kiberbiztonsági Koordinációs Tanács**: Az e-közigazgatásért felelős miniszter (jelenleg a belügyminiszter) által vezetett Nemzeti Kiberbiztonsági Koordinációs Tanács a Kormány javaslattevő, véleményező szerveként gondoskodik az Ibtv. hatálya alá tartozó szervezetek információbiztonsági tevékenységeinek összehangolásáról. [13]
- **Nemzeti Kibervédelmi Intézet**: A kiberfenyegetések okozta kihívásokra reagálva, a kiberbiztonság növelése, az egységes és hatékony, párhuzamosságokkal kevésbé tagolt kibervédelmi struktúra megteremtése érdekében jött létre a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI). Az NKI legfőbb feladata és célja, hogy Magyarország egy összehangolt, szervezett tevékenység keretében legyen képes a modern kor egyik legnagyobb kihívásának, a kiberbiztonság megteremtésének és erősítésének az élharcosa és a kibervédelem letéteményese lenni, a globális és a hazai kibertérből érkező fenyegetéseket hatékonyan kezelni, azok megelőzésére szakszerű segítséget nyújtani. [13]
- **Nulladik napi (0-day) sérülékenység**: Olyan számítógépes szoftveres biztonsági rés, amely ismeretlen azok számára, akik érdekeltek lennének a sebezhetőség enyhítésében, befoltozásában (beleértve a célszoftver gyártóját is). A biztonsági rést kihasználva a hackerek hozzáférhetnek a számítógépes programokhoz, adatokhoz, további számítógépekhez vagy hálózatokhoz. Egy nulladik napi sebezhetőségre irányuló támadást nulladik napi exploitnak (kihasználásnak) vagy

nulladik napi támadásnak neveznek. [13]
- **Obfuszkáció**: A forrás vagy gépi kód ember általi megértésének szándékos megnehezítése. [13]
- **Paid archive**: A hamis szoftver-telepítők a 2009-2010-es években jelentek meg, céljuk szintén nem a rendszerben történő károkozás, hanem hogy rávegyék a gyanútlan és hiszékeny felhasználókat a támadó által kért összeg kifizetésére. Ezeket nevezik "paid archive"-eknek is, melyek olyan ön-kicsomagoló állományok, amiket csak fizetés után lehet kicsomagolni. Általában valamilyen (többnyire) ingyenesen letölthető, valós, hiteles program (például Skype, Adobe Flash Player, böngésző, Microsoft termék, tömörítő program, zenelejátszó stb.) telepítőjének tűnnek. [8]
- **PDCA ciklus**: Plan – Do – Check – Act, más néven a Tervezés – Végrehajtás – Ellenőrzés – Beavatkozás ciklusa. A PDCA bármilyen műveletre, tevékenységre, folyamatra, rendszerre, működtetésre, koncepcióra, elgondolásra vonatkoztatható, zárt hatásláncú, folytonosan ismétlődő körfolyamat-elv. A PDCA modell négy szakaszból áll. Az első szakasz a Tervezés (Plan), amely a fennálló helyzet tanulmányozását, adatgyűjtést és a javítás megtervezését foglalja magában. A második szakasz a Végrehajtás (Do) mely során megvalósul a terv kipróbálása kísérleti jelleggel egy kisebb projekt vagy a felhasználók egy szűkebb körén belül alkalmazva. A harmadik szakasz az Ellenőrzés (Check), amely változtatások hatásának elemzése és értékelése. A negyedik szakasz a Beavatkozás (Act), amely magában foglalja a bevált módszer bevezetését és szabványosítását. Ez a ciklus minden folyamatjavító koncepció alapja. [3]
- **Pharming**: Más néven az eltérítéses adathalászat célja, hogy a legitim szolgáltatást használni kívánó felhasználót a szolgáltatás domain nevének eltérítésével a hamisított weboldalra irányítsa. [8]
- **Piggybacking**: Ez a technika tulajdonképpen más jogosultságának felhasználását jelenti, és általában az épületbe való jogosulatlan bejutás megvalósításához szokták alkalmazni a social engineerek. Leginkább szoros követésnek, vagy besurranásnak lehet fordítani. Legjobb példája, amikor a támadó egy munkatársnak, vagy legalábbis belépésre jogosult személynek adja ki magát, s az irodába igyekezvén eljátssza, hogy otthon felejtette kulcsát vagy belépőkártyáját, és megkér valakit, hogy engedje be a sajátjával. [8]
- **Planting of backdoors**: Azaz a hátsó kapuk nyitva hagyása. Sok esetben szeretné a támadó biztosítani, hogy később is hozzá férhessen a korábban megtámadott rendszerhez, ezért olyan úgynevezett backdoorokat hagy hátra, ami segítségével ez lehetséges lesz számára. A médiában lehet hallani olyan eseteket, ahol eszközökben, szolgáltatásokban előre dedikált hátsó kapuk találhatóak, melyet a gyártók maguktól, esetleg kormányzati hatásra hagytak termékeikben. [23]
- **POC**: Proof Of Concept. Valamilyen koncepció mentén elkészített terv kipróbálása a gyakorlatban. [19]
- **PreDeCo (Preventive-Detective-Corrective) elv**: Ezen elv magába foglalja a megelőzést, azaz a fenyegetés által okozható hatás bekövetkezésének elkerülését, a korai figyelmeztetést, azaz olyan aktív szervezeti cselekvést, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni, az észlelést, azaz a biztonsági esemény bekövetkezésének felismerését, és a reagálást, amely a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedéseket. Továbbá a biztonsági események kezelését, amely magába foglalja a dokumentálást, a következmények felszámolását, a bekövetkezés okainak és felelőseinek megállapítását, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet. [34]
- **Preventív vagy megelőző intézkedés**: Amikor egy szervezet meghatározott időközönként a megelőző intézkedés keretein belül feltérképezi az általuk használt informatikai rendszerek sebezhetőségét, sérülékenységét, ezzel meghatározza a külső és belső „hiányosságokat", gyenge pontokat és lehetséges javaslatokat, intézkedéseket tesz az esetleges támadások megelőzésére és elhárítására. [12]

- **Privilegizált jogosultság**: Olyan kiemelt jogosultság, amelyet jellemzően a rendszer működéséért felelős személyek (rendszergazdák, adminisztrátorok) vagy processzek, programok, technikai felhasználók és alkalmazások birtokolnak. [19]
- **Proaktív biztonsági intézkedés**: Proaktív intézkedésről akkor beszélünk, amikor egy szervezet védelmi rendszere képes valós idejű reakcióra a szervezetet érő támadás esetén. A proaktív magatartás tulajdonképpen egy megelőzésre törekvő magatartás, a reaktív magatartás helyett. Ebbe a típusba tartozik az előző, azaz a preventív szakaszban- talált sérülékenységek javítása. [12]
- **Puffer túlcsordulás**: Olyan szoftverhiba, sokszor biztonsági rés, melynél egy processz a fix hosszúságú tömbbe (puffer) történő íráskor nem ellenőrzi annak határait, így azt (például túl hosszú bemeneti adatok miatt) túlírva a szomszédos memóriaterületet írja felül. A felülírt memóriaterületen más adatok, a program változói, a program futását vezérlő adatok (programkód) is lehet. Ez a program hibás működéséhez, futásának befejeződéséhez (lefagyás) vagy a rendszer biztonságának sérüléséhez is vezethet. [13]
- **Ransomware***:* Célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsarolóprogramok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó egy zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejé-ben visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, akkor a zsaroló kiterjeszti a fizetésre rendelkezésre álló időt vagy törli az adatokat a felhasználó infokommunikációs eszközéről. [35]
- **Reaktív biztonsági intézkedés:** A szervezetet ért támadásra, incidensre a védelmi rendszer később reagál, azaz egy követő magatartást jelent. Ebben az esetben az adott szervezetet ért támadás miatt már nagy eséllyel a bekövetkezett kár, valamint a meg nem tett védelmi intézkedések költségei megfizetésre kell, hogy kerüljenek. [12]
- **Reagálás:** a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés. [5]
- **Rendelkezésre állás elve**: Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak. [5]
- **Rendszergazda**: Hálózati szolgáltatást nyújtó számítógép adminisztrátora.
- **RFI**: Request For Information. Információkérő dokumentum, amely alapul szolgálhat egy szervezetnek további döntéselőkészítő anyagok készítéséhez. [19]
- **Robothálózat**: A robothálózat egy sor internetre csatlakoztatott eszköz, amelyek mindegyike egy vagy több botot futtat. A botnetek elosztott szolgáltatásmegtagadási támadások (DDoS támadás) végrehajtására, adatok ellopására, spam küldésére használhatók, és lehetővé teszik a támadó számára az eszközhöz és annak kapcsolatához való hozzáférést. A botok távolról vezérelhető automatikusan futó szoftverek. [13]
- **Scanning:** Az IT támadások egyik lépése, a szkennelés szakasza. E lépés alkalmával a támadó felhasználja a korábban szerzett információkat és sokkal finomabb, precízebb felderítést tud végezni a különböző erre dedikált eszközökkel (például Nmap), hogy megismerhesse az elérhető szolgáltatásokat, eszközöket. Információt gyűjthet itt például a használt operációs rendszerek típusáról, illetve megfelelő gyakorlattal a hálózati biztonsági megoldások egy része, a topológia is felderíthető ennek segítségével. [23]
- **Scareware**: Ál-vírusirtók és egyéb más hamis biztonsági termékek csoportja, összefoglaló nevükön scareware-ek. Ahogyan az elnevezésük is utal rá, ezek a kártevők valamilyen vírusirtó programnak, esetleg biztonsági frissítésnek, vagy más biztonsági terméknek álcázzák magukat. Általános jellemzőjük, hogy ingyenesek (legalábbis kezdetben, míg nem akarják meggyőzni a felhasználót a „teljes verzió” megvásárlásáról), és semmilyen, vagy legalábbis minimális víruseltávolító képességgel rendelkeznek – viszont annál több kártékony programot töltenek le a számítógépre. [8]
- **Screenlogger**: Egy összetett malware, mely egyszerre képes figyelni a felhasználó által bevitt

adatokat és a képernyőn található információkat is, ezáltal képes kijátszani a képernyő alapú beviteli megoldásokat, például egy on-screen billentyűzet használatát. [8]

- **Search engine phishing**: Az internetes keresők adathalász célú felhasználása esetén, a támadók nem bajlódnak az üzenetküldéssel, hanem saját honlapot hoznak létre, ahol valamilyen szolgáltatást, terméket, illetve egy kihagyhatatlan ajánlatot kínálnak. A támadó által létrehozott oldal a Google általi kereséssel megtalálható. [22]
- **Sértetlenség elve:** Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [5]
- **Sérülékenység**: Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [5]
- **Sérülékenységmenedzsment**: A sérülékenységmenedzsment a sebezhetőségek azonosításának, osztályozásának, helyreállításának és enyhítésének ciklikus gyakorlata. Ez a gyakorlat általában számítógépes szoftveres sebezhetőségre utal, de hardveres menedzsment is elképzelhető. [13]
- **Sérülékenységvizsgálat**: Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása. [5]
- **Sérülékenységvizsgálati tevékenység**: A sérülékenységvizsgálatot célszoftverek segítségével végzik, amelyek a biztonsági vizsgálati eljárás során kifejezetten a sérülékenységvizsgálat egyes fázisainak végrehajtására kifejlesztett alkalmazások. A programok beállítása, valamint a vizsgálati eljárás mélysége alapján megkülönböztetünk automatizált és manuális vizsgálatot. [13]
- **Session hijacking**: Magyarul munkamenet-eltérítés, egy olyan támadási forma, ahol a kártékony kód a böngésző komponensként figyeli a felhasználói tevékenységet. Amikor a felhasználó belép egy oldalon a felhasználói fiókjába vagy egyéb hitelesítést igénylő tranzakciót végez, a malware „eltéríti" az adott munkamenetet, hogy felhasználva a megszerzett hitelesítő adatokat egyéb akciókat hajtson végre a felhasználó jogosultságával. [22]
- **Shoulder surfing**: Más néven „váll-szörf", amely annak a módszere, hogy hogyan lehet megszerezni egy felhasználó jelszavát, vagy más általa begépelt információt lényegében a válla feletti átnézéssel, azaz a támadó az áldozat közelébe férkőzve, észrevétlenül megnézni, hogy mit gépelt be az illető. [8]
- **Smishing**: SMS-en keresztül történő adathalászat technikája, mely során a támadó üzenetet küld az áldozatnak, mely szerint a bankkártyája zárolásra került, és bővebb információkat a megadott számon kérhet, amely felhívását követően a támadó megpróbálja kicsalni a felhasználó bizalmas adatait. [8]
- **Social engineering***:* Az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését. [8]
- **Social Media Engineering**: A Social Engineering támadások közösségi média felületen keresztül elkövetett formája. [8]
- **Spear phising (célzott adathalászat)**: A célzott adathalászat azonban egy adott személy ellen indított támadás. A célzott támadás sokkal körültekintőbben van felépítve és előkészítve, mint egy általános adathalászat, éppen ezért az áldozat sokszor észre sem veszi, hogy egy adathalász célpontja lett. [8]
- **SQL injection**: Más néven SQL befecskendezés. Ez egy olyan exploit, amely azokat az adatbázis lekérdező programokat használja ki, ahol nem tesztelték le alaposan a lekérdezések metódusát. Az SQL injection parancsokat küld a web szerverhez kapcsolt SQL adatbázisnak. Ha a szerver nem megfelelően lett tervezve és erősítve, akkor a űrlap mezőkbe – mint például a felhasználónév – közvetlen parancs adható meg az SQL szervernek. Így például a támadó a meg-

felelő parancs megadásával kinyerheti, az adott oldal összes felhasználójának nevét, vagy egyéb kritikusabb táblák információit is. [22]

- **Súlyos biztonsági esemény**: Olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek. [13]
- **Számítógépes eseménykezelő központ (CERT/CSIRT):** Az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)]. [31]
- **Számítógépes féreg***:* Egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá, illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. [5]
- **Számítógépes bűnözés:** Haszonszerzés vagy károkozás céljából, az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek sértetlensége és rendelkezésre állása elleni bűncselekmények összefoglaló megnevezése. (Az informatikai eszközök felhasználásával elkövetett bűncselekményekre is szokták alkalmazni.) [5]
- **Személyes adat**: Az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés. [20]
- **Szolgáltatásmegtagadásos támadás***:* Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **Stuxnet**: A kártevő még 2010 nyarán bukott le Iránban, Busehr (Bushehr) város erőműjének egyik számítógépén. Akkor mintegy százezer számítógépet sikerült megfertőznie. Csak az országban legalább 45 ezer felügyeleti számítógép és szerver hordozta a vírust. Az már a felfedezés utáni első elemzések során kiderült, hogy a Stuxnetet ipari folyamatirányító rendszerek ellen fejlesztették ki. A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. [16]
- **System reconfiguration attack**: A rendszer konfiguráció módosítása egy olyan támadási forma, mely előkészítő vagy megvalósító fázisa lehet egy man-in-the-middle támadásnak. A legelterjedtebb rendszer konfiguráció módosítások közé tartozik például a DNS szerver vagy a web proxy beállítás megváltoztatása, illetve wireless evil twin támadás. [22]
- **Tailgating**: A social engineering technikák egy válfaja, magyarra szoros követésnek, vagy vonatozásnak fordítható. A technika lényege, hogy a támadó úgy tesz, mintha egy vendég- vagy munkáscsoport (például karbantartók) tagja lenne, majd hozzájuk csapódva egyszerűen besurran az épületbe. [8]
- **Tanúsítás**: Egy informatikai biztonsági vizsgálat (értékelés) eredményeit igazoló formális nyilatkozat kibocsátása, melyből kiderül, hogy az értékelési követelményeket, kritériumokat megfelelően alkalmazták. Ang.: Certification. [5]

- **Teljes körű védelem**: Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [5]
- **Termelési biztonság**: A termelési biztonság a környezeti feltételekért felelős, ilyen elemek például az áramellátás folyamatossága, a klimatizálás, a munkavédelmi felszerelés vagy a biztonságos munkakörnyezet, amelyek a fizikai rendszer működését biztonságossá teszik. [16]
- **„Tisztaasztal, tisztaképernyő" szabály**: E szabály alkalmazása elengedhetetlen, lényege, hogy az aktuális feladathoz csak a legszükségesebb anyagokat kell az asztalon hozzáférhetően, a képernyőn láthatóan tartani. Munkaidőn túl az iratokat az íróasztalokon nem lehet tárolni, el kell zárni azokat. [36]
- **Trójai progam***:* Egy olyan malware program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az úgynevezett hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a céleszközhöz. Ezek a programok látszólag vagy akár valójában is hasznos funkciókat látnak, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak könyvtárakat, vagy akár adatállományokat törölnek. [11]
- **Tűzfal**: Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is. [36]
- Üzletmenet-folytonosság **tervezés**: Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. Ang.: Business Continuity Planning (rövidítve: BCP). [5]
- **Védelmi intézkedések**: Kockázatok csökkentésére, a védendő rendszerek biztonsági szintjének emelésére meghatározott intézkedések, amelyek lehetnek logikai, fizikai és adminisztratív jellegűek. [5]
- **Végfelhasználói eszköz**: Minden olyan informatikai eszköz, amely nem a központi rendszerek működtetésére használt eszköz. [16]
- **Vezérlőszerver (C&C)**: A támadók által használt, az infrastruktúra üzemeltetését segítő rendszer, melynek segítségével parancsokat küldhet a támadó az uralma alatt álló rendszernek. [16]
- **Vishing:** Más néven telefonos adathalászat, amely hanghálózaton, elsősorban VoIP csatornán keresztül terjed. A technika lényege, hogy a támadó a tömeges tárcsázás módszerével végigtelefonálja egy adott körzet összes hívószámát, és ahol felveszik a telefont, ott egy előre rögzített üzenetet játszanak le, amiben értesítik az áldozatot, hogy bizonyos problémák miatt zárolták vagy letiltották a bankkártyáját, ezért felajánlanak egy telefonszámot, hogy hívja fel a probléma megoldása érdekében. Amikor az ügyfél felhívja a telefonszámot, kérik, hogy adja meg bank- vagy hitelkártya információt, mint például a felhasználó nevét, kártyájának számát, banki azonosítóját, illetve a régi és új PIN kódját, hogy ezzel a kártyáját újra aktiválni tudják. [8]
- **Vírus**: A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve az által, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A vírusok a rendszerbe a felhasználó engedélye nélkül kerülnek be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD kártya, merevlemez, MP3 és videó lejátszó, mobiltelefon stb.), vagy akár hálózati kapcsolat (Internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tartalmát is törölheti vagy módosíthatja, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nem csak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként, vagy akár az internetről letöltött tartalmakon,

dokumentumokon keresztül is. [11]

- **Virtuális magánhálózat (VPN):** Olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva, és így a nyilvános hálózaton belül védett kommunikációt valósít meg. [5]
- **Web trojans**: Olyan kártékony kódok, melyek a bejelentkezési oldalak esetén tűnnek fel, úgynevezett pop-up felületként (például böngészők saját hitelesítési ablaka). A felhasználó jóhiszeműen beírja a hitelesítő adatait, melyek azonban nem az általa meghívott weboldalhoz, hanem a trójai által a támadóhoz kerülnek. [22]
- **Whaling**: Az elnevezés „bálnavadászatnak" fordítható, egyben utalva arra, hogy ezzel a technikával a „nagy halakat", vagyis a vállalatok vezetőit szeretnék megtéveszteni. A speciálisan cégvezetőknek, középvezetőknek készült levelek (vagy akár telefonhívások) általában üzleti partnerek vagy állami intézmények nevében érkeznek. [8]
- **WiFi (Wireless Fidelity), WLAN**: Szabványos vezeték nélküli adatátviteli technika. A szabad frekvenciatartományt használó rendszer átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság). [22]
- **Wireless evil twin támadás**: A felhasználó számítógépének wifi beállításai módosulnak úgy, hogy a támadó által üzemeltetett Wi-Fi hálózathoz kapcsolódjon. Így minden hálózati kommunikációt rögzíteni képes a támadó, melyből később bármilyen adatot kinyerhet. [22]
- **XSS**: A rövidítés a cross side scripting kifejezéssel oldható fel. Magyarul oldalakon keresztül végrehajtott közvetett szkripthívás. A támadók célja, hogy egy kártékony szkriptet futtassanak le a célgépen. Létezik perzisztens és nem perzisztens fajtája. Ez utóbbi alkalmával a kártékony kód az URL-be kerül beillesztésre, mely rákattintás esetén lefut és elvégzi a felhasználó által nem kívánt tevékenységet. Az értő szemnek valószínűleg feltűnik, hogy a „script" kifejezést, vagy például a javas scriptre utaló „.js" kifejezés el van bújtatva az URL-ben. Tipikusan phishing támadásoknál alkalmazható jó. A perzisztens változat során magán a webszerveren helyezik el a szkriptet, mely egy weboldal minden megtekintésénél így lefut. Az ilyen módon történő rosszindulatú kódsor elhelyezésre példa a nem megfelelő beviteli védelemmel ellátott blogoldalak bejegyzései adnak lehetőséget. [22]
- **Zárt védelem**: Az összes számításba vehető fenyegetést figyelembe vevő védelem. [5]

12.1. A fogalmak forrásjegyzéke

[1] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*.

[2] Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár*. Elérhetőség: https://www.naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2018. március 22.)

[3] MUHA L., KRASZNAY Cs. (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem.

[4] *Az Európai Parlament és a Tanács 2002/65/EK irányelve (2002. szeptember 23.) a fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról.*

[5] MUHA L. (2004): Fogalmak és definíciók. In. *Az informatikai biztonság kézikönyve.* Elérhetőség: http://lmuha.hu/defins.html (A letöltés ideje: 2018. március 22.)

[6] SÁGI G. (2017): Informatikai rendszer támadási folyamata. *Műszaki Katonai Közlöny*. Elérhetőség: http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/015_Sagi_Gabor.pdf (utolsó letöltés: 2018. március 24.)

[7] RÉDECSI M., TÓTH G. (2013): *Android*. Elérhetőség: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (utolsó letöltés: 2018.03.24.)

[8] OROSZI E. (2008): *Social Engineering.* Budapest: Budapesti Corvinus Egyetem.

[9] GYURÁK G. (2015): *Informatikabiztonság I.* Pécs: Pécsi Tudományegyetem Műszaki és

Informatikai Kar.
[10] *A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet*
[11] HAIG Zs., KOVÁCS L. (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Elérhetőség: http://hdl.handle.net/11410/285 (utolsó letöltés: 2018. március 24.)
[12] CSER O. (2018): Célzott támadás a pénzügyi szektor ellen. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó.
[13] MARSI T. (2018): A célzott támadások és megelőzésük sérülékenységvizsgálattal. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó.
[14] *A Big Data a hivatalos statisztikában* (2016). Elérhetőség: https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (utolsó letöltés: 2018. március 24.)
[15] MÁTRAI J. (2016): *Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás*. Elérhetőség: http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (utolsó letöltés: 2018. június 4.)
[16] SEBŐK V. (2018): Új típusú támadások az államok és szervezetek ellen. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó.
[17] SÁGI G. (2018): Célzott támadási modellek és műszaki védelem lehetőségek. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó.
[18] HAIG Zs., KOVÁCS L. (2008): Fenyegetések a cybertérből. *Nemzet és Biztonság.* Elérhetőség: *http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf* (utolsó letöltés: 2018. március 28.)
[19] SOLYMOS Á. (2018): Identitás- és jogosultságkezelés, mint a célzott támadások megelőzésének technológiai eszköze. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó.
[20] *Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény*
[21] Compuworks Informatikai Zrt. – *Chipkártyás technológia* Elérhetőség: http://www.compuworx.hu/a_chipkartyas_technologia (A letöltés ideje: 2018. június 04.)
[22] KACZUR G. (2018): Spearphishing. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó.
[23] VÁCZI D. (2018): Célzott támadások módszertana. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó, 2018.
[24] Firmware. Elérhetőség: https://pcforum.hu/szotar/?term=firmware&tm=miaz (utolsó letöltés: 2018. március 22.)
[25] Emmanuel Carabott: *Hacking Motivations – Hactivism* (2011). Elérhetőség: http://www.gfi.com/blog/hacking-motivations-hacktivism/ (A letöltés ideje: 2018.03. 22.)
[26] LÁSZLÓ G. (2014): *Kockázatértékelés, kockázatmenedzsment*. Elérhetőség: http://vtki.uninke.hu/uploads/media_items/kockazatertekeles_-kockazatmenedzsment.original.pdf (utolsó letöltés: 2018. március 22.)
[27] SZARVÁK A. (2018): Felderítés/célzott támadások. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó.
[28] Kóbor Á.: *Mi az a „dolgok internete”?* (2014). Elérhetőség: https://ithub.hu/blog/post/Mi_az_a_dolgok_internete/ (utolsó letöltés: 2018. június 03.)
[29] KRASZNAY Cs. (2012): A polgárok védelme egy kiberkonfliktusban, *Hadmérnök* 2012/4. Elérhetőség: http://hadmernok.hu/2012_4_krasznay.pdf (utolsó letöltés: 2018. március 22.)
[30] RESPERGER I. (2002): *Kockázatok, kihívások és fenyegetések a XXI. században*. Budapest, ZMNE, Az Országos Kiemelt Kutatási Tanulmányok pályázata.
[31] BODÓ A. P., ZÁMBÓ N. (2018): Újdonságok a kibervédelmi szabályozásban. In. *Célzott támadások*. Budapest: Dialóg Campus Kiadó.
[32] *A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló*

2012. évi CLXVI. tv.
[33] SZAPPANOS G. (2018): Kártékony kódok használata a célzott támadások végrehajtásában. In. *Célzott támadások*. Budapest, Dialóg Campus Kiadó.
[34] BODÓ A., ZÁMBÓ N. (2018): A közreműködők kötelezettségei a célzott támadások elhárításában az ibtv. szerint. In. *Célzott támadások*. Budapest, Dialóg Campus Kiadó.
[35] YAQOOB, I., AHMED, E., IMRAN, M. (2017): The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, 6 September. Elérhetőség: https://doi.org/10.1016/j.comnet.2017.09.003 (utolsó letöltés: 2017. október 20.)
[36] GYARAKI R. (2018): Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban. In. *Célzott támadások*. Budapest, Dialóg Campus Kiadó.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Dékán

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Császár-Biró Anna
Kiss Eszter

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-062-9 (PDF)

A hatályosított kiadvány
a **KÖFOP-2.1.1-VEKOP-15-2016-00001**
„A közszolgáltatás komplex kompetencia,
életpálya-program és oktatás technológiai fejlesztése”
című projekt keretében jelent meg.

MAGYARORSZÁG
KORMÁNYA

Európai Unió
Európai Szociális
Alap

BEFEKTETÉS A JÖVŐBE