Célzott kibertámadások

Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2018

BODÓ ATTILA PÁL – MARSI TAMÁS – SEBŐK VIKTÓRIA – 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 készült el és jelent meg.

Szerkesztő:
Deák Veronika

Szerzők:
Dr. Bodó Attila Pál
Marsi Tamás
Sebők Viktória
Dr. Zámbó Nóra

Szakmai lektor:
Dr. Bonnyai Tünde

Olvasószerkesztő:
Kiss Eszter
Császár-Biró Anna

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 Bevezető gondolatok

Az elmúlt években világszerte egyre erősödnek a globális kibertérből[1] 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[2] 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 EU-n 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 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] 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.

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

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.[3] 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*”[4] ***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)[5], amely rögzíti az EU intézményei, a tagállamok és a szociális partnerek intézkedéseit a következő 10 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. Eredmények és következő lépések: a globális kiberbiztonság felé”* című dokumentummal.[6] Ezen állásfogla-

[3] http://www.consilium.europa.eu/media/30811/qc7809568huc.pdf (utolsó letöltés: 2018. szeptember 13.)

[4] http://ec.europa.eu/transparency/regdoc/rep/1/2009/HU/1-2009-149-HU-F1-1.Pdf (utolsó letöltés: 2018. szeptember 13.)

[5] http://ec.europa.eu/eu2020/pdf/1_HU_ACT_part1_v1.pdf (utolsó letöltés: 2018. szeptember 13.)

[6] https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012IP0237&qid=1521197299768&from=HU (utolsó letöltés: 2018. szeptember 13.)

lás 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[7] közötti koordinációnak a szükségességét.

Látható, hogy az EU számos dokumentumot fogadott el az ezredfordulót követően, mégis a kiberbiztonság[8] 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[9] 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.[10] 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 kere-

7 CERT – Computer Emergency Response Team = úgynevezett Számítógépes Vészhelyzeti Reagáló Egység.

8 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.

9 http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (utolsó letöltés: 2018. szeptember 13.)

10 http://europa.eu/rapid/press-release_SPEECH-17-3165_hu.htm (utolsó letöltés: 2018. szeptember 13.)

ténekre[11] megerősítése;

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[12] 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 4 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[13] (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

[11] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf (utolsó letöltés: 2018. szeptember 13.)

[12] http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf (utolsó letöltés: 2018. szeptember 13.)

[13] http://www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljeszt%C3%A9si_strat%C3%A9gia_.pdf (utolsó letöltés: 2018. szeptember 13.)

indult el 2014-ben a *Digitális Nemzet Fejlesztési Program,*[14] amelynek folytatása a jelenleg megvalósítás alatt álló, számos intézkedést tartalmazó *Digitális Jólét Program* (a továbbiakban: DJP) első[15] és második[16] 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[17], a Digitális Gyermekvédelmi Stratégiában[18] 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.

---

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

15 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.

16 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).

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

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

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),[19] és
- az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) az Európai Unió Általános Adatvédelmi Rendelete[20] (angolul: General Data Protection Regulation, a továbbiakban: GDPR).[21]

1.3.1 NIS irányelv

A NIS irányelv[22] 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[23]:

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.[24]

---

19 https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148&from=HU (utolsó letöltés: 2018. szeptember 13.)

20 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.

21 https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=EN (utolsó letöltés: 2018. szeptember 13.)

22 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.

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

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

A NIS irányelv védett jogi tárgya az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók hálózati és információs rendszere,[25] amely:

a) a 2002/21/EK irányelv[26] 2. cikkének a) pontja szerinti elektronikus hírközlő hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt, vagy kapcsolatban álló eszközök csoportja, 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,[27]
b) előírja egy vagy több nemzeti hatóság kijelölését, amely felügyeli a NIS irányelv átültetését és végrehajtását,[28]
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;[29]
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 6 hónapon belüli) kijelölését;
e) biztonsági és bejelentési követelményeket állapít meg az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára;[30]
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;[31]
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.[32]

Fenti megfelelés érdekében került sor az Ibtv. és végrehajtási rendeleteinek a 1.4. pontban ismertetett módosítására.

---

25 NIS 4. cikk, 1. pont.
26 Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról.
27 NIS irányelv 7. cikk.
28 NIS irányelv 8. cikk.
29 NIS irányelv 8. cikk.
30 NIS irányelv 14-17. cikk.
31 NIS irányelv 11. cikk.
32 NIS irányelv 12. cikk.

1.3.2 Az Általános Adatvédelmi Rendelet

Míg a NIS irányelv szabályozásának célcsoportját a szolgáltatók képezik és elsődleges célja a hálózatbiztonság megteremtése, addig a GDPR rendelet[33] fókuszában a természetes személyek, mint felhasználók állnak, illetve a személyes adatok és a magánszféra védelmét szolgáló rendelkezéseket tartalmazza. A 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 biztosítani 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.[34] 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.[35] Ehhez első sorban 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[36] 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,[37] 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.[38] 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

[33] 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.

[34] GDPR 5. cikk.

[35] GDPR 30. cikk.

[36] GDPR 25. cikk.

[37] GDPR 20. cikk.

[38] GDPR 17. cikk.

vagy e személyes adatok másolatát, illetve másodpéldányát is).

A GDPR szabályozza az adatvédelmi hatásvizsgálat[39] 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[40] kijelölését, amelyet meg kell tenni:

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[41] 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[42] 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[43] 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.

39 GDPR 35. cikk.
40 GDPR 37. cikk.
41 GDPR 33. cikk.
42 GDPR 83. cikk.
43 GDPR 70. cikk g) és h) pontja.

1.4 Változások a nemzeti jogban

Az előzőekben ismertetett uniós és nemzeti stratégiai törekvések, valamint joganyagok meghatározták a nemzeti jogalkotás irányultságát, így az 5 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-től történő kötelező alkalmazásával összefüggően került sor. A módosítás a Nemzeti Elektronikus Információbiztonsági Hatóság[44] (a továbbiakban: Hatóság) feladataként írja elő az Elektronikus Ügyintézési Felügyelettel[45] való együttműködést a szabályozott elektronikus ügyintézési szolgáltatás[46] szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében.[47] 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.[48] 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[49] 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.[50]

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-vel 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

---

44 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.

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

46 E-ügyintézési törvény 29. §.

47 Ibtv. 14. § (2) bekezdés h) pont.

48 Ibtv. 14. § (3b) bekezdés.

49 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.

50 Ibtv. 29. §.

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[51]. 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[52],
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.) Korm. rendelet (a továbbiakban 185/2015. (VII. 13.) Korm. rendelet)[53]
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[54] (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[55] (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[56] 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[57] 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

[51] 187/2015. (VII. 13.) Korm. rendelet 4/A. A hatóság regisztrációs eljárása és a hatósági nyilvántartásba vétel alcíme.
[52] 41/2015. (VII. 15.) BM rendelet 7. §-a, hatályos 2018. május 10-től.
[53] 185/2015. (VII. 13.) Korm. rendelet 23. §-a hatályos 2018. május 10-től.
[54] 271/2018. (XII. 20.) Korm. rendelet 31. §-a hatályos 2019. január 2-től.
[55] 187/2015. (VII. 13.) Korm. rendelet 31. §-a, hatályos 2018. május 10-től.
[56] 187/2015. (VII. 13.) Korm. rendelet 6. § (1) bekezdés, hatályos 2018. május 10-től.
[57] 187/2015. (VII. 13.) Korm. rendelet 6. § (1) bekezdés i)–n) pont, hatályos 2018. május 10-től.

nyújtóként azonosított szolgáltatók[58] 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[59] 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,

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[60] 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.[61] A módosítás a BM OKF feladataként nevesíti az alábbiakat:[62]

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 fenntartásá-

58 NIS irányelv.

59 187/2015. (VII. 13.) Korm. rendelet 6. § (1a) bekezdés, hatályos 2018. május 10-től.

60 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.

61 187/2015. (VII. 13.) Korm. rendelet 25. § (1) bekezdés, hatályos 2018. május 10-től.

62 187/2015. (VII. 13.) Korm. rendelet 25. § (4) bekezdés, hatályos 2018. május 10-től.

hoz 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[63] fogalma. További módosítás 2018. január 1-től a szervezet[64] fogalmának átvétele az Ibtv-ből, illetve a hatósági nyilvántartás[65] 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[66] jelenik meg a 187/2015. (VII. 13.) Korm. rendeletben, amely kapcsolódik az E-ügyintézési törvény végrehajtásához is. Ezen rendelkezések rögzítik,[67] 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:
   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.[68]

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.[69] Ilyen csoportnak minősül a kormányzati eseménykezelő központ[70] (a továbbiakban: GovCert),

---

63 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.

64 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.

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

66 187/2015. (VII. 13.) Korm. rendelet 4/A. A hatóság regisztrációs eljárása és a hatósági nyilvántartásba vétel alcíme.

67 187/2015. (VII. 13.) Korm. rendelet 10/A. – 10/D. §-ok.

68 187/2015. (VII. 13.) Korm. rendelet 3. §, 25. § (6)-(7) bekezdés.

69 185/2015. (VII. 13.) Korm. rendelet 1. § 15. pont – hatályos 2018. május 10-től.

70 Ibtv. 19. §.

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.[71]

Rögzítette továbbá, hogy a GovCert:

a) részt vesz a CSIRT-ek hálózatának tevékenységében, amelynek keretében ellátja a többi eseménykezelő központ képviseletét,[72]
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.[73]

A BM OKF-et, mint a létfontosságú rendszerelemmé kijelölt rendszerelemek elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelésére kijelölt szervezetet,[74] 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 kapcsolatos 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.[75]

A BM OKF az észlelt, valamint a tudomására jutott biztonsági eseményekről haladéktalanul tájékoztatja a GovCertet, amely tájékoztatásnak tartalmaznia kell:[76]

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

71 185/2015. (VII. 13.) Korm. rendelet 3. § (1) bekezdés h-j) pontok – hatályos 2018. május 10-től.
72 185/2015. (VII. 13.) Korm. rendelet 5. § (2) bekezdés e) pont – hatályos 2018. május 10-től.
73 185/2015. (VII. 13.) Korm. rendelet 5/A. § – hatályos 2018. május 10-től.
74 185/2015. (VII. 13.) Korm. rendelet 6. § (3) bekezdés – hatályos 2018. május 10-től.
75 185/2015. (VII. 13.) Korm. rendelet 6. § (3a)-(3b) bekezdései – hatályos 2018. május 10-től.
76 185/2015. (VII. 13.) Korm. rendelet 6. § (3c) bekezdése – hatályos 2018. május 10-től.

események kezelésére vonatkozó, jogszabályban nem részletezett eljárásrendjéről.[77]

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

1.5 Irodalomjegyzék

- 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 URL: http://ec.europa.eu/transparency/regdoc/rep/1/2009/HU/1-2009-149-HU-F1-1.Pdf (utolsó letöltés: 2018. március 31.)
- A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”) URL: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf (utolsó letöltés: 2018. március 31.)
- Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér: URL: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (utolsó letöltés: 2018. március 31.)
- EURÓPA 2020 – Az intelligens, fenntartható és inkluzív növekedés stratégiája URL: http://ec.europa.eu/eu2020/pdf/1_HU_ACT_part1_v1.pdf (utolsó letöltés: 2018. március 31.)
- Európai Biztonsági Stratégia – Biztonságos Európa egy jobb világban URL: http://www.consilium.europa.eu/media/30811/qc7809568huc.pdf (utolsó letöltés: 2018. március 31.)

[77] 185/2015. (VII. 13.) Korm. rendelet 6. § (3d)-(3e) bekezdései – hatályos 2018. május 10-től.

[78] A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet 2/A. §.

- Jean-Claude Juncker elnök beszéde – Az Unió helyzete 2017 URL: http://europa.eu/rapid/press-release_SPEECH-17-3165_hu.htm (utolsó letöltés: 2018. március 31.)
- Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia, URL: http://www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljeszt%C3%A9si_strat%C3%A9gia_.pdf (utolsó letöltés: 2018. március 31.)
- Nemzeti Infokommunikációs Stratégia: URL: 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.)

2. SEBŐK VIKTÓRIA: ÚJ TÍPUSÚ TÁMADÁSOK AZ ÁLLAMOK ÉS A SZERVEZETEK ELLEN

2.1 Bevezető gondolatok az új típusú támadásokról

A tanulmány célja, hogy könnyed, emészthető stílusban mutasson be olyan, az IT biztonság témakörét jelentősen meghatározó eseteket, eseményeket, példákat, amelyen keresztül átfogó képet kaphat egy állami vagy ipari létesítményt működtető vezető arról, hogy milyen támadási típusokkal, illetve fenyegetésekkel kell számolnia az elkövetkezendő időszakban.

Ma már csupán történelmi példa lehet, amikor még 2007-ben internetes támadást hajtottak végre Észtország ellen. Az incidens során tömeges internetes támadások érték különböző észt intézmények szervereit. A támadások idején megpróbálták megbénítani különböző észt honlapok működését, megakadályozva, hogy a „normál felhasználók" elérhessék azokat, ezenfelül egyes esetekben azok tartalmát is igyekeztek megváltoztatni. Például az ország második bankja, a SEB Eesti Uhisbank a tömeges internetes támadások miatt kénytelen volt felfüggeszteni azt a szolgáltatását, amelynek segítségével külföldről is be lehet lépni a pénzintézet egyes rendszereibe. Ezek az akciók azért (is) okoztak komoly problémát, mivel a kis balti ország élenjár a világháló használatában.

Az események során az észt hatóságok igyekezték meggyőzni az EU-t és a NATO-t, hogy hatékonyabban lépjenek fel, mert szerintük szervezett terrortámadás történt. Az eset óta beszélhetünk olyan kiberbiztonsági fenyegetésekről, amelyek állami rendszerek ellen elkövetett támadásokról szólnak.

Az ilyen és ehhez hasonló, úgynevezett kritikus infrastruktúrákra leselkedő veszélyforrások köre sajnálatos módon bővült azóta, amellett, hogy igen sokrétűvé is vált, ezért több szempontból és irányból készült gyűjtés arra vonatkozóan, hogy bemutassa, a digitális világ mára valódi háborús övezetté alakult át, ahol különböző komplexitású védelmi intézkedésekre és megoldásokra van szükség.

Talán nem véletlen, hogy a vállalatok 2017-ben átlagosan 11,7 millió dollárt költöttek többféle kiberbiztonsági intézkedésekre. Ez 23 százalékos növekedést jelent az előző évhez képest, amely komoly emelkedésnek mondható, ugyanakkor mégsem éri el a fenyegetések bővülésének arányát. A szervezetek ugyanis 2016-hoz képest 27 százalékkal több, átlagosan 130 incidenst észleltek az elmúlt évben. Minden jel arra mutat, hogy még több támadás várható, ezért célszerű azonosítani a gyenge pontokat, és megerősíteni a védelmet.[79]

[79] http://www.novell.hu/hirek/20180116_Novell_trendek_joslat_kiberbiztonsag.html (utolsó letöltés: 2018. január 29.)

Fenyegetés forrása	Motiváció	Tevékenység
Hacker, Cracker	Kihívás, ego, lázadás	Hackelés, social engineering, behatolás, jogosulatlan hozzáférés
Számítógépes bűnöző	Információ megsemmisítése, illegális információ közlés, pénz szerzés, jogosulatlan adat megváltoztatás	Rendszer behatolás, spoofing, megvesztegetés, hacker technikák
Terroristák	Megsemmisítés, kihasználás, bosszú, rémhír terjesztés	Rendszer támadás, DDOS, rendszer penetráció, rendszer hamisítás, információs háború
Ipari kémek (vállalatok, külföldi kormányzatok, más kormányzati érdekeltségek)	Gazdasági előnyök szerzése, verseny előnyök, hírszerzés	Információ lopás, social engineering, személyes adatok felhasználása, jogosulatlan rendszer hozzáférések (bizalmas adatok, technológiai adatok, stb.)
Belső személyek	Kíváncsiság, ego, információ szerzés, pénz szerzés, bosszú, hibák	A munkavállaló megfenyegetése, rossz hír terjesztése, számítógépes csalás, információ lopás, megszakítás, meghamisított adatok, rendszer szabotálás, stb.

1. ábra: Fenyegetések forrásai
Forrás: Benyó Pál: Az információbiztonság speciális témakörei – Incidensmenedzsment

Az előrejelzések szerint idén és az elkövetkező években is rengeteg régi és új típusú informatikai fenyegetéssel kell majd szembenézni. A legtöbb biztonsági jelentés leginkább a zsarolóvírusokra, a kritikus infrastruktúrák elleni támadásokra, a várható kártevőkre és a kiberbűnözők elleni küzdelemre hívja fel a figyelmet. A zsarolóvírusok óriási figyelmet kaptak 2017-ben is, és a jövőben is számolni kell velük. Az olyan kibertámadások, mint a WannaCry és a Nyetya ugyanakkor jól mutatják a hagyományos zsarolóvírusnak tűnő, de sokkal rombolóbb támadások gyors terjedését és kiterjedt hatását.

Veszélyessé váltak az úgynevezett „destruction of service” (DeOS) támadásoknak nevezett akciók is, amelyek után a vállalatoknak nincs lehetőségük adataik visszaállítására. Az úgynevezett Ransomware-as-a-Service szolgáltatások növekedése a bűnözők számára könnyebbé teszik a kibertámadások kivitelezését. Az olyan hagyományos fenyegetések, mint a „Distributed Denial of Service” (DDoS) típusú támadások, valamint a spam, a kémprogramok (spyware), a hirdetés típusú vírusok (adware) mellett egyre nagyobb anyagi károkat okoznak a vállalati elektronikus levelezőrendszerek elleni támadások is.

A biztonsági iparban ugyanakkor gőzerővel folynak az automatizációra, gépi tanulásra és mesterséges intelligenciára alapozó fejlesztések. A felderítési idő (*time to detection – TTD*) csökkentése kritikus jelentőségű a kiberbűnözők megfékezésében, illetve a károk csökkentésében. A hálózatok legújabb generációja pedig már arra is képes, hogy azonosítsa az ismert fenyegetések nyomait, még akkor is, ha azok titkosítva vannak, a kódolás visszafejtése vagy az adatvédelembe való beavatkozás nélkül.[80]

Mindezek mellett egyre kiemeltebb figyelmet kapnak az úgynevezett APT (*Advance Persistent Threat*) támadássorozatok, illetve a speciális, ipari környezetet megbénító technológiák, amelyek célpontjai általában a piaci nagyvállalatok (például ipari kémkedés, zsarolás), a stratégiai fontosságú állami nagyvállalatok (például kritikus infrastruktúrák), illetve a kormányzati szektor (például kémkedés vagy választási kampányok).

[80] http://www.piacesprofit.hu/kkv_cegblog/6-technologiai-trend-2018-ra/ és http://www.isafe.hu/6_technologiai_trend_2018-ra (utolsó letöltés: 2018. január 30.)

2.2 Új trendek az ipari létesítmények elleni támadásokban

Egy nagy volumenű ipari létesítmény azért kiváló célpont, mivel hatalmas károk keletkezhetnek például az elektromos tápellátás kiiktatásával vagy a kommunikáció blokkolásával. A logikai biztonság szintjén is elterjedtek már olyan vírusok, amelyek kifejezetten ipari létesítményeket támadnak.

Az ipari és kritikus rendszerek esetében figyelembe kell venni, hogy a biztonság mindhárom szintjén is történhetnek incidensek. Ezért érdemes figyelmet fordítani a biztonság három alappillérére a *fizikai*, a *termelési*, illetve a *logikai biztonságra.*

Ennek értelmében a *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.

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.

A logikai biztonság körébe tartoznak a vírusok, a rosszindulatú kódok, az adathalászattal kapcsolatos támadások, az ilyen típusú támadások elleni védekezés, valamint a hekker támadások, az adatlopás, az illetéktelen hozzáférés és módosítás, illetve az illetéktelen közzététel kapcsán tehető megelőző intézkedések.

2.2.1 Grafitbomba

A termelési biztonság szintjén rombol például az úgynevezett grafitbomba, amelyet állítólag még az Öböl-háborúban vetettek be legelőször, és amely szinte teljesen megsemmisítette az egész elektromos ellátórendszert.

Az Egyesült Királyságban működő The Independent szerint jelenleg Észak-Korea áll hasonló fenyegetettségben, miután Dél-Korea állítólag bármikor kész kifejleszteni az emberekre ártalmatlan „áramszünet bombát", amellyel képes megbénítani Észak-Korea áramellátó rendszerét. A szerkezet úgy rombol, hogy kémiailag kezelt grafitszálakat áraszt az elektromos alkatrészek fölé, így okozva rövidzárlatot.[81]

2.2.2 Stuxnet vírus története sztorija

A termelési és a logikai biztonság szintjén indított támadást az úgynevezett Stuxnet vírus, amivel ipari rendszereket támadtak, s amely támadás új fejezetet nyitott a cyber-hadviselés történelmében. A vírus állítólag az iráni atomprogram lelassítására irányult, és egy WinCC/PCS7 ipari vezérlőrendszer sebezhetőségét használta ki.

A kártevőt még 2010 nyarán fedezték fel 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. Felfedezésekor kiderült, hogy az erőműre szerencsére nem jelentett közvetlen veszélyt, de a sikeres támadás ténye mindenképpen elgondolkoztató volt a biztonsági szakemberek számára.

Azt feltételezik, hogy a Stuxnet-et izraeli tesztkörnyezetben építették ki a Siemens Simatic rendszerével és IR-1 centrifugákkal, s itt fejlesztették ki a Stuxnet támadó blokkját is. A centrifugák

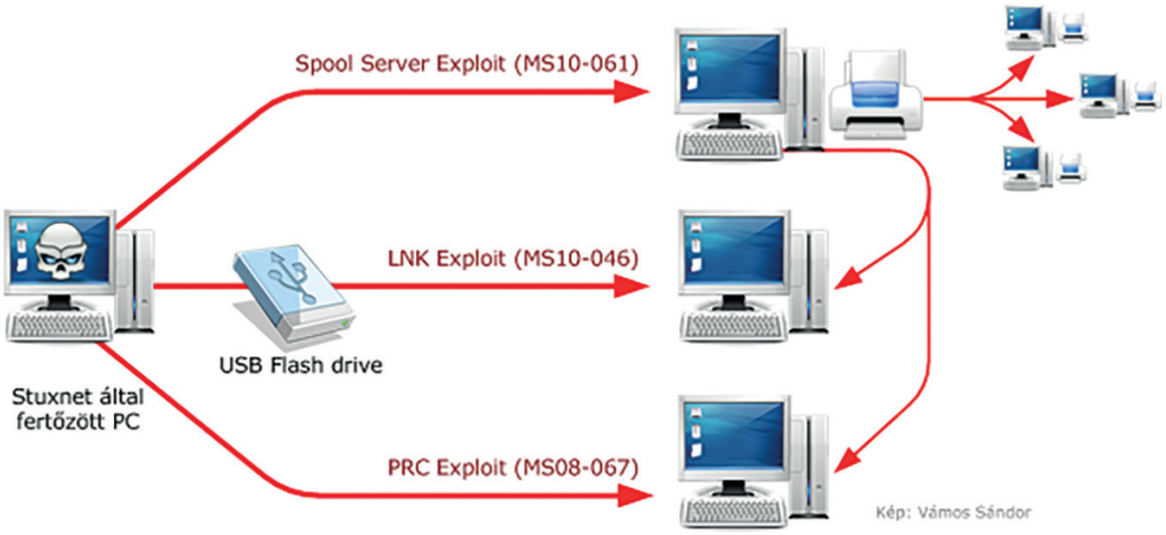
[81] https://24.hu/kulfold/2017/10/09/grafitbombat-dobnanak-eszak-koreara/ (utolsó letöltés: 2018. február 25.), illetve: https://www.telegraph.co.uk/news/2017/10/09/south-korea-developing-graphite-blackout-bombs-paralyse-norths/

vezérléséről speciális kontrollerek (PLC-k) gondoskodnak. Ezek veszik át a kezelőktől a SCADA[82] rendszereken keresztül a parancsokat és továbbítják a működési paramétereiket.

A kártevő komplexitása és fejlett hatásmechanizmusa kizárja, hogy hobbi hekkerek fejlesztették volna:

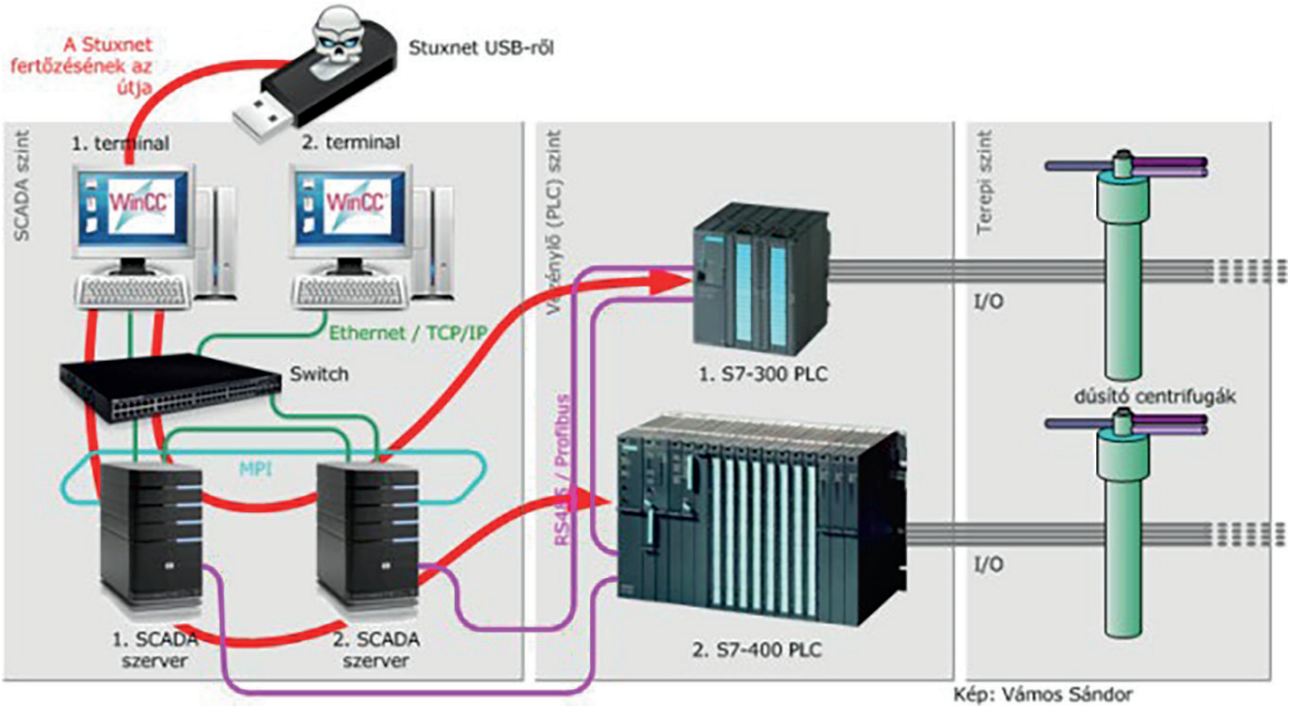
- A kódban található egy DEADF007 hivatkozás is, amelynek eredetije a DEADFOOT, ez a pilóták szlengjében a hajtómű-meghibásodást jelenti. Az „o” betű 0-nak és „T”-nek pedig a 7-es számmal való írása nem véletlen elgépelés. A „leet speech” nevet kapta, alternatív ábécé szerint írták, ahol egyes betűket számokkal helyettesítenek. Érdekessége továbbá, hogy a DEADF007 felbontható hexadecimális számok sorozatává, mint DE AD F0 07. Ugyanakkor, a vége „007” utalhat James Bond-ra is.
- A fejlesztéshez kiindulásként valószínűleg, egy korábbi kártevő, a Conficker kódját használták. A féreg tevékenységéről egy maláj és egy dán szerverre folyamatosan jelentéseket küldött, majd a nantanzi támadás után ezeket a szervereket lekapcsolták üzemeltetőik.

2010. november 16-án Irán leállította az urándúsítóit, miután a centrifugák több mint 20 százaléka megsemmisült a Stuxnet tevékenysége miatt. A kártevő ugyanis a feltételezések szerint az igazi pusztítást a nantanzi urándúsító létesítményben fejtette ki: mintegy ezer IR-1 típusú urándúsító centrifugát égetett le. Ezeknek a berendezéseknek a hajtómotorja ugyanis 1007 cps-nél (cycles per second, másodpercenkénti fordulatszám) is már tönkremegy, a Stuxnet viszont rövidebb fázisokat, észrevétlenül 1064 cps-es tempót diktált nekik, így hajtva szét őket.



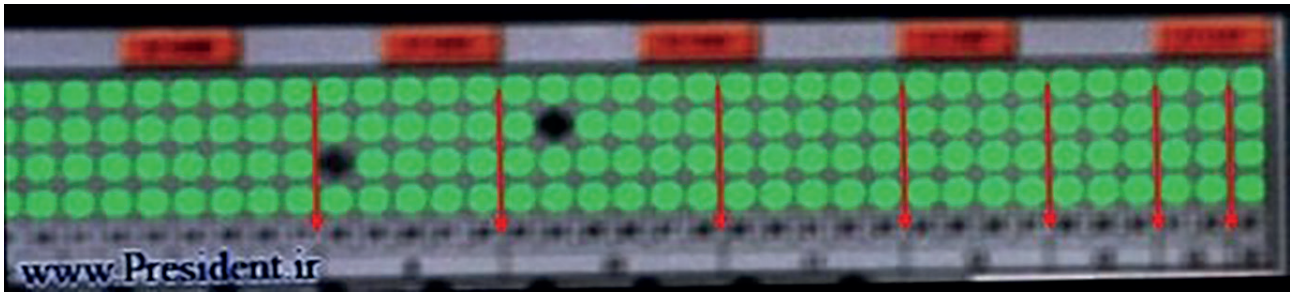
2. ábra: A vírus alapvetően egy (nem publikált) Windows hibát (0-day Windows exploit) kihasználva pendrive-ról fertőzött, majd a fertőzést követően – további operációs rendszerhibákat kihasználva – a hálózatokon terjedt.
Forrás: http://passport.blog.hu/2017/06/30/a_stuxnet_sztori

[82] SCADA-technológia működteti az ipari folyamatirányító és szabályozó rendszereket. Ezen infrastruktúrák döntő többségben jól elkülönülten működnek a többi rendszerhez képest. Nem véletlen, hogy célzott támadás esetén, elsősorban a SCADA-alapú megoldásokat ostromolják a támadók, hiszen a rendszerek blokkolása után megbénulhat például egy régió áramellátása. Többek között emiatt is érdemes kiemelt figyelmet szentelni a rendszerek integritásellenőrzésére.



3. ábra A vírus a fertőzést követően a WinCC jelenlétét kezdte keresni a gépen. Ez egy Siemens SCADA rendszer, amelyen keresztül technológiák felügyeletét lehet megvalósítani. Forrás: http://passport.blog.hu/2017/06/30/a_stuxnet_sztori

Sokáig rejtély maradt, hogy a vírus melyik létesítmény szabotálására íródott, miután kiderült, hogy felépítése olyan speciális, hogy csak egy célzott támadásra volt alkalmas.



4. ábra: Egy sajtófotó segített leleplezni a rejtélyt. A képen a zöld pontok a működő centrifugákat jelölik, ezek összesen 4, 8, 12, 16, 20, 24, 20 egységet tesznek ki, ugyanúgy, ahogy a Stuxnet kódjában. Forrás: president.ir / Ralph Langner; http://passport.blog.hu/2017/06/30/a_stuxnet_sztori

A Stuxnet sztori bebizonyította, hogy mekkora károkat okozhat az ipari létesítmények elleni támadás.[83]

[83] http://passport.blog.hu/2017/06/30/a_stuxnet_sztori (utolsó letöltés: 2018. február 25.)

2.2.3 Crash override vagy industroyer

Csak említésképpen, a Crash Override vagy Industroyer néven ismert kártevőt 2016 decemberében egy ukrán erőmű ellen bekövetkezett kibertámadásáért tették felelőssé.

2.2.4 Crypto-bányász programok[84]

A „Most Wanted" rosszindulatú programok közül a crypto-bányászok világszerte a vállalatok 55 százalékára jelentenek veszélyt. A 100 legelterjedtebb rosszindulatú program között tíz különböző verzió szerepelt, míg a TOP3-ban kettő. A cyber-bányászattal a cyber-bűnözők túszul ejtik az áldozat CPU (központi processzor) vagy GPU teljesítményét, valamint elérhető erőforrásait, és ezek használatával bányásznak crypto-valutát.

Állítólag a crypto-valuta bányászok bejutottak néhány vezető weboldalra, elsősorban média streaming és file-megosztó szolgáltatókéra, a felhasználók értesítése nélkül. Miközben ezen tevékenységek egy része legális és legitim, az eszközök meghekkelhetőek, és így nagyobb dominanciát tudnak szerezni, illetve több hasznot tudnak termelni, akár a végfelhasználók CPU teljesítményének 65 százalékos elfoglalásával.

A szakértők úgy látják, hogy a felhasználók egyre kevésbé bíznak meg a pop-up és banner hirdetésekben, ezért hirdetéseket blokkoló szoftvereket használnak, így a weboldalak egyre inkább crypto-bányászokat használnak, mint alternatív bevételforrásokat, gyakran a felhasználók tudta és engedélye nélkül. Valószínű, hogy ez a trend a következő időszakokban erősödik.

TOP3 (2017 december) rosszindulatú programjai

1. Coinhive:

a Monero crypto-valuta online bányászatára tervezett crypto-bányász, amely akkor kezd akcióba, amikor a felhasználó a saját engedélye nélkül látogat meg egy weboldalt.

2. Rig EK (Exploit Kit):

a Rig a Flash, a Java, a Silverlight és az Internet Explorer programokkal él vissza.

3. Cryptoloot:

Crypto-bányász, amely az áldozat CPU vagy GPU teljesítményét, valamint elérhető erőforrásait használja crypto-bányászatra, tranzakciókat rendelve a blockchainhez, így szabadítva fel új valutát.

TOP3 (2017 december) rosszindulatú mobil családja

1. Triada:

moduláris backdoor (hátsó ajtó) az Android eszközök számára, amely kiemelt felhasználói jogosultságokat ad a letöltött rosszindulatú programnak.

2. Lokibot:

Android-alapú, banki tevékenységre specializálódott trójai és információ tolvaj, amely a telefont feloldó, rosszindulatú programmá is képes átalakulni.

3. Lotoor:

az Android operációs rendszer sérülékenységeit kihasználva root jogosultságokra szert tevő hack-eszköz.

[84] Check Point® Security Report 2017. decemberi adatokat feldolgozó Global Threat Intelligence Trends elemzése (Sajtóanyag, lásd 1. számú melléklet).

2.3. Hekker támadások új típusai

Állítólag a The Pirate Bay elhelyezett egy külső forrásból betöltődő (JavaScript) kódot a weboldalán, ami egy böngészőben futó kriptovaluta bányászprogramot futtat a felhasználóknál. Ez a gyakorlatban azt jelenti, hogy a The Pirate Bay látogatóinak számítógépét és okostelefonját a Bitcoinhoz és az Ethereumhoz hasonló Monero digitális pénz bányászatára használják, ezzel pedig saját bevételeiket növelik.

5. ábra: The Pirate Bay elhelyezett egy külső forrásból betöltődő (JavaScript) kódot a weboldalán, ami egy böngészőben futó kriptovaluta bányászprogramot futtat a felhasználóknál. Forrás: https://makay.net/hacker/bitcoin-banyaszat-weboldal-serulekenyseg-vizsgalat.html (Utolsó letöltés: 2018.01.30.)

Az ötletet átvették a kiberbűnözők is, aminek következtében számos olyan alkalmazást juttattak fel a Google Play kínálatába, ami a háttérben szintén kriptovalutát bányászik az elkövetők javára a felhasználók androidos okostelefonjának processzorával.

Mivel ezek a bányászszolgáltatások nem igényelnek extra tudást, időt és befektetést, a jövőben a kiberbűnözés egyik legfontosabb tényezőjévé válhat az áldozatok eszközeivel történő illegális bányászat, az úgynevezett *cryptojacking.*

A trendek alapján várhatóan a magas látogatottságú blogok lesznek az első számú célpontok. Persze a számos sebezhetőségben szenvedő (WordPress, Drupal és Joomla alapon futó), sosem vizsgált oldalak eddig is célpontok voltak, de innentől kezdve még szofisztikáltabb támadásokat indíthatnak ellenük, ráadásul ebből a látogatók és az üzemeltetők szinte semmit nem fognak észrevenni.

A kiberbűnözőknek nem kell ügyfél-adatbázisok értékesítésével, sem botnet szolgáltatás biztosításával bíbelődniük. Ha egy célpontnál sikeresen elhelyezték a bányászkódot, onnantól a látogatók készülékei által termelt pénz szinte egyenesen az elkövetők zsebébe kerül.[85]

A támadási módszer ellen jelenleg kizárólag olyan reklámblokkolókkal (például: AdBlock Plus) lehet védekezni, amelyek képesek felismerni és letiltani a bányászkódok futtatását a böngészőben.

2.3.1 Mit okozhat, ha megbénul az informatikai rendszer

Az energiaiparban különösen a nukleáris létesítmények, a gáz- és olaj alapú erőművek a népszerű célpontok a hekkerek számára. Egy ipari létesítmény biztonsági rendszerének feltörése komoly tudást igényel. Az elmúlt években a támadók egy része mégis a létfontosságú rendszerelemek ostromlásába fogott. A biztonsági rendszer kijátszásával egy létesítmény gyakorlatilag bármelyik része felett át lehet venni az ellenőrzést, úgy, hogy az üzemeltetők észre sem veszik.

[85] https://makay.net/hacker/bitcoin-banyaszat-weboldal-serulekenyseg-vizsgalat.html (utolsó letöltés: 2018. január 30.)

2.3.1.1 Ipari vállalatok

Sikeres hekkertámadás egy erőmű ellen[86]

A FireEye[87] közlése szerint hekkerek állítólag egy közel-keleti szervezet Triconex iparbiztonsági technológiáját célozták meg. Az okok mögött megbújhat, hogy Irán 2012 és 2017 között számos támadást intézett szaúd-arábiai hálózatok ellen a Shamoon nevű vírus felhasználásával.

A vizsgálatok szerint az erőművet ért támadás során a hekkerek átprogramozták a biztonsági eseményeket észlelő vezérlőket. Ezek közül néhány „fail-safe" módba kapcsolt, amivel a vezérlőkhöz köthető folyamatokat leállásra késztette.

Ez egyben le is buktatta a támadókat, mivel az üzemeltető kiszúrta a rendellenes működést.

2.3.1.2 Állami szervezetek

Az amerikai kormányzat és számos, magánkézben levő IT-biztonsági cég is nyilvános figyelmeztetések özönét adta ki az elmúlt években az iráni, észak-koreai, orosz és más, állami támogatással dolgozó hekkerek (várható és bekövetkezett) támadásai miatt.

Különösen a kritikus infrastruktúrákat üzemeltető szervezetek és létesítmények vannak veszélyben, mivel a támadók kiemelt érdeklődést mutatnak mind az állam, mind a magánszféra által működtetett rendszerek irányába.

Kémprogrammal mérték be a tüzérséget[88]

Orosz hekkercsoportot tettek felelőssé az amerikai Demokrata Párt elleni támadásokért és ők „nyúlhattak bele" ukrán katonai fejlesztésekbe is. A szakértők szerint ugyanaz a malware található meg abban az alkalmazásban is, amelyet az ukrán tüzérségnél a lőelemek feldolgozásának gyorsítására használtak.

Állítólag az applikációt még a háború előtt írta egy tüzértiszt, és az ukrajnai polgárháborúban 2014 és 2016 között a szovjet időkből származó D-30-as tarackok több perces célzási idejét akarták általa csökkenteni. A csoport megszerezte az applikációt és sikeresen megfertőzték a rendszereket az Agent-X nevű rosszindulatú kód egyik variánsával.

2.3.1.3 Kritikus infrastruktúrák

Adathalászat pénzintézeteknél[89]

A sérülékeny weboldalak továbbra is az adathalászok célpontjai lesznek hazai környezetben is, ahogyan az utóbbi hónapok során több alkalommal is találkozhattunk bankkártya adatok lopására kihegyezett nyereményjátékokkal és online számlaértesítőkkel.

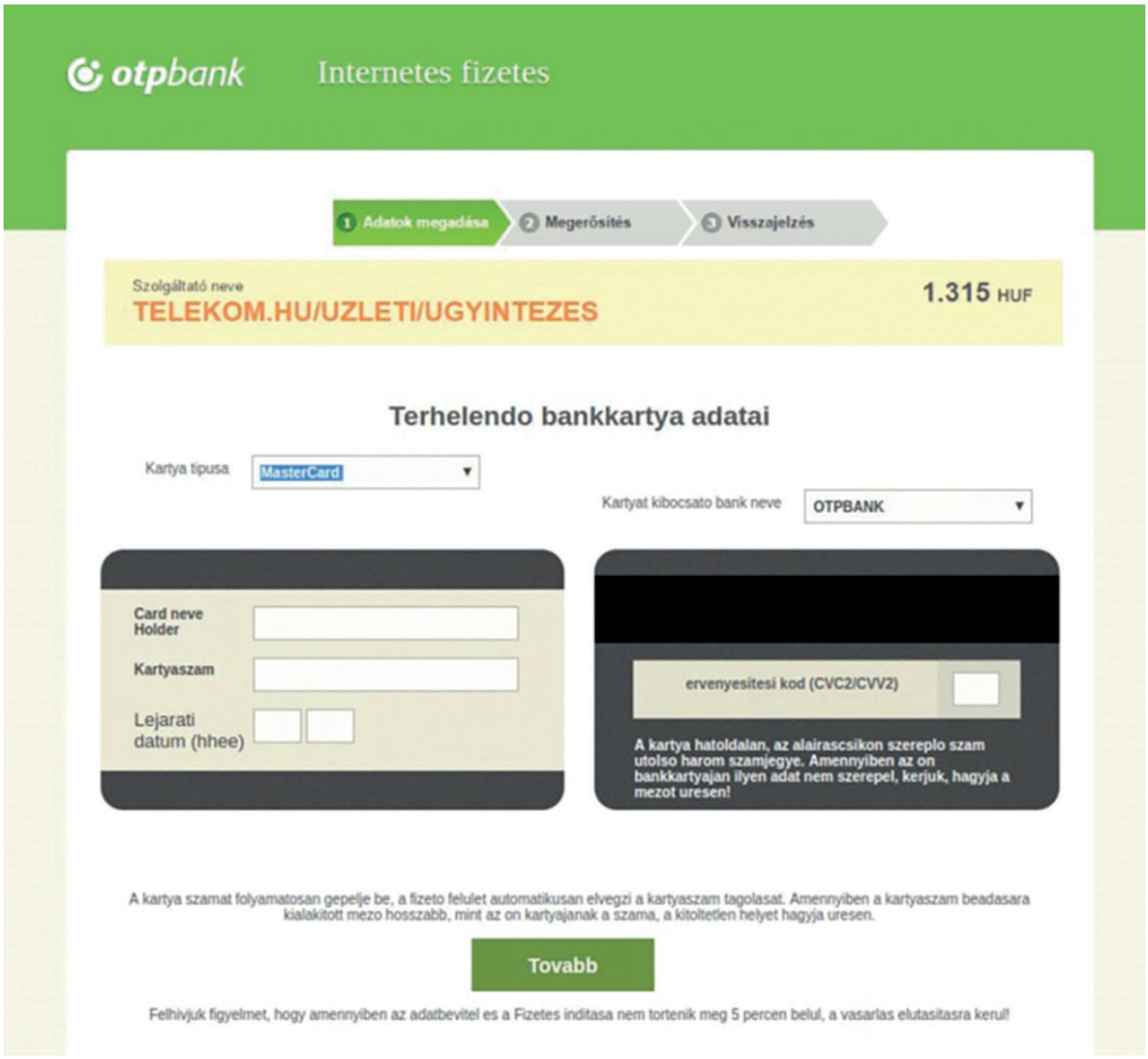
---

86 http://bitport.hu/sikeres-hackertamadas-egy-eromu-ellen (utolsó letöltés: 2018. február 04.)

87 FireEye: Ashar Aziz 2004-ben alapította a FireEye kiberbiztonsági vállalatot, amely cég mára az informatikai biztonsági piac elismert szereplőjévé vált. A FireEye Labs csapata számos sérülékenységet azonosított, többek között a Windows operációs rendszer és az Adobe Flash Player nulladik napi támadását (zero-day), a STUXNET vírust, vagy például az Androidos eszközök sebezhetőségét is.

88 http://bitport.hu/sikeres-hackertamadas-egy-eromu-ellen (utolsó letöltés: 2018. február 04.)

89 https://makay.net/hacker/bitcoin-banyaszat-weboldal-serulekenyseg-vizsgalat.html (utolsó letöltés: 2018. január 30.)



6. ábra: Hamis, bankkártya adatok megszerzését célzó „OTP-oldal”
Forrás: https://makay.net/hacker/bitcoin-banyaszat-weboldal-serulekenyseg-vizsgalat.html

Az ilyen tranzakciók az esetek többségében visszavonhatatlanok és azonosíthatatlanok, így szinte esélytelen, hogy az áldozatok valaha visszakapják a pénzüket.

Riasztást adott ki a Magyar Posta – minden ügyfél érintett[90]

Egy másik példa arra, milyen trükköket vetnek be az adathalászok. Ez esetben a Magyar Posta Zrt. nevében – a vállalat logóját felhasználva – ismeretlen személy vagy személyek megtévesztő nyereményjátékot hirdetettek meg internetes oldalakon. A megtévesztő, hamis tartalom kérdőív kitöltésért mobiltelefon nyerési lehetőséget ajánlottak.

A Magyar Posta Zrt. felhívta a figyelmet, hogy jelenleg nincs olyan nyereményakciója, amellyel telefonkészüléket lehet nyerni. Az állami cég továbbá arra kérte ügyfeleit, hogy fokozottan ügyeljenek adataik védelmére, és hagyják el azon weboldalakat, ahol nincs feltüntetve adatvédelmi tájékoztató és/vagy játékszabályzat.

2.4 Vezetői feladatok célzott kibertámadások esetében

2.4.1 Vezetői feladatok[91]

A tanulmány ezen része mindössze összefoglaló jelleggel sorolja fel, melyek azok a folyamatok, intézkedések és eszközrendszerek, amelyek egy incidens menedzselésekor segíthetik a vezetői döntéshozatalt.

Vezetői feladatok észleléskor (Detect events):

- Információk, incidens jelentések és figyelmeztetések fogadása és vizsgálata.
- Besorolás, sorrendbe állítás (triage).
- Meghatározni mi történt és milyen hatása van (analízis).
- Meghatározni milyen károkat okozott, milyen elhárítási vagy kárenyhítési stratégia alkalmazható.
- Megoldás vagy kárcsökkentés, ellenlépések koordinálása, információk megosztása, nyomonkövetési stratégiák kialakítása, hogy az incidens még egyszer ne fordulhasson elő.

2.4.2 Preventív megoldások

A biztonsági eseményekre való felkészülésben és a védelmi intézkedések meghozatalában az alábbi lépések segítik a vezetőt:

- Értesítések, riportok (sérülékenységről, kártékony szoftverekről).
- Technológia figyelés (trend analízisek, védelmi technikák).
- Hálózat monitoring (behatolás figyelés).
- Biztonsági eszközök fejlesztése.
- Biztonsági auditok.
- Egyéb megelőző intézkedések.

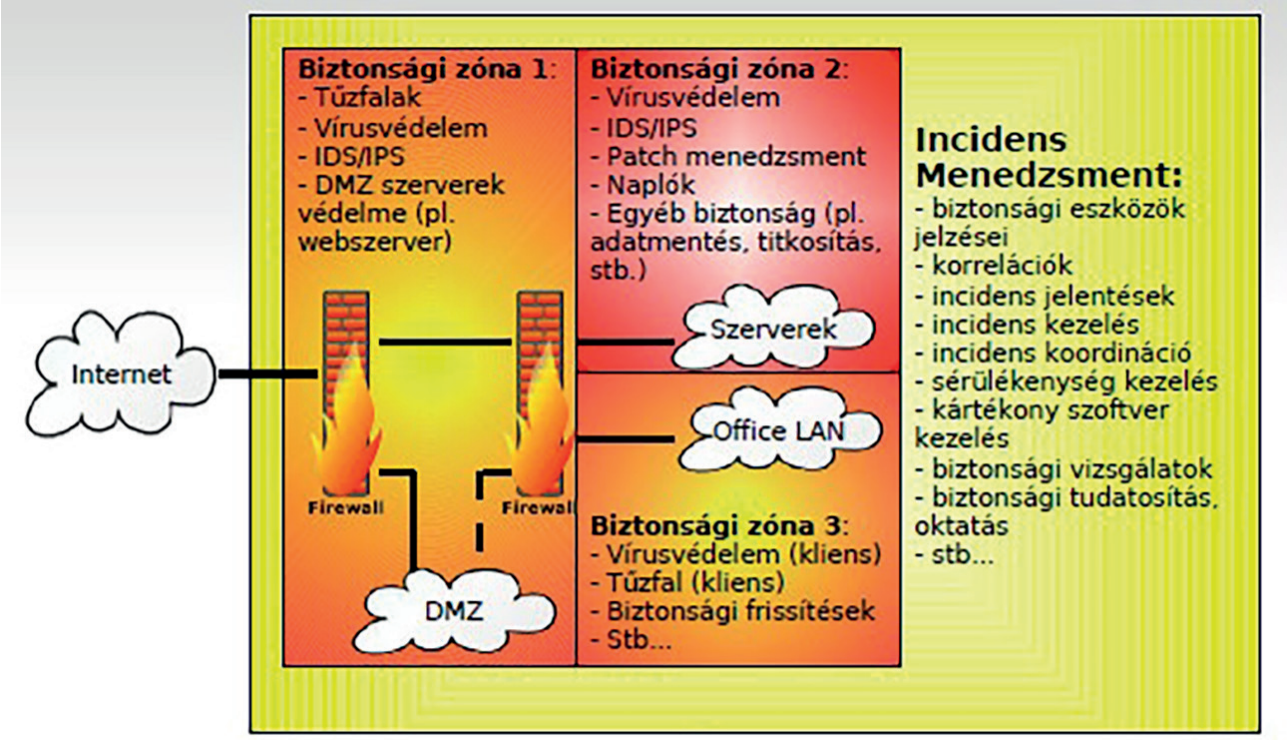
[90] https://www.napi.hu/magyar_vallalatok/riasztast_adott_ki_a_magyar_posta_minden_ugyfel_erintett.657099.html?utm_source=index.hu&utm_medium=doboz&utm_campaign (utolsó letöltés: 2018. február 22.)

[91] Benyó Pál: Az információbiztonság speciális témakörei – Incidensmenedzsment. (utolsó letöltés: 2018. március 04.)

Szolgáltatások, amelyek segítségével fokozható a szervezet ellenálló képessége, azaz a biztonság minősége:

- Kockázat analízis
- Katasztrófa tervek
- Biztonsági tanácsadás
- Tudatosítás és oktatás
- Egyebek

2.4.3 Előkészületi folyamatok



8. ábra: Incidensmenedzsment – Felkészülés a védelemre
Forrás: Benyó Pál: Az információbiztonság speciális témakörei – Incidensmenedzsment (IM)

A szervezeteknek minőségi stratégiára és folyamatokra van szüksége, azaz a megelőzésre és a bekövetkezés megakadályozására is gondolni kell:

- Biztonsági incidens kapacitások terve és implementációja.
- Megerősített és biztonságos infrastruktúra.
- Felismerés, sorrendbe állítás, válaszadás, amikor az esemény bekövetkezik.

2.4.4 Tervezési és karbantartási eszközök

Felkészülés (Prepare):

- Előzetes Incidensmenedzsment (IM) kapacitás megtervezése és implementálása.
- Az IM kapacitás működtetése.
- A meglévő kapacitás fejlesztése folyamatos tanulással és értékeléssel.
- Egyes IM intézkedések utólagos áttekintése, ha szükséges.
- Az infrastruktúra fejlesztési javaslatok átvezetése a védelmi szakaszba.

Sorrendbe állítás (Triage events):

- Az események kategorizálása és korrelációinak meghatározása.
- Az események prioritásának meghatározása.
- Döntés esemény kezeléséről vagy válaszadásról.
- A szükséges információk továbbítása a válaszadási szakasz részére.
- Az IM folyamatba nem tartozó események továbbadása az illetékes helyre.
- A lezárható események lezárása.

Eszközök:

- **Incidens kezelés:** Ticketing rendszer, telefonok, fax, publikációs lehetőségek (például webszerver).
- **Sérülékenység kezelés:** Publikációs lehetőség, adatbázis, analízis eszközök (például labor, virtuális gépek).
- **Kártékony kódok kezelése:** Információ-gyűjtő eszközök, szeparált labor a vizsgálatokhoz, publikációs lehetőségek.

2.5 Best practice, avagy esettanulmány a gyakorlatból

2.5.1 Invitel csoport adatközpont bővítése a 21. Század kiberbiztonsági kihívásainak tükrében[92]

- A kiberbiztonsági fenyegetések fényében, miért vált olyan fontossá, hogy egy vállalat adatközpontban tárolja adatait?

Kemendi Zsolt: Elvesztett üzleti lehetőségeket, bevételcsökkenést és presztízs veszteséget eredményezhet, ha egy vállalat nem védi rendszereit, adatait megfelelően (*adatokat lásd 9. ábra*). Az informatikai biztonság egyre nagyobb jelentőséggel bír a gazdasági élet szereplői számára, legyen szó akár multinacionális vállalatról vagy állami tulajdonú cégről. A kiberfenyegetések valódiak, viszont azok az ügyfelek, akik adatközponti szolgáltatást vesznek igénybe tőlünk, a legmagasabb szintű minősített biztonságot és rendelkezésre állást kapják meg, tehát kisebb kockázatokkal kell számolniuk.

[92] Interjú Kemendi Zsolttal, az Invitech Solutions műszaki igazgatójával (készítette: Sebők Viktória 2017. november 22.)

9. ábra A kibertámadások kockázatai
Forrás: Invitech Solutions

- Milyen szigorú előírások alapján kell egy adatközpontot felkészíteni?

Kemendi Zsolt: Az Invitech Solutions-höz tartozó „DC10" adatközpont-park bővítésének tervezésekor az volt a cél, hogy a rendelkezésre állásra vonatkozó igen szigorú nemzetközi előírásoknak és szabványoknak mindenben megfelelő, a legkorszerűbb biztonsági rendszerekkel ellátott létesítményt valósítsunk meg. A több mint ezer négyzetméteres új egységet, a „DC10-III"-t az adatközpontokat világszerte minősítő szervezet, az Uptime Institute tervdokumentációi alapján készítettük fel a „TIER III" minősítésre. Ilyen magas szintű elvárásoknak megfelelő létesítmény a Magyarországgal határos országokban is mindössze csak három van. Emellett többrétegű biztonságot és igény esetén távmenedzselt intelligens biztonsági szolgáltatásokat is biztosítunk.

- Milyen további szempontokat kellett figyelembe venniük az adatközpont „felkészítése" során?

Kemendi Zsolt: Miután a vállalatok évről évre egyre nagyobb mennyiségben kezelnek adatokat, ésszerűnek tűnik, ha felhőalapú technológiákat kölcsönöznek, és rugalmas kapacitásokat vesznek igénybe. Minden ilyen esetben alapvető szempont az információbiztonság és az adatvédelem, továbbá a rendelkezésre állás kérdése, ezért az adatközpontokat és felhőmegoldásokat üzemeltető cégek elsősorban ezeknek a szempontoknak kívánnak megfelelni. Emellett a különböző hazai törvényi és katasztrófavédelmi előírásokat, illetve a speciális ügyféligényeket is figyelembe kell venni.

A logikai védelem mellett a fizikai védelemre, például fegyveres őrszolgálatra is hangsúlyt kell helyeznünk. A fizikai védelem esetében továbbá biztosítanunk kell a fizikai szegregációt, amely ketreceket vagy komplett különtermeket jelent, például bankok vagy kormányzati szervek esetében.

10. ábra „DC10” adatközpont-parkakkumulátor-telep
Forrás: Invitech Solutions; Fotó: Noguchi Partners

- Az Invitel Csoport új adatközpontjának szempontjából van-e különbség egy állami vállalat vagy egy nagyvállalat adatainak és informatikai rendszereinek védelme között?

Kemendi Zsolt: A mi esetünkben azért nincs, mivel a „TIER III” kategória egy igen szigorú biztonsági szabvány, ennek köszönhetően eleve a legmagasabb szintű védelmet biztosíthatjuk. A „TIER III” tanúsítás lényege a magas rendelkezésre állás. Az adatközpontban karbantartás, berendezés-csere vagy bármilyen más nem üzemszerű állapot esetén is garantáltak a szolgáltatási paraméterek, ugyanis minden aktív eszközből rendelkezésre áll tartalék. Emellett a tanúsítás előírja, hogy minden ellátási útvonal – azaz például az adatátvitel, a villamosenergia-betáplálás vagy a hűtés – kettőzött legyen. Szemben az átlagos, inkább az adminisztratív folyamatokra koncentráló tanúsításokkal, ez a minősítés az éles helyzetekre, a technológiára fókuszál. Érdekesség, hogy számos nemzetközi cég, főleg pénzintézet követel meg ilyen komoly szintű elvárásokat.

- Milyen új típusú támadásokra készültek fel az adatközpont tervezésekor?

Kemendi Zsolt: A támadó technológiák folyamatosan fejlődnek, illetve kijelenthető, hogy tökéletes védelem nincs. Az adatközponti szolgáltatások esetében fontos, hogy réteges, egymásra épülő és dinamikus megoldásokat alkalmazzunk. Nagyon elterjedt és könnyen hozzáférhető – bár nem újszerű – támadás típus a túlterheléses (DDos) támadás. Figyelembe véve, hogy az okoseszközök száma folyamatosan emelkedik, ezért a potenciális támadóeszközök száma a jövőben hasonlóképpen emelkedni fog.

A réteges elem fontos része a központi felügyelet és naplóelemzés, ami képessé tesz bennünket a teljes hálózat felügyeletére, az események azonnali elemzésére, és azok összekapcsolására. A nagy mennyiségű adathalmazból kell kiszűrnünk azt az 1-2 százalékot, ami kártékony lehet.

Például egy gyakorlati teszt során, egy nem tökéletesen védett (gyenge adminisztrátor jelszó, hiányzó biztonsági frissítések) kiszolgálót tettünk szándékosan elérhetővé. Kevesebb, mint három óra (!) alatt megtörték a tesztkörnyezetet. Számunkra az volt a megdöbbentő, hogy bár az internethálózat

egy gigantikus rendszer, mégis a hálózatba kapcsolástól számítva mintegy 15 (!) perc múlva már megkezdődött a rendszer támadása. 3 órán belül pedig egy bitcoin bányában dolgozott a kapacitás. Nekünk erre kell tehát felkészülnünk, és folyamatosan fenn kell tartanunk ezt a készültséget.

2.6. Összefoglalás

Összegzésképpen elmondható, hogy bár a támadók gyakran előrébb járnak, a veszteségek egy része elkerülhető lenne, ha egy vállalat naprakész IT-biztonsági rendszerekre és kompetens szakértőkre támaszkodhatna. Ami fontos még, hogy olyan adatkezelő rendszerek kapcsolódjanak az adatfeldolgozó egységekhez, amelyek biztosítják az adatkezelés teljes életciklusát. Ehhez pedig olyan keretmegoldásokra van szükség, amelyek képesek ellenállni a célzott támadásoknak.

Ezért egyfelől komplex intézkedésekre, folyamatos gondozásra és természetesen a legmagasabb szintű védelemre van szükség.

Ha a logikai védelem szintjét vizsgáljuk, akkor érdemes egyfajta ernyő rendszereket működtetni, amelyhez rugalmas és skálázható megoldásokat lehet integrálni. Nagy hangsúlyt kell helyezni továbbá a határvédelemre, a logmenedzsmentre és a felügyeleti megoldásokra is.

Határozottan látszik, hogy hogy mind a támadási, mind a védelmi technológia mára olyan fejletté alakult, hogy elsősorban a folyamatok és a módszertanok határozzák meg tulajdonképpen a védelmet, nem pedig fordítva.

2.7 Irodalomjegyzék

Interjú

Sebők Viktória: Kemendi Zsolttal, az Invitech Solutions műszaki igazgatójával készített interjú (2017. november 22.)

Sajtóanyag

Check Point® Security Report: 2017. decemberi adatokat feldolgozó Global Threat Intelligence Trends elemzése (lásd 1. számú melléklet)

URL letöltések

A rosszindulatú programcsaládok teljes, 2017 decemberi Top 10 listája (Check Point Blog): http://blog.checkpoint.com/2018/01/15/decembers-wanted-malware-crypto-miners-affect-55-businesses-worldwide/ (Utolsó letöltés: 2018.01.29.)

A Check Point fenyegetésekkel szembeni védelmi forrásainak elérhetősége: http://www.checkpoint.com/threat-prevention-resources/index.html http://www.novell.hu/hirek/20180116_Novell_trendek_joslat_kiberbiztonsag.html (Utolsó letöltés: 2018.01.29.)

http://www.piacesprofit.hu/kkv_cegblog/6-technologiai-trend-2018-ra/ http://www.isafe.hu/6_technologiai_trend_2018-ra (Utolsó letöltés: 2018.01.30.)

https://makay.net/hacker/bitcoin-banyaszat-weboldal-serulekenyseg-vizsgalat.html (Utolsó letöltés: 2018.01.30.)

http://m.sg.hu/cikkek/52426/orosz_internetes_tamadas_esztorszag_ellen (Utolsó letöltés: 2018.02.04.)

http://bitport.hu/sikeres-hackertamadas-egy-eromu-ellen (Utolsó letöltés: 2018.02.04)

https://www.napi.hu/magyar_vallalatok/riasztast_adott_ki_a_magyar_posta_minden_ugyfel_erintett.657099.html?utm_source=index.hu&utm_medium=doboz&utm_campaign (Utolsó letöltés 2018.02.22.)

https://24.hu/kulfold/2017/10/09/grafitbombat-dobnanak-eszak-koreara/ (Utolsó letöltés: 2018.02.25.)

http://passport.blog.hu/2017/06/30/a_stuxnet_sztori (Utolsó letöltés: 2018.02.25.)

PDF letöltés:

Benyó Pál: Az információbiztonság speciális témakörei – Incidensmenedzsment (Utolsó letöltés: 2018.03.04.)

2.8. Mellékletek

1. SZÁMÚ MELLÉKLET

A „Most Wanted" rosszindulatú programok közül a crypto-bányászok világszerte a vállalatok 55%-ra jelentenek veszélyt

A Check Point® Software Technologies Ltd. (NASDAQ: CHKP), a világszerte vezető szerepet betöltő cyber-biztonsági megoldásokat szállító vállalat által összeállított, 2017. decemberi adatokat feldolgozó *Global Threat Intelligence Trends* elemzés szerint, a kérdéses hónapban meredeken emelkedett a crypto-bányász, rosszindulatú programok tevékenysége. A Check Point kutatói szerint a cryptobányászok világszerte a szervezetek 55%-ra voltak hatással a hónap során; a 100 legelterjedtebb rosszindulatú program között tíz különböző verzió szerepelt, míg a top 3-ban kettő. A cyberbányászattal a cyber-bűnözők túszul ejtik az áldozat CPU vagy GPU teljesítményét, valamint elérhető erőforrásait, és ezek használatával bányásznak crypto-valutát.

Mi több, a Check Point vizsgálatai szerint a crypto-valuta bányászok bejutottak néhány vezető weboldalra, elsősorban média streaming és file-megosztó szolgáltatókéra, a felhasználók értesítése nélkül. Miközben ezen tevékenységek egy része legális és legitim, az eszközök meghackelhetőek, és így nagyobb dominanciát tudnak szerezni, illetve több hasznot tudnak termelni, akár a végfelhasználók CPU (központi processzor) teljesítményének 65%-os elfoglalásával. Maya Horowitz, a Check Point Threat Intelligence csoportmenedzsere a következőket mondta: „A felhasználók egyre kevésbé bíznak meg a pop-up és banner hirdetésekben, ezért a hirdetéseket blokkoló szoftvereket használnak, így a weboldalak egyre inkább crypto-bányászokat használnak mint alternatív bevételforrásokat – gyakran a felhasználók tudta és engedélye nélkül." Maya hozzátette: „Ennek eredményeképp, a fenyegetések kezdeményezői ugyancsak crypto-bányász eszközöket alkalmaznak, hogy minél inkább saját céljaikra tudják használni a felhasználók számítástechnikai teljesítményét. Valószínű, hogy ez a trend a következő hónapokban is folytatja a növekedést."

2017 decemberében a Coinhive nevű crypto-bányász átvette a RoughTed helyét a legelterjedtebb fenyegetések rangsorában, míg a Rig ek megőrizte második helyét. A top 10 egy másik új szereplője, a Cryptoloot nevű crypto-bányász a harmadik helyen szerepel.

2017 decemberének top három rosszindulatú programja:

**A nyilak a helyezés előző hónaphoz képesti változását jelzik.*

1. ↑ **Coinhive** – A Monero crypto-valuta online bányászatára tervezett crypto-bányász, mely akkor kezd akcióba amikor a felhasználó a saját engedélye nélkül látogat meg egy weboldalt.
2. ↔ **Rig ek** – A Rig a Flash, a Java, a Silverlight és az Internet Explorer programokkal él vissza.
3. ↑**Cryptoloot** – Crypto-bányász, mely az áldozat CPU vagy GPU teljesítményét, valamint elérhető erőforrásait használja crypto-bányászatra, tranzakciókat rendelve a blockchainhez, így felszabadítva új valutát.

A Triada, az Android eszközökre kifejlesztett moduláris backdoor (hátsó ajtó) továbbra is a szervezetek mobileszközei elleni támadások legkedveltebb rosszindulatú programja, melyet a Lokibot és a Lotoor követ a sorban.

2017 decemberének top három rosszindulatú mobil családja:

1. **Triada** – Moduláris backdoor (hátsó ajtó) az Android eszközök számára, mely kiemelt felhasználói jogosultságokat ad a letöltött rosszindulatú programnak.

2. **Lokibot** – Android-alapú, banki tevékenységre specializálódott trójai és információ tolvaj, mely a telefont feloldó, rosszindulatú programmá is képes átalakulni.

3. **Lotoor** – Az Android operációs rendszer sérülékenységeit kihasználva root jogosultságokra szerttevő, hack eszköz.

A Check Point ThreatCloud Map alapja a Check Point's ThreatCloudTM intelligence, a legnagyobb, a cyber bűnözéssel szemben harcoló, kollaboráción alapuló hálózat, mely fenyegetésekkel kapcsolatos adatokat és támadási trendekkel kapcsolatos információkat szolgáltat a szenzorok globális hálózata számára. A ThreatCloud adatbázis több mint 250 millió címet (melyeket botok beazonosítása céljából elemez), 11 milliónál is több rosszindulatú aláírást és 5,5 millió feletti fertőzött weboldalt tartalmaz, illetve napi szinten több millió rosszindulatú programtípust azonosít be.

* A rosszindulatú programcsaládok teljes, 2017 decemberi Top 10 listája megtalálható a Check Point Blogon: http://blog.checkpoint.com/2018/01/15/decembers-wanted-malware-crypto-miners-affect-55-businesses-worldwide/

A Check Point fenyegetésekkel szembeni védelmi forrásainak elérhetősége:
http://www.checkpoint.com/threat-prevention-resources/index.html

Check Point Software Technologies Ltd.

A Check Point Software Technologies Ltd. (www.checkpoint.com) világszerte a kormányzati és vállalati ügyfelek vezető cyber-biztonsági szállítója. Megoldásai megvédik ügyfeleit a cyber-támadásoktól, aminek alapja a rosszindulatú és zsaroló programokkal, illetve más támadás típusokkal szembeni, iparágvezető eredményesség. A nagyvállalatok felhőit, hálózatait és a mobil eszközeit védő, teljes körű biztonsági architektúrát kínál, valamint a legátfogóbb és legintuitívabb, egyetlen pontról irányítható biztonság-menedzsment rendszert. A vállalat 100.000-nél több, különböző méretű szervezet védelmét biztosítja.

Check Point Blog: http://blog.checkpoint.com/
Twitter: www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

3. MARSI TAMÁS: A CÉLZOTT TÁMADÁSOK ÉS MEGELŐZÉSÜK SÉRÜLÉKENYSÉGVIZSGÁLATTAL

3.1. A kibervédelem állami szervezetrendszere

3.1.1 A szervezetrendszer

Az Országgyűlés a 2013. év során – figyelembe véve Magyarország Nemzeti Biztonsági Stratégiáját, Magyarország Nemzeti Kiberbiztonsági Stratégiáját, valamint az ez utóbbit is megalapozó Európai Unió kiberbiztonsági stratégiáját – megalkotta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (a továbbiakban: Ibtv.), amely 2013. július 1-jén lépett hatályba. Az Ibtv. célként fogalmazta meg a nemzeti elektronikus adatvagyon, valamint az állami- és önkormányzati szervek elektronikus információs rendszereinek, illetve a létfontosságú rendszerek és rendszerelemek biztonságának erősítését.

Az Ibtv. deklarálja, hogy az elektronikus információs rendszerek biztonságáért az üzemeltető, működtető állami szerv a felelős. Ezen felelősség keretében az állami szervek feladata a rendszerek biztonsági osztályokba történő sorolása, az egyes biztonsági osztályokhoz a jogszabályban meghatározott fizikai, adminisztratív, személyi és logikai védelmi intézkedések kialakítása, a rendszerek biztonságáért felelős helyi szervezeti struktúra és belső szabályozás kialakítása.

A törvény továbbá létrehozta a hazai kibervédelmi szervezetrendszert, amelynek alapvető rendeltetése, hogy az állami szervek információbiztonsági feladatainak végrehajtását biztonsági szolgáltatásokkal támogassa, ellenőrizze, az állami szervezetrendszer egésze tekintetében a biztonságtudatosságot fejlessze.

A szervezetrendszer stratégiai szintű eleme a Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács), mint a Kormány javaslattevő, véleményező szerve, és az annak keretében működő munkacsoportok.

A szervezetrendszer operatív elemei a Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: NEIH), a Kormányzati Eseménykezelő Központ (a továbbiakban: GovCERT) és egyéb ágazati eseménykezelő központok, ágazati hatósági szervek.

3.1.2 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.[93]

Az elnök mellett a Tanács tagjai, az emberi erőforrások minisztere, a honvédelmi miniszter, az igazságügyi miniszter, a külgazdasági és külügyminiszter, a nemzeti fejlesztési miniszter, a nemzetgazda-

[93] 2013. évi L. törvény 21. § (1) bekezdés.

sági miniszter, a földművelésügyi miniszter által delegált 1 fő állami vezető, a Tanács tagja továbbá a kormányzati tevékenység összehangolásáért felelős miniszter által delegált kiberkoordinátor is.[94]

A Tanács munkáját a Tanács elnökének felkérésére az Állami Számvevőszék elnöke, a Magyar Nemzeti Bank elnöke, a Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke, a Nemzeti Hírközlési és Informatikai Tanács elnöke, a Nemzeti Média- és Hírközlési Hatóság elnöke, valamint a Magyar Energetikai és Közmű-szabályozási Hivatal elnöke segítheti.[95]

3.1.3 kiberbiztonsági ágazati munkacsoportok

A Tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását ágazati és funkcionális kiberbiztonsági munkacsoportok segítik a következő szakterületeken:

- eseménykezelés,
- belbiztonság,
- e-közigazgatás,
- energetika,
- gyermekvédelem.

A fentieken kívül a Tanács felkérésére további kiberbiztonsági munkacsoportok is létrehozhatóak.

A kiberbiztonsági munkacsoportok tagjai a kiberkoordinátor, és az általa felkért állami szervek által delegált közszolgálati tisztviselők. A kiberbiztonsági munkacsoportok üléseinek állandó résztvevője a kiberkoordinátor által felkért nem kormányzati szakértő. A kiberbiztonsági munkacsoportok javaslatára a Tanács jogi kötelező erővel nem rendelkező ajánlásokat adhat ki a kibertámadások kezelése és az elektronikus információbiztonság területén alkalmazandó legjobb gyakorlatokról.[96]

3.1.4 A nemzeti kibervédelmi intézet

A kiberfenyegetések komplexitása és volumene a 21. században a technika fejlődésével és elterjedésével együtt folyamatosan növekszik, a kiberbűnözésből származó károk világszinten egyre nagyobb összegre rúgnak. Ezzel párhuzamosan egyre erőteljesebben jelennek meg az állami szereplők és a vélhetően államilag támogatott kiberkémkedési műveletek is.

Ezekre a 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 tehát, 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.

Kiemelten fontos nemzeti érdek a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú rendszerek és rendszerelemek elektronikus információs rendszereinek biztonsága.

Ezen kívül társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.[97]

---

94 484/2013. (XII. 17.) Korm. rendelet 1. § (1)-(3) bekezdés.
95 484/2013. (XII. 17.) Korm. rendelet 1. § (4) bekezdés.
96 484/2013. (XII. 17.) Korm. rendelet 3. §.
97 2013. évi L. törvény preambulum.

3.1.4.1 A hatóság

A Nemzeti Elektronikus Információbiztonság Hatóság (a továbbiakban: hatóság) jogszabályi működési kereteit, az Ibtv., valamint annak végrehajtási rendeletei és számos egyéb jogszabály adja. A hatóság ügyfélkörét a törvény jelöli ki, amely nagy vonalakban megegyezik a Kormányzati Eseménykezelő Központ ügyfélkörével.

A hatóság egyik legfontosabb feladatként elbírálja a törvény 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.

A hatóságon kívül más szervek is látnak el, szűkített körű hatósági feladatokat. A zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátására a Kormány a zárt célú elektronikus információs rendszert működtető szerv vezetőjét jelöli ki.[98]

3.1.4.2 A Kormányzati Eseménykezelő Központ

A GovCERT legfőbb feladatait és hatáskörét az Ibtv. határozza meg. A feladatokról részletesen 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 továbbiakban: kormányrendelet) rendelkezik, mely összességében az Ibtv. végrehajtási rendelete. Ezen kívül is számos jogszabály kapcsolódik a GovCERT tevékenységéhez, és segíti munkáját adatkérési, valamint egyéb jogosultságok biztosítása révén.

A jogszabályok alapján a GovCERT-nek több, egymástól jól elhatárolható folyamata azonosítható.

- A fenyegetettség menedzsment feladat keretében adatgyűjtés, adatelemzés, offline monitorozás, valamint adatmegosztás történik. Ebben a folyamatban keletkeznek a publikációk és az egyéb termékek, mint a riasztások, tájékoztató hírlevelek, rendszeres sérülékenység tájékoztatók és a Nemzeti Kiberbiztonsági Koordinációs Tanács részére készülő negyedéves jelentés.
- A biztonsági események kezelése, más megfogalmazásban incidenskezelés a különböző eseményeknek a keletkezést követő feldolgozása, koordinációja, technikai kivizsgálása, kapcsolattartás az ügyfelekkel, illetve a munkát megkönnyítő nyilvántartások vezetése.
- A Kormányzati Eseménykezelő Központ végzi a hatáskörébe tartozó rendszerek sérülékenységvizsgálatát is, amelynek célja a rendszerek gyenge pontjainak beazonosítása, valamint javaslatok tétele a biztonság növelése céljából.
- A megelőző és támogató tevékenység részeként a GovCERT információbiztonsági tudatosító és tanácsadó tevékenységet végez, részt vesz Magyarország kiberkoordinációjában, valamint kibervédelmi gyakorlatokat szervez, és azokban részt vesz.

3.1.5 Ágazati eseménykezelő központok

Magyarországon működnek úgynevezett ágazati eseménykezelő központok, amelyek a jogszabályokban előírt rendszerek esetén végzik az eseménykezelést, ezekkel a GovCERT aktív kapcsolatot tart, és folyamatos együttműködést folytat.

[98] 187/2015. (VII. 13.) Korm. rendelet 8. fejezet.

A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelését a Katonai Nemzetbiztonsági Szolgálat Kibervédelmi Központja (korábban MilCERT); a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelését az IntCERT végzi.[99]

A jogszabályi felhatalmazás alapján működő ágazati eseménykezelő központok mellett működnek úgynevezett „kvázi ágazati" CERT-ek is. Több minisztérium is létrehozott olyan eseménykezelőt, ami az adott ágazat állami szereplőnek információbiztonsági tevékenységét igyekszik koordinálni, incidenskezelési szempontból. Kvázi ágazati CERT-nek tekinthető többek között a Kormányzati Informatikai Fejlesztési Ügynökség Nemzeti Információs Infrastruktúra Fejlesztési Program (KIFÜ-NIIF) által működtetett eseménykezelő központ is.

Ezen kívül működik még az MTA SZTAKI keretén belül 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.[100]

3.2. A sérülékenységvizsgálati tevékenység háttere, tartalma, lebonyolítása

3.2.1 A Sérülékenység

A sérülékenység, sebezhetőség vagy biztonsági rés az Ibtv. definíciója alapján az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.[101]

A nemzetközileg elismert egyik definíció szerint a biztonsági rés olyan gyengeség, amelyet egy fenyegető szereplő (például támadó) kihasználhat, annak érdekében, hogy egy számítógépes rendszeren belül jogosulatlan lépéseket hajthasson végre. A biztonsági rések három elem metszéspontjában találhatóak: a célrendszer érintett egy bizonyos problémával, a támadó hozzáférhet a hibához és ki is használhatja azt.[102]

Sérülékenységek vonatkozhatnak a rendszerek fizikai környezetére, a személyzetre, a vezetésre, a szervezeten belüli adminisztratív eljárásokra és biztonsági intézkedésekre, az üzleti szolgáltatásokra,

[99] 271/2018. (XII. 20.) Korm. rendelet 6. § (1)-(2) bekezdés.
[100] https://www.cert.hu/a-hun-cert-csoportrol.
[101] 2013. évi L. törvény 1. § 40. pont.
[102] https://en.wikipedia.org/wiki/Vulnerability_(computing) (utolsó letöltés: 2018. szeptember 13.)

a kommunikációs berendezésekre és létesítményekre, valamint leggyakrabban említve a hardver és szoftver elemekre.

Ilyen sérülékenység lehet, ha egy támadó egy memóriatúlcsordulási sebezhetőséget talál és használ ki káros programok telepítéséhez, vagy a támadó ráveszi a felhasználót, hogy egy e-mail üzenet mellékeltét nyissa meg, de akár egy titkosított és szigorított szabályok szerint készült program bennfentes általi lemásolása és feltörése is.[103]

3.2.1.1 A sérülékenységek okai

A sérülékenységek kialakulásának több oka is lehet. A nagy, összetett rendszerek növelik a hibák és a nem kívánt hozzáférési pontok keletkezésének valószínűségét. A nyílt forráskódú, jól ismert kódok, szoftverek, operációs rendszerek, hardverek használata növelheti annak valószínűségét, hogy a támadónak van-e olyan ismerete és eszköze, amellyel felkutathatja és kihasználja a biztonsági hibát. A fizikai kapcsolatok, jogosultságok, portok, protokollok, szolgáltatások is kiszolgáltatottá teszik a rendszereket, indokolatlanul növelhetik a kompromittáció kockázatát.

A felhasználók és viselkedésük a rendszerben az egyik legnagyobb kockázatot rejti magában. A felhasználó megfelelő szabályrendszer hiányában például olyan egyszerű jelszavakat használhat, amelyeket úgynevezett nyers erős vagy hibrid támadással gyorsan fel lehet törni. Sok felhasználó olyan helyen tárolja a jelszavait, amelyhez más is hozzáférhet, vagy többször, több helyre is azonos jelszót használ. Ezek mind növelik a rendszerek kitettségét.

Az operációs rendszer tervezője dönthet úgy is, hogy a felhasználói és programkezelésre szuboptimális (vagyis nem megfelelő) irányelveket alkalmaz. Például az operációs rendszerek alapértelmezetten engedélyezik minden program és minden felhasználó számára a teljes hozzáférést az egész számítógéphez, ezzel lehetővé téve a vírusok és rosszindulatú programok futását akár a rendszergazda nevében is. A szuboptimális irányelvek alkalmazásával indokolatlanul sok veszély keletkezhet az operációs rendszereket futtató hálózatokban.

Egyes internetes oldalak káros tartalmat hordozhatnak (például spyware vagy adware programok), amelyek a látogatás következtében automatikusan települnek számítógépes rendszerekre. Miután a felhasználó meglátogatja ezeket a weboldalakat, a számítógépes rendszerek megfertőződhetnek, az ilyen módok összegyűjtött adatoka a káros programok üzemeltetői a személyes adatokat összegyűjthetik és átadhatják harmadik személyeknek.

Gyakran előfordul, hogy a programozó hibásan végzi a munkáját és figyelmetlenségből egy kihasználható biztonsági rés keletkezik az elkészült szoftverben, amelyet rosszindulatú személyek felkutathatnak, majd azzal visszaélhetnek.

A program sajnos alaptalanul feltételezheti, hogy minden felhasználói bevitel biztonságos. A felhasználói adatbevitelt nem ellenőrző programok lehetővé tehetik a parancsok vagy például egyéb utasítások nem kívánt, közvetlen végrehajtását (puffer túlcsordulások, SQL injektálás vagy más nem

[103] https://en.wikipedia.org/wiki/Vulnerability_(computing)#Examples_of_vulnerabilities (utolsó letöltés: 2018. szeptember 13.)

ellenőrzött, validált bemenetek). Speciálisan formázott, trükkösen elkészített parancsokkal gyakran élnek vissza a támadók.

Egy kutatás megállapította, hogy a legtöbb információs rendszer legsérülékenyebb pontja maga az ember: felhasználó, operátor, tervező, ebből kifolyólag az úgynevezett social engineering egyre komolyabb biztonsági problémát jelent.[104] A social engineering információbiztonsági tekintetben az emberek pszichológiai manipulálással különböző cselekvések végrehajtására és bizalmas információk átadására történő meggyőzése.[105] Ilyen lehet például egy minimális előzetes információkkal, jól értesültnek tűnő és rámenős támadó, aki további ügyfél információkat szerezhet egy telefonbeszélgetés során az ügyfélszolgálati munkatárstól.

3.2.1.2 A 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.

A sérülékenységmenedzsment tevékenység keretében az üzemeltetők általában összegyűjtik a rájuk bízott szoftver és hardvereszközök részletes listáját, folyamatosan figyelik a napvilágot látott sérülékenységeket és „befoltozzák" a biztonsági réseket vagy a sérülékenységek kihasználásának megakadályozása érdekében megkerülő megoldásokat (például hálózati tiltások) alkalmaznak.[106] Tehát a sérülékenységmenedzsment egy megelőző célú, üzemeltetői tevékenység és nem azonos a sérülékenységvizsgálattal.

3.2.1.3 Nulladik napi sérülékenység

A nulladik napi (más néven 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.

A számítógépes biztonsági szakzsargonban a „Day Zero" az a nap, amikor az érdekelt fél (feltételezhetően a célrendszer szállítója) tudomást szerez a sérülékenységről. Egészen eddig a napig a sebezhetőség nulladik napi sebezhetőségnek számít. Amikor a gyártó értesül a biztonsági rés létezéséről, megkezdődik a verseny a támadók és a fejlesztők között. Minél kevesebb idő telik el a sérülékenység napvilágra kerülésétől, annál kisebb az esélye, hogy a gyártó elkészítette a javítást, így annál nagyobb a valószínűsége annak, hogy a támadó szoftver elleni támadása sikeres lesz. Miután a gyártó tudomást szerez a sérülékenységről, általában javításokat, foltozásokat (patch) készít, vagy tanácsot ad annak mérséklése érdekében (workaround).

Egy nulladik napi sérülékenység esetén annak foltozása gyakorlatilag lehetetlen, így napjainkban az ilyen támadások nagy veszélyeket hordoznak magukban. Különösen nagy a kitettsége az olyan rendszereknek, amelyek csatlakoznak az internethez is.[107]

A nulladik napi sérülékenységek felkutatása egy erőforrás-igényes tevékenység, nagy szakértelmet, erős infrastruktúrát és rengeteg időt igényel egy-egy ilyen sérülékenység megtalálása. Ebből következően egy nulladik napi sérülékenység drága eszköz, és éppen ezért általában célzott támadások kivitelezéséhez szokták használni a támadók.

---

104 https://en.wikipedia.org/wiki/Vulnerability_(computing)#Causes (utolsó letöltés: 2018. szeptember 13.)

105 https://en.wikipedia.org/wiki/Social_engineering_(security) (utolsó letöltés: 2018. szeptember 13.)

106 https://en.wikipedia.org/wiki/Vulnerability_(computing) (utolsó letöltés: 2018. szeptember 13.)

107 https://en.wikipedia.org/wiki/Zero-day_(computing) (utolsó letöltés: 2018. szeptember 13.)

3.2.2 A Sérülékenységvizsgálat

A sérülékenységvizsgálat az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárására irányuló tervezett és szervezett tevékenység.[108] Az Ibtv. alapján 3-as, vagy annál magasabb biztonsági osztályba sorolt új elektronikus információs rendszer esetén kötelező sérülékenységvizsgálatot végezni, amely a GovCERT ügyfelei számára ingyenes szolgáltatás.

A vizsgálat célja továbbá a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében.[109]

Fontos megjegyezni, hogy az érintett rendszer különböző irányokból történő kompromittálhatóságának mérése a vizsgálat ideje alatti állapotra vonatkozik, tehát a rendszerben történő változtatással más sérülékenységek és biztonsági rések is keletkezhetnek, ekkor új vizsgálatra lehet szükség.

A nemzetbiztonsági védelem alá eső szervek elektronikus információs rendszerei, az európai vagy nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt állami és önkormányzati szervek rendszerelemeinek elektronikus információs rendszerei, valamint bizonyos kivétellel[110] a zárt célú elektronikus információs rendszerek sérülékenységvizsgálatát a Kormányzati Eseménykezelő Központ végzi. A GovCERT jogosult továbbá az Ibtv. alapján feljogosított állami szervként[111] a sérülékenységvizsgálat lefolytatására.[112]

A sérülékenységvizsgálat tárgya az adatok és az információk kezelésére használt elektronikus információs rendszerek, rendszerelemek, eszközök, eljárások és kapcsolódó folyamatok vizsgálata, valamint az ezeket kezelő személyek általános informatikai felkészültségének, és az érintett szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.[113]

3.2.3 Sérülékenységvizsgálati tevékenység

A sérülékenységvizsgálatot célszoftverek segítségével végzik, amelyek a biztonsági vizsgálati eljárás során kifejezetten a sérülékenységvizsgálat egyes fázisainak végrehajtására kifejlesztett alkalmazások.[114] A programok beállítása, valamint a vizsgálati eljárás mélysége alapján megkülönböztetünk automatizált és manuális vizsgálatot.

Az automatizált informatikai biztonsági vizsgálat olyan biztonsági vizsgálati eljárás, amely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre.[115]

A kézi vagy manuális informatikai biztonsági vizsgálat olyan biztonsági vizsgálati eljárás, amely során az érintett szervezet informatikai rendszerének sérülékenységei a vizsgálatot végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával kerülnek feltérképezésre.[116]

---

108 2013. évi L. törvény 1. § 41. pont.
109 2013. évi L. törvény 15. § (1) bekezdés.
110 271/2018. (XII. 20.) Korm. rendelet 22. § (2-3) bekezdés.
111 2013. évi L. törvény 18. § (3) bekezdés.
112 271/2018. (XII. 20.) Korm. rendelet 22. § (1) bekezdés.
113 2013. évi L. törvény 15. § (2) bekezdés.
114 271/2018. (XII. 20.) Korm. rendelet1. § 7. pont.
115 271/2018. (XII. 20.) Korm. rendelet 1. § 3. pont.
116 271/2018. (XII. 20.) Korm. rendelet 1. § 10. pont.

3.2.3.1 Irányultságok

A sérülékenységvizsgálat során az eljárást megalapozó dokumentációban (a projektalapító dokumentumban) meghatározottak szerint sor kerül külső informatikai biztonsági vizsgálatra, webes vizsgálatra, belső informatikai biztonsági vizsgálatra, illetve vezeték nélküli hálózat informatikai biztonsági vizsgálatára.

A belső informatikai biztonsági vizsgálat olyan vizsgálati eljárás, amelynek során az érintett szervezet informatikai rendszerének sérülékenységvizsgálata a belső hálózati végpontról – a megrendelő aktív támogatásával – közvetlenül történik.[117]

Az ilyen irányultságú vizsgálatok első fázisa a regisztrált felhasználói jogosultság nélküli felderítés. A második fázisban (személyi, technikai, logisztikai feltételek teljesülése esetén) a jogosultsággal végzett vizsgálatok következnek, beleértve a különböző speciális vizsgálati lehetőségeket. Eszköz- és szoftverkonfigurációs ellenőrzések során az érintett rendszerelemek beállításainak megfeleltetése történik a szakmai elvárások és irányelvek teljesülése érdekében. Vastagkliens architektúrában a saját fejlesztésű kliens-szerver alkalmazások vizsgálata zajlik le. Forráskód analízis tekintetében a Microsoft által meghatározott Security Development Lifecycle (SDL) módszertan implementációs fázisa szerint végzi a GovCERT a vizsgálatait.

A külső vizsgálat az informatikai rendszer internet felőli, külső sérülékenységvizsgálata, amelynek során, az interneten fellelhető, nyilvános adatbázisokban való szabad keresésre, célzott információgyűjtésre, valamint az elérhető számítógépek szolgáltatásainak, sebezhetőségének feltérképezésére kerülhet sor.[118]

A külső vizsgálat általában interneten fellelhető, publikus adatbázisokban való releváns adatok keresésére és gyűjtésére; a hálózati struktúráról, illetve a telepített hardver- és szoftverelemekről való célzott információgyűjtésre; célszegmensben elérhető számítógépek, eszközök operációs rendszerének, szolgáltatásainak, azok verziószámának és sebezhetőségeinek feltérképezésére; a határvédelmi eszközök és sebezhetőségeinek feltérképezésére; szolgáltatás megtagadásra; vagy terheléses analízisre irányul.

A webes vizsgálat egy olyan eljárás, amely során automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei.[119] A webes alkalmazások sérülékenységvizsgálata az OWASP Testing Guide v4 ajánlásai alapján történik. A vizsgálatok az automatizált sérülékenység-elemző szoftverek használatával kezdődnek, majd technológiától és szempontoktól, valamint az automata vizsgálat eredményétől függően intuitív kézi elemzésre is szükség lehet.

A vezeték nélküli hálózat informatikai biztonsági vizsgálata alkalmával a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, a titkosítási eljárások elemzése, valamint a titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik.[120] Ezen kívül sor kerülhet az elérhető vezeték nélküli hálózatok sebezhetőségének vizsgálatára célszoftverek segítségével, hamis vezeték nélküli hozzáférési pont installálására és a kliensek forgalmának eltérítési kísérletére, a vezeték nélküli kapcsolódási házirend alkalmazásának tesztelésére, valamint a hálózati eszközök naplózási beállításainak vizsgálatára.

A felhasználói tudatosság meglétét leginkább úgynevezett social engereering vizsgálattal lehet vizsgálni. A vizsgálat lényege, hogy bevett social engereering módszerekkel (például pretexting, phishing, spear phishing, water holing) tesztelik a vizsgálók a felhasználók információbiztonsági tudatosságát, így a szervezet megbizonyosodhat az ilyen irányú kitettségéről is.

A pretexting egy olyan támadásforma, amellyel a támadók az áldozatokkal kapcsolatos információkból előzetesen nyílt forrásból vagy adathalászattal felkészülnek és így próbálnak meg általában telefonon még több információhoz jutni. A phishing vagy adathalászat segítségével a támadók csalárd

[117] 271/2018. (XII. 20.) Korm. rendelet 1. § 5. pont.
[118] 271/2018. (XII. 20.) Korm. rendelet 1. § 12. pont.
[119] 271/2018. (XII. 20.) Korm. rendelet 1. § 18. pont.
[120] 271/2018. (XII. 20.) Korm. rendelet 1. § 19. pont.

módon, általában e-mailben szereznek magánjellegű információkat az áldozatuktól. A spear phishing vagy célzott adathalászat az előzőekhez hasonló technika, de a támadók rendkívül testreszabott e-maileket küldenek kisszámú végfelhasználónak. A water holing támadás kihasználja a felhasználók által a rendszeresen látogatott webhelyekbe vetett bizalmat, a támadók rosszindulatú kódot helyeznek el ott.[121]

3.2.3.2 Jogosultsági szintek

A megrendelő által biztosított jogosultsági szintek alapján megkülönböztetünk regisztrált felhasználói jogosultság nélküli (black box), regisztrált felhasználói (korlátozott) jogosultsággal rendelkező (grey box), valamint adminisztrátori jogosultsággal rendelkező (white box) vizsgálatokat. Az egyes vizsgálatoknak más és más a célja, ezért szükséges ez a megkülönböztetés.

A regisztrált felhasználói jogosultság nélküli informatikai biztonsági vizsgálat egy olyan eljárás, amelynek során a vizsgálatot végző személy semmilyen előzetes információval nem rendelkezik az érintett szervezet informatikai rendszeréről, és nincs felhasználói jogosultsága a rendszerhez.[122]

A regisztrált felhasználói jogosultsággal rendelkező informatikai biztonsági vizsgálat során a vizsgálatot végző személy a számára külön létrehozott felhasználói jogosultsággal végzi a vizsgálatot.[123]

Az adminisztrátori jogosultsággal rendelkező informatikai biztonsági vizsgálat alkalmával a vizsgálatot végző személy rendszergazdai jogosultsággal rendelkezik, és az eljárás célja, hogy megfelelőségi listák alapján az érintett szervezet teljes informatikai rendszerének állapota ellenőrzésre kerüljön.[124]

3.2.4 A sérülékenységvizsgálati projekt kezdete

A sérülékenységvizsgálati projektek keletkezhetnek beérkező ügyfélmegrendeléssel vagy hatósági elrendeléssel. A GovCERT ügyfelei a korábban részletezett típusú vizsgálatokat kezdeményezhetnek, valamint a hatóság határozatban is kötelezhet ügyfelet meghatározott vizsgálatok elvégeztetésére.

A bejövő megrendelés esetén meg kell állapítani, hogy a szervezet jogosult-e vizsgálatot kezdeményezni, valamint kapacitás felmérést kell végezni annak érdekében, hogy a vizsgálat mindkét fél számára kedvező véghatáridővel kerüljön lebonyolításra.

A megrendelő feladata a vizsgálati kezdeményezés okának és lényeges körülményeinek ismertetése, annak a megállapítása céljából, hogy a vizsgálandó rendszer a GovCERT kizárólagos sérülékenységvizsgálati hatáskörébe tartozik-e, illetve mi a vizsgálat kezdeményezésének indoka (új rendszer vagy szolgáltatás bevezetése, meglévő rendszer vagy szolgáltatás felülvizsgálata, stb).

A vizsgálatokat a GovCERT elosztott erőforrásból, projektszerűen valósítja meg, amelynek célja az erőforrások minél hatékonyabb felhasználása és elosztása. A sérülékenységvizsgálati projektek általában több munkatárs csapatmunkáján alapulnak, a kollégák általában különböző vizsgálatok szakszerű és alapos végrehajtására szakosodnak annak érekében, hogy a különböző vizsgálati típusokat és módszereket a legnagyobb szakértelemmel és a legnaprakészebb tudással végezhessék.

Egy-egy vizsgálat során egy elemző munkatárs központi koordinációs szerepet, úgynevezett projektgazdai pozíciót tölt be, akit a jogosultság-, és kapacitásvizsgálatot követően a projekt kezdeti szakaszában jelölnek ki. Nagyobb projektek esetén a terhek megosztása érdekében kijelölésre kerülhet egy helyettes projektgazda is. A projektgazda felelős a vizsgálat sikeres lebonyolításáért a kezdetektől egészen a végső jelentés elkészüléséig, annak kiküldéséig, valamint az utókövetésig. A projektgazda

---

121 https://en.wikipedia.org/wiki/Social_engineering_(security)#Techniques_and_terms (utolsó letöltés: 2018. szeptember 13.)

122 271/2018. (XII. 20.) Korm. rendelet 1. § 13. pont.

123 271/2018. (XII. 20.) Korm. rendelet 1. § 14. pont.

124 271/2018. (XII. 20.) Korm. rendelet 1. § 1. pont.

felelős továbbá a felek közötti találkozók megszervezésért, az azokra való felkészülésért, oroszlánrészt vállal a dokumentációk elkészítésében, ő az elsődleges kapcsolati pont a vizsgálatot végző csapat és a megrendelő között. Ezen kívül összehangolja a csapat működését is, a szakterület vezetőjével közösen részt vállal a tervezésben.

A kapcsolattartás elsődleges formája a telefon és az e-mail, azonban több projekt esetén szükséges személyes egyeztetés is. A személyes egyeztetésen részt vesz a megrendelő oldaláról felelős személy (vezető), az érintett szakterület vagy projekt képviselője és esetenként a fejlesztő is.

A vizsgálat különböző szakaszainak nyomon követése, auditálása okán a GovCERT egy többfunkciós projektmenedzsment szakrendszert használ. Az alkalmazás segítségével lehetőség nyílik a projekttel kapcsolatos adatok biztonságos tárolására, a feladatok hatékony elosztására, különböző státuszok használatára, a feladatokkal történő haladások nyomon követésére, az elakadások detektálására, a vezetők gyors és hatékony tájékoztatására. A rendszer ezen kívül alkalmas még a különböző dokumentumok elkészítésének támogatására is.

A kezdeti szakaszban kiküldésre kerül az intézménynek egy általános tájékoztató és egy adategyeztető lap, amely segít az ügyfélnek a zökkenőmentes kapcsolatfelvételben és adategyeztetésben, a vizsgálati lehetőségek megismerésében, valamint a projekt céljának megértésében, a projektgazdával történő hatékony együttműködésben.

Az általános tájékoztatóban leírásra kerülnek a módszertani elemek, az irányultságok és a jogosultságok, tartalmazza továbbá a különböző módszerek részletes leírását, valamint a sérülékenység elemzési módszertant és a javaslatok kidolgozásának metodikáját. Az adategyeztető lap információkat kér a megrendelőtől a vizsgálat indokáról, céljáról, a vizsgált rendszerről, a különböző dokumentumokról (osztályba sorolás, rendszer dokumentumok stb.), valamint a végrehajtással kapcsolatos adatokról (kapcsolattartók, technikai feltételek stb.).

A sérülékenységvizsgálat végrehajtásának személyi, technikai, időbeli és egyéb feltételei is vannak.

A személyi feltételek keretében kerül sor azon kapcsolattartó személyek kijelölése, akik a vizsgálattal érintett felek (vizsgáló, vizsgált rendszer tulajdonosa, vizsgált rendszer üzemeltetője stb.) közötti, a vizsgálat koordinációja tárgyában közvetlen kapcsolattartásért felelősek.

Technikai feltételként szükséges a hozzáférési jogosultságok biztosítása, valamint a szükséges fizikai és logikai összeköttetések létrehozása.

Időbeli kötöttségként jelentkezik az egyes sérülékenységvizsgálati feladatokhoz rendelhető javasolt kezdési és befejezési időpontok meghatározása.

Ezeken kívül jelentkezhetnek egyéb befolyásoló, illetve korlátozó tényezők, amelyek a hatással lehetnek a sérülékenységvizsgálat lefolytatására (például projekt ütemezés, rendszer használatában vagy környezetében várható változások, vizsgálatból kizárt kritikus szolgáltatások vagy kritikus időszakok stb.)

A vizsgálandó rendszerekről, illetve a vizsgálandó funkcionalitásról rendelkezésre álló releváns adatokat tartalmazó alábbi dokumentációkra elektronikus formában lehet szüksége az elemzést végző csapatnak:

- az Ibtv. szerinti biztonsági osztályba sorolással kapcsolatos dokumentumok (amennyiben korábban a GovCERT vagy NEIH részére átadásra került, akkor ezek hivatkozási számai),
- a korábbi nem hatósági ellenőrzések (auditok) és sérülékenységvizsgálatok dokumentációi,
- rendszer-dokumentációk, ezen belül a fizikai és logikai hálózati topológia, rendszerelemek, külső kapcsolatok és külső elérhetőségek jegyzéke,
- a védelmi infrastruktúrával kapcsolatos dokumentációk, a biztonsági rendszerelemeket és konfigurációjukat, ezen belül is határvédelem, naplózás, IDM, IDS/IPS, jogosultság-menedzsment információkat tartalmazó üzemeltetési és telepítési kézikönyv,
- az alkalmazás-dokumentációk (funkciók, interfészek stb.), és a kritikus szolgáltatások megjelölése,

- az átadandó dokumentumok jegyzéke, amely tartalmazza a dokumentum megnevezését (fájlnév), leírását, terjedelmét, kiadási dátumát és a tartalom érvényességét (naprakészségét),
- azon – az Ibtv. és végrehajtási rendeletein túlmutató – jogszabályi előírások vagy egyéb szabályzatok jegyzéke, amelyeknek – funkcionális vagy biztonsági szempontból – meg kell feleltetni a vizsgálandó elektronikus információs rendszerüket.

3.2.4.1 A projektalapító dokumentum

Az adategyeztető lap kitöltésének ellenőrzését, valamint a hiánypótlásokat és javításokat követően kerülhet sor a vizsgálat alapjául szolgáló projektalapító dokumentum elkészítésének megkezdésére. A dokumentációban a GovCERT rögzíti a vizsgálati feladatokat, célokat, a technikai és személyi feltételeket, a módszertant, az egyeztetéseket, a sérülékenységvizsgálat várható befejezésének dátumát, az eredménytermékeket, a kritikus tényezőket, valamint a siker mérésének módszertanát.[125] A dokumentumot általában a projektgazda készíti el és egyezeti a megrendelővel. A dokumentum elkészítéséhez szükséges adatokat a projektgazda rögzíti a sérülékenységvizsgálati szakrendszerbe, amely azok alapján képes előállítani a projektalapító dokumentum tervezetét is.

Ha a vizsgálatot a NEIH rendeli el, akkor a sérülékenységvizsgálati dokumentációban a határozatban rögzített vizsgálati feladatokat kell feltüntetni. A sérülékenységvizsgálat egyedi kezdeményezése esetén a vizsgálati feladatokra a kezdeményező javaslatot tehet, amelyről a GovCERT vezetője dönt.[126]

A projektalapító dokumentumot a GovCERT – minden esetben belső ellenőrzést és jóváhagyást követően – egyezetés céljából megküldi az érintett szervezet részére, általában elektronikus (pdf) formában. Az érintett szervezet a dokumentáció tartalmára a kézhezvételtől számított nyolc napon belül észrevételt tehet. Az észrevétel nem érintheti a hatóság által elrendelt vizsgálatokat. Az észrevételekről a GovCERT jogosult dönteni.[127]

Egyetértés esetén a felek, tehát a megrendelő megfelelő jogosultsággal rendelkező munkatársai és a Nemzeti Kibervédelmi Intézet vezetője elfogadják, majd aláírásukkal hitelesítik a dokumentumot.

A projektalapító dokumentum elkészültét követően történik a vizsgálat tervezése. A tervezés célja a megfelelő erőforrás-menedzsment, az ütemezéssel a hatékonyság növelése és a párhuzamosságok elkerülése. Sor kerül a lépések megtervezésére, a terv dokumentálására, valamint a vizsgálathoz szükséges hozzáférések beszerzésére. Amennyiben a vizsgálat lefolytatása megköveteli, indokolt rendszer-beavatkozási kérelem is elküldésre kerül az intézmény részére, valamint szükség esetén további egyeztetés is kezdeményezhető az érintett szervezettel.

3.2.5 A sérülékenységvizsgálat lefolyása

A Kormányzati Eseménykezelő Központ az általánosan bevett eljárások, különböző nemzetközi módszertanok, a „legjobb szakmai gyakorlatok” (best practices) és trendek szerint, a projektalapító dokumentumban, illetve a kormányrendeletben lefektetett keretekben és módon végzi a vizsgálatait.

A GovCERT a sérülékenységvizsgálat során kellő gondossággal eljárva törekszik a vizsgált elektronikus információs rendszer által nyújtott szolgáltatások szükségesnél nem nagyobb mértékű korlátozására, a vizsgálat a szolgáltatás szempontjából nem kritikus időszakban történő elvégzésére. A GovCERT feladata a korlátozás várható mértékéről és időtartalmáról az érintett szervezetet előzetesen tájékoztatni.[128]

Hatósági határozat alapján elrendelt vizsgálat esetén az érintett szervezet köteles a sérülékenység-

[125] 271/2018. (XII. 20.) Korm. rendelet 25. § (1) bekezdés.
[126] 271/2018. (XII. 20.) Korm. rendelet 25. § (2) bekezdés.
[127] 271/2018. (XII. 20.) Korm. rendelet 25. § (3) bekezdés.
[128] 271/2018. (XII. 20.) Korm. rendelet 26. § (1) bekezdés.

vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a Kormányzati Eseménykezelő Központ rendelkezésére bocsátani, ezen felül tűrni a sérülékenységvizsgálatból fakadó, a vizsgált elektronikus információs rendszeren bekövetkezett szolgáltatáscsökkenést.[129]

Egyedi kezdeményezés esetén az érintett szervezet kizárhatja azon vizsgálatokat, amelyek jelentős szolgáltatáscsökkenést eredményeznek a rendszerben.[130] Jellemzően ilyen lehet a szolgáltatásmegtagadásos támadások különböző módszereinek tesztelése.

A vizsgálatok közben folyamatosan dokumentálás történik, amely a későbbi jelentés alapjául szolgál. A dokumentálásban szöveges leírás, valamint a találatok alátámasztására szolgáló adatok, speciális fájlok, képernyőképek kerülnek elmentésre. Amennyiben az érintett szervezet igényli, akkor az egyes sérülékenységek felderítésekor azonnali értesítést kaphat a kockázatok mérséklése érdekében.

3.2.6 A határidők

A vizsgálat határideje a hatóság határozatának keltétől, illetve az előzetesen egyeztetett kezdési időponttól számítva külső informatikai biztonsági vizsgálat esetén harminc nap, webes vizsgálat esetén hetvenöt nap, belső informatikai biztonsági vizsgálat esetén kilencven nap, a vezeték nélküli hálózat informatikai biztonsági vizsgálat esetén harminc nap.[131] A GovCERT a sérülékenységvizsgálatra irányadó határidőt annak letelte előtt egy alkalommal, legfeljebb harminc nappal meghosszabbíthatja, és erről az érintett szervezetet, valamint a hatóságot értesíti.[132]

Az átlagostól eltérő elektronikus információs rendszerek esetén az elemzés összetettsége miatt speciális határidős szabályokat lehet alkalmazni.

Az érintett szervezet elektronikus információs rendszere az átlagostól jelentősen eltér, ha az elektronikus információs rendszer a külső internetes tartományban több mint 20 IP címen elérhető eszközzel, több mint 10 webes szolgáltatással, a belső hálózat tekintetében több mint 50 szerverrel, több mint 500 munkaállomással, több mint 5 vezeték nélküli hálózattal, vagy több mint 500 fős felhasználói létszámmal rendelkezik. Ha az érintett szervezet több mint három telephelyen rendelkezik a vizsgálattal érintett elektronikus információs rendszerrel, szintén átlagostól eltérőnek minősül.[133]

Ha az érintett szervezet elektronikus információs rendszere, rendszereleme az átlagostól jelentősen eltér és emiatt egyedi vizsgálati eljárás szükséges, a sérülékenységvizsgálati határidő további harminc nappal meghosszabbítható.[134]

3.2.7 A vizsgálatot nehezítő, akadályozó körülmények kezelése

Ha a projektalapító dokumentumban foglalt feltételrendszer, rendszerelem, illetve azok egy része a vizsgálat elindulásakor azonnal, vagy a projekt közben nem áll fenn, a megrendelő tájékoztatása haladéktalanul megtörténik, valamint a GovCERT tájékoztatást kér a feltétel fennállásáról. Ez minden esetben ellenőrzésre kerül, továbbá a projektgazda értesíti a megrendelőt a sikerességről.

Előállhatnak olyan estek, amikor a projekt haladásának érdekében köztes egyeztetésre van szükség, amely általában személyes találkozót igényel. A megbeszélésen a felelős vezetőkön kívül többségében az illetékes szakemberek, fejlesztők és a vizsgálatot végzők vesznek részt.

Amennyiben az elem valamely okból nem állítható vissza, akkor meg kell vizsgálni, hogy a vizs-

[129] 271/2018. (XII. 20.) Korm. rendelet 26. § (2) bekezdés.
[130] 271/2018. (XII. 20.) Korm. rendelet 26. § (3) bekezdés.
[131] 271/2018. (XII. 20.) Korm. rendelet 24 § (3) bekezdés.
[132] 271/2018. (XII. 20.) Korm. rendelet 26 § (4) bekezdés.
[133] 271/2018. (XII. 20.) Korm. rendelet 28. § (1) bekezdés.
[134] 271/2018. (XII. 20.) Korm. rendelet 28. § (2) bekezdés.

gálat további folytatásához szükséges-e módosítani a projektalapító dokumentumot. Amennyiben a vizsgálat e nélkül nem folytatható, a módosítás a keletkezésre vonatkozó egyeztetési és elfogadási szabályokat betartva történik.

3.2.8 Kritikus sérülékenység kezelése

Amennyiben a GovCERT kritikus besorolású sérülékenységre bukkan a vizsgálat során, arról minden esetben azonnali hatállyal tájékoztatja a megrendelő intézmény kapcsolattartó személyét.

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.

A sérülékenységről szóló jelentést belső ellenőrzést és jóváhagyást követően, amennyiben erre lehetőség van, szóban és írásban közlik a megrendelő szerv felelős vezetője részére.

Amennyiben a sérülékenység biztonsági esemény is egyben, a projektgazda gondoskodik az incidens bejelentéséről. Ebben az esetben a bejelentés észlelésnek minősül és a GovCERT incidenskezelési eljárása szerint történik az eset kezelése.

3.2.9 A sérülékenységvizsgálat lezárása

A sérülékenységvizsgálat lezárásakor a GovCERT minden esetben állásfoglalást készít. A szakértők részletes jelentése alapján a kockázatok értékelésére kerül sor, valamint a feltárt sérülékenységek kezeléséhez szükséges javaslatokkal segítik a megrendelők későbbi munkáját. A vizsgálat közben az azt végző munkatársak a sérülékenység találatokat típusonként szintén rögzítik a sérülékenységvizsgálati szakrendszerben. Ezzel lehetővé válik az állásfoglalás tervezetének gyors, pontos és automatikus elkészítése.

Az állásfoglalás elkészítését belső szakmai ellenőrzés és jóváhagyás követi. Először egy másik sérülékenységvizsgálattal foglalkozó munkatárs tekinti át az elkészült jelentést, majd ezt követően kerül sor a vezetői jóváhagyásra. A GovCERT az elkészült dokumentumot nyolc napon belül megküldi az érintett szervezet és – hatósági kezdeményezés esetén – a NEIH részére.[135] Az állásfoglalás tartalmazza a vizsgálati eredmények leírását, valamint a rövid, közép és hosszú távú intézkedésekre vonatkozó javaslatokat.[136]

A GovCERT állásfoglalása az esetek többségében tartalmazza a tapasztalatokat összegző vezetői összefoglalót, amelyben megjelennek a javasolt cselekvési folyamatok és egy kockázati összesítő is. A kockázatokat értékelő fejezet meghatározza a kockázati szinteket, magukat a – kritikus, magas, közepes és alacsony kategóriákba sorolt – kockázatokat. A vizsgálatok műszaki leírása fejezetben a vizsgálati módszerek, használt technológiák leírására kerül sor.

Az állásfoglalást követően az intézmény kérése esetén a projekt gazdája prezentáció keretében mutatja be a sérülékenységvizsgálat eredményét megjelenítő dokumentumokat és az esetlegesen felmerülő kérdések megválaszolására is sor kerülhet.

[135] 271/2018. (XII. 20.) Korm. rendelet 29. § (1) bekezdés.
[136] 271/2018. (XII. 20.) Korm. rendelet 29. § (2) bekezdés.

3.2.10 A sérülékenységvizsgálat egyéb szabályai

A polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereinek sérülékenységvizsgálatát az IntCERT,[137] a honvédelmi célú elektronikus információs rendszerek vizsgálatát a Katonai Nemzetbiztonsági Szolgálat Kibervédelmi Központja végzi.[138]

A kormányrendelet lehetőséget biztosít külső sérülékenységvizsgálattal foglalkozó gazdasági társaság bevonására is. Külső társaságok abban az esetben végezhetnek vizsgálatot, ha a gazdasági társaság nevében és alkalmazásában eljárva a vizsgálatban részt vevő személy a törvényben meghatározott feltételeken túl rendelkezik a vizsgálat lefolytatásához szükséges ismeretek meglétét igazoló végzettséggel, és ezen a szakterületen legalább 2 év szakmai tapasztalattal, valamint a gazdasági társaság bejegyzésre került a sérülékenységvizsgálat lefolytatására jogosult gazdasági társaságok nyilvántartásába.[139]

A sérülékenységvizsgálat lefolytatására jogosult gazdasági társaságokról az Alkotmányvédelmi Hivatal olyan nyilvántartást vezet, amely személyes adatot nem tartalmaz, azonban szerepelnek benne az érintett gazdasági társaság adatai, a vizsgálatban részt vevő személyek száma és a vizsgálatok lefolytatásához szükséges ismereteket igazoló végzettség megnevezése és megszerzési ideje.[140]

A nyilvántartásba való felvételt a gazdasági társaság kezdeményezi az Alkotmányvédelmi Hivatalnál, a feltételek meglétét igazoló okiratok benyújtásával, a feltételek szakmai megfelelősége tekintetében a GovCERT nyilatkozata irányadó.[141]

3.3. A célzott támadás (apt) megelőzése sérülékenységvizsgálattal

3.3.1 A célzott támadás meghatározása

Az advanced persistent threat (APT), magas szintű, tartós vagy más néven 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 motivációk vezérlik az elkövetőket, a cél általában információszerzés, de előfordult már olyan támadás is, amelynek célja a szabotázs volt.

Az angol kifejezésben az „advanced" jelző arra utal, hogy a támadók kifinomult technikák és rosszindulatú szoftverek segítségével, általában a rendszerek nulladik napi sebezhetőségeinek kihasználásával jutnak be a rendszerbe és maradnak hosszú ideig ott. A „persistent" kifejezés lényege, hogy a támadók a célrendszerbe bejutva hosszú ideig észrevétlenül maradnak jelen, valamint egy vezérlőszerver segítségével folyamatosan figyelik és szivárogtatják az adatokat onnan. A „threat" az emberi beavatkozást jelzi a támadás kivitelezésében.

Az APT rendszerint egy olyan csoportra (például kormányra) is utalhat, amely mind a képességgel, mind a szándékával kitartóan és hatékonyan célozza meg a kiválasztott célpontot. A kifejezést általában az ilyen jellegű számítógépes fenyegetésekre is használják, különösen az internet segítségével lebonyolított kémkedésre, amely különféle információgyűjtő technikákat alkalmaz az érzékeny információk megszerzéséhez.[142]

---

137 271/2018. (XII. 20.) Korm. rendelet 22. § (2) bekezdés.
138 271/2018. (XII. 20.) Korm. rendelet 22. § (3) bekezdés.
139 271/2018. (XII. 20.) Korm. rendelet 22. § (4) bekezdés.
140 271/2018. (XII. 20.) Korm. rendelet 22. § (5) bekezdés.
141 271/2018. (XII. 20.) Korm. rendelet 22. § (7) bekezdés.
142 https://en.wikipedia.org/wiki/Advanced_persistent_threat (utolsó letöltés: 2018. szeptember 13.)

3.3.2 A célzott támadások természete

A célzott támadások az eddig feltárt eseteket alapul véve hasonló metodika mentén bonyolódtak le:

- Külső felderítés, kezdeti lépések
- Távoli hozzáférés biztosítása
- Jogosultsági szint emelés
- Belső felderítés
- Oldalirányú terjedés
- Jelenlét fenntartása
- Küldetés befejezése[143]

3.3.2.1 A támadás kezdeti szakasza

A támadások kezdeti szakaszában általában social engineering és célzott adathalászat (spear phishing) használatával, általában e-mailben keresik fel áldozatukat a támadók. A célzott támadások esetén jellemző a jól megformált és jól megfogalmazott tartalom, a spameknél tapasztalt magyartalan megfogalmazás ugyanis kevés sikerrel kecsegtet. Az áldozatokat nyílt forrásból származó információk alapján például a közösségi oldalukon megosztott tartalmak alapján feltérképezik, és ezen információk felhasználásával készítenek olyan tartalmat, amely felkelti az érdeklődésüket.

A szofisztikátlan megszerkesztett e-mail általában egy káros kódot tartalmazó mellékletet (az esetek többségében egy dokumentum, táblázat vagy pdf) vagy egy kártékony weboldalra való hivatkozást tartalmaz. Mindkét esetben felhasználói interakcióra van szükség ahhoz, hogy a káros tartalmú fájl vagy weboldal betöltődjön. A támadók gondot fordítanak arra is, hogy az e-mailek ne túl sok célszemélyhez jussanak el, továbbá általában igyekeznek olyan célszemélyeket választani, akik nagyobb eséllyel lesznek a „segítségükre".

A kártékony kódok általában ellenőrzik azt, hogy a célszervezet gépén futtaták-e, a fájl megnyitása után változatos technikával megnyíló és betöltődő kód az operációs rendszer metaadataiban próbálja azonosítani az intézményt, a weboldal ugyanezt teszi csak általában IP cím és a felhasználó web profilja alapján. Miután a káros kód meggyőződött arról, hogy a megfelelő helyen van, letölti a támadás további szakaszáért felelős programcsomagot.

A sikeres támadáshoz sok esetben szükség van jogosultsági szint emeléshez, amelyhez vagy már ismert, de még kevésbé elterjedt, kevéssé javított, frissen nyilvánosságra került vagy pedig nulladik napi sérülékenységeket használnak. Sok esetben a sérülékenységet jelszófeltöréssel is kombinálni szükséges az adminisztrátori jogosultság megszerzése céljából. Legtöbbször az első káros kód lefuttatatására is sérülékenységet kell kihasználni, tehát előfordulhat olyan célzott támadás is, amelyhez két nulladik napi sérülékenységet használnak a támadók.

Ezek a lépések általában egy-két nap alatt meg is történnek egy átlagos támadás esetén.

3.3.2.2 Infrastruktúra kialakítása és a terjedés

A sikeres települést követően kiépül egy csatorna a távoli támadók és az áldozatok között, amelynek segítségével lehetővé válik a kommunikáció. Ez a robothálózatok infrastruktúrájához hasonló vezérlőszerverhez (command and controll, C&C, C2) biztosít kapcsolatot. Ennek segítségével adja ki a támadó az utasításokat, így képes például további eszközöket megfertőzni és a káros kódot frissíteni, de mivel az esetek döntő többségében rendszergazdai jogosultságot szereznek a támadott eszközökön, ezért a lehetőségek száma igen nagy. A támadók nagy gondot fordítanak a rejtőzködésre, így a kapcsolat kialakításánál is változatos eszközöket vetnek be a kommunikáció felfedezésének minimalizálására.

[143] https://en.wikipedia.org/wiki/Advanced_persistent_threat#Life_cycle (utolsó letöltés: 2018. szeptember 13.)

Miután sikerült kiépíteni a kapcsolatot megkezdődik a támadott szervezet belső hálózatának felderítése. A támadók célja legtöbb esetben az adatszerzés, ezért olyan eszközöket keresnek, amelyeken jó esély van nagy mennyiségű bizalmas adat megszerzésére. A támadók elsősorban Windows Domain, adatbázis-, fájl- és levelezőszervereket keresnek, azonban a felhasználói munkaállomások is általában áldozatul esnek a támadóknak. A támadók a kompromittálandó adatok növelése érdekében általában törekednek az összes elérhető eszköz feltérképezésre.

Ezt követően kerül sor az oldalirányú terjedésre (lateral movement). Ennek keretén belül a támadók igyekeznek kiterjeszteni az irányításukat a feltérképezés során relevánsnak tartott eszközök felett. A terjedés célja, hogy minél több eszközön megtörténjen az adatok összegyűjtése és az információszivárogtatás.

3.3.2.3 A cél elérése

A támadók egyik legfontosabb célja, hogy amennyiben sikerült egy rendszerbe betenni a lábukat, akkor a jelenlétet folyamatossá akarják tenni. Ennek érdekében folyamatosan ellenőrzik a jelenlét meglétét, a káros kód működését és a megszerzett jogosultságokat, valamint folyamatosan biztosítják a hozzáférési csatornákat is. Egy átlagos APT hónapokig, sőt akár évekig is képes feltűnésmentesen megbújni a célrendszerekben és ez idő alatt folyamatosan monitoroz és végzi a rá bízott feladatot.

A célzott támadás akkor éri el valódi célját, ha a támadóknak sikerül észrevétlenül kijuttatniuk nagy mennyiségű adatot a rendszerekből. Mivel cél az is, hogy tartósan a rendszerben maradjanak, ezért az adatszivárogtatásra is speciális módszereket dolgoztak ki, általában lassan és valamilyen legális tevékenységnek álcázva történik, az adatok kijuttatása a vezérlőszervezek felé.

3.3.3 Célzott támadások megelőzése sérülékenységvizsgálaTtal

A célzott támadások megelőzése, hatásának enyhítése és elhárítása tehát nem könnyű feladat, mivel a támadók olyan technikai repertoárral, olyan nagymennyiségű tapasztalattal és erőforrásokkal rendelkeznek, amely némely esetben a küzdelmet könnyen egyoldalúvá teheti. Ennek ellenére minden rendszer esetén, különösen azon rendszerek esetén, amelyek segítségével nagy mennyiségű bizalmas vagy személyes adatot tárolnak és használnak fel, törekedni kell a célzott támadások kivédésére, a támadók dolgának megnehezítésére.

Több vírusvédelmi megoldásokat is gyártó és forgalmazó szervezet is készít ilyen célzott támadások detektálására és megakadályozására szolgáló megoldásokat, úgynevezett anti-APT eszközöket és szoftvereket, azonban jelen fejezet nem ezen (egyébként sok esetben hasznos) eszközöknek a bemutatásáról szól. A cél inkább az, hogy a hagyományos eszközökkel milyen védekezési lehetőségeink vannak, és e védekezési lehetőségek állapotára milyen módon tud rávilágítani egy esetleges sérülékenységvizsgálat.

A rendszerek biztonságának erősítése az alábbi szempontok mentén is elvégezhető:[144]

- Szoftverek naprakészen tartása
- Felhasználói fiókok védelme
- Megbízható szoftverek használata
- Rendszerhelyreállítási terv elkészítése és frissítése
- Aktív rendszer-és konfigurációkezelés
- Proaktivitás a hálózati anomáliadetekcióban
- Modern hardverelemek és a hardverbiztonság használata
- Hálózati szegmentáció kialakítása

[144] NSA's Top Ten Cybersecurity Mitigation Strategies felhasználásával.

- Fenyegetettség menedzsment aktív használata
- Többfaktoros autentikáció használata
- Felhasználói tudatosság folyamatos erősítése

3.3.3.1 Szoftverfrissítés azonnal

Üzemeltetési alapvetésnek tűnhet, de a tapasztalatok szerint egyáltalán nem triviális, hogy alkalmazni kell az összes rendelkezésre álló szoftverfrissítést, valamint amennyire lehetőség van rá, automatizálni kell ezt a folyamatot. Számos szoftver már képes automatikus frissíteni magát, ezt azonban érdemes megfelelően beállítani és konfigurálni.

Az automatizálás azért is szükséges, mert a támadók sok esetben visszafejtik a sérülékenységet a kiadott biztonsági frissítés segítségével, és lassabb frissítés esetén könnyen és gyorsan ki is tudják azokat használni. Ezek az „N napos" kihasználások ugyanolyan károsak lehetnek, mint egy nulladik napi sérülékenység.

A gyártói frissítéseknek megbízhatónak és hitelesnek kell lenniük. A frissítéseket jellemzően digitálisan aláírja a gyártó és védett linkeken keresztül érkeznek a tartalom integritásának biztosítására. Gyors és alapos frissítés nélkül a támadók akár ki is használhatják az automatikus frissítést saját céljaik elérésére, például kompromittálnak egy security update-et.

A sérülékenységvizsgálat képes lehet rávilágítani a patch menedzsment hiányosságaira esetleges hibás konfigurációkra is, amellyel komoly támadások is megakadályozhatóak lehetnek.

3.3.3.2 Fiókok védelme

A különböző felhasználói fiókok, de különösen a magas szintű, adminisztrációs fiókok védelme minden rendszerben kulcskérdés lehet a komplex támadások megakadályozása érdekében.

Olyan jogosultságrendszert kell létrehozni minden rendszer esetén, amely ezen a kockázati kitettségen alapul, de a szükséges műveletek fenntartásához biztosítja a jogosultságokat. Általános alapelv a legkisebb jogosultság elve (PoLP), amelynek lényege, hogy egy számítógépes környezet adott absztrakciós rétegében minden modul (mint például processz, felhasználó vagy alkalmazás) kizárólag olyan információkhoz és erőforrásokhoz fér hozzá, amelyek szükségesek a modul legitim céljainak eléréséhez.[145]

Érdemes megfontolni úgynevezett Privileged Access Management (PAM) megoldás használatát, amelynek segítségével monitorozható és ellenőrizhető a magasabb jogosultsággal rendelkező fiókok tevékenysége. A célzott támadások szempontjából magas kitettséggel rendelkező szervezetek számára egy ilyen megoldás alkalmazása különösen fontos, mivel az APT-k döntő többsége igényel magasabb szintű hozzáférést, mivel többek között az oldalirányú terjeszkedés egyik alapfeltétele is lehet ez.

A sérülékenységvizsgálatot végző etikus hekkerek szintén megpróbálnak magasabb jogosultsági szintet szerezni a támadókhoz hasonló módszerek felhasználásával, így sok sérülékenység, konfigurációs vagy strukturális hiányosság is kiderülhet egy-egy ilyen vizsgálat során.

3.3.3.3 Megbízható szoftverek

Olyan modern operációs rendszereket érdemes használni, amely a különböző szkriptek, futtatható állományok (executables), eszközillesztők (device drivers) és rendszer firmwarek esetén kikényszeríti azok digitális aláírásának ellenőrzését. A rendszernek rendelkeznie kell egy megbízható tanúsítványok listájával, amelyek megléte megakadályozhatja és felderítheti az illegitim kódok használatát, vagy befecskendezését.

---

[145] https://en.wikipedia.org/wiki/Principle_of_least_privilege (utolsó letöltés: 2018. szeptember 13.)

Ezen irányelvek akkor biztosítják a rendszer lehető legteljesebb integritását, ha a rendszer betöltődéséhez szükséges (boot) kódokra is alkalmazzuk azokat. A még nagyobb biztonság eléréséhez szoftver whitelist alkalmazása is lehetséges, tehát csak meghatározott programok meghatározott verziói futhatnak egy adott rendszerben.

Az aláírás nélküli, nem megbízható aláírással ellátott vagy ismeretlen gyártótól származó szoftverek engedélyezése lehetővé teszi a támadók, a célzott támadások kivitelezését végző csoport számára, hogy betegyék a lábukat a rendszerbe.

A szoftverek mellett a hardverek biztonságára is érdemes külön hangsúlyt fektetni, mivel egy ismeretlen beszállítótól származó egyszerű, hétköznapinak és veszélytelennek tűnő hardver eszköz (például egy billentyűzet) is magában hordozhat ilyen jellegű veszélyeket.

A sérülékenységvizsgálat során a vizsgálatot végzők több különböző eszközön gyakran tesznek kísérletet ilyen jellegű kódok futtatására, így egy vizsgálat ilyen irányú sebezhetőséget is feltárhat.

3.3.3.4 Rendszerhelyreállítási terv

Rendszer-helyreállítási terv létrehozása, valamint folyamatos felülvizsgálata és rendszeres gyakorlása az adatok visszaállításának biztosítása érdekében az átfogó katasztrófa-helyreállítási stratégia részeként egyik állandó feladata az informatikai biztonsági szakterületnek.

A tervnek meg kell védenie a kritikus adatokat, konfigurációkat és naplókat, hogy biztosítsa a műveletek folytonosságát a váratlan események miatt. További védelem érdekében a biztonsági másolatokat titkosítani, a helyszínen tárolni, lehetőség szerint offline állapotban kell tartani, és támogatniuk kell a rendszerek és eszközök teljes helyreállítását.

A szervezeteknek rendszeres tesztelést kell végezniük, valamint értékelniük is szükséges a biztonsági tervet. A tervet változó hálózati környezethez igazodóan folyamatosan frissíteni kell.

3.3.3.5 Aktív rendszer- és konfigurációkezelés

Egy rendszerhez hozzátartozik a hálózati eszközök és a szoftverek folyamatosan aktualizált listája (inventory) is. Az eszközök és a programok használatát monitorozva lehet találni olyan elemeket, amelyeket nagyon ritkán vagy egyáltalán nem használnak.

Ezek csak feleslegesen növelik a kitettséget, valamint a hibajavítás (patchelés) is fölöslegesen terheli az üzemeltetés amúgy is általában szűk időkeretét. Ilyen vizsgálatokat időnként érdemes ütemezetten elvégezni, és az esetlegesen kevéssé használt elemeket a rendszerből el lehet távolítani.

Az aktív rendszer és konfigurációkezelés biztosítja, hogy a rendszerek alkalmazkodni tudjanak a gyakran változó veszélyforrásokhoz, miközben skálázhatóvá teszik és egyszerűsítik az adminisztrációs folyamatokat.

Egy sérülékenységvizsgálatnál, mivel a hálózat különböző szegmenseit a vizsgálók feltérképezik, a különböző alkalmazásokban sérülékenységeket keresnek, ezért ebben a fázisban készülhet szoftver leltár is, amely nagyban tudja segíteni akár az üzemeltetés munkáját. Ez a szoftver leltár azonban valószínűleg nem lesz teljes, mivel akadhatnak olyan alkalmazások, eszközök, amelyeket a vizsgálat során nem azonosítanak, mert például abban az időben, annak ellenére, hogy működött, nem volt használatban.

3.3.3.6 Proaktív hálózati behatolásdetekció

A hálózaton belüli rosszindulatú tevékenység észlelése, tárolása, illetve a forrás és célcímek azonosítása is fontos állomása a célzott támadások elleni harcnak. A passzív észlelési mechanizmusok, mint például a biztonsági naplóállományok és a biztonsági eseménykezelés (Security Information and Event Management, SIEM), a végpontvédelmi megoldások (Endpoint Detection and Response, EDR), és más adatelemzési képességek felbecsülhetetlen eszközök a rosszindulatú vagy rendellenes

viselkedés azonosításához, felfedezéséhez.

A tevékenység része továbbá a proaktív szemléletű, folyamatos behatolás keresés, a biztonsági események észlelésének képessége, megléte és alkalmazása jól dokumentált incidensreagálási eljárások segítségével. Az ilyen és ehhez hasonló proaktív szemlélet és a proaktivitás irányába mutató lépések megteremtése el fogja mozdítani a szervezetet az okok utólagos keresésétől (reaktivitás) a fenyegetések valós idejű felderítése és az azonnali hibaelhárítás irányába, így téve még ellenállóbbá a rendszereket a komolyabb támadásokkal szemben is.

3.3.3.7 Modern hardverbiztonság

Ha szoftverek biztonságán túlmenően a hardverek biztonságára is egyre nagyobb figyelmet kell fordítani. Léteznek, és egyre inkább terjednek olyan hardverbiztonsági szolgáltatások, mint az Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Platform Module (TPM) és a hardveres virtualizáció, amellyel fokozható a rendszerek biztonsága, és amelyek megléte, helyes konfigurációja sérülékenységvizsgálattal ellenőrizhető. Ezen kívül fontos lehet még a régebbi hardver eszközök ütemezett frissítése, újabbra, biztonságosabbra cserélése.

A fent említett korszerű hardverfunkciók növelik a rendszerindítási folyamat integritását, biztonságát, biztosítják a rendszer tanúsítását és támogatják a nagy kockázatú alkalmazások elszigetelését. A korszerű operációs rendszer használata az elavult hardvereken csökkenti a rendszer, a kritikus adatok és a felhasználói beavatkozások védhetőségét, mivel a hardver nem támogatja a szoftver biztonsági komponenseit.

3.3.3.8 Hálózati szegmentálás

A kritikus adatokat tartalmazó vagy feladatot ellátó hálózatok és szolgáltatások elkülönítésére nagy hangsúlyt kell fektetni. Az ilyen hálózatokban alkalmazásfigyelő hálózati (application-aware networking) védelmet használnak, amely képes a nem megengedett hálózati forgalmat tiltani, valamint a biztonsági házirend és viselkedés alapján korlátozni a tartalmat.

A hagyományos behatolásdetekciós eszközök (IDS), amelyek az ismert, rosszindulatú szignatúrák felismerésén alapulnak a titkosítás és az obfuszkáció miatt ma már nem hatékonyak. A támadók a rosszindulatú tevékenységet képesek gyakran használt protokollokba (például http vagy DNS) rejteni, amely csak szofisztikált, alkalmazásfigyelő védelmi mechanizmusokkal detektálható. Ilyen rejtett forgalmat sérülékenységvizsgálat során is lehet generálni, amely rávilágít a rendszer védelmi szintjére.

3.3.3.9 Fenyegetésmenedzsment aktív használata

Manapság egy nagy rendszer biztonságos üzemeltetéséhez és információbiztonságának szavatolásához elkerülhetetlen több forrásból származó fenyegetésmenedzsment információk (például fájladatok, DNS kérések, URL-ek, IP-címek és e-mail címek) folyamatos, ütemezett felhasználása.

Az úgynevezett cyber threat intelligence-k (CTI) segítenek az események felderítésében és megelőzésében, valamint lehetővé teszik a gyors és globális reagálást a különböző fenyegetésekre, csökkentve az ismert fenyegetésekkel szembeni kitettséget. Ezen kívül az információk hozzáférést biztosítanak egy sokkal nagyobb fenyegetéselemzési képességhez, mint amelyet egy szervezet önmagában nyújtani tud.

A mai világban a felmerülő fenyegetések, akár célzott, akár globális kampányok, dinamikusabban fordulnak elő, mint ahogy a legtöbb szervezet képes reagálni rájuk, ezzel biztosítva teret az új támadások gyors terjedéséhez és magas sikerszázalékához. A több forrásból származó CTI szolgáltatások gyorsabb és hatékonyabb biztonságot nyújtanak a dinamikusan változó eszközöket és módszereket használó, fejlett támadókkal szemben.

3.3.3.10 Többfaktoros authentikáció

A magas szintű adminisztrációs jogosultságok, a távoli hozzáférés vagy a nagy értékű eszközök védelme kiemelt fontosságú. A fizikai, token alapú hitelesítési rendszereket olyan tudásalapú autentikációs rendszerek kiegészítésére kell felhasználni, mint a jelszavak és a PIN kódok.

A szervezeteknek a kiemelt fiókok esetében a lehető leghamarabb át kell térniük az egyfaktoros hitelesítésről, például a könnyebben manipulálható jelszavas rendszerekről, a többfaktoros (például tudás és birtoklás alapú) autentikációt támogató rendszerekre, mivel a jelszó, dacára a jól felkészített rendszereknek, amelyek ellenállnak a különböző (például nyers erős) támadásoknak, social engineering technikákkal viszonylag könnyen megszerezhető vagy kitalálható.

3.3.3.11 A felhasználói tudatosság

Mindezen védelmi intézkedések, az eszközök folyamatos karbantartása és naprakésszé tétele mit sem ér azonban, ha a felhasználók biztonságtudatossági szintje alacsony és a támadók a felhasználók segítségével könnyen és hatékonyan tudnak támadásokat kivitelezni a szervezet irányába.

Mivel a legtöbb támadásban szerepet kap a felhasználói interakció, sok esetben a leggyengébb láncszem is az ember, ezért a szervezet munkatársait, különösen azokat a munkatársakat, akik külső szervezetekkel és szereplőkkel is kapcsolatba kerülnek, folyamatosan tudatosítási képzésekben kell részesíteni.

A tudatosító előadásnak rendszeresnek, interaktívnak és közérthetőnek kell lennie. Az a leghatékonyabb, ha rengeteg példát hoz az előadó a különböző támadásokról, annak érdekében, hogy a hallgatóság később képes legyen magától is felismerni egy megtévesztő tartalmat, egy gyanús telefonhívást. Ezen kívül érdemes időnként (havonta, negyedévente) különböző közérthető és információgazdag anyagokat a szervezet belső rendszerén közzétenni, amelyekben újabb és újabb trendeket esetleg védekezési módszereket ismerhetnek meg a szervezet munkavállalói. Ilyen kiadványai a Nemzeti Kibervédelmi Intézetnek is vannak, amelyek elérhetőek a szervezet weboldalán keresztül.

A sérülékenységvizsgálat is egy eszköz lehet a menedzsment kezében a szervezet informatikai tudatosságának felmérésére. A vizsgálók social engineering technikákkal, a támadókhoz hasonló módon megpróbálhatnak fontos és lényeges információkhoz jutni a szervezet infrastruktúrájáról, jelszavakat, egyéb belépési adatokat szerezhetnek meg.

3.4 Irodalomjegyzék

- Berzsenyi Dániel – Gyaraki Réka – Hámornik Balázs Péter – Hirsch Gábor – Kiss Attila – Marsi Tamás – Orbók Ákos – Simon Béla – Solymos Ákos – Tikos Anita – Zsíros Péter (2018): Incidensmenedzsment. Dialóg Campus Kiadó, Budapest.
- Hadarics Kálmán (2014): Incidens-menedzsment gyakorlat. Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel URL: http://archiv.vtki.uni-nke.hu/uploads/media_items/incidens-menedzsment-gyakorlat_-bcp_-drp-integracio.original.pdf (utolsó letöltés: 2017. április 6.)
- Tihanyi Norbert – Vargha Gergely – Frész Ferenc (2014): Biztonsági tesztelés a gyakorlatban. Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel URL: http://archiv.vtki.uni-nke.hu/uploads/media_items/biztonsagi-teszteles-a-gyakorlatban.original.pdf (utolsó letöltés: 2017. április 6.)
- Európai Hálózat- és Információbiztonsági Ügynökség (2006): Részletes leírás a CSIRT-Csoportok létrehozásáról, URL: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-hungarian/at_download/fullReport (utolsó letöltés: 2017.április 15.)
- Cert Coordination Center (2003): Handbook for CSIRTs, URL: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf (utolsó letöltés: 2017. április 10.)
- Európai Hálózat- és Információbiztonsági Ügynökség (2016): Incident Handling Management tananyag, URL: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/setting-up-a-csirt#Incident_Handling_Management (utolsó letöltés: 2017. április 15.)
- AT&T Consulting- Advanced Persistent Threat security assessment URL: https://www.business.att.com/content/productbrochures/advanced-persistent-threats-product-brief.pdf (utolsó letöltés: 2018. március 5.)
- Advanced Persistent Threats: A Symantec Perspective URL: https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (utolsó letöltés: 2018. március 5.)
- Advanced Persistent Threats and Real-Time Threat Management URL: http://www.trendmicro.it/media/misc/ebook-advanced-persistant-threats-and-real-time-threat-management.pdf (utolsó letöltés: 2018. március 5.)
- Best Practices for Mitigating Advanced Persistent Threats URL: http://www.trendmicro.de/media/wp/gartner-best-practices-for-mitigating-apts-whitepaper-en.pdf (utolsó letöltés: 2018. március 5.)
- NSA's Top Ten Cybersecurity Mitigation Strategies URL: https://www.iad.gov/iad/custom-cf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/security-tips/assets/public/upload/NSA-s-Top-Ten-Cybersecurity-Mitigation-Strategies.pdf&WpKes=aF6woL7fQp3dJimtw59wWQymsrNnZsfNZ4SZF6 (utolsó letöltés: 2018. március 5.)
- Protecting the Way People Work: Practices for Detecting and Mitigating Advanced Persistent Threats URL: https://www.ciosummits.com/Online_Assets_Proofpoint_Gartner_Best_Practices.pdf (utolsó letöltés: 2018. március 5.)

4. JOGSZABÁLYTÁR

4.1. Magyar jogszabályok

2001. évi XXXV. törvény az elektronikus aláírásról

https://mkogy.jogtar.hu/?page=show&docid=a0100035.TV

2003. évi C. törvény az elektronikus hírközlésről

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV

2009. évi CLV. törvény a minősített adat védelméről

http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131

2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1000157.tv

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

https://net.jogtar.hu/jogszabaly?docid=A1100128.TV

2011. évi CXII. törvény információs önrendelkezési jogról és az információszabadságról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv

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

http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158

2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól

https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV

2015. évi CXLIII. törvény a közbeszerzésekről

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500143.TV

2016. évi CL. törvény az általános közigazgatási rendtartásról

https://net.jogtar.hu/jogszabaly?docid=A1600150.TV

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

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99700086.KOR

168/2004. (V. 25.) Korm. rendelet a központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400168.KOR

83/2012. (IV. 21.) Korm. rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200083.KOR&txtreferer=A1500042.BM

85/2012. (IV. 21.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól

http://njt.hu/cgi_bin/njt_doc.cgi?docid=148205.295314

84/2012. (IV. 21.) Korm. rendelet az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.korű

65/2013 (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300065.kor

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

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300301.KOR&txtreferer=A1300050.TV

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

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300484.kor

535/2013. (XII. 30.) Korm. rendelet a pénzügyi intézmények, a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300535.KOR&txtreferer=A1300235.TV

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf

60/2014. (III. 6.) Korm. rendelet a támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1400060.kor

1631/2014. (XI. 6.) Korm. határozat a Digitális Nemzet Fejlesztési Program" megvalósításáról

http://net.jogtar.hu/jogszabaly?docid=A14H1631.KOR&getdoc=1

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

http://njt.hu/cgi_bin/njt_doc.cgi?docid=211839.362368

186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor

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

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR

1052/2015. (II. 16.) Korm. határozat a Közigazgatás- és Közszolgáltatás-fejlesztési Stratégiával kapcsolatos feladatokról

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

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

https://net.jogtar.hu/jogszabaly?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT

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

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600157.KOR&timeshift=fffffff4&txtreferer=00000001.TXT

228/2016. (VII. 29.) Korm. rendelet az állami szervek informatikai fejlesztéseinek koordinációjáról

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1600228.kor

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

https://net.jogtar.hu/jogszabaly?docid=A16H1488.KOR&timeshift=fffffff4&txtreferer=00000001.TXT

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

https://net.jogtar.hu/jogszabaly?docid=A16H1536.KOR&timeshift=fffffff4&txtreferer=00000001.TXT

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

https://net.jogtar.hu/jogszabaly?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT

23/2013. (XI. 6.) MNB rendelet a jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank alapvető feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről

https://www.mnb.hu/letoltes/23-2013-xi-6-mnbrendelet.pdf

26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300026.KIM

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

http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/9.pdf

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

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm

42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm

4.2. Európai Uniós jogi aktusok

Számítástechnikai bűnözésről szóló Egyezmény (2001) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa405

Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10) az Európai Hálózat és Információbiztonsági Ügynökség létrehozásáról

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML

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

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013R0526&from=HU

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

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU

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

https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52017PC0477R%2801%29

Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU

Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU

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

https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33193&from=EN

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

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU

Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=HU

Közös Közlemény az Európai Parlamentnek és A Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése vonatkozásában

http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

Az ENSZ Közgyűlés a 2003. december 8-i 58/32-es számú határozata

https://undocs.org/A/RES/58/32

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))

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

A Tanács következtetései a kiberdiplomáciáról (2015)

http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf

A Bizottság 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról

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

A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (2017):

http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf

4.3. Külföldi jogi aktusok

Az EBESZ Állandó Tanácsának PC.DEC/1039 számú döntése:

https://www.osce.org/pc/90169?download=true

Az EBESZ bizalomépítő intézkedései: PC.DEC/1106

https://www.osce.org/pc/109168

5. 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, lekér-

dezése, 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. Mind-

ez 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 (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: 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 levelező-rendszerek, 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, elérhetetlenné 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 jogosultsággal 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 szá-

mítástechnikával 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 internet-szerű 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 **például**: 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 közügyekben 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 nem-

zeti 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 kideríthetjük, hol van-

nak 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-vel 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 megfelelő 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]

5.1. A fogalmak forrásjegyzéke

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

Nemzeti Adatvédelmi és Információszabadság Hatóság: Adatvédelmi Értelmező Szótár. URL: https://www.naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2018. március 22.)

Muha L. – Krasznay Cs. (2014): Az elektronikus információs rendszerek biztonságának menedzselése. Budapest: Nemzeti Közszolgálati Egyetem.

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.

Muha L.: Fogalmak és definíciók. In. Az informatikai biztonság kézikönyve. 2004. http://lmuha.hu/defins.html (utolsó letöltés: 2018. március 22.)

Sági G.: Informatikai rendszer támadási folyamata. Műszaki Katonai Közlöny, 2017. http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/015_Sagi_Gabor.pdf (utolsó letöltés: 2018. március 24.)

Rédecsi M., Tóth G.: Android. 2013. Forrás: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (utolsó letöltés: 2018. március 24.)

Oroszi E. (2008): Social Engineering. Budapest: Budapesti Corvinus Egyetem.

Gyurák G. (2015): Informatikabiztonság I. Pécs: Pécsi Tudományegyetem Műszaki és Informatikai Kar.

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.

Haig Zs., Kovács L.: Kritikus infrastruktúrák és kritikus információs infrastruktúrák. 2012. http://hdl.handle.net/11410/285 (utolsó letöltés: 2018. március 24.)

Cser O. (2018): Célzott támadás a pénzügyi szektor ellen. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Marsi T. (2018): A célzott támadások és megelőzésük sérülékenységvizsgálattal. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

A Big Data a hivatalos statisztikában. 2016. https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (utolsó letöltés: 2018. március 24.)

Mátrai J.: Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás. 2016. http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (utolsó letöltés: 2018. július 04.)

Sebők V. (2018): Új típusú támadások az államok és szervezetek ellen. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Sági G. (2018): Célzott támadási modellek és műszaki védelem lehetőségek. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Haig Zs. – Kovács L. (2008): Fenyegetések a cybertérből. Nemzet és Biztonság. http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf (utolsó letöltés: 2018. március 28.)

Solymos Á. (2018): Identitás- és jogosultságkezelés, mint a célzott támadások megelőzésének technológiai eszköze. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

Compuworks Informatikai Zrt. – Chipkártyás technológia http://www.compuworx.hu/a_chipkartyas_technologia (utolsó letöltés: 2018. 07. 04.)

Kaczur G. (2018): Spearphishing. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Váczi D. (2018): Célzott támadások módszertana. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Firmware. https://pcforum.hu/szotar/?term=firmware&tm=miaz (utolsó letöltés: 2018. március 22.)

Emmanuel Carabott (2011): Hacking Motivations – Hactivism. http://www.gfi.com/blog/hacking-motivations-hacktivism/ (utolsó letöltés: 2018. március 22.)

László G. (2014): Kockázatértékelés, kockázatmenedzsment. http://vtki.uni-nke.hu/uploads/media_items/kockazatertekeles_-kockazatmenedzsment.original.pdf (utolsó letöltés: 2018. március 22.)

Szarvák A. (2018): Felderítés/célzott támadások. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Kóbor Á. (2014): Mi az a „dolgok internete”? https://ithub.hu/blog/post/Mi_az_a_dolgok_internete/ (utolsó letöltés: 2018.07.03.)

Krasznay Cs.: A polgárok védelme egy kiberkonfliktusban, Hadmérnök 2012/4, 2012. http://hadmernok.hu/2012_4_krasznay.pdf (utolsó letöltés: 2018. március 22.)

Resperger I. (2002): Kockázatok, kihívások és fenyegetések a XXI. században. Budapest, ZMNE, Az Országos Kiemelt Kutatási Tanulmányok pályázata.

Bodó A. P. – Zámbó N. (2018): Újdonságok a kibervédelmi szabályozásban. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. tv.

Szappanos G. (2018): Kártékony kódok használata a célzott támadások végrehajtásában. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Bodó A. – Zámbó N. (2018): A közreműködők kötelezettségei a célzott támadások elhárításában az ibtv. szerint. In. Célzott támadások. Budapest: Dialóg Campus Kiadó.

Yaqoob, I. – Ahmed, E. – Imran, M.: The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 6 September (2017) https://doi.org/10.1016/j.comnet.2017.09.003 (utolsó letöltés: 2017. október 20.)

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:
Kiss Eszter
Császár-Biró Anna

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-060-5 (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 készült el és jelent meg.

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE