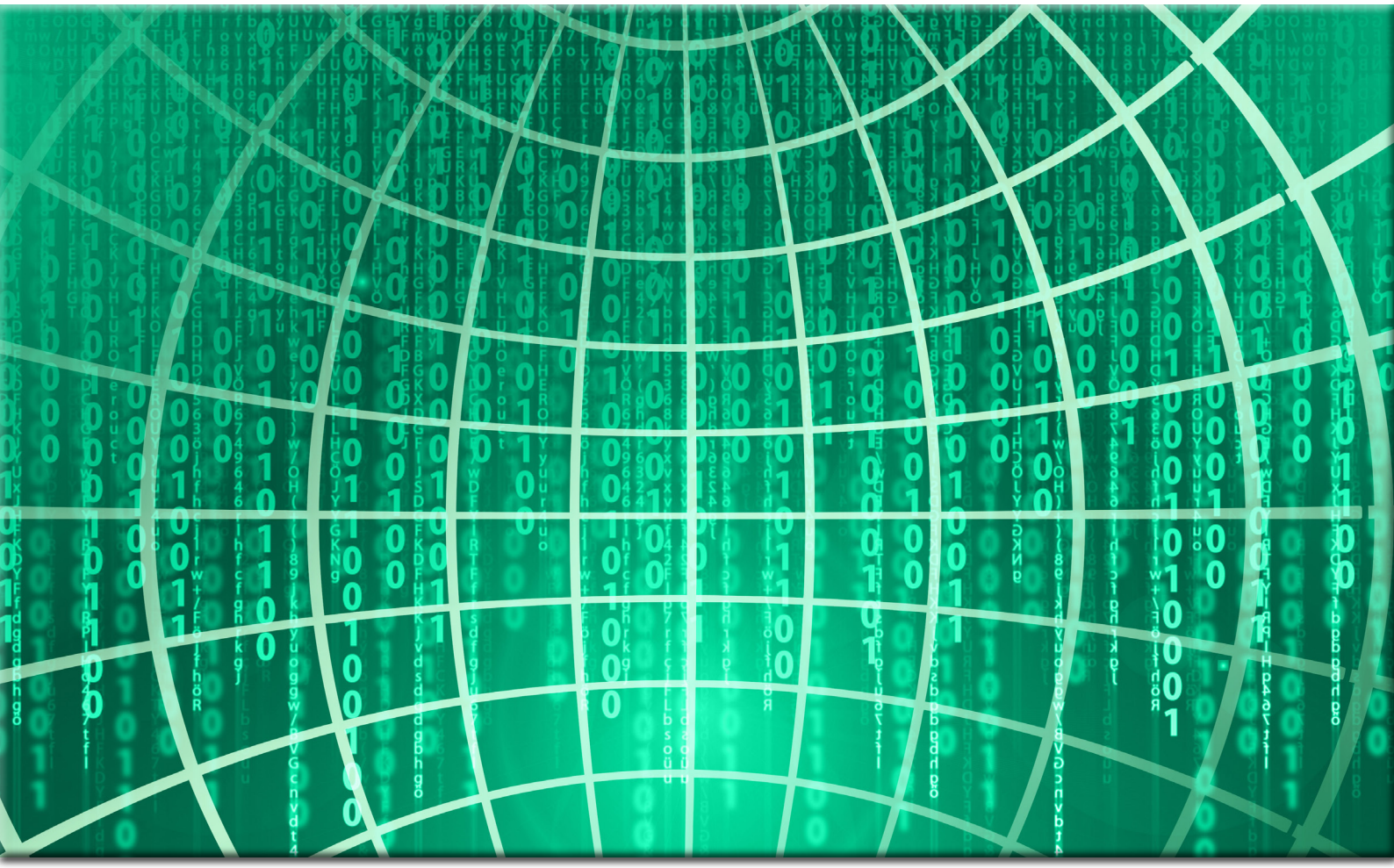
BODÓ ATTILA PÁL – JOÓ TAMÁS –
PALICZ TAMÁS



AZ IBTV. GYAKORLATA

Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2020

Nemzeti Közszolgálati Egyetem, Budapest

AZ IBTV. GYAKORLATA

Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2020

Szerzők:
Dr. Bodó Attila Pál
Dr. Palicz Tamás
Joó Tamás

Szakmai lektor:
Dr. Szócska Miklós

Szerkesztő:
Deák Veronika

A kézirat lezárásának dátuma:
2020. szeptember 16.

A hatályosított kézirat lezárásának ideje:
2022. február 25.

Hatályosítást 2022-ben végezte:
Mikula Fanni

Hatályosításért felelős szakmai szakértő:
Legárd Ildikó

TARTALOM

1. DR. BODÓ ATTILA PÁL: IBTV. A MINDENNAPOKBAN – SZERVEZETI TAPASZTALATOK

1.1. Bevezetés

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (a továbbiakban: Ibtv.) 2013. április 15-ei ülésnapján fogadta el az Országgyűlés, és 2013. július 1-jén lépett hatályba, amit számos végrehajtási rendelet magalkotása követett. A kialakított szabályozási környezet hozzájárult az információbiztonság közigazgatási szervezetrendszerben való érvényesítéséhez és a biztonságtudatos magatartás fejlesztéséhez, mind szervezeti és mind személyi szinten egyaránt. A szabályozás az elmúlt időszakban elősegítette a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (II. 21.) Korm. határozattal megfogalmazott kormányzati célkitűzések és intézkedések elérését, a szervezeti feladatellátás gyakorlati adaptációját. Az Ibtv. megfelelő keretet ad az információbiztonsági alapokat ismerő, biztonságtudatos szervezeti működéshez. Az elmúlt időszak számos tapasztalattal gazdagította mind a jogalkotói, mind a jogalkalmazói oldalt, azonban ezek teljes körű tárgyalására jelen jegyzet keretében sem a témameghatározás, sem a terjedelem miatt nem kerülhet sor. Az alább leírtakban a jogalkalmazás szervezeti oldaláról nézve azok az alapvetések kerülnek rögzítésre, amelyek az információbiztonsággal kapcsolatos szervezeti feladatok szakszerű ellátásához szükségszerűek a szabályozás alapján. Ezen szabályozási elemek esetében az is kérdés, hogy ezek hogyan érvényesültek a hatálybalépés óta, mely esetekben merültek fel végrehajtási kérdések vagy gyakorlati problémák. A jegyzet megírásának célja, hogy fő részében rövid alcímek alá szervezve – mint amolyan „Örkény-egypercesek" – útmutatást biztosítson lépésről lépésre a szervezetek részére az Ibtv. által előírt kötelezettségek alapszintű ellátásához és a minimumkövetelmények ellenőrzéséhez.

1.2. Szervezeti feladatok

A jogalkalmazói tapasztalatok alapján rögzíthető, hogy az Ibtv. és végrehajtási rendeletei szabályainak jogérvényesülésére fokozottan került sor a hatálya alá tartozó szervezeti körre nézve. A hatálybalépést követően a preventív jellegű hatósági tevékenységnek, valamint a növekvő számú biztonsági fenyegetések hatására fokozódó társadalmi érdeklődésnek köszönhetően egyre tudatosabb magatartásformákat tanúsítottak az érintett szervezetek. Napjainkra ezen szervezetek esetében az információbiztonsági szabályok betartása mind a szervezeti, mind az emberi (felhasználói) magatartásokban realitássá vált azzal, hogy az érintettek követik a szabályozás előírásait. Ez a megváltozott magatartási forma a szervezetek oldaláról számos olyan, a szabályozási környezethez kapcsolódó alapfeladatot

rögzít, amelyek végrehajtása a biztonságtudatos működéshez és a kötelezettségek teljesítéséhez szükséges. Ezek, logikai sorrendet vázolva, mint egymást követő intézkedési lépések sorozata rögzíthetők az alábbiak szerint.

1.2.1. Elektronikus adatvagyon-felmérés és az adatkezelők vagy adatfeldolgozók

Az Ibtv. hatálya alá tartozó szervezeteknek az elektronikus információs rendszereikben kezelt adatokra és információkra vonatkozóan a bizalmasság,[1] a sértetlenség[2] és a rendelkezésre állás[3] követelményeinek érvényesüléséhez biztosítaniuk kell az elektronikus információs rendszer zárt, teljes körű, folytonos és kockázatokkal arányos védelmét annak teljes életciklusában.[4] Ezen kötelezettség teljesítésére megfelelő szakmai színvonalon és minőséggel nem kerülhet sor anélkül, hogy a szervezet tisztában legyen azzal, hogy elektronikus információs rendszereiben milyen adatokat kezel.

Azaz a szervezetnek rendelkeznie kell elektronikus adatvagyon-nyilvántartással, amely tartalmazza, hogy a szervezet:

a) milyen kategóriába tartozó adatot[5] (személyes adat, különleges adat, bűnügyi személyes adat, közérdekű adat, közérdekből nyilvános adat, minősített adat),
b) mely közfeladat[6] ellátása érdekében,
c) milyen mennyiségben (pl. nem kezel, csekély-, közepes-, nagy-, jelentős mennyiségben kezel),
d) milyen elektronikus információs rendszerben kezel.

Az Ibtv. hatálybalépését követő első időszakban gyakorlati problémát okozott a szervezetek részéről, hogy megállapítsák, milyen adatkategóriákat kezel az általuk üzemeltetett elektronikus információs rendszer, és így milyen adatok vonatkozásában vizsgálják az előírt kötelezettségek teljesítését. Az idő előrehaladtával és a szabályozási környezet változásával szükségszerűvé és egyértelművé vált, hogy az adatok ismerete nélkül a végrehajtás nem lesz megfelelő. Ehhez szükség van az elektronikus adatokról egy ún. adatkataszter elkészítésére és ezen nyilvántartás folyamatos karbantartására. Ennek az elektronikus adatvagyon nyilvántartásnak az elkészítése a szervezeten belül több szereplős feladat. Célszerű, ha ezt az elektronikus információs rendszer biztonságáért felelős személy és az adatkezelő vagy adatfeldolgozó az adatvédelmi tisztviselő bevonásával közösen készíti el, azzal, hogy az adatok rendelkezésre állásáért és szakszerűségéért az adatkezelő vagy adatfeldolgozó a felelős. Az Ibtv. 2015-től[7] tartalmazza az adatkezelő vagy adatfeldolgozó fogalmának meghatározását, amelyszerint adatfeldolgozó az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött

[1] Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról – Ibtv. 1. § (1) bekezdés 8. pont.

[2] Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség), és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható – Ibtv. 1. § (1) bekezdés 39. pont.

[3] Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek – Ibtv. 1. § (1) bekezdés 38. pont.

[4] Ld. bővebben: Ibtv. 5. §.

[5] Infotv. 3. § és Mavtv. 3. §.

[6] Jogszabály által meghatározott állami vagy helyi önkormányzati feladat.

[7] A rendelkezés hatályos 2015. július 16-tól.

szerződést is - adatok feldolgozását végzi.[8] Adatkezelő az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.[9]

Az elektronikus adatvagyon-nyilvántartás kapcsolódik az adatkezelő és adatfeldolgozó részéről felmerülő azon kötelezettséghez is, amely a GDPR által előírt, az adatkezelési tevékenységhez kapcsolódó nyilvántartás-vezetési kötelezettséget írja elő valamennyi elvégzett adatkezelési tevékenység esetében.[10]

1.2.2. Elektronikus információs rendszerek azonosítása

A szervezet részéről az elektronikus információs rendszerek azonosítása nemcsak az elektronikus adatvagyon nyilvántartás elkészítése céljából bír jelentőséggel, hanem alapkövetelmény az Ibtv. szerinti biztonsági osztályba sorolás[11] elvégzéséhez is. Az Ibtv. hatálybalépését követő kezdeti időszakban a végrehajtás során nehézségekbe ütközött az elektronikus információs rendszer fogalmának értelmezése és gyakorlati átültetése, ezáltal a rendszerek azonosítása a biztonsági osztályba sorolás alkalmával. A probléma hatékony kezelését a szervezetek Informatikai Biztonsági Szabályzataiban alkalmazott azon rendelkezés biztosította, amely rögzítette, hogy mely esetekben nem kell a biztonsági osztályba sorolást elvégezni. A jó gyakorlat szerint ide tartoznak azok az alkalmazások, szoftverek, amelyek nem minősülnek önálló elektronikus információs rendszernek a kezelt adatok, illetve a megvalósított funkciók alapján (pl. az operációs rendszerek és részeik, a segédprogramok, a célszoftverek – kép-, illetve fájlkezelő szoftverek, irodai szoftverek), valamint az adott informatikai tevékenységet, funkciót megvalósító eszközök vagy megoldások (pl. tűzfal, switch, szerver, mentőeszköz, router).

Az elektronikus információs rendszer fogalma[12] 2019. január 1-től változott, a megváltozott fogalom már igazodik a NIS-irányelv hálózati és információs rendszer fogalmához.[13] A hatályos rendelkezés alapján elektronikus információs rendszernek minősül:

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;[14]
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 a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

---

8 Ibtv. 1. § (1bekezdés) 3 pont
9 Ibtv. 1. § (1bekezdés) 5 pont
10 GDPR 30. cikk.
11 Ibtv. 1. § (1) bekezdés 12. pont.
12 Ibtv. 1. § (1) bekezdés 14b. pont.
13 NIS irányelv 4. cikk 1. pont.
14 Elektronikus hírközlő hálózat: jelek vezetékes vagy vezeték nélküli úton elektronikus hírközlő eszközökkel történő továbbítását lehetővé tevő, állandó infrastruktúrán vagy központilag adminisztrált kapacitáselosztáson alapuló rendszerek, továbbá adott esetben kapcsoló vagy útválasztó eszközök, valamint más erőforrások, beleértve a nem aktív hálózati elemeket is. Elektronikus hírközlő hálózat különösen a műholdas hálózat, a helyhez kötött - vezetékes vagy vezeték nélküli - hálózat és a mobil rádiótelefon-hálózat; az energiaellátó kábelrendszerek olyan mértékben, amennyiben azokat a jelek továbbítására használják, valamint a műsorterjesztő hálózat. – 2003. évi C. törvény 188.§ 22 pont).

Ezen fogalmi meghatározás mellett az Ibtv. 1. § (3) bekezdésének normaszövege szerint *„egy elektronikus információs rendszernek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében az adatok, információk kezelésére használt eszközök - így különösen környezeti infrastruktúra, hardver, hálózat és adathordozók -, eljárások - így különösen szabályozás, szoftver és kapcsolódó folyamatok -, valamint az ezeket kezelő személyek együttesét”..*

A NIS-irányelv jogharmonizációját követő fogalom módosítása a hálózati megközelítést helyezte előtérbe, azonban megmaradt az adatok kezelésére használt eszközök és eljárások, valamint a kezelő személyek együttesére vonatkozó meghatározás is, így a korábbi, és fentebb rögzített jó gyakorlat a továbbiakban is alkalmazható a végrehajtás támogatásához.

1.2.3. Fenyegetések azonosítása

A tapasztalatok alapján a már azonosított elektronikus információs rendszerekkel szemben fennálló fenyegetések feltárása és rangsorolása, majd az így kapott fenyegetettségi lista alapján a kockázatelemzés elvégzése a kezdeti időszakban elmaradt, vagy nem megfelelően került elvégzésre. A fenyegetés értelmezéséhez az Ibtv. értelmező rendelkezése nyújt támogatást – ez a fogalom a hatálybalépés óta nem változott –, amely alapján 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*”.[15]

A fogalmi meghatározásból következik, hogy fenyegetésnek kell tekinteni mind a külső és mind a belső irányultságú, kockázatot hordozó tényezőket és eseményeket, amelynek az egyenes és az eshetőleges szándékoltságon alapuló megjelenési formájával egyaránt számolni kell a szervezetnek. A fenyegetettségek jelentkezhetnek:

a) az adat, információ szintjén (pl. adatvesztés vírustámadás miatt, illetéktelen adathozzáférés),
b) az infrastruktúrát illetően a hardver és a szoftver oldalon (pl. frissítések elmaradása szoftver vagy hálózati oldalon, karbantartások, eszközcserék elmaradása),
c) a fizikai környezet tekintetében (pl. élőerős védelem, áramellátás, tűzvédelem), valamint
d) az emberi tényezőknél (pl. hanyagság, ismeret hiánya, szándékos károkozás).

A fenyegetettségek azonosítását több tényező figyelembevételével lehet elvégezni, ezek között a legygyakrabban alkalmazottak az alábbiak:

a) adott időszakra vonatkozóan (pl. 6–12–24 hónap) szerzett üzemeltetési tapasztalatok,
b) biztonsági események elemzése (adott időszakban bekövetkezett eseményekre vetítve),
c) biztonságtudatos képzésen szerzett tapasztalatok, felhasználói jelzések,
d) Nemzeti Kibervédelmi Intézettől érkező tájékoztatások, riasztások,
e) nemzetközi és hazai szervezetek információ megosztása.

A kialakított listákban a lehetséges fenyegetettségek között – eltérő rangsorral, a bekövetkezési valószínűség és a kármérték figyelembevételével – szinte minden érdemleges tényező előfordult (pl. social engineering, jogosulatlan adathozzáférés, kéretlen levelek, kártékony kódok, célzott támadások, szolgáltatás kiesések stb.). Ezen túlmenően kockázati tényezőként kerültek azonosításra a meglévő szervezeti erőforrásokra vonatkozó hiányosságok (pl. infrastruktúra- – hálózat-, tárhely- – kapacitásproblémák, üzemeltetési hiányosságok – mentések, frissítések, javítócsomagok telepítésének hi-

[15] Ibtv. 1. § (1) bekezdés 19. pont.

ánya), valamint a szervezetfejlesztési problémák (pl. szabályozási hiányosságok) is. A fenyegetések rangsorolása az a feladat, amely nem hagyható el a szervezetek részéről annak érdekében, hogy az elektronikus információs rendszerek biztonsági osztályba sorolásához szükséges kockázatelemzés elvégzése megfelelő legyen.

1.2.4. Osztályozási eljárás és biztonságiszint-meghatározás

Az elektronikus információs rendszerek biztonsági osztályba és a szervezet biztonsági szintbe sorolásánál[16] több olyan kezdeti probléma is azonosításra került, amelyek kezelését szervezeti keretek között, megfelelő jogértelmezést követően biztosítani lehetett. Ezek az alábbiak:

a) a biztonsági osztályba sorolásra nem kockázatelemzés alapján került sor, figyelmen kívül hagyva ezáltal a kockázatokkal arányos védelem elvét,
b) az 1-5-ig történő osztályozási fokozatot, mintegy „iskolai" osztályzatot vették figyelembe, ezáltal az elektronikus információs rendszereket vagy a szervezetet „túl- vagy alulértékelték" (1-es elégtelen, 5-ös kitűnő), figyelmen kívül hagyva a fokozatok emelkedésével párhuzamosan szigorodó védelmi előírásokat,
c) a biztonsági osztályba sorolás eljárásrendjét és fokozatát, valamint a biztonsági szintbe sorolás eredményét az informatikai biztonsági szabályzatban nem rögzítették.

Az Ibtv. előírja[17], hogy a biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A hatálybalépést követően az Ibtv. hatálya alá tartozó szervezeteknek[18] az előírt felülvizsgálatot az alábbiak figyelembe vételével kell elvégezniük:

a) az elektronikus információs rendszer biztonságát érintő jogszabályban változás következik be,
b) a szervezet új elektronikus információs rendszert vezet be,
c) a szervezet státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában változás következik be

a felülvizsgálatot soron kívül, a hároméves ismétlődő időszaktól függetlenül el kell végezni. Ezen felülvizsgálati szabályok gyakorlati alkalmazását az érintett szervezetek eltérően végezték el, a soron kívüli felülvizsgálatra vonatkozó előírás nehézkesen érvényesült. A jogszabályi előírások érvényesítésére további kiegészítő szabály került hatálybaléptetésre 2015-től[19], amely rögzítette, hogy új elektronikus információs rendszer bevezetése, vagy már működő fejlesztése során a megállapított biztonsági osztályhoz tartozó követelményeket a használatbavételig teljesíteni kell. Ennek végrehajtása szervezeti oldalról megköveteli, hogy az elektronikus információbiztonságért felelős személyt már a tervezési szakaszban bevonják az új beszerzésekbe, illetve a fejlesztési prioritások meghatározásába. Erre azonban esetenként csak megkésve, a projekt előrehaladott állapotában került sor. Ezeknek az előírásoknak a kikényszeríthetősége a szervezeti szabályozás oldalról támogatható (pl. beszerzési szabályok ez irányú módosítása) és rendszeres ellenőrzéssel (pl. vezetői ellenőrzés, belső ellenőri vizsgálat) biztosítható.

16 Ibtv. 7-10. §.
17 Ibtv. 8. §.
18 Ibtv. 2. §.
19 Ibtv. 8. § (7) bekezdés, Hatályos 2015. július 16-tól.

Az elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintjének kezdeti kötelező besorolása[20] a szervezeteket olyan biztonsági követelmények elé állította, amelyek végrehajtása a teljes szervezetre nézve esetenként indokolatlan volt és aránytalan terhet jelentett, ezért 2015-ben módosításra került ez a rendelkezés. A módosított szabály[21] lehetővé tette, hogy az elektronikus információs rendszer fejlesztését vagy üzemeltetését végző, illetve üzemeltetéséért vagy információbiztonságáért felelős szervezeti egységeit a szervezettől elvárt, eltérő biztonsági szintekbe lehessen sorolni. Ez a szabály könnyebb végrehajtást eredményezett a szervezetek részére, és biztosította, hogy az elvárt védelemi intézkedések megvalósítására ott kerüljön sor, ahol azt a kockázatok indokolják, úgy, hogy a szervezet védelemre való felkészültsége továbbra is az irányadó legyen.

A szervezet vagy szervezeti egység biztonsági szintjének elérésére, ha az elvárt biztonsági szintnek való megfelelés hiányzik, ugyanúgy cselekvési tervet kell készíteni,[22] mint a biztonsági osztályba sorolás hiányosságainak pótlásánál. Az Ibtv. hatálybalépését követően érzékelni lehetett, hogy a hatálya alá tartozó szervezetek esetében a biztonsági szint (a szervezet biztonsági „érettsége") alacsonyabb az előzetesen elvártnál, így a felkészülési időszak meghosszabbításra került. A hatálybalépésnél az 1. szint eléréséhez szükséges intézkedések megtételére egy, majd a 2015-ös módosítást követően két év állt rendelkezésre. Ez az időszak 2016-ban 4 évre, 2017-ben 5 évre, 2018-ban 6 évre, 2019-ben 8 évre, majd legutóbb 2021-ben 10 évre módosult.[23] Az 1. szinthez rendelkezésre álló időszak „folyamatos" emelése jogalkalmazói és jogalkotói szemmel egyaránt kérdéseket vet fel abból a szempontból, hogy a végrehajtást jobban támogatná, ha szervezeti formára nézve strukturált részletszabályok kialakítására kerülne sor. Figyelemmel kell lenni arra is, hogy az előírt, magasabb biztonsági szint teljesítésére vonatkozóan a 2 évenkénti fokozatos elérés lehetősége továbbra is biztosított.[24]

A végrehajtás során a biztonsági szintbe sorolásánál is érvényesíteni kell a felülvizsgálat követelményét, amelyet:

a) alapesetben az előírt biztonsági szint elérését követően legalább háromévenként,
b) soron kívül az elektronikus információs rendszer biztonságát érintő változás, illetve új elektronikus információs rendszer bevezetésekor

kell megismételni.[25]

1.2.5. Védelmi intézkedések meghatározása

A biztonsági osztályba és a biztonsági szintbe sorolás hatályos követelményrendszerét az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben megha-

[20] Ibtv. 9. § (2) bekezdése, hatályos 2015. július 15-ig.
a) Köztársasági Elnöki Hivatal, Országgyűlés Hivatala, Alkotmánybíróság Hivatala, Alapvető Jogok Biztosának Hivatala, a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalai és a hatósági igazgatási társulások esetén legalább a 2. biztonsági szint,
b) a központi államigazgatási szervek, a bírósági szervezetrendszer, az ügyészségi szervezetrendszer, az Állami Számvevőszék, a Magyar Nemzeti Bank, a fővárosi és megyei kormányhivatalok esetén legalább a 3. biztonsági szint,
c) Magyar Honvédség esetén legalább a 4. biztonsági szint,
d) a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói, az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek esetén legalább az 5. biztonsági szint.

[21] Ibtv. 9. § (2) bekezdése, hatályos 2015. július 16-tól.

[22] Ibtv. 10. §.

[23] Ibtv. 10. § (3) bekezdés.

[24] Ibtv. 10. § (4) bekezdés.

[25] Ibtv. 10. § (5)–(6) bekezdés.

tározott 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 (továbbiakban: BMr.) mellékletei tartalmazzák. [A BMr. az azonos című és tárgyú 77/2013. (XII. 19.) NFM rendeletet helyezte 2015-ben hatályon kívül.]

A szervezetek az Ibtv. 14. §-a szerinti hatóság által közzétett és ingyenesen letölthető, a BMr. 1., 3. és 4. mellékletén alapuló *„Osztályba sorolás és védelmi intézkedés* űrlap"-ot (a továbbiakban: OVI-tábla) a biztonsági osztályba sorolás elvégzéséhez, a BMr. 2. mellékletén alapuló *„Szintbe sorolás és védelmi intézkedés* űrlap"-ot (a továbbiakban: SZVI-tábla) használhatják fel a kötelezettségek teljesítésére.

Az OVI-tábla támogatja az elektronikus információs rendszerek biztonsági osztályba sorolását a bizalmasság, sértetlenség és rendelkezésre állás szempontjából úgy, hogy a kitöltés során nyomon követhető a megállapított biztonsági osztályhoz tartozó védelmi intézkedések teljesülése vagy azok hiánya. A hiányosságok alapján a szervezet elkészítheti az Ibtv. által előírt cselekvési tervét.[26] A SZVI-tábla felhasználásával az információbiztonságért felelős, az üzemeltetésért felelős, az üzemeltetést végző és a fejlesztést végző szervezeti egységeknek, valamint a teljes szervezetnek a biztonsági szintbe sorolására vonatkozó követelmények teljesülése vagy azok hiánya állapítható meg. A hiányosságok alapján ez esetben is elkészíthető az Ibtv. által előírt cselekvési terv.[27]

Az OVI-tábla és a SZVI-tábla a szervezetek részére gyakorlatias és a végrehajtást támogató megoldást biztosít a követelmények ellenőrzéséhez, használatuk az évek során elterjedt. Ettől függetlenül szükséges felhívni a figyelmet két olyan tényezőre, amely a végrehajtás szintjén visszatérően felmerülő kérdés. Az egyik a BMr. azon rendelkezése, amely szerint a szervezet biztonsági szintje 4-es, ha a szervezet vagy szervezeti egység elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt. Ezen rendelkezés alapján akár egy elektronikus információs rendszer üzemeltetésével a minimum biztonsági szint 4-es lesz, amely esetenként figyelmen kívül hagyásra került.

A másik kérdéskör a BMr. 4. mellékletének 1.2. pontjában rögzített „Egyedi eltérések" és a 2. pontban rögzített „Helyettesítő biztonsági intézkedések" alkalmazása. Ehhez kapcsolódóan a BMr. 4. melléklete rögzíti, hogy a szervezet az itt rögzített eltérésekkel és helyettesítő intézkedésekkel teljesítheti a BMr. védelmi intézkedési katalógusában meghatározott minimális követelményeket a megfelelő intézkedések kiválasztásával.

Az eltérések tekintetében a BMr tételesen felsorolja azokat az eseteket (pl. fizikai infrastruktúra, technológia, szabályozás), amelyek figyelembe vehetők, rögzíti továbbá, hogy *„a helyettesítő biztonsági intézkedés olyan eljárás, amelyet az érintett szervezet az adott biztonsági osztályhoz tartozó biztonsági intézkedés helyett alkalmazni kíván, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosít minden külső vagy belső követelménynek (például törvényeknek vagy szervezeti szintű szabályzóknak) való megfelelést".*[28] A helyettesítő intézkedések fogalmához igazodóan az alkalmazásának feltételeit is meghatározza a BMr., amelyek között szerepel:

a) az elektronikus információs rendszerek biztonságára vonatkozó szabványokban vagy hazai ajánlásokban fellelhető helyettesítő intézkedés, vagy egy, az adott helyzetben megfelelő helyettesítő intézkedés alkalmazása,
b) a helyettesítő intézkedést csak abban az esetben szabad használni, ha a biztonsági intézkedések katalógusa nem tartalmaz az adott viszonyok között alkalmazható intézkedést,
c) be kell mutatni, hogy a helyettesítő intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, védelmi követelményének szintjét, és azt, hogy miért nem használhatók a vonatkozó alapkészlet biztonsági intézkedései,

[26] Ibtv. 8. § (5) bekezdés.
[27] Ibtv. 10. § (2) bekezdés.
[28] BMr. 4. melléklet 2.1. pont.

d) fel kell mérni és a kockázatkezelési eljárási rendnek megfelelően el kell fogadni a helyettesítő intézkedés alkalmazásával kapcsolatos kockázatot,
e) a helyettesítő biztonsági intézkedések alkalmazását dokumentálni, és az eljárási rendnek megfelelően jóvá kell hagynia az érintettnek.

Az egyedi eltérések és a helyettesítő intézkedések alkalmazása olyan lehetőség, amelyet a szervezet akár átmenetileg, a cselekvési tervben rögzített intézkedések végrehajtásáig is alkalmazhat, ha megfelel a fenti feltételeknek. Ezen lehetőség esetenként nem ismert és nem alkalmazott az Ibtv. hatálya alá tartozó szervezetek esetében.

1.2.6. Cselekvési terv készítése

Az Ibtv. előírja,[29] hogy ha a szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, vagy a meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre vagy szervezeti egységre meghatározott biztonsági szint, akkor a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a hiányosság megszüntetésére és az előírt biztonsági szint elérésére.

A cselekvési tervek elkészítésénél minden esetben figyelembe kell venni az Ibtv. azon rendelkezéseit, amelyek szerint az elektronikus információs rendszerre vonatkozó védelem elvárt erősségének és a szervezet vagy szervezeti egység előírt biztonsági szintjének fokozatos eléréséhez a szervezetnek 2 év áll rendelkezésére.[30] Ezeknek az idősávoknak a cselekvési terv ütemezésénél van jelentősége, mint alapvető tartalmi elem.

A cselekvési terv összeállítása során – amely a tapasztalatok alapján nem minden esetben kerül teljeskörűen rögzítésre – az alábbi tartalmi elemek szerepeltetése alapvető követelményként jelenik meg. A cselekvési terv önálló dokumentum, amelyben szerepel:

a) a feladat meghatározása,
b) a feladat végrehajtására rendelkezésre álló határidő és annak ütemezése,
c) a feladat végrehajtásáért felelős személy és a közreműködő személyek megjelölése,
d) a feladat végrehajtásához szükséges erőforrások felsorolása,
e) a feladat végrehajtásának elmaradásával járó kockázatok felsorolása,
f) a cselekvési tervet készítő és jóváhagyó személy megnevezése.

A cselekvési tervet az elektronikus információbiztonságért felelős személy az érintettek (pl. adatkezelő, adatfeldolgozó, IT-szakterület, adatvédelmi tisztviselő, gazdálkodási szakterület) bevonásával készíti el, és a szervezet vezetője hagyja jóvá. Ezekben a tervekben a konkrét intézkedések meghatározása és a kapcsolódó adatok rögzítése mellett kiemelt figyelmet kell fordítani az ún. PDCA-elv[31] beépítésére és későbbi érvényesítésére is, mivel az ellenőrzés és az ellenőrzés tapasztalatainak visszacsatolása által biztosítható az Ibtv. 6. §-ban rögzített elveknek[32] megfelelő védelmi intézkedések köre.

[29] Ibtv. 8. § (5) bekezdés és 10. § (2) bekezdés.
[30] Ibtv. 8. § (3) bekezdés és 10. § (4) bekezdés.
[31] PDCA-elv (Plan-Do-Check-Act = Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás).
[32] Megelőzés, korai figyelmeztetés, észlelés, reagálás, biztonsági események kezelése.

1.2.7. Biztonsági események kezelése

A gyakorlatban fontos szerepe van annak, hogy a biztonsági osztályba soroláshoz igazodóan meghozott védelmi intézkedések által elkerülhető legyen a biztonsági események[33] bekövetkezése. Ha a biztonsági esemény bekövetkezik, a szervezetnek megfelelő intézkedéseket kell hoznia annak kezelésére, mivel az esemény által kiváltott hatásnál figyelembe kell venni, hogy az milyen időtartamban állt fenn, milyen kiterjedtségű volt, milyen mértékű problémát/zavart okozott, hány felhasználót és/vagy szolgáltatást érintett.

Az Ibtv. a biztonsági esemény kezelését – az adminisztratív, a fizikai és a logikai védelmi intézkedéseket meghatározó magatartásszabályokkal összhangban – fogalmi szinten határozza meg, ide sorolja:

a) a dokumentálást,
b) a következmények felszámolását,
c) a bekövetkezés okainak és felelőseinek megállapítását, és
d) a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet.[34]

Fentiek alapján a biztonsági esemény kezelése történhet:

a) a védelmi intézkedések kiegészítésével vagy megerősítésével,
b) a szabályozás javításával,
c) az érintettek oktatásával és
d) egyéb módon,

azzal, hogy az eseménykezelés lényege minden esetben az, hogy minden eseménykezelési tevékenység járuljon hozzá ahhoz, hogy a további biztonsági események bekövetkezésének a valószínűsége csökkenjen, és az bekövetkező kár minimalizálható legyen.

A biztonsági események kezelése tehát tervszerű tevékenység, amelyet a szervezet részéről tudatosan kell alakítani. A tapasztalatok szerint ez azonban esetenként problémát jelent.

A tervezéshez a szabályozási környezet támpontot ad, mivel a BMr. szerint a szervezeteknek 3. biztonsági osztályba sorolt elektronikus információs rendszer esetén már kötelező a biztonsági eseménykezelési eljárás kialakítása, amely magában foglalja az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást. Emellett kötelező továbbá biztonsági eseménykezelési terv elkészítése is, amely:[35]

a) iránymutatást tartalmaz a biztonsági esemény kezelési módjaira,
b) ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,
c) átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek a szervezetbe,
d) tartalmazza a szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeket,
e) meghatározza a bejelentésköteles biztonsági eseményeket,
f) meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (pl. súlyosság) kritériumrendszerét,

[33] 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 – Ibtv. 1. § (1) bekezdés 9. pont.

[34] Ibtv. 1. § (1) bekezdés 10. pont.

[35] BMr. 4. melléklet 3.1.5. alcím 3.1.5.8.1. pont.

g) támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére,
h) meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

A szervezet kötelezettsége,[36] hogy a biztonsági eseménykezelési tervet:
a) kihirdesse és ismertesse a biztonsági eseményeket kezelő személyek és szervezeti egységek részére, nyilatkoztassa őket annak tudomásulvételéről,
b) meghatározott gyakorisággal felülvizsgálja,
c) frissítse, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat.

A szervezet részéről a biztonsági események kezelése kapcsán fentiek gyakorlati alkalmazása szükséges a védelmi képességek megfelelő szintű fenntartásához.

1.2.8. Informatikai biztonsági szabályzat

Az Ibtv. 11. § (1) bekezdés f) pontja szerint kiadott informatikai biztonsági szabályzat (a továbbiakban: IBSZ) elkészítése a BMr. szerint már 1-es biztonsági osztályba sorolt elektronikus információs rendszer esetén is kötelező, így mint adminisztratív védelmi intézkedés a legkisebb szinten, mintegy alapvetésként jelenik meg a szabályozásban. Az IBSZ részletezettsége és „minősége" szigorodik a magasabb biztonsági osztályba sorolt elektronikus információs rendszer használatával. Ettől függetlenül az IBSZ elkészítésére vonatkozóan nincs „mintaszabályzat" rendszeresítve, formai és tartalmi elemeit a jogszabályok figyelembevételével a szervezet maga határozza meg, ezért van egy-két olyan – főleg a hatálybalépést követő kezdeti időszakra és a központi közigazgatási körön kívüli szervezetekre jellemző – probléma, amely időszakosan visszatérő volt. Ezek közé tartozik:
a) az információbiztonsági és az adatvédelmi szabályok elhatárolásnak hiánya (pl. esetenként a még alkalmazott szabályzat elnevezése „informatikai és adatvédelmi szabályzat" volt, amelyben az adatvédelmi rész feltüntetésére a 2012. január 1-től hatálytalan adatvédelmi törvény[37] alapján került sor), amely problémakör a GDPR hatálybalépését követően „kikopott" a gyakorlatból,
b) a biztonsági osztályba és a biztonsági szintbe sorolás rögzítésének elmaradása,
c) az információbiztonság szereplői és felelősségi szabályai kidolgozottságának eltérése.

A tapasztalatok alapján az IBSZ felépítésére vonatkozóan az alábbi tartalmi elemek rögzítését célszerű követni a gyakorlatban:
a) Általános rész, ezen belül: az IBSZ célja és hatálya, alapelvek, alapfogalmak;
b) Elektronikus adatvagyonleltár és elektronikus információs rendszerleltár;
c) Kockázatelemzés és kockázatkezelés;
d) Biztonsági osztályba és biztonsági szintbe sorolás;
e) Szervezeti- és személyi biztonság, ezen belül: szervezeti szerepkörök, jelszó és jogosultságkezelés, felhasználókra vonatkozó szabályok;
f) Fizikai védelem (BMr. szerinti intézkedések figyelembevételével a biztonsági osztályba sorolás értéke alapján);
g) Adminisztratív védelmi intézkedések (BMr. szerinti intézkedések figyelembevételével a biztonsági osztályba sorolás értéke alapján);

[36] BMr. 4. melléklet 3.1.5. alcím 3.1.5.8.1.2. – 3.1.5.8.1.3. pont.
[37] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.

h) Logikai védelmi intézkedések (BMr. szerinti intézkedések figyelembevételével a biztonsági osztályba sorolás értéke alapján);
i) Mellékletek: biztonsági osztályba és biztonsági szintbe sorolás eredménye, elektronikus információs rendszer leltár.

Az IBSZ kidolgozására vonatkozó tartalmi elemek az elektronikus információs rendszerek biztonsági osztályba és a szervezet biztonsági szintbe sorolása alapján eltérőek, a kiadásra vonatkozó jogalkotási követelmények (pl. jegyzői, főigazgatói, elnöki, miniszteri utasítás) a szervezet jogi státuszától függően változnak. Felépítését tekintve fenti felsorolás, mint zsinórmérték szolgálhat az Ibtv. és a BMr. általi kötelezettségek teljesítéséhez.

1.2.9. Elektronikus információs rendszer biztonságáért felelős személy

Az Ibtv. a hatálybalépéskor előírta[38], hogy a szervezet vezetőjének elektronikus információs rendszer biztonságáért felelős személyt (a továbbiakban: IBF) kell kineveznie, vagy megbíznia, aki azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.) szerinti biztonsági vezetővel. Ezen rendelkezés ellenére az IBF alkalmazásával kapcsolatban az alábbi főbb problémák merültek fel a gyakorlatban.

a) Kell-e főállású munkavállaló kinevezése a feladatra?
b) Lehet-e kapcsolt feladat-, munkakörben foglalkoztatni a személyt?
c) Hol helyezkedik el a szervezeti hierarchiában az IBF?

A felmerült kérdésekre a választ az Ibtv. 2015-ös módosítása[39] sem rendezte megnyugtatóan, amely szerint a szervezet vezetőjének kötelezettsége az elektronikus információs rendszer biztonságáért felelős személyt kinevezése vagy feladatellátására vonatkozó megbízás kiadása. A módosítás hatálybalépését követően is az alábbi alapvetéseket kell rögzíteni fenti kérdéskörre vonatkozóan.

a) Annak eldöntése, hogy főállású vagy egyéb jogviszonyban (pl. megbízás, részmunkaidő) szükséges az IBF-et foglalkoztatni – fenti Ibtv. szabály alapján – a szervezet vezetőjének a feladat- és hatásköre. Ezen döntését a vezető a szervezet jogi státusza és „mérete", a kezelt elektronikus adatvagyon minősége és mennyisége, valamint az elektronikus információs rendszerek száma, mérete és biztonsági igényei alapján mérlegelheti, amelyhez kapcsolódik az Ibtv. további rendelkezése:[40] *„Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet."*
b) A kapcsolt feladat-, munkakörre vonatkozóan – a korábbi megengedő szabály hatályon kívül helyezését követően – tiltó rendelkezés nincs, így ennek mérlegelése is vezetői hatáskörbe került. A gyakorlatban az alábbi szerepkörök tekintetében merült fel a kérdés az együttes feladatellátásra:
   ba) ba) A Mavtv. szerinti biztonsági vezető, amely foglalkoztatási feltételeit a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet 5. §-a írja elő. E szerepkör együttes ellátása lehetséges, feltéve, hogy a Mavtv. 20. § (2) bekezdésének

[38] Ibtv. 11. § (1) bekezdés c) pontja – hatályos 2015. július 15-ig.
[39] Ibtv. 11. § (1) bekezdés c) pontja – hatályos 2015. július 16-tól.
[40] Ibtv. 13. § (4) bekezdés.

f) pontja alapján a Nemzeti Biztonsági Felügyelet egyetértési jogát gyakorolva engedélyezte a feladatellátást.

bb) A GDPR szerinti adatvédelmi tisztviselő. A GDPR 38. cikk (6) bekezdése szerint: *„Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség."* A GDPR és az Infotv. az összeférhetetlenségről nem rendelkezik, főszabály szerint a szervezetnek kell biztosítania, hogy e feladatellátásából adódóan ne álljon elő összeférhetetlenség. Mind a GDPR 29. cikke alapján létrehozott Adatvédelmi Munkacsoportnak az adatvédelmi tisztviselőkkel kapcsolatban kiadott iránymutatása,[41] mind a Nemzeti Adatvédelmi és Információszabadság Hatóságnak az adatvédelmi tisztviselő kinevezésével kapcsolatban kiadott tájékoztatója[42] szerint az összeférhetetlenség szempontjából kiemelten kezelendők azok a munkakörök, feladatok, ahol az adatvédelmi tisztviselőnek az adatkezelés célját és eszközeit illetően kellene döntést hoznia (pl. felső vezetői pozíciók – vezérigazgató, ügyvezető igazgató, pénzügyi igazgató, főorvos, IT- vagy HR-vezető), vagy a szervezeti struktúrában alacsonyabb szinten lévő azon pozíciók, amelyek az adatkezelés céljainak és eszközeinek meghatározásával járnak. Fentiek alapján az IBF és az adatvédelmi tisztviselő együttes ellátása nem elfogadott megoldás.

bc) Az integritás-tanácsadó. E személy feladatellátását az államigazgatási szervek integritásirányítási rendszeréről és az érdekérvényesítők fogadásának rendjéről szóló 50/2013. (II. 25.) Korm. rendelet (a továbbiakban: Korm. rendelet) határozza meg.

A szabályozás szerint az integritás-tanácsadó adatvédelmi felelősi, esélyegyenlőségi referensi és fegyelmi biztosi feladatot is elláthat, azonban belső ellenőri feladatok ellátásával egyidejűleg nem bízható meg.[43] A Korm. rendelet a megengedő felsorolásban az IBF szerepkörét nem említi, mivel azonban tiltó szabály nincs rá, és ez esetben a Korm. rendelet 5. § (2) bekezdésében[44] előírtak is teljesülnek, az együttes feladatellátás nem ütközik jogszabályi akadályba, vezetői döntési jogkörbe tartozik az érvényesítése. A vezetői döntés gyakorlásához tartozik, hogy a kijelöléshez a felettes szerv vezetőjének és a rendészetért felelős miniszternek az előzetes, írásbeli egyetértése szükséges.[45]

c) Az a kérdéskör, amely arra vonatkozik, hogy hol kerüljön elhelyezésre a szervezeti hierarchiában az IBF, az Ibtv. előírásai alapján kezelhető. Az IBF kötelezettségei között került rögzítésre, hogy feladatának ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.[46] Ezen rendelkezésre és a fentebb már említett, Ibtv. 11. § (1) bekezdés c) pontja által előírt vezetői kötelezettségre figyelemmel az IBF feladatellátása és információ megosztása tekintetében független a szervezeti hierarchiától, beszámolási kötelezettsége a szervezet vezetője felé terjed ki, aki egyben utasítási jogot gyakorol felette. (A b) pontban részletezett feladatkörök mindegyikére ez a független-

41 A 29. cikk szerinti Adatvédelmi Munkacsoport Iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban 19. oldal – 16/HU WP 243 rev.01 Legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.

42 Tájékoztató az adatvédelmi tisztviselő kinevezésével kapcsolatban – Nemzeti Adatvédelmi és Információszabadság Hatóság.

43 Korm. rendelet 6. § (5) bekezdés.

44 Az integritás-tanácsadó a hivatali szervezet vezetőjének közvetlen irányítása alatt áll. Az egyéb feladatköröket is ellátó integritás-tanácsadó egyéb feladatköreiben a hivatali szervezet vezetője által kijelölt más személy által is utasítható lehet, ha ez integritás-tanácsadói feladatainak ellátását nem veszélyezteti. – Korm. rendelet 5. § (2) bekezdés.

45 Korm. rendelet 5. § (3) bekezdés.

46 Ibtv. 13. § (1) bekezdés.

ség jellemző.) Ennek a szabálynak a megalkotása arra irányult, hogy az IBF irányítási és munkajogi oldalról is független legyen a szervezeti hierarchiában, és a szervezet vezetője mellé kerüljön elhelyezésre. A gyakorlatban tapasztaltak szerint azon megoldások, amelyek alapján az IBF az IT terület állományából kerül(t) kijelölésre – néhol kapcsolt munkakörrel – bár adott esetben szükségszerű, azonban helytelen megoldás. Az esetlegesen felmerült kapacitásproblémák – az a) pontban ismertetett szabály alapján – akár részmunkaidős megbízással vagy külső személy bevonásával is kezelhetők, figyelemmel az Ibtv. 13. § (8) bekezdésében előírt személyi feltételek fennállására. Ezen feltételek a következők: büntetlen előélet, a feladatellátáshoz szükséges felsőfokú végzettség és szakképzettség megléte.

1.2.10. Szerződéses kapcsolatok rendezése

Azon szervezeti kör esetében, akikre nem terjed ki közvetlenül az Ibtv. hatálya, kiegészítő szabályozás került rögzítésre az Ibtv. által előírt kötelezettségek érvényesítésére. Ez esetben a gyakorlati átültetés elhúzódó jelleggel került érvényesítésre, és esetenként még mindig jogalkalmazási és jogérvényesítési problémákat okoz egyes szereplőknek.

A kötelezettség a szervezet vezetője esetében arra vonatkozik, hogy ha a szervezet:

a) az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában, vagy
b) az adatkezelési vagy az adatfeldolgozási tevékenységhez

közreműködőt vesz igénybe, a vezető az elektronikus információs rendszerek védelme érdekében gondoskodik arról, hogy az Ibtv.-ben foglaltak szerződéses kötelemként teljesüljenek.[47] Ezen felelősség csak abban az esetben megosztott, ha a szervezet jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kötelezően vesz igénybe.[48] Az IBF ezen kötelezettséghez kapcsolódóan mint a biztonsági követelmények teljesüléséért felelős személy látja el feladatát, ha a szervezet:

a) az elektronikus információs rendszere tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában, továbbá
b) az adatkezelési vagy az adatfeldolgozási tevékenységéhez

közreműködőt vesz igénybe.[49]

A gyakorlatban minden, a szervezet által kötött olyan szerződés esetében, amely elektronikus információs rendszer tervezésére, fejlesztésére, létrehozására, üzemeltetésére, auditálására, vizsgálatára, kockázatelemzésére és kockázatkezelésére, karbantartására, javítására, továbbá adatkezelési vagy adatfeldolgozási tevékenységhez kapcsolódik, rögzíteni javasolt, hogy a szerződő fél az Ibtv. és a BMr. rendelkezéseit ismeri és azokat alkalmazza. Amennyiben erre még nem került sor, a már meglévő szerződéses jogviszonyok felülvizsgálatát javasolt elvégezni, és szükség esetén az érintett szerződéseket módosítani. Új szerződések megkötése során ezen kötelem érvényesítésére kiemelt figyelmet kell fordítani.

47 Ibtv. 11. § (1) bekezdés k) és l) pont.
48 Ibtv. 11. § (2) bekezdés.
49 Ibtv. 13. § (5) bekezdés.

1.2.11. Képzési követelmények

Az Ibtv. a biztonságtudatos szervezeti működés érdekében rögzítette a képzésekre vonatkozó alapkövetelményeket. A szabályozás szerint – amely a hatálybalépés óta nem változott – az IBF-nek és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyeknek rendszeres szakmai képzésen, továbbképzésen kell részt venniük.[50] A képzésekhez kapcsolódó szakmai követelményeket és oktatási programot a Nemzeti Közszolgálati Egyetem dolgozza ki.[51]

A képzések formája és igénybevétele az Ibtv. hatálybalépését követően ütemezetten jelentkezett, ennek oka egyrészt az a szabály,[52] amely szerint az Ibtv. hatálybalépésekor az IBF feladatait ellátó személyeknek a képzési követelményeket a hatálybalépést követő öt éven belül kell teljesítenie, másrészt a türelmi időhöz kapcsolódva a szervezetek információ- és „beiskolázási" hajlandóságának hiánya. 2015-ben került hatálybaléptetésre az a rendelkezés,[53] amely szerint a képzési kötelezettség teljesítésére megállapított ötéves határidőt a 2014. július 1-jét követően az Ibtv. hatálya alá kerülő szervezetek esetében:

a) az Ibtv hatálya alá tartozó, a 2. § (1) bekezdés a) pontjában tételes taxációval felsorolt szervezet esetében a létesítését megalapozó döntés hatálybalépésétől,
b) az a) pont szerinti szervek számára adatkezelést végzők esetében az adatkezelés megkezdésétől,
c) a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói esetében az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépésétől,
d) az európai vagy nemzeti létfontosságú rendszerelem[54] esetében a kijelölő határozat véglegessé válásától
e) az alapvető szolgáltatást nyújtó szereplők esetében az alapvető szolgáltatást nyújtó szereplőként történő azonosításról szóló határozat véglegessé válásától

kell számítani.

A képzésre vonatkozó azon részletszabályokat, amelyek a végrehajtást segítik, és iránymutatást adnak a képzési kötelezettség teljesítéséhez, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet (a továbbiakban: KIM rendelet) tartalmazza. A KIM rendelet értelmező rendelkezései szerint képzésre az alábbi személyi kör kötelezett:[55]

a) az elektronikus információs rendszer biztonságáért felelős személy, aki az Ibtv. 13. §-ában foglalt feladatok ellátására kijelölt IBF;
b) az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy, aki az állami és önkormányzati szervek esetében a szervezeti és működési szabályzat és a munkaköri leírások alapján, az Ibtv. hatálya alá tartozó egyéb szervek esetében a munkaköri leírásban vagy egyéb módon a feladatok ellátásával megbízott személy;
c) az elektronikus információs rendszerek védelméért felelős vezető, aki az állami és önkormányzati szervek esetében a szervezeti és működési szabályzat alapján, az Ibtv. hatálya alá tartozó egyéb szervek esetében munkaköri leírásban vagy egyéb módon kijelölt vezető.

50 Ibtv. 13. § (11) bekezdés.
51 Ibtv. 23. §.
52 Ibtv. 26. § (4) bekezdés.
53 Ibtv. 26. § (7) bekezdés.
54 Ibtv. 2. § (2) bekezdés c) pont
55 KIM rendelet 2. § 2–4. pontok.

Ezen személyi kör részére a biztonságtudatosság erősítése és szinten tartása, a szakmai ismeretek bővítése érdekében a KIM rendeletben előírt képzéseken való részvétel különböző formákban kötelező. A gyakorlatban ezen képzések kiválasztása és az azokon történő aktív részvétel bizonytalanságot mutat(ott) a szervezetek részéről. A kötelezetteket az alábbi képzések érintik:

a) minden kötelezett esetében a kétféléves, szakirányú továbbképzés,[56] kivéve, ha mentességgel rendelkezik a kötelezett személy,
b) továbbképzés, amelyen egy alkalommal kötelező részt venni az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személynek és az elektronikus információs rendszerek védelméért felelős vezetőnek, kivéve, ha már elvégezte az a) pont szerinti szakirányú továbbképzést, vagy a KIM rendeletben meghatározott, mentességet biztosító oklevéllel rendelkezik,[57]
c) éves továbbképzés, amelyen minden kötelezett személynek részt kell vennie, ha:
   ca) az IBF az a) pont szerinti szakirányú továbbképzést elvégezte, vagy mentesül annak elvégzése alól, illetve a b) pont szerinti továbbképzést elvégezte,
   cb) az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy és az elektronikus információs rendszerek védelméért felelős vezető, ha a b) pont szerinti továbbképzést elvégezte.[58]

Az Ibtv. alapján[59] a kötelezett mentessége az a) pont szerinti szakirányú továbbképzés elvégzése alól abban az esetben áll fenn, ha rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal. A KIM rendelet alapján akkreditált nemzetközi képzettségnek minősül:

a) az Information Systems Audit and Controll Association (ISACA) által kiadott:
   aa) Certified Information System Auditor (CISA), vagy
   ab) Certified Information Security Manager (CISM), vagy
   ac) Certified in Risk and Information Systems Control (CRISC),
b) az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP)

érvényes oklevél megléte, valamint szakmai gyakorlatként kell elfogadni:

a) az információbiztonsági irányítási rendszer:
   aa) tervezése,
   ab) kialakítása,
   ac) működtetése során,
b) az információbiztonsági ellenőrzés vagy felügyeleti tevékenység területén,
c) az információbiztonsági kockázatelemzés területén,
d) az elektronikus információs rendszerek információbiztonsági tanúsítási tevékenysége során, vagy
e) az elektronikus információs rendszerek információbiztonsági tesztelésében (etikus hacker tevékenységben)

szerzett szakmai tapasztalatot.[60] A szakmai gyakorlatot munkáltatói igazolással lehet a bizonyítani.

Fenti képzéseken túl a szervezet belső szabályzóiban (pl. IBSZ, képzési terv) célszerű a biztonságtudatosságra vonatkozó képzési lehetőségeket is rögzíteni. Ennek összhangban kell állni a BM rendelet 3. melléklet Adminisztratív védelmi intézkedések 3.1.7.2. alpontjában előírt – és az 1. biztonsági osz-

[56] KIM rendelet 4–8. §-ok.
[57] KIM rendelet 9–13. §-ok.
[58] KIM rendelet 14–18. §-ok.
[59] Ibtv. 13. § (10) bekezdés.
[60] KIM rendelet 7. §.

tálytól kötelező – képzési eljárásrenddel, ami szervezeti alapfeladat a kötelezettségek teljesítéséhez.

1.3. Összegzés

Jelen jegyzet megírásával az volt a cél, hogy az Ibtv. hatálya alá tartozó szervezetek részére, előírt kötelezettségeik teljesítéséhez olyan segédletként, sorvezetőként szolgáljon, amely alapján a feladatok számbavételével a szervezet saját biztonságtudatos működésének minimumfeltételeit rögzítheti.

A megfelelés és a hatékony végrehajtás érdekében a szervezeti kultúrába ágyazott tevékenységek mentén az érintetteknek (személyek és szervezet egyaránt) tisztában kell azzal lennie, hogy:

a) milyen adatokat kezelnek feladatellátásuk során,
b) milyen adatokat és milyen mennyiségben használnak a feladatellátást támogató elektronikus információs rendszereik,
c) az elektronikus információbiztonságban előírt védelmi intézkedések kialakításához milyen fenyegető tényezőkkel és veszélyekkel kell számolnia a szervezetnek,
d) rendelkeznek-e megfelelő szabályozási elemekkel a végrehajtáshoz,
e) mennyire biztonságtudatos a szervezet működése és a hozzá rendelet védelmi intézkedések milyen módon és mértékben érvényesülnek.

Reményeim szerint fenti feladatok gyakorlati adaptációjával, az ismertetett problémák kiküszöbölésével és a hiányosságok pótlásával a szervezetek felkészültsége megfelelő szintű lesz és képessé válnak kötelezettségeik teljesítésére.

1.4. Irodalomjegyzék

1. A 29. cikk szerinti Adatvédelmi Munkacsoport Iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban – 16/HU WP 243 rev.01 Legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.
   Forrás: https://naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf
   Letöltve: 2020. április 19.
2. Nemzeti Adatvédelmi és Információszabadság Hatóság – Tájékoztató az adatvédelmi tisztviselő kinevezésével kapcsolatban
   Forrás: https://naih.hu/files/Tajekoztato-adatvdedelmi-tisztviselo-kinevezeserol-2018-09-19.pdf
   Letöltve: 2020. április 19.

2. DR. PALICZ TAMÁS – JOÓ TAMÁS: AZ INFRASTRUKTÚRA-VÉDELEM ÉS AZ INFORMÁCIÓBIZTONSÁG KAPCSOLATA

Jelen dokumentum célja, hogy a közigazgatás különböző területein dolgozók számára továbbképzési anyag keretében mutassa be, hogy milyen gyakorlati szempontjai vannak az adat- és információbiztonságnak az egészségügy területén. A bemutatott gyakorlati példákkal azt szeretnénk szemléltetni, hogy az egészségügy területén az információbiztonságnak emberéletekben mérhető hatása van.

2.1. Bevezetés, előzmények

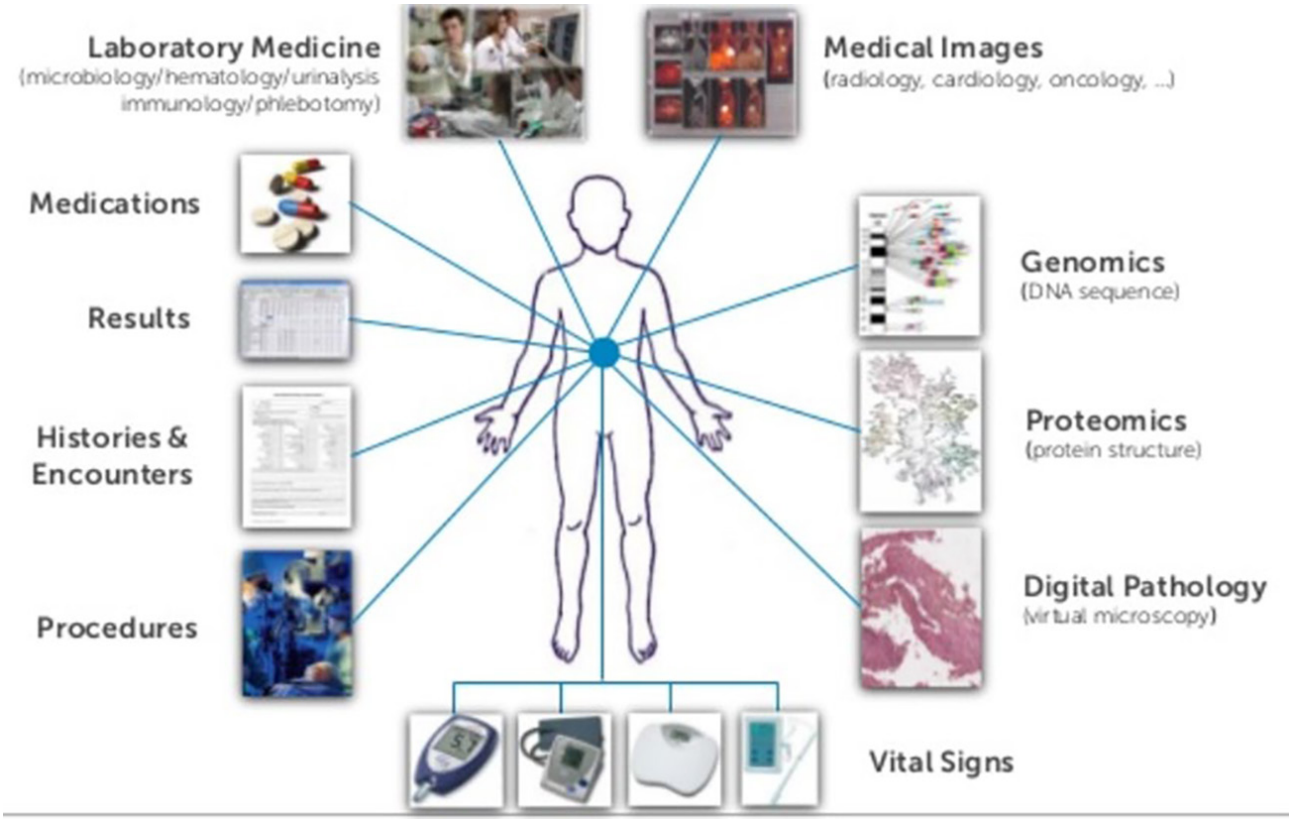
A *The Economist* 2017. májusában címlapján mutatta be az adatot, mint a gazdaság új hajtóerejét (Data is the new oil?) (1. ábra). Az azóta eltelt közel három év bizonyította, hogy az adatokkal foglalkozó multinacionális vállalatok elképesztő befolyásra tettek szert, extrém jövedelemtermelő képességgel rendelkeznek, és a rendelkezésre álló adataik révén valamennyi szektor növekedését érdemben tudják befolyásolni. Ezek a techcégek az egészségügyre mint a jövőbeli növekedés egyik terepére tekintenek. Ez és a folyamatos technológiai fejlődés együtt jár azzal, hogy az egészségügyben keletkező adatok már nemcsak az ezen a területen jártas szakemberek számára válnak értékessé, hanem a bennük rejlő gazdasági potenciál miatt tényleges piaci értékük lesz.

1. ábra: A The Economist címlapján mutatja be a XXI. század „új olaját”, az adatot, amelyet a legértékesebb erőforrásnak tekint

A digitális világ változása, az innováció elképesztő sebessége, és az a tény, hogy a jelenlegi egészségügyi és orvosi eszközök szinte mindegyike rendelkezik valamilyen informatikai háttérrel, szükségessé teszi, hogy az eszközöket indikáló, az azokat felhasználó vagy éppen beültető, egészségügyben dolgozók tisztában legyenek a potenciális veszélyekkel, hogy a orvosi esküjük egyik legfontosabb hitvallását teljesíteni tudják: Nil nocere –vagyis: Nem ártani!

2.2. Az adatvezérelt egészségügy

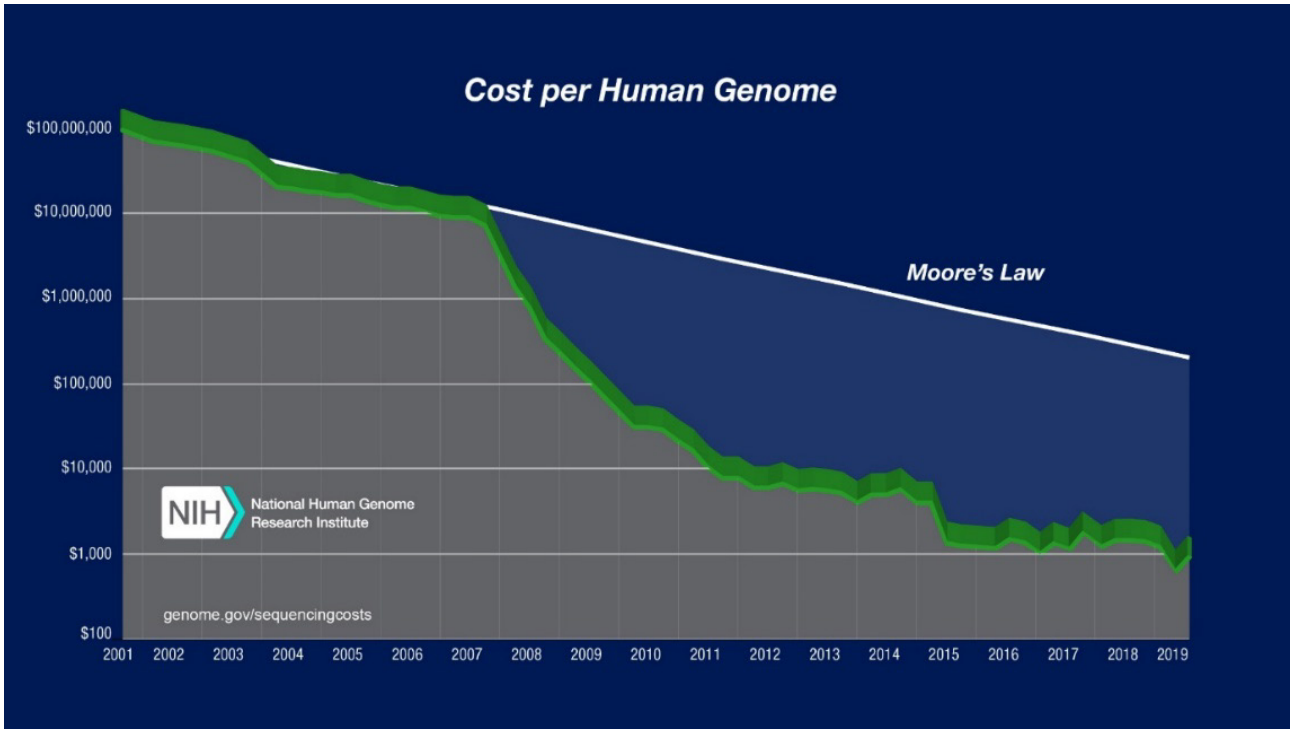
Napjainkra az egészségügy lett az az ágazat, ahol az adatok talán a legnagyobb jelentőséggel rendelkeznek. Az adatok keletkezésének és a mennyiség folyamatos növekedésének részint technológiai okai vannak, másrészt a felhasználói szokások változása szintén hozzájárul a folyamatosan bővülő adatokhoz. A technológiai okok között érdemes megemlíteni egyrészt, hogy jelentősen bővült azoknak a szakterületeknek a száma, amelyek képesek digitális adatot „termelni". Míg évekkel ezelőtt alapvetően a képalkotó diagnosztikai eszközök voltak képesek nagyobb mennyiségű digitális adat előállítására, napjainkban szinte minden szakterületen digitálisan keletkezik a beteggel kapcsolatos dokumentáció. Az „adattermelést" segíti az a tény is, hogy a születésünktől a halálunkig keletkeznek az adatok: az elmúlt évtizedekben a várható élettartam növekedése kitolta azt az időszakot, amelyben az adatok keletkeznek. Ráadásul a későbbi életkor során egyre nagyobb mértékben vesszük igénybe az egészségügyi szolgáltatásokat, ezért nagyobb mértékben keletkeznek adatok is.



2. ábra: A korábbiakhoz képest jelentősen növekedett azon szakterületek száma, ahol digitálisan képződik az adat. A klasszikus területek mellett megjelentek azok a tevékenységek és eszközök is, amelyek minimális ismerettel is használhatók, azonban fontos élettani paramétereket rögzítenek (pl. vérnyomásmérő, pulzusszámláló). Az egészségügyi adat keletkezésének új területeit jelentik a speciális diagnosztikai eszközök, mint pl. a gén- és fehérjediagnosztika (genomikai, proteomikai adatok)

3. ábra: Manapság szinte minden orvosi és egészségügyiszakterület képes digitális kép és adat előállítására, amelyek részletgazdagsága évekkel ezelőtt elképzelhetetlen volt

Szintén a technológiai háttér biztosítja, hogy az adatkör kibővült az „omics"-ok (pl. proteomics, genomics stb.) adataival: ma a genetikaitól a fehérjeadatokig szintén minden tárolható. Ehhez a térnyeréshez jelentősen hozzájárult az, hogy az elmúlt években jelentősen csökkent ezeknek az adatoknak az előállítási költsége. Míg évekkel ezelőtt egy emberi genom (teljese DNS-állomány) feltérképezése több millió dollárba került, ezt manapság 1000 dollár (!) körül elvégzik (4. ábra).



4. ábra: Az ábra azt mutatja be, hogy hogyan csökkent a genetikai vizsgálatok költsége és egy egységnyi tárolási kapacitás költsége. Jól látható, hogy a genetikai vizsgálatok költségcsökkenése jelentősen hozzájárul ahhoz, hogy olcsón, nagy mennyiségű digitális adat keletkezzen egy-egy emberről

Szintén a technológiai fejlődés tette lehetővé, hogy a képalkotó diagnosztikai eljárások területén is ugrásszerű az adatmennyiség növekedése. Míg korábban egy-egy digitális kép néhány tíz megabájt méretű volt, ma már egy részletgazdag digitális szövettani kép több tíz gigabájt (!) méretű.

A felhasználói (beteg?) szokások változása is azt eredményezi, hogy ma már szinte minden tevékenységünkkel kapcsolatban „adatot termelünk": ha elmegyünk futni, vagy úszunk, vagy éppen egy étkezés kapcsán valamennyi tevékenységünkről digitális adathalom keletkezik. Ez a tevékenység pont azokra az elsősorban fiatalabb generációkra vonatkozik, amelyek korábban nem termeltek jelentős mennyiségben orvosi/egészségügy adatot: ők nem jelentek meg az ellátórendszerben, ezért nem is képződött velük kapcsolatban semmilyen dokumentumalapú adat.

Ezzel szemben napjaninkban az életmód változása, a digitális eszközök elterjedtsége, a technológiai lehetőségek és ezen generációk digitális környezettel kapcsolatos szokásai és elvárásai biztosítják, hogy megfelelő mennyiségben keletkezzenek adatok. Ezek a legegyszerűbb eszközökön keresztül is létrejöhetnek, azonban lehetőség van bonyolultabb, személyes használatú eszközön keresztül további adatot is rögzíteni és továbbítani (alvás, pulzus, EKG, légzésszám stb.). Ezek az adatok tárolódhatnak olyan „személyes" felhőben, amely azonban gyakran valamelyik eszközgyártó saját felhője.

A személyes egészségügyi adatokat (Personal Health Information – PHI) elkülönítik a személy azonosításra alkalmas adatoktól (Personal Identically Information – PII). Ennek oka elsősorban az, hogy míg a PII esetében az adatok módosíthatók (pl. a személyi igazolvány száma, bankszámlaszám stb.), és ez lehetővé teszi, hogy valamilyen adatvisszaélés kapcsán az adat törlésre, megsemmisítésre kerüljön, addig a PHI esetében ez nem, vagy csak nagyon körülményesen történhet meg. A személyhez kötődő egészségügyi, biometrikus vagy genetikai adatok állandóak. Gondoljunk csak arra, hogy az nem változik, hogy hány kilogrammal születtünk, milyen egy génünk bázissorendje (ami ráadásul valamelyik rokonunknál is fellelhető), vagy hogyan alakult egy gyógyszer szedése kapcsán a vérnyomásunk. Ez akkor is ránk lesz jellemző, ha valamilyen ok miatt pl. a személyazonosságunkat meg kell változtatni. Ezek a sajátosságok különösen megnövelik az egészségügyi adatok értékét, mert így felhasználhatók pl. egy személy felkutatásában, azonosításában, vagy éppen az egészségügyi innováció kapcsán válhat értékessé.

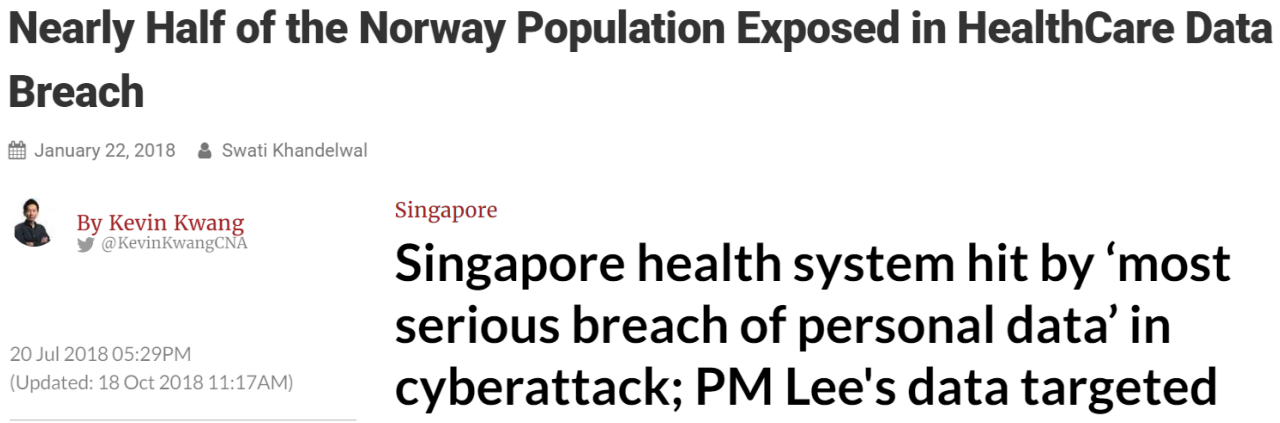
Kiberbiztonsági szakértők szerint az egészségügyi adatok a feketepiacon jelentősen meghaladják a szokványosan kapható adatok értékét, legalább egy nagyságrendi különbség biztosan van ezek között. Egy személyazonosításra alkalmas (PII) adat 1-2 dollárt ér a piacon, addig ugyanilyen adategység a PHI esetében 350-400 dollár körül van. Ebből könnyen belátható, hogy az adatok megszerzése, majd azok értékesítése jelentős vonzerőt képvisel a feketegazdaság szereplőinek. Egyes feltételezések szerint a maffia ilyen alapú bevételei ma már megközelítik a „hagyományos" üzletágakban termelt bevételeket.

2.3. Visszaélés az egészségügyben keletkezett adatokkal (data breaches)

Az adatokkal történő visszaélések kapcsán több olyan felmérés is készült, amelyek a különböző szektorok veszélyeztetettségét mérik fel. Ebből egyértelműn kiderül, hogy az egészségügy az egyik olyan terület, amely a leginkább kitett az adatokkal történő visszaéléseknek és az adatok megszerzésére tett kísérleteknek.

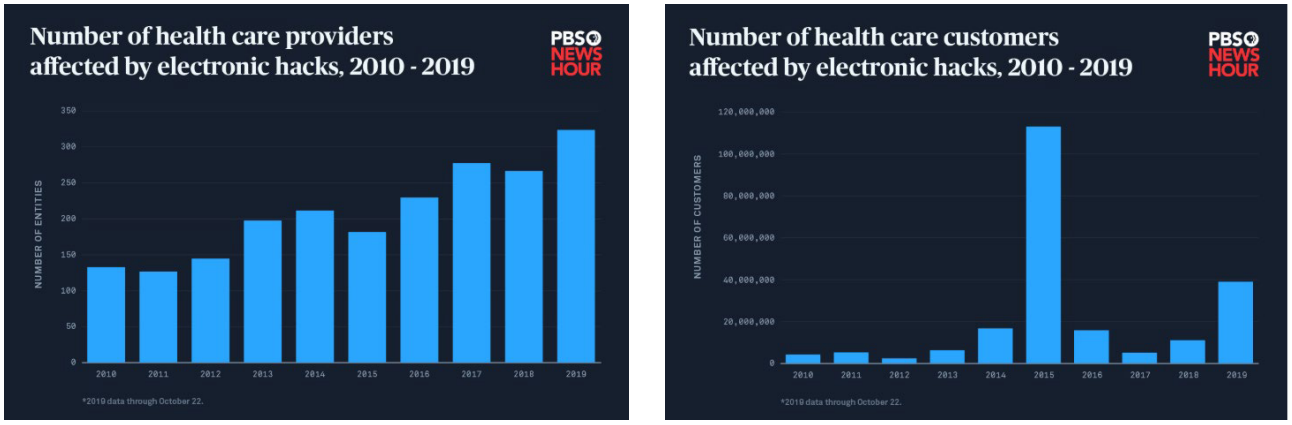
Egy 2017-es amerikai felmérés szerint a kórházak 94% már volt kitéve ilyen támadásnak, és ezeknek az érinetett intézményeknek körülbelül a fele már legalább ötször szenvedett el ilyen támadást. Ez mindenképpen azt jelzi, hogy az egészségügy a kiberbűnözés egyik kiemelt területe. Ez érthető, ha figyelembe vesszük az egészségügyi adatok feketepiaci értékét, illetve azt, hogy az egészségügyi szolgáltatók esetében az információbiztonsági tudatosság, a szervezetek felkészültsége, a technológiai lehetőségek – általában – alacsony szintűek.

Szintén fontos adat, hogy ha a lakosság egészére vonatkozóan vizsgáljuk a kitettséget, akkor olyan fejlett országokban is, mint Norvégia vagy Szingapúr, nagyon jelentős az egészségügyi adatokkal kapcsolatos visszaélések száma (5. ábra).



5. ábra: Internetes hírek szalagcímei egészségügyi adatvisszaélésekre vonatkozóan fejlett egészségüggyel rendelkező országokból

Az Amerikai Egyesült Államokban 2010 óta rendszeresen gyűjtik azon egészségügyi adatvisszaélések számát, amelyek legalább 500 ügyfelet/beteget érintettek. Az adatokból jól látható, hogy a visszaélések száma folyamatosan nő – ez különösen az érintett intézmények számának növekedéséből derül ki (6. ábra).



6. ábra: Az USA kormányának egészségügyért felelős területe által 2010–2019 között gyűjtött adatok alapján az adatvisszaélésekkel kapcsolatos növekedési tendencia jól látható

Ha az adatvisszaélések forrását vizsgáljuk, akkor a nemzetközi adatok is egyértelműen azt mutatják, hogy míg általában az jellemző, hogy az adatok megszerzése érdekében valamilyen külső támadás éri a rendszert, addig az egészségügyi adatvisszaélések kapcsán a belső, gyakran emberi tényezőt tartják jelentősebbnek.

Felismerve a fentiek jelentőségét, 2017-ben az Európai Bizottság az egészségügyet a négy legveszélyeztetettebb terület közé sorolta a pénzügyi szektor, a közlekedés és az Internet of Things eszközök mellett.

2.4. A Stuxnet egészségügyi vonatkozásai

A Stuxnet-sztori kiberbiztonsági szempontból az egyik legfontosabb alapeset: Stuxnet volt az első, igazoltan katonai céllal létrehozott vírus. 2010 júniusában derült fény a létezésére, amikor egy orosz biztonsági cég feltárta, hogy az iráni atomprogramhoz kapcsolódóan kb. 45 000 számítógép fertőződött meg, míg világszerte a fertőzött gépek száma megközelítően elérte a 100 000-t. Az előkészítést – valószínűsíthetően – az amerikai és izraeli hadsereg különleges egységei végezték. Ennek során nemcsak létrehoztak azt a speciális vírust, amely végül az iráni atomprogram leállításához vezetett, hanem kialakítottak egy olyan tesztkörnyezetet is, amelyben kipróbálták a vírus működését.

A vírus „sikerét" jelzi, hogy 2010 novemberében leállították az iráni programot, mert a dúsítását végző speciális centrifugák 20%-a tönkrement.

A Stuxnet-történet az egészségügy számára is fontos, éspedig a következő tanulságok miatt:

- Egy magas biztonsági fokozatba sorolható, kritikus infrastruktúra is sikeresen megtámadható (atomerőmű).
- A támadás során nagyon nehéz a támadó kilétét azonosítani.
- A támadás évekig nem volt felismerhető.
- A támadás nagyon specifikus lehet, csak bizonyos infrastruktúrákra irányulhat (Siemens-vezérlők).
- A támadással fizikai kárt lehet okozni (centrifugák tönkretétele).
- A támadás során nemcsak a behatolást, hanem a hatást is lehet maszkolni (centrifugák működése).

Vagyis ebben az esetben a digitális károkozó (kórokozó!) fizikai hatást eredményezett (a centrifugák fordulatszám-változása miatt azok tönkretétele). Innen logikailag is csak egy lépés, hogy a fizikai hatást biológiai hatássá transzformáljuk, vagyis pl. egy besugárzó eszköz (röntgenkészülék, radioterápiás eszköz) esetében a dózis maszkolt, elfedett növelésével érjünk el kedvezőtlen biológiai hatást (pl. egészséges sejtek, szövetek elpusztítása, sugárbetegség).

Ha orvosi szempontból nézzük, akkor szintén fontos szempont az, hogy különleges kiberbiztonsági intézkedések nélkül el lehet érni, hogy az általunk felügyelt gépek, eszközök tényleges tevékenységéről ne szerezzünk tudomást, és döntéseinket nem valós adatokra alapozva hozzuk meg. Például laborvizsgálatok esetében a fenti Stuxnet-analógia alapján egy, a valóságtól eltérően mért érték is bekerülhet a laborvizsgálat értékei közé.

2.5. Kiberbiztonság és beültethető eszközök

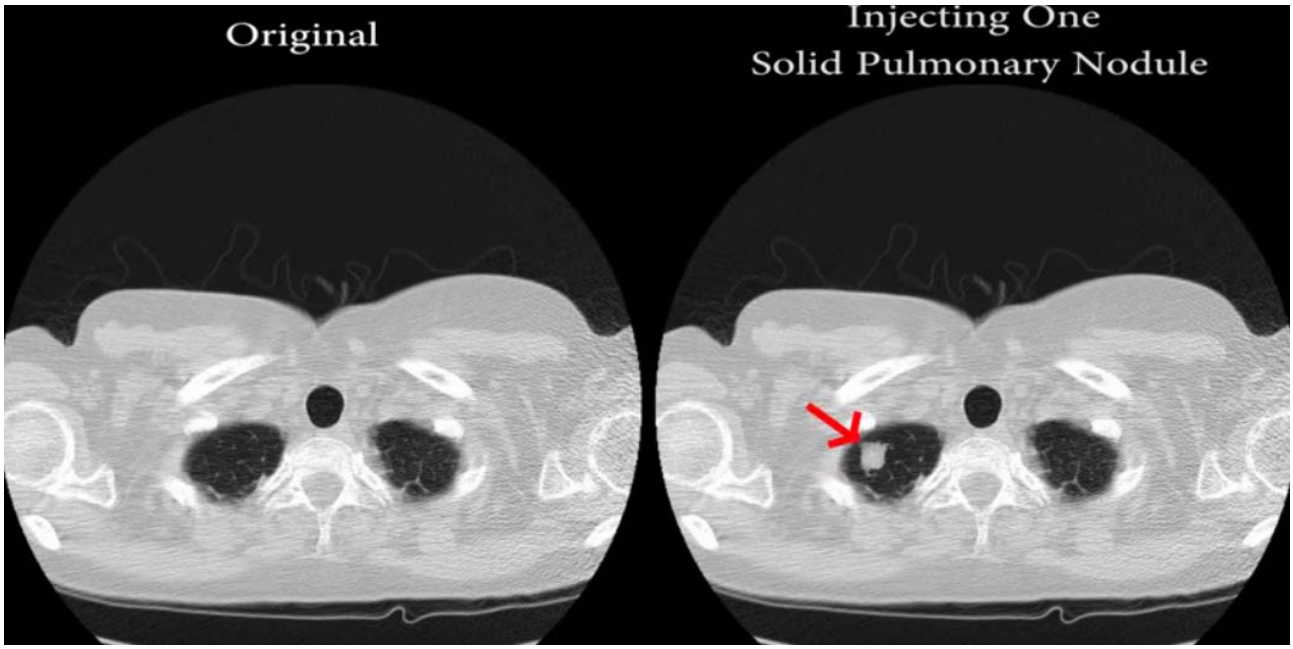
Az egészségügy területén az első komolyabb, egészségügyet érintő life-hackinget Barneby Jackson mutatta be. 2011-ben egy nyilvános konferencián egyszerű eszközök segítségével több 10 méter távolságából egy inzulinpumpát hekkelt meg úgy, hogy nem ismerte a pumpa gyártási azonosítóját, és a beadott inzulin mennyiségét növelte többszörösére (25 egység helyett 300 egységre, vagyis halálos adagig!), miközben a kijelzőn nem lehetett észlelni (!) a megváltozott mennyiséget (7. ábra).

7. ábra: Beépített inzulinpumpa, amely távolról is meghekkelhető, ezáltal a beadott inzulinmennyiség változtatható meg anélkül, hogy a kijelzőn megjelenne a megemelt mennyiség

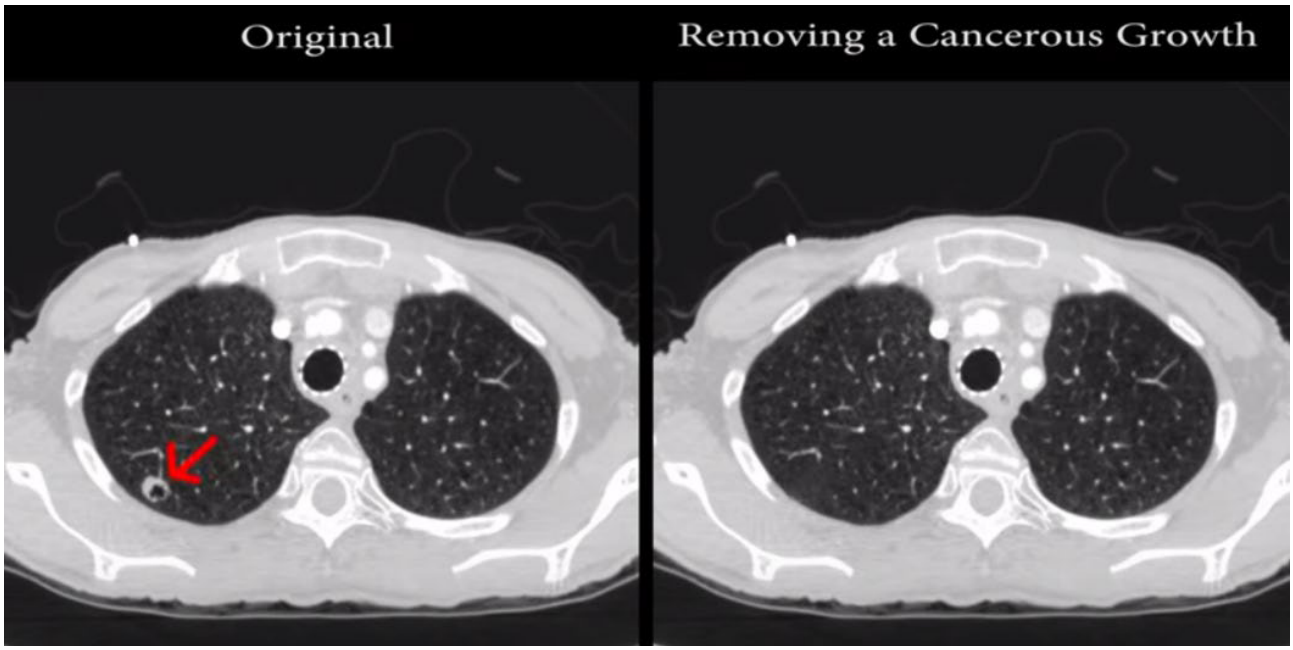
Azóta szinte minden olyan egészségügyi eszközt (medical devices) sikeresen meghekkeltek, amelyek valamilyen informatikai alkatrészt tartalmaznak. Ezek közül talán érdemes kiemelni a beültethető pacemakereket, amelyek esetében még 2019-ben is nagyon magas kockázati osztályba sorolható sérülékenységet tártak fel, így az amerikai Élelmiszer és Gyógyszer Hatóságnak (FDA) (ez a szervezet felügyeli az USA-ban az orvosi eszközöket is) külön fel kellett hívni a gyártó és az érintett betegek figyelmét a veszélyre. Érdekességként említhetjük meg, hogy az öt szívinfarktuson és négy koszorúér műtéten átesett korábbi alelnök, Dick Cheney esetében 2007-ben ültettek be defibrillátor-pacemakert, amelynek rádiofrekvenciás befolyásolhatóságát nemzetbiztonsági okok miatt később kikapcsolták. Erről maga Cheney számolt be 2013-ban.

2.6. Kiberbiztonság és az egészségügyi mesterséges intelligencia

2019 tavaszán a *The Washington Post* érdekes kontextusban hivatkozott egy izraeli kiberbiztonsági kutatók által közölt tudományos publikációra. Mielőtt bemutatták volna a kutatók által feltárt újdonságot, az újságírók azzal a gondolattal vezették be a cikket, hogy a 2016-os elnökválasztási kampányban volt egy időszak, amikor Hillary Clinton köhögött. Készítettek akkor CT-felvételt róla, de az elkészült képek a 2019-es tudásunkkal már egészen másképp is értékelhetők lettek volna. Az izraeli kiberbiztonsági kutatók azt mutatták ki, hogy nagyon egyszerű eszközökkel be tudtak jutni egy kórház képalkotó diagnosztikai rendszerébe, és ott az elvégzett CT-felvételeket mesterségesintelligencia-algoritmus segítségével módosítani tudták. Ennek eredményeképpen a teljesen egészséges felvételre daganatos elváltozást helyeztek el (8. ábra), illetve a beteg, daganatos tüdő képéről azt eltávolították (9. ábra). Ezt követően tapasztalt radiológus orvosoknak mutatták meg a képeket, akiket a mesterséges intelligencia „átvert”, vagyis ők nem ismerték fel, hogy egy daganat eredetileg is volt-e, vagy az algoritmus révén került oda.



8. ábra: A mesterségesintelligencia-algoritmus segítségével a vizsgált személyről készült képbe (egészséges) egy szolid tüdőcsomót (pl. daganat) „rajzolnak”



9. ábra: A mesterségesintelligencia-algoritmus segítségével a vizsgált személyről készült képről (daganatos tüdő) egy szolid tüdőcsomót eltávolítanak, ezáltal „meggyógyítják”

A kutatók felismerése felveti azt, hogy milyen sokféle lehetőség létezik az egészségügyi diagnosztikus beavatkozások eredményeinek manipulálására, ezáltal akár politikai játszmákba történő beavatkozásra, vagy éppen egy-egy gyógyszerkipróbálás eredményeinek befolyásolására. A cikk azzal zárul, hogy vajon hatással lett volna-e az elnökválasztásra, ha Hillary Clinton CT-vizsgálatának eredményeit valamilyen módon manipulálják.

2.7. „Pénzt vagy életet” – Védelem zsarolóvírusokkal szemben

Képzeljük el, hogy egy beteget beutalnak egy megyei kórház sürgősségi osztályára, ahol dolgozunk. A beteg érkezésekor azonban kiderül, hogy nem tudunk alapvető diagnosztikai vizsgálatokat (pl. laboratórium, képalkotó) végezni, és emiatt a beteget sem tudjuk fogadni: a sürgősségi osztály működőképtelenné vált az informatikai rendszer hibája miatt. A monitorokon egy zsarolóvírus üzenete jelenik meg: „A fájlok elérhetetlenné váltak. Amennyiben hozzájuk akarsz férni, fizess!”

A filmbe illő jelenet a valóságban is megtörtént: 2019 szeptemberében az USA egyik középső részén levő egészségügyi központban (Campbell County Health), ahol 20 kórház volt érintett egy, a fentiekhez hasonló incidensben. A kórház 8 órán keresztül kénytelen volt a betegeket a kb. 100 km-re levő másik egészségügyi intézménybe irányítani. Számos diagnosztikai modalitás – elsősorban laboratórium – nem működött, és 17 napot vett igénybe, amíg teljesen helyreállították a kórházi működéshez szükséges adatokat. A működésképtelenség hátterében zsarolóvírus-támadás állt.

A zsarolóvírusok számának alakulására nincsenek megbízható adatok. A különböző biztonsági és biztonsági tanácsadással foglalkozó cégek évente adnak ki jelentéseket a legfontosabb tendenciákról és számokról. 2019 végén jelent meg az EMSISOFT nevű cég kimutatása, amely az USA számait publikálta. Az éves jelentésük előkészítése során a konkrét számokat és a tendenciákat olyan jelentősnek találták, hogy már 2019. december közepén közzé tették a jelentést, majd év végén aktualizálták. A jelentés szerint 2019-ben a zsarolóvírus támadás által leginkább érintett szektor az egészségügy volt: 764 egészségügyi szolgáltatót ért ilyen támadás, miközben 113 állami vagy helyi önkormányzati szervet és hivatalt és 89 oktatási intézményt (egyetem, főiskola, tankerület) támadtak meg. A ransomware-vírusok által okozott károk költségét 7,5 Mrd dollárra becsülte a tanácsadó cég (ez valamennyi szektorra vonatkozó becslés). Egy másik elemzés 2019-re globálisan 11,5 Mrd dollárra becsülte a zsarolóvírusok által okozott károk költségét. Ugyanezen becslés 2021-re 20 Mrd dollárra teszi az okozott károkat. Ez azt is jelenti, hogy a becslés szerint 2021 végére minden 11-ik másodpercben történik majd egy zsarolóvírus-támadás. Ha ezt összevetjük az EMSISOFT 2019-es tényadataival, amelyek a szektorokat hasonlítják össze, egyértelműen megállapítható, hogy az egészségügy lesz az a szektor, amely a leginkább ki lesz téve a zsarolóvírus-támadásoknak. A kezdeti lineáris növekedést 2020–2021 fordulóján egy exponenciális ugrás váltja. Ennek okai között a korábban már felsorolt tényezők játszanak szerepet: alacsony belépési korlát, magas megtérülési ráta (return on investment – ROI), kriptovaluták miatti láthatatlanság.

Ezzel összhangban van a Malwarebytes 2019. negyedik negyedévben kiadott jelentése, amely az egészségügyre jellemző előző évi adatokat és tendenciákat foglalja össze a kiberbűnözés szempontjából. A rendelkezésükre álló USA-beli adatok alapján 2018 végéhez képest 45%-kal nőtt a végpontokon észlelt incidensek száma (14 000-ről 20 000-re). Kiemelkedően nőttek a trójai malwarekkel történt visszaélések (82%-os növekedés). Ezek közül az Emotet és a Trickbot nevű trójai fertőzés fordult elő számottevően. Ez a jelentés is megerősíti, hogy figyelembe véve a trójai fertőzések dinamikáját és az azt követő hatásokat, 2020-ban várhatóan növekedni fog a zsarolóvírussal kapcsolatos incidensek száma is.

Érdemes megemlíteni az FBI által 2019. október 2-án kiadott jelentést, amelynek adatai mintha nem esnének teljesen egybe a biztonsági cégek jelentéseivel. Az FBI szerint a zsarolóvírus-támadások száma 2018-hoz képest érdemben nem változott (ez valamennyi szektor adatait tartalmazta), azonban sokkal szofisztikáltabb, specifikusabbak és drágábbak lettek a zsarolóvírus-támadások által okozott károk és azok közép- és hosszú távú következményei.

A zsarolóvírus-támadások esetében külön érdemes kiemelni a WannaCry vírust, amely 2017-ben okozott jelentős funkciózavart több ország egészségügyi ellátórendszerében (más szektort is érintett, de erre nem térünk ki). A Wannacry egy Windows-rendszereket célzó káros kód, amely – más zsarolóvírushoz hasonlóan – a felhasználó fájljait titkosította, és ezt követően a titkosítás feloldásához szükséges jelszóért pénzt kért. A Kaspersky Lab’s elemzése szerint a WannaCry egy SMBv1 tá-

voli kódfuttatást kezdeményez a Microsoft Windows rendszerben. A titkosítást követően a fájlok „.WCRY" kiterjesztést kapnak. 2017. április 14-én a Shadowbrokers csoport által megszellőztetett kódok révén egy EternalBlue nevű exploit vált elérhetővé. Az exploit által kihasznált sérülékenységet a Microsoft már 2017. március 14-én javította, azonban számos vállalati környezetben nem frissítették a rendszert.

A vírus elterjedtségét mutatja, hogy több mint 230 000 számítógépet fertőzött meg világszerte, összesen 99 országban és 28 nyelven hozott létre zsarolóoldalakat (10. ábra).

10. ábra: A WannaCry által érintett országok és számítógépek egy 2017. májusi infografikán (a pontok nagysága és sűrűsége az érintett gépekkel arányos, MalwareTech adatai alapján)

A WannaCry kritikus hatással volt az angol Nemzeti Egészségügyi Szolgálat (NHS) működésére 2017 májusában. A 2017. május 12-én, pénteken induló világszintű fertőzés délután 13 órára 4, délután 16 órára 16 egészségügyi intézményt ért el Angliában. A fertőzés egy héten keresztül zajlott, és május 19-én, 17.30-kor nyilvánították lezárultnak. A gyors válaszlépéseket három fázisra bontották: 1. a sürgősségi ellátási útvonalak biztonságának megteremtése (május 12–14. között) 2. az alapellátás stabil működésének biztosítása (május 13–15. között) 3. folyamatos javítások, rendszerszintű beavatkozások, antivírus-aktualizálás (folyamatosan). Akkori, friss elemzések szerint mintegy 90 millió font kárt okozott, 19 000 orvos-beteg találkozást kellett lemondani vagy átütemezni a mintegy 80 érintett egészségügyi intézményben (ez az összes intézmény 1/3-a) és az 595 érintett háziorvosnál (az összes háziorvos 8%-a). A támadást követően nem sokkal jelentős informatikai és információbiztonsági fejlesztések indultak az NHS rendszerében.

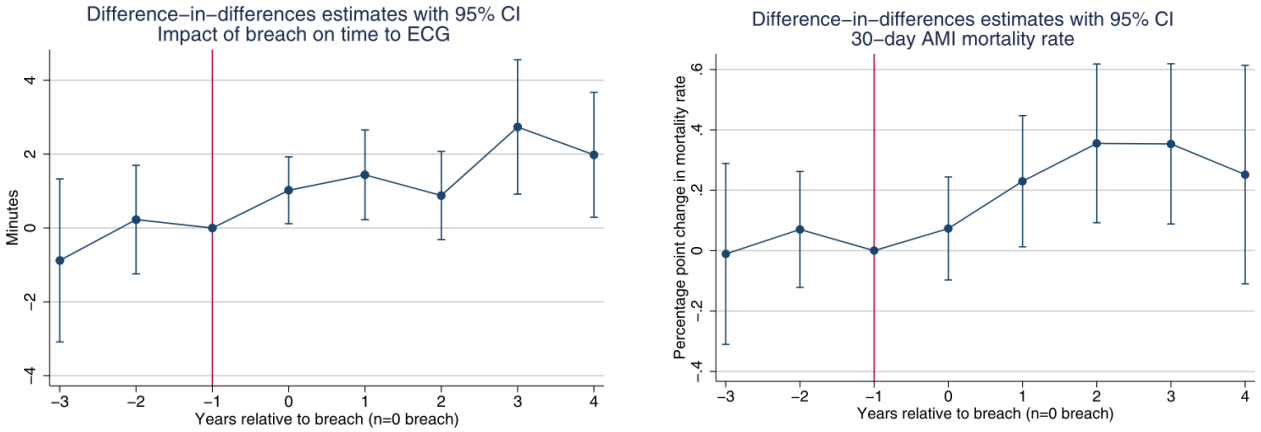
2019-ben az NHS-ben elvégezték az adatok szisztematikus, részletes elemzését. A legfontosabb vizsgált paraméterek a következők voltak: törölt járóbeteg-időpontok, tervezett és sürgősségi felvételek száma a kórházakba, baleseti és sürgősségi (A&E) megjelenések száma és a halálesetek száma az A&E-ben. A kiindulási értékhez viszonyítva a WannaCry támadás hete alatt nem volt szignifikáns a különbség, ha a teljes egészségügyi ellátórendszer szintjén értékelték az adatokat. A ransomware-vel fertőzött kórházakban azonban szignifikánsan kevesebb sürgősségi és tervezett felvétel történt: a napi felvételek mintegy 6%-kal csökkentek, 4%-kal kevesebb sürgősségi és 9%-kal kevesebb tervezett betegfelvétel valósult meg. A halálozásban nem találtak eltérést. Az elemzés szerint

további kutatásokra van szükség annak érdekében, hogy pontosabban megállapíthassuk a kibertámadások és az ezek révén keletkező információbiztonsági problémák hatásait a betegek és az ellátás biztonságára.

A jelenlegi magyar jogszabályi környezetben a Nemzetbiztonsági Szakszolgálat szervezeti keretei között működő Nemzeti Kibervédelmi Intézet (NKI) gyűjti azokat a rosszindulatú információbiztonsági eseményeket, amelyek az egészségügyi intézményeket érik. Ehhez azonban az események jelentése szükséges, ami esetleges, és sok esetben ezekre jóval az incidenseket követően kerül sor. Az események korai jelzése nemcsak a helyreállítást segíti, hanem segíthet a károkozó eredetének és szándékának kiderítésében, valamint a főbb sérülékenységek feltárása hozzájárul az egészségügyi intézmény információbiztonságának növeléséhez is. A fentiek miatt az NKI adatai nem tekinthetők reprezentatívnak, azonban 2020. első negyedévi adatok alapján elmondható, hogy a magyar egészségügyi intézményekben a zsarolóvírusok okozta támadások a harmadik leggyakoribb típusú támadást jelentik.

2.8. Az egészségügyi adatvisszaélések rendszerszintű hatásai

Az első nagyobb vizsgálat, amely az adatvisszaélések és a kórházi halálozások összefüggéseit kutatta, 2012 és 2016 közötti adatokat vizsgált. A 2019 októberében megjelent eredmények 3025 kórház klinikai eredményeit vetették össze az amerikai kormány által gyűjtött adatokkal (ezekre korábban már hivatkoztunk, Department of Health and Human Services publikus adatbázisa az 500 főnél nagyobb érintettségű adatvisszaélésekről). A vizsgálatokkal azt mutatták ki, hogy heveny szívizominfarktus (acut myocardialis infarctus – AMI) esetében a 30 napon belüli halálozások 100 000 lakosra vetítve 36-al nőttek, míg a beteg beérkezése és az EKG készítése közötti idő 2,7 perccel nőtt azokban a kórházakban, ahol voltak adatvisszaélések. Mindkét indikátor nagyon fontos paraméter a korai halálozás tekintetében (11. ábra). Az ok-okozati összefüggések kutatására még szükség van, azonban az valószínűsíthető, hogy azok a kórházak, ahol az adatvisszaélések előfordultak, rosszabb minőségű munkát végeznek, és ez emberi életekben is mérhető.



11. ábra: Az amerikai kormányzati és kórházi adatok alapján azokban a kórházakban, ahol valamilyen adatvisszaélés történt, megnőtt a heveny szívizomelhalásos betegek korai halálozása, és nőtt a beérkezés és első EKG készítés között eltelt idő

2.9. Összefoglalás

A fenti gyakorlati példákkal azt mutattuk be, hogy az információbiztonsági ismeretek és azoknak gyakorlati vonatkozásai hogyan érvényesülhetnek az egészségügyben, és hogyan járulhatnak hozzá közvetlenül az ellátás minőségének javulásához, illetve betegéletek megmentéséhez. A legfontosabb megállapításaink:

1. Az egészségügy és a technológiák elmúlt években bekövetkezett fejlődése nagyban hozzájárult az egészségügy adatgazdagságához. Ezek az adatok jelentős értéket képviselnek.
2. Az egészségügyben folyamatosan nő az adatokkal kapcsolatos visszaélések száma, ezért elektronikus információbiztonsági szempontból kiemelt területet jelent.
3. A szektorban dolgozó információbiztonsági szakértőként figyelemmel kell kísérni az orvosi eszközök és technológiák sérülékenységeit is, mert ezek kockázatot jelentenek a betegek ellátására, bizonyos esetekben az életükre.
4. A zsarolóvírusok különös veszélyt jelentenek, különösen az idő szorításában dolgozó egységek esetében (pl. sürgősségi osztály, intenzív osztály, diagnosztikai egységek).
5. A mesterséges intelligencia az egészségügyi kiberbűnözésben is megjelent, ami teljesen új, eddig nem ismert kihívásokat jelent az egészségügyi és az információbiztonsági szakemberek számára.

Jó felkészülést!

JOGSZABÁLYTÁR

3.1. Magyar jogszabályok

- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről https://net.jogtar.hu/jogszabaly?docid=99700047.tv
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről https://net.jogtar.hu/jogszabaly?docid=a0100108.tv
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól Elérhetőség: https://net.jogtar.hu/jogszabaly?docid=a1500222.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
- 2021. évi XCI. törvény a nemzeti adatvagyonról https://net.jogtar.hu/jogszabaly?docid=a2100091.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
- 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról; https://net.jogtar.hu/jogszabaly?docid=a1100038.kor
- 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
- 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.kor
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól https://net.jogtar.hu/jogszabaly?docid=a1600451.kor
- 1035/2012. (II. 21.) Korm. határozata - Magyarország Nemzeti Biztonsági Stratégiájáról https://net.jogtar.hu/getpdf?docid=A13H1139.KOR&targetdate=&printTitle=1139/2013.+%28III.+21.%29+Korm.+hat%C3%A1rozat&getdoc=1
- 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 Hatályon kívül helyezte: 2015. évi CCXXII. törvény 121. § (1) b) https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV
- 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 https://net.jogtar.hu/jogszabaly?docid=a1300026.kim

- 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/jogszabaly?docid=a1300065.kor
- 360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről Hatályon kívül helyezte: 374/2020. (VII. 30.) Korm. rendelet 22. § https://net.jogtar.hu/jogszabaly?docid=a1300360.kor
- 512/2013. (XII. 29) Korm. rendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról https://net.jogtar.hu/jogszabaly?docid=a1300512.kor
- 540/2013. (XII. 30) Korm. rendelet a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről https://net.jogtar.hu/jogszabaly?docid=A1300540.KOR
- 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről https://net.jogtar.hu/jogszabaly?docid=a1300541.kor
- 2015. évi CCXXII. törvény - Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól https://net.jogtar.hu/jogszabaly?docid=a1500222.tv
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről https://net.jogtar.hu/jogszabaly?docid=a1500041.bm
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről Hatályon kívül helyezte a 44/2017. (XII. 29.) BM rendelet. https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről https://net.jogtar.hu/jogszabaly?docid=A1500246.KOR
- 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
- 39/2016. (XII. 21.) EMMI rendelet az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról https://net.jogtar.hu/jogszabaly?docid=a1600039.emm
- 386/2016. (XII. 2.) Korm. rendelet az egészségbiztosítási szervekről https://net.jogtar.hu/jogszabaly?docid=a1600386.kor
- 257/2016. (VIII. 31.) Korm. rendelet - Az önkormányzati ASP rendszerről https://net.jogtar.hu/jogszabaly?docid=a1600257.kor
- 249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 148/2018. (VIII. 13.) Korm. rendelet az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet és az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet módosításáról https://net.jogtar.hu/getpdf?docid=a1600257.kor&targetdate=&printTitle=257/2016.+%28VIII.+31.%29+Korm.+rendelet

- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről https://net.jogtar.hu/jogszabaly?docid=A1800270.KOR
- 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 https://net.jogtar.hu/jogszabaly?docid=a1800271.kor
- 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról http://njt.hu/cgi_bin/njt_doc.cgi?docid=212067.363096

3.2. Európai Uniós jogi aktusok

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

- **Adat**: Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. [1]
- **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, amelynek lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben, vagy éppen szalagcímhirdetésekben – 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, amely alkalmas adatok megőrzésére, tárolására. Az Európai Parlament és a Tanács 2002/65/EK irányelve szerint, amely már tartós adathordozóként nevesít: olyan eszköz, amely lehetővé teszi a fogyasztó számára a személyesen neki címzett adatoknak a jövőben is hozzáférhető módon és az adat céljának megfelelő ideig történő tárolását, valamint a tárolt adatok változatlan formában történő megjelenítését. Így adathordozó a pendrive, a DVD, CD, SSD-kártya, amely alkalmas kisebb vagy nagyobb mennyiségű adat tárolására. [4]
- **Adatkezelés***:* Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése. [2]
- **Adatkezelő***:* Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja. [2]
- **Adatvédelem***:* A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások.[5]

- **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot, nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens. [2]
- **Adattal rendelkezés:** A birtokban tartás, az adat alapján további adat készítése, az adat másolása, sokszorosítása, a betekintés engedélyezése, a feldolgozás és felhasználás, a minősítés (biztonsági osztályba sorolás) felülvizsgálata, a minősítés (biztonsági osztályba sorolás) felülbírálata, a nyilvánosságra hozatal, a titoktartási kötelezettség alóli felmentés, a megismerési engedély kiadása. [5]
- **Adatokat érintő beavatkozás:** információs rendszerekben található digitális adatok törlése, károsítása, rongálása, megváltoztatása, eltávolítása vagy hozzáférhetetlenné tétele. A fogalom emellett magában foglalja az adatlopást, valamint a pénzeszközök, a gazdasági erőforrások, illetve a szellemi tulajdon eltulajdonítását is. [6]
- **Adatkifürkészés**: digitális adatok információs rendszeren belüli, oda irányuló vagy onnan kiinduló nem nyilvános továbbításának – így például az információs rendszerből kibocsátott, ilyen digitális adatokat hordozó elektromágneses jeleknek – a kifürkészése műszaki eszközökkel. [6]
- **Advanced persistent threat (APT)**: Magas szintű, tartós vagy más (és az anyagban is használt) 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 motívumok vezérlik az elkövetőket, a cél általában információszerzés, de előfordult már olyan támadás is, melynek célja a szabotázs volt. [7]
- **Aktív kiberbiztonság (Active Cyber Defence Cycle** – ACDC): Aktív kiberbiztonsági intézkedések gyűjtőfogalma. Az aktív kiberbiztonság négy nagyobb tevékenységből áll, ezek a fenyegetéselemzés és információgyűjtés (threat intelligence consumption); az eszközleltár és hálózatbiztonsági monitoring; az incidenskezelés; és a fenyegetés és környezet kezelése (threat and enviroment manipulation). [8]
- **Android**: Linux kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve. [9]
- **Application Programming Interface**: Alkalmazásprogramozási interfész, amely hozzáférést biztosít egy adott szoftver vagy eszköz utasításkészletéhez. [10]
- **ASP-szolgáltatás**: Az alkalmazásszolgáltató (Application Service Provider – ASP) központon keresztül olyan hardver- és szoftver-infrastruktúra, arra épülő keret- és szolgáltatási rendszer jön létre, amely által az önkormányzatok szakrendszeri és egyéb szolgáltatásokat vehetnek igénybe egymással integrált módon. [11]
- **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). [12]
- **Automatizált informatikai biztonsági vizsgálat**: Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre. [13]
- **Backdoor (hátsó ajtó) program:** A felhasználók számára általában nem látható elem, amely 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 rendszeradmi-

nisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként). [14]

- **Betörésdetektáló eszköz:** Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e, vagy sem. Fajtái a mintaalapú betörésdetektáló eszközök (signatura-based IDS) és a viselkedést vizsgáló betörésdetektáló eszközök (behavior-based IDS). Intrusion Detecting Systems (rövidítve: IDS). [15]
- **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. [16]
- **Biometrikus azonosítás**: Olyan eszközök és eljárások összessége, amelyek 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. [17]
- **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. [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. [18]
- **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 az etikus és az etikátlan hackerek között húzható meg. [19]
- **Bot-eszközök**: automatizált rendszerek, amelyek valamilyen tevékenységet hajtanak végre emberi beavatkozás nélkül. [20]
- **Célzott támadások** (Targeted Attacks): Célzott támadásoknak nevezzük az olyan fenyegetéseket, amelyeket 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. [15]

- **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]
- **Cleartext jelszavak**: Titkosítatlanul, szöveges formátumban tárol jelszavak. [20]
- **Cloud computing**: („számítástechnikai felhő", „felhőalapú informatika"): A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azokat nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhőalapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhőalapú informatikaalapon 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 felhőalapú szolgáltatástól szabadulni. [2]
- **CMS (Content Management System):** Más néven tartalomkezelő rendszer, olyan komplex webes környezet, ami lehetővé teszi, hogy tartalmainkat – webfejlesztő szakemberek segítsége nélkül – saját magunk, webes felületeken keresztül módosítsuk. [10]
- **CRM (Customer Relationship Manager)**: Olyan eszközök összessége, amelyek segítik a potenciális és meglévő ügyfelekkel való együttműködést, beleértve az ügyfélszerzéssel, marketinggel, értékesítéssel és ügyfélszolgálattal kapcsolatos tevékenységeket. [10]
- **Dead drop**: Az alkalmazott módszer lényege, hogy a kereskedő valamilyen nyilvánosan elérhető rejtekhelyen elrejti az árut, majd a rejtekhelyről értesíti a vásárlót, aki a rejtekhelyen felszedi a megvásárolt terméket. A dead drop módszer előnye, hogy teljesen aszinkron, azaz az értékesítő (vagy közvetítő) és a vásárló nem tartózkodik egy időben az átadási ponton, nem lehet a csomagokat követni vagy feltartóztatni, a vásárlónak nem kell kontakt vagy más személyes adatot megadnia a kézbesítéshez (pl. cím, postafiók stb.), így a kereskedőnek nem is kell ezeket az adatokat tárolnia és megvédenie, nem tudnak egymásra vagy egymás ellen vallani. [20]
- **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]

- **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**:
  a) az elektronikus hírközlésről szóló törvény 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 a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

  Egy elektronikus információs rendszernek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében az adatok, információk kezelésére használt eszközök - így különösen környezeti infrastruktúra, hardver, hálózat és adathordozók -, eljárások - így különösen szabályozás, szoftver és kapcsolódó folyamatok -, valamint az ezeket kezelő személyek együttesét. [1]
- **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]
- **Elektronikus hírközlő hálózat**: Átviteli rendszerek és – ahol ez értelmezhető – a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások – beleértve a nem aktív hálózati elemeket is –, amelyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára.[23]
- **Elosztott 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 számítógéprendszer 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]
- **ENISA (Európai Uniós Kiberbiztonsági Ügynökség):** az EU elsőszámú kiberbiztonsággal foglalkozó intézménye, a kiberbiztonsággal kapcsolatos tanácsadásért felelős ügynökség, amely információs és tudásközpontként működik. [21]
- **EPCIP (European Programme for Critical Infrastructure Protection):** a kritikus infrastruktúrák védelmére irányuló európai program, amelynek célkitűzése, hogy javítsa a létfontosságú infrastruktúrák védelmét az Európai Unióban. [21]
- **Ethernet**: A DEC, az Intel és a Xerox cégek által kidolgozott alapsávú LAN-ra vonatkozó specifikáció. Az Ethernet-hálózatok az ütközések feloldására a CSMA/CD-t használják. Számos kábeltípuson (csavart érpár, optika stb.) működik legalább 10 Mbps sebességgel). [22]
- **Europol:** Európai Rendőrségi Hivatal, amelynek fő feladata segítséget nyújtani az EU-s tagállamok bűnüldöző hatóságainak a terrorizmus elleni fellépésben, illetve a súlyos nemzetközi bűncselekmények felderítésében. [21]

- **Eseménykezelő Szakterület (Event Detection Team):** Intézmények közti megállapodás keretében a biztonság növelése érdekében folyamatosan monitorozza a hálózati forgalom különböző szegmenseit. A szakterület által végzett feladat preventív és detektív jellegű, hiszen alapvetően passzív adatforgalom-ellenőrzésről és annak elemzéséről van szó. A szisztematikusan összegyűjtött támadási kísérletek rendszerezett adatai alapján azonosíthatjuk a támadók által felhasznált internetes erőforrások címeit, másrészt – különböző elemző algoritmusok segítségével – felfedezhetjük a behatolási módszerek alkalmazási trendjeinek aktuális alakulását, valamint következtetéseket vonhatunk le az internetre épülő szolgáltatások hátterét nyújtó szoftverkörnyezet esetleges gyenge pontjairól, illetve sebezhetőségeiről. [21]
- **Exploit**: Olyan forráskódban terjesztett bináris program, adathalmaz vagy parancssorozat, amely alkalmas egy szoftver vagy hardver biztonsági résének, illetve hibájának kihasználására, így érve el a rendszer tervezője által nem várt viselkedést.[10]
- **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]
- **Folytonos védelem**: Az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [1]
- **Fluxus**: A fluxus a felületet metsző mágneses erővonalak mennyisége. [21]
- **Fuzzing**: Egy leginkábban automatizált módon végrehajtott szoftvertesztelési technika, amelynek során érvénytelen, véletlenszerű, illetve nem várt adatokat adunk meg a program bemeneteként, majd a kimenetet megvizsgálva próbáljuk megtalálni a sérülékeny pontokat. Ezzel a technikával főkent overflow, illetve DoS jellegű sérülékenységeket kereshetünk hatékonyan, miközben a szoftver kivételkezeléséről és robosztusságáról is képet kaphatunk. [10]
- **Gateway**: Átjáró, konverter eszköz, különböző protokollon kommunikáló eszközök között. [22]
- **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.
- **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, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadásokat, 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. [24]
- **Hálózat**: Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége. [5]

- **Hálózati és információs rendszer:** elektronikus hírközlő hálózat, vagy minden olyan eszköz vagy egymással összekapcsolt eszközök csoportja, amelyek digitális adatokat dolgoznak fel, valamint a tárolt, kezelt, visszakeresett vagy továbbított digitális adatok. [6]
- **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, amelyek ideiglenesen, vagy állandó módon csatlakoztathatok az eszközhöz. [25]
- **Hash függvények**: Olyan, elsősorban informatikában használt egyirányú eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Az így kapott véges adat neve *hash* érték. [10]
- **Hitelesség**: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [5]
- **Honeypot (csapdarendszer)**: Elsődleges célja az, hogy – valós működést szimulálva – elhitessék a támadókkal, hogy éles szolgáltatást nyújtó rendszert sikerült elérniük. Mindeközben azonban a jól felépített csapdarendszerek a támadó valamennyi tevékenységét letapogatják, módszeresen összegyűjtik, rögzítik és naplózzák. Tekintettel arra, hogy a csapdarendszer valójában nem működtet „igazi" szolgáltatást, a rajta észlelt valamennyi tevékenység jogtalannak minősíthető, azaz potenciális támadásként fogható fel. A csapdarendszerek tehát lényegében arra szolgálnak, hogy a támadók saját magukat leplezzék le egy olyan álcázott környezetben, ahol minden tevékenységük nyomot hagy. [26]
- **IKT-szolgáltatás**: Olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll. [21]
- **IKT-termék:** Valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja. [21]
- **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, amelynek 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. [25]
- **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]
- **Internet of Things (Iot)**: A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra és azok internetszerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt

felismerni, „mérni”, és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő, vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek. [27]

- **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.
- **Kémprogramok** (**spyware**): A rendszerbe jutva a háttérből figyelik a rendszerben lezajló eseményeket, amelyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [14]
- **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. [1]
- **Kiberfenyegetés**: bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat. [21]
- **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, amely rendkívül adaptív tulajdonsággal jellemezhető, 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. [28]
- **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]
- **Kombólista:** olyan gyűjtemény, amelynek a forrása nem ismert. Általában a kombólisták értéke meglehetősen csekély, több terabyte **méretben érhetők el különféle oldalakon vagy** szolgáltatásokban, például a Collections adatszivárgás jelentős része kombólista, csupán felhasználónevet és jelszót tartalmaz, amelyekről a legtöbb esetben nem lehet tudni, hogy honnan származnak, azaz hova lehet belépni ezekkel az adatokkal. [20]
- **Korai Figyelmeztető Rendszer (Early Warning System – EWS):** Az EWS az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának az ún. szenzorokkal történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményt. [26]

- **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.
- **Kritikus információk**: Azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük, hatékony tervezéséhez és végrehajtásához. [21]
- **Kritikus infrastruktúra**: azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotórészei, amelyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszú távon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére. [14]
- **Kvantumkriptográfia (Quantum cryptography):** Olyan technikák összessége, amelyekkel egy adott fizikai rendszer kvantummechanikai tulajdonságainak mérése révén –
- beleértve a kifejezetten a kvantumoptika, kvantumtérelmélet vagy kvantum-elektrodinamika által meghatározott fizikai tulajdonságokat is – közös „rejtjelezési" kulcs hozható létre. [31]
- **Létfontosságú információs rendszerelem**: Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené. [1]
- **Létfontosságú rendszerelem:** a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 1. mellékletben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, - és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.[32]
- **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. [14]
- **MFP (Multi-Functional Printer):** Olyan multifunkcós nyomtató, amely fénymásolóként, szkennerként, nyomtatóként és néha faxként is működik, miközben gyakran hálózatra csatlakoztatható. [10]
- **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. A „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása, nyilvánosságra hozatala bűncselekmény. [5][61]

- **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. [15]
- **Nemzeti adatvagyon**: a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.[33]
- **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. [15]
- **P2P: peer-to-peer** Olyan kommunikáció, ahol a szereplők kitüntetett csomópont vagy központi szerver nélkül, közvetlenül egymással kommunikálnak [20]
- **PDCA:** Plan-Do-Check-Act = Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás.
- **Port kopogtatás (port knocking):** Olyan módszer, amely segítségével megfelelő sorrendben próbálunk, előre meghatározott portokon keresztül kommunikálni, aminek hatására más portok is elérhetővé válnak. [10]
- **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. [34]
- **Rendelkezésre állás elve**: Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak. [5]
- **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

[61] Ld, bővebben Mavtv. 3.§ 1. pont

minimális víruseltávolító képességgel rendelkeznek – viszont annál több kártékony programot töltenek le a számítógépre. [18]

- **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]
- **Sérülékenységvizsgálat**: Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.[5]
- **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. [18]
- **SPF (Sender Policy Framework):** Egy olyan DNS rekord, amit annak igazolására használnak, hogy az email feladója, valóban a domén jogos tulajdonosa-e, illetve, hogy abból az IP-címtartományból történik-e az üzenet feladása, amelyből adott domén esetében ez lehetséges. [10]
- **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. [15]
- **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]). [35]
- **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]
- **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. [36]
- **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 számítógéprendszer 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]
- **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 me-

tódusát. Az SQL injection parancsokat küld a webszerverhez kapcsolt SQL-adatbázisnak. Ha a szerver nem megfelelően lett tervezve és erősítve, akkor az 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]

- **TCP/IP** = A TCP/IP betűszó az angol Transmission Control Protocol/Internet Protocol (átviteli vezérlő protokoll/internetprotokoll) rövidítése, mely az internetet felépítő protokollstruktúrát takarja. Nevét két legfontosabb protokolljáról kapta, a TCP-ről és az IP-ről. [22]
- **Teljes körű védelem**: Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [5]
- **TOR (The Onion Router)**: Ezen hálózat azzal biztosítja a felhasználók anonimitását, hogy hagymaszerűen felépülő, többrétegű titkosítást alkalmaz. Ez biztosítja, hogy maga a kommunikáció, sőt az egyes adatcsomagok útvonala hétköznapi eszközökkel nem fejthető vissza. A hálózatot TOR-klienst futtató gépek alkotják, ezek lehetnek node-ok vagy ún. TOR-exitek. [10]
- **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. [14]
- **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. [37]
- **UAV (Unnamed Aerial Vehicles):** Ember nélküli légi járművek. [38]
- Üzletmenet-folytonosság **tervezése**: 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]
- **Vezeték nélküli személyi hálózat (WPAN)**: A vezeték nélküli személyi hálózat célja tipikusan egy adott felhasználó közvetlen környezetében, néhány méteres távolságon belül levő intelligens eszközök összekötése egy rádiós interfész segítségével. [39]
- **Vírus**: A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve azáltal, 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 videólejátszó, 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 törölhetik vagy módosíthatják, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nemcsak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként, vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [14]

- **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]
- **Wardriving**: Eredetileg a nyílt, vagy gyengén védett WE- titkosítást használó wifi-hálózatok felkutatását jelentette, és GPS-adatokat is rögzítettek a hálózati paraméterekkel egy időben, hogy később adatbázisokban rögzítve az adatokat másokkal is megoszthassák az információkat. Manapság sokszor összemossák a piggybacking fogalmával, pedig a fontos különbség a kettő között, hogy az egyiknél publikus információkat gyűjtünk, a másiknál pedig engedély nélkül csatlakozunk is a hálózathoz, és adatforgalmat bonyolítunk rajta. [10]
- **Webalkalmazás tűzfalak (WAF):** olyan eszközök, melyek webalapú, illetve adatbázis-alapú támadások elleni védelmet nyújtanak azáltal, hogy mind a klienstől érkező, mind a kimenő forgalmat adott szabályok szerint elemzik, és a szabályokra való illeszkedés alapján blokkolják, átengedik, vagy módosítják. [10]
- **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, amely 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 jól. A perzisztens **változat során magán a webszerveren helyezik el a** szkriptet, amely egy weboldal minden megtekintésénél így lefut. Az ilyen módon történő rosszindulatú kódsor-elhelyezésre például a nem megfelelő beviteli védelemmel ellátott blogoldalak bejegyzései adnak lehetőséget. [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, amelyből később bármilyen adatot kinyerhet. [22]
- **Zárt védelem**: Az összes számításba vehető fenyegetést figyelembe vevő védelem. [5]

4.1. A fogalmak forrásjegyzéke

[1] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*.

[2] Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár*. Forrás: https://www.naih.hu/adatvedelmi-szotar.html (Utolsó letöltés: 2020. 09. 03.)

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

[4] *Az Európai Parlament és a Tanács 2002/65/EK irányelve (2002. szeptember 23.) a fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról.*

[5] Muha L. (2004): Fogalmak és definíciók. In *Az informatikai biztonság kézikönyve.* URL: http://lmuha.hu/defins.html (Utolsó letöltés: 2020. 09. 08.)

[6] Molnár A. (2019): Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége. In *Kritikus információs infrastruktúrák védelme.* Dialóg Campus Kiadó, Budapest.

[7] Sági G. (2017): Informatikai rendszer támadási folyamata. *Műszaki Katonai Közlöny,* URL: http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/015_Sagi_Gabor.pdf (Utolsó letöltés: 2020. 09. 08.)

[8] Tikos A. (2019): A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései. In *Kritikus információs infrastruktúrák védelme.* Dialóg Campus Kiadó, Budapest.

[9] Rédecsi M. – Tóth G.: (2013) *Android*. URL: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (Utolsó letöltés: 2020. 09. 11.)

[10] Arányi G. (2020): Sérülékenységvizsgálatok tapasztalatai a hazai kibertérben. In *Kibertéri fenyegetések.* Dialóg Campus Kiadó, Budapest.

[11] Jerabek Gy. (2020*):* Információbiztonság az önkormányzati szektorban. In *Az Ibtv. gyakorlata.* Dialóg Campus Kiadó, Budapest.

[12] Gyurák G. (2015): *Informatikabiztonság I.* Pécsi Tudományegyetem Műszaki és Informatikai Kar, Pécs.

[13] *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.*

[14] Haig Zs. – Kovács L. (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. URL: http://hdl.handle.net/11410/285 (Utolsó letöltés: 2020. 09. 11.)

[15] Marsi T. (2018): A célzott támadások és megelőzésük sérülékenységvizsgálattal. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[16] *A Big Data a hivatalos statisztikában*. 2016. URL: https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (Utolsó letöltés: 2020. 09. 08.)

[17] Mátrai J. (2016): *Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás*. URL: http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (Utolsó letöltés: 2020. 09. 08.)

[18] Oroszi E. (2008): *Social Engineering.* Budapesti Corvinus Egyetem, Budapest.

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

[20] Kocsis T. (2020): Történetek a Darknet mélyéről – Adatszivárgási esettanulmányok. In *Kibertéri fenyegetések.* Dialóg Campus Kiadó, Budapest.

[21] Bonnyai T. (2019): Kritikus információs infrastruktúra védelem. In *Kritikus információs infrastruktúrák védelme*. Dialóg Campus Kiadó, Budapest.

[22] Kaczur G. (2018): Spearphishing. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[23] *2003. évi C. törvény. az elektronikus hírközlésről.*

[24] Carabott, E. (2011): *Hacking Motivations – Hactivism*, URL: http://www.gfi.com/blog/hacking-motivations-hacktivism/ (Utolsó letöltés: 2020. 08. 22.)

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

[26] Marsi T. (2019): Incidenskezelés kritikus infrastruktúrák esetén. In *Kritikus információs infrastruktúrák védelme.* Dialóg Campus Kiadó, Budapest.

[27] Kóbor Á. (2014): *Mi az a „dolgok internete”?* URL: https://ithub.hu/blog/post/Mi_az_a_dolgok_internete/ (Utolsó letöltés: 2020. 09. 03.)

[28] Cser O. (2018): Célzott támadás a pénzügyi szektor ellen. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[29] Krasznay Cs. (2012): A polgárok védelme egy kiberkonfliktusban. *Hadmérnök*, 2012/4, URL: http://hadmernok.hu/2012_4_krasznay.pdf (Utolsó letöltés: 2020. 09. 11.)

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

[31] Tóth K. (2020): Az egészségügyi információs rendszerek információbiztonsága, In *Az Ibtv gyakorlata.* Dialóg Campus Kiadó, Budapest.

[32] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.*

[33] *2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.*

[34] Yaqoob, I. – Ahmed, E. – Imran, M. (2017): *The rise of ransomware and emerging security challenges in the Internet of Things.* Computer Networks, 6 September (2017), URL: https://doi.org/10.1016/j.comnet.2017.09.003 (Utolsó letöltés: 2020. 09. 11.)

[35] Bodó A. – Zámbó N.: A közreműködők kötelezettségei a célzott támadások elhárításában az ibtv. szerint. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[36] *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.*

[37] Gyaraki R. (2018): Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[38] Bódi A. (2020): Információbiztonság a közlekedés, mint létfontosságú rendszerelem esetén. In *Az Ibtv. gyakorlata.* Dialóg Campus Kiadó, Budapest.

[39] Haddad, R. (2019): Okoseszközök a kritikus információs infrastruktúrákban. In *Kritikus információs infrastruktúrák védelme*. Dialóg Campus Kiadó, Budapest.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert rektorhelyettes

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Dorogi Katalin

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-497-9 (PDF)