Incidensmenedzsment

Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2017

BERZSENYI DÁNIEL – ZÁMBÓ NÓRA

Nemzeti Közszolgálati Egyetem, Budapest

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

Szerzők:
Berzsenyi Dániel
Dr. Zámbó Nóra

Szakmai lektor:
Prof. Dr. Nemeslaki András

Olvasószerkesztő:
Császár-Biró Anna

A hatályosítást végezte:
Deák Veronika

A kézirat lezárásának dátuma:
2019. május 1.

Kiadja:

Felelős kiadó:
Prof. Dr. Kis Norbert
Dékán

TARTALOM

I. Berzsenyi Dániel: A kibertér aktuális nemzetközi biztonságpolitikai kihívásai 5

1. Bevezető gondolatok 5
2. Biztonsági trendek a kibertérben 6
3. Lokális folyamatokat érintő kiberbiztonsági kihívások 9
4. Regionális folyamatokat érintő kiberbiztonsági kihívások. 10
5. Globális folyamatokat érintő kiberbiztonsági kihívások 13
6. Kiberbiztonság a nemzetközi béke és biztonság tükrében 20
7. Irodalomjegyzék 21

II. Zámbó Nóra: Biztonsági eseménykezeléssel kapcsolatos elvárások a hazai és nemzetközi jogban 23

1. Bevezető gondolatok 23
2. Eseménykezelés a NIS irányelv tükrében 23
   2.1. A NIS irányelv és ami mögötte van 23
   2.2. A NIS eszközrendszere 27
3. Eseménykezelési elvárások a GDPR szabályozásában 30
   3.1. Fogalomrendszer 30
   3.2. GDPR alapok. 33
   3.3. Adatbiztonság és adatvédelmi incidens a GDPR-ban és a kapcsolódó szabályok 33
4. Eseménykezelés az Ibtv. és végrehajtási szabályai tükrében 38
   4.1. Alapfogalmak. 38
   4.2. AZ Eseménykezeléssel összefüggő szabályok. 39
   4.3. Az eseménykezelésben részt vevő nemzeti szervezetek 43
5. Intézkedési terv a biztonsági események kezelésére 45
6. Irodalomjegyzék 46
7. Jogszabálytár 46

Fogalomtár. 49

I. BERZSENYI DÁNIEL: A KIBERTÉR AKTUÁLIS NEMZETKÖZI BIZTONSÁGPOLITIKAI KIHÍVÁSAI

1. Bevezető gondolatok

Napjainkban egyre szélesebb körben ismert és elfogadott tény, hogy korunk biztonságpolitikai kihívásai között kiemelkedő szerepet töltenek be a kibertérből érkező kihívások, fenyegetések és veszélyek. Ennek legfőbb oka, hogy számuk folyamatosan növekszik, és a mindennapi életünk egyre több területén fejtenek ki egyre jelentősebb hatást, tehát a fenyegetési spektrum is dinamikusan tágul. Miközben az információs társadalomban természetesnek vesszük, hogy a kibertérből elérhető adatok és információk folyamatos növekedést mutatnak, sokak számára kevésbé nyilvánvaló, hogy ezeknek az adatoknak és információknak a megfelelő szintű védelméről is gondoskodnunk kell. Tovább súlyosbítja a helyzetet, hogy az infokommunikációs technológia fejlődése következtében egyre több társadalmi folyamat zajlik a kibertérben vagy annak felhasználásával, és a folyamatosan gyarapodó információkhoz egyre többféle módon és egyre többféle eszközzel férhetünk hozzá.

Korábban egy átlagos felhasználó számára a legnagyobb probléma az volt, ha óvatlansága miatt számítógépe vírussal fertőződött meg, és ennek következtében kéretlen reklámüzeneteket kapott, vagy átmenetileg nem tudott csatlakozni a hálózathoz. Idővel azonban kialakult egy olyan alapvető biztonságtudatosság, amelynek köszönhetően ma már a legtöbb számítógépes felhasználó számára egyértelmű, hogy a megfelelő célszoftverekkel (víruskereső, tűzfal) jelentős mértékben csökkenteni tudja kitettségét. Az elmúlt néhány évben viszont gyökeresen átalakult a kiberbiztonság helyzete nemcsak az egyéni, hanem nemzeti, regionális és globális szinten egyaránt. A jelenleg is tartó átalakulás rendkívül gyorsan és komplex módon zajlik. A kibertérben elérhető szolgáltatások dinamikus bővülése, az okos eszközök rohamos elterjedése, a gyártók felelőtlensége, a rosszindulatú felhasználók és az általuk alkalmazott módszerek gyarapodása, valamint a technológiai és tudástranszfer következtében mára egy átlagos felhasználó kitettsége sokszorosára nőtt a kibertérből érkező támadásokkal szemben. Napjainkban az imént említett célszoftverek, vagyis egy számítógépre telepített víruskereső és tűzfal kombináció az alapvető biztonság szavatolásához is kevés lehet, ha emellett nem gondoskodunk adataink, kommunikációs csatornáink és okos eszközeink védelméről, nem használunk megfelelő hosszúságú és bonyolultságú jelszavakat, több lépcsős azonosítási módszereket, és nem ismerjük fel időben az emberi hiszékenységen, illetve megtévesztésen alapuló támadásokat *(social engineering)*.

Az átlagos felhasználó jellemzően nincs tisztában azzal, hogy a kibertámadásokkal szembeni kitettsége mekkora mértéket ölt, és nem is lehet reális elvárás, hogy mindenki önmaga kiberbiztonsági szakembere legyen. Ugyanakkor a kiberbiztonsági tudatosság fejlesztésére és terjesztésére egyre jelentősebb igény mutatkozik, hiszen a kibertér sajátosságaiból fakadóan az egyén tájékozatlansága és felelőtlen felhasználói magatartása könnyedén megbéníthat egy egész szervezetet, de akár veszélyt jelenthet a nemzetbiztonságra is. A kibertérben nincsenek államhatárok, ahol ellenőrzést lehetne folytatni, az ott zajló események gyakran a másodperc tört része alatt következnek be, miközben hatásuk évekig eltarthat, a folyamatok attribútumainak bizonyító erejű meghatározása pedig a legtöbb esetben

rendkívül bonyolult, sokszor lehetetlen. Szintén eltér a hagyományos *(offline)* világunk szabályszerűségeitől, hogy a kibertérben a nemzetállamok korántsem egyeduralkodók, a társadalom megannyi szereplője megtalálható a multinacionális cégektől a szervezett bűnözői és aktivista csoportokon át egészen az egyéni felhasználóig. A kibertér említett jellemzői jól mutatják, hogy milyen sokszínű és bizonyos tekintetben mennyire eltérő a virtuális világ a hagyományoshoz képest.

A kibertér sajátosságait figyelembe véve a nemzetállamok a világon mindenütt próbálnak a hagyományos területekkel foglalkozó nemzetközi együttműködésekhez hasonló szövetségeket létrehozni a kibertér biztonságának szavatolása érdekében. Ezek az együttműködési kezdeményezések elsősorban az elmúlt évek kiberbiztonsági trendjeinek köszönhetők, amelyek rádöbbentették a kormányokat arra, hogy önállóan nem képesek megvalósítani a kibertér biztonságos használatának alapvető feltételeit. A kibertérhez kapcsolódó nemzetközi együttműködések legtöbbször a szabályozatlanság problémájára próbálnak megoldást találni, de egyre több a kiberbűnözés elleni határokon átnyúló összefogás, illetve a szellemi tulajdon védelmében és a kibertérben folytatott kémkedés ellen létrehozott multinacionális kooperáció. Magyarország több nemzetközi kiberbiztonsági kezdeményezésben is érintett egyrészt az euroatlanti szövetségi rendszerhez kapcsolódó beágyazottsága, másfelől az önálló, illetve harmadik fél általi regionális kezdeményezések révén. Utóbbiak közül kiemelkedő a 2013 májusában Ausztria és Csehország kezdeményezésére létrehozott Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform – CECSP), amelynek hazánk mellett Lengyelország és Szlovákia is tagja.

Annak érdekében, hogy egy szervezet különböző szintjein megjelenő kiberbiztonsági probléma kapcsán ne csak az aktuális kihívást lássuk és adott esetben az akut elhárításon, illetve „tűzoltáson" túl hosszabb távú megoldást lehessen kidolgozni, érdemes egy pillanatfelvételt készítenünk azokról a nemzetközi kiberbiztonsági trendekről, amelyekre az előző bekezdésben már utaltunk. A biztonságpolitikai megközelítés egyik alapja, hogy egy incidens vagy konfliktus kialakulása számos tényezőre vezethető vissza. Ezeknek a tényezőknek a feltérképezésében és azonosításában jelentős szerepe van a körülöttünk zajló lokális, regionális és globális folyamatoknak, amelyeknek értékelése és figyelemmel kísérése elengedhetetlen ahhoz, hogy a szükséges helyen és időben megfelelően felkészültek lehessünk. Az offline világunk hagyományos incidenseihez vezető út elemzése, az események monitorozása, illetve újabbak előrejelzése olyan tevékenység, amely teljes mértékben alkalmazható a kibertérre vonatkozóan is, így a kiberbiztonsági problémák kezelhetőbbé válnak.

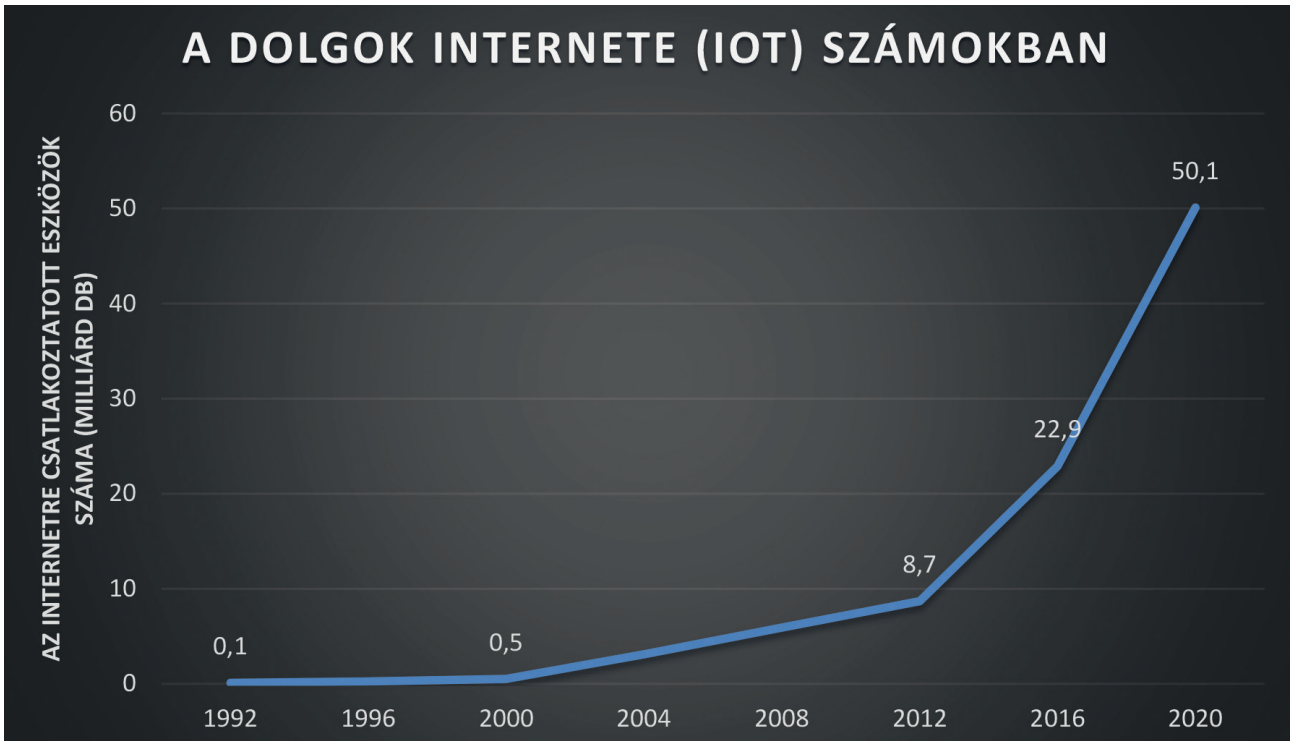
2. Biztonsági trendek a kibertérben

Amikor kiberbiztonsági kérdésekkel foglalkozunk, előbb vagy utóbb fontos szerepe lesz a kibertérben zajló folyamatoknak és trendeknek, illetve az ezeket számszerűsítő kimutatásoknak és statisztikai adatsoroknak. Például egy kiberbiztonsági incidens kapcsán az egyik elsőként felmerülő kérdés, hogy hány felhasználót vagy rendszert érint az adott eset. Annak érdekében, hogy tisztában legyünk az ember alkotta virtuális világ méretével, népességével és arányaival, ajánlott az aktuális trendeket áttekinteni. Számos forrás és adatsor található arra vonatkozóan, hogy hány ember él a világon és használja manapság az internetet, ugyanakkor az egyes földrajzi és gazdasági régiók között jelentős eltérések mutatkoznak több tekintetben is. Az egyik megbízható forrásnak számító Nemzetközi Távközlési Egyesület (International Telecommunication Union, a továbbiakban ITU) 2016 júniusában kiadott adatai szerint a világ lakosságának több mint fele továbbra sem fér hozzá az internethez. Ugyan az ITU szerint 2016 végére 3,9 milliárd főre csökkent azoknak a száma, akik nem használják az internetet, regionális bontásban például Afrikában a lakosság 75%-a nem fér hozzá a világhálóhoz, miközben Európában ugyanez az arány csupán 21%. Az adatok sajátos bemutatása az ENSZ Fenntartható Fejlődési Célkitűzéseihez köthető. Ha ugyanis megfordítjuk a megközelítést, azonnal látható, hogy 47%-os lefedettség mellett, globális szinten majdnem minden második ember hozzáféréssel

rendelkezik a világhálóhoz. Európában a háztartások 84%-a csatlakozik az internethez, miközben a széles sávú mobil előfizetések aránya meghaladja a 76%-ot. (ITU, 2016) A 738 millió fős európai lakosságra (UN ESA, 2015) vetítve ez több mint fél milliárd felhasználót jelent csak az öreg kontinensen. Tovább szűkítve a vizsgálati kört, Magyarországon a rendszeres internethasználók aránya eléri a 72%-ot (KSH, 2016), ami több mint 7 millió felhasználót jelent hazánkban.

Más megközelítésben érdemes elgondolkodni azon, hogy mi történik az interneten, ha egyetlen szűk perc keresztmetszetét próbáljuk megvizsgálni. Egy 2016 nyarán megjelent felmérés szerint gigantikus méreteket ölt a különböző online tartalmak generálása. A kutatási eredményeket publikáló jelentés „tartalomsokknak" nevezi a jelenséget, amelynek következtében a 2013-ban egy perc leforgása alatt elküldött e-mailek száma 182,9 millióról 2015-re 205,6 millióra nőtt. De hasonló adatokat mutat a legnépszerűbb internetes keresőmotor (Google) használata is: itt a 2013-as egy perc alatt indított 2,6 millió keresés 2015-re elérte a 3,1 milliót, míg a világelső közösségi oldalon (facebook) közzétett posztok száma 2,5 millióról 3,3 millióra nőtt. Ennél is jelentősebb a változás a legnépszerűbb közösségi videomegosztó (YouTube) oldal esetében, ahol 2013-ban egy perc alatt még csak 100 órányi videotartalmat töltöttek fel a felhasználók, 2015-ben viszont már 400 órányit. Szignifikáns a különbség az egyik népszerű azonnali üzenetküldő (WhatsApp) alkalmazás esetében is, amelynek segítségével a felhasználók 2013-ban még 11,8 millió üzenetet küldtek egy perc leforgása alatt, 2015-ben viszont már 44,4 millió üzenetet továbbított ugyanez az alkalmazás percenként. (Hubspot, 2016) Az említett adatok azt mutatják, hogy jelentős és folyamatos növekedés mutatkozik mind a felhasználók számában, mind pedig a felhasználás mértékében. A kiberbiztonság jelentőségének megértéséhez további folyamatokat is feltétlenül figyelembe kell venni, amelyek közül kettő egymással összefüggő tendenciát fontos kiemelni.

Korábban már szóba került, hogy a mindennapi életünk során egyre több szálon kapcsolódunk a virtuális világhoz. Míg korábban elsősorban az asztali vagy hordozható számítógépünk segítségével kommunikációra használtuk a kiberteret, később pedig pénzügyi tranzakciók lebonyolítására vagy multimédiás tartalmak fogyasztására, ma már egyre több eszközünk kapcsolódik a kibertérhez, amelyek a legkülönbözőbb funkciókon keresztül képesek digitalizálni mindennapjainkat. Gondoljunk a manapság oly divatos okos eszközökre (telefonok, televíziók, karórák, stb.), amelyek mindegyike egy-egy újabb szálon kapcsol bennünket a kibertérhez. Az okos eszközök által dominált virtuális világ angol elnevezése az Internet of Things (IoT), vagyis a dolgok internete, és jóval túlmutat a ma elterjedt okos eszközök képességein és lehetőségein. A dolgok internete tulajdonképpen nem más, mint hálózatba kapcsolt eszközök, járművek, épületek és egyéb ember alkotta tárgyak, amelyek a beépített elektronikának, szoftvereknek és szenzoroknak köszönhetően képesek egymással kommunikálni a hálózati kapcsolataikon keresztül. Távoli eléréssel a hálózaton keresztül érzékelhetők és irányíthatók ezek az eszközök, aminek köszönhetően egyre inkább elmosódik a határ a fizikai és a virtuális világ között. Az ITU 2012-ben kiadott ajánlása értelmében az IoT nem más, mint az információs társadalom infrastruktúrája. (ITU, 2012) Az előrejelzések alapján az IoT térnyerése következtében robbanásszerűen megnövekszik az internethez csatlakoztatott dolgok (eszközök) száma az elkövetkező néhány évben. Már most is közel 23 milliárd eszköz csatlakozik az internethez globális szinten, de ez a szám 2020-ra elérheti, sőt nagy valószínűséggel meg is haladja majd az 50 milliárdot. Ez azt jelenti, hogy a világ 7,4 milliárd lakójára vetítve már ma is minden földlakó három különböző eszközzel éri el az internetet.



1. ábra: Az internetre csatlakozó eszközök száma 2012 után kezdett igazán dinamikus növekedésbe, aminek eredményeként 2020-ra több mint 50 milliárd eszközzel csatlakozunk a virtuális világhoz1

A IoT térhódítása több szempontból is megállíthatatlannak tűnik. Az internetre csatlakoztatott eszközök száma már 2008-ban meghaladta a Föld népességének számát (Evans, 2011), 2017-ben pedig az IoT eszközök piaca nagyobb lesz, mint az asztali számítógépek, tabletek és telefonok piaca együtt. (Business Insider, 2014) Ez számokban kifejezve azt jelenti, hogy a 2013-as 1,9 billió dolláros szintről 2020-ra az IoT piac 7,1 billió dollárra nő. (The Economic Times, 2015) Hamarosan olyan hétköznapi használati tárgyaink és eszközeink is kapcsolatban lesznek a kibertérrel, mint az autónk, a háztartási eszközeink (hűtő, mosógép, sütő, kávéfőző stb.), vagy akár az otthonunk teljes gépészeti, elektromos és egyéb rendszerei.

A másik kiemelendő folyamat tulajdonképpen nem más, mint a fenti trendek árnyoldala, amellyel ma még a kiberbiztonsági szakembereken kívül meglehetősen kevesen foglalkoznak. A legtöbb felhasználóban nem tudatosul, hogy az internetre kapcsolódó eszközök számának növekedésével együtt növekszik az a támadási felület is, amin keresztül a rosszindulatú felhasználók károkat okozhatnak. Jó példa erre a világ egyik legjelentősebb kiberbiztonsági konferenciája a DefCon, ahol 2016-ban 21 gyártó 23 eszközében összesen 47 sérülékenységet mutattak be a résztvevők. (Mészáros, 2016) Ugyanakkor a már jelenleg is kiterjedt támadási felület nagyságát jól szemlélteti egy 2015-ben megjelent tanulmány, amely azt vizsgálta, hogy milyen szintű Magyarország kiberbiztonsági kitettsége az internethez csatlakozó ipari folyamatirányító rendszerek tekintetében, amelyek jellemzően erőművek vezérléséért, a közüzemi szolgáltatások működéséért, vagy éppen különféle gyártósorok üzemeltetéséért felelősek. A tanulmányban bemutatott, 4 és fél óra alatt elvégzett mérés eredményei szerint 6100 olyan támadási pont volt található a kibertérben, amelyen keresztül a hazai szolgáltatások és infrastruktúrák működése megzavarható vagy leállítható lett volna és milliós nagyságrendűre becsülhető azoknak a sérülékenységeknek a száma, amelyek kritikus infrastruktúrákat irányító rendszerekben találhatók. (Berzsenyi–Ványi, 2015).

[1] Forrás: A CompTIA Projecting the 'Things' Behind the Internet of Things grafikonja alapján szerkesztette a szerző. Az eredeti grafikon elérhető: blogs-images.forbes.com/gilpress/files/2016/08/Slide2.jpg?width=960 (utolsó letöltés: 2016. november 4.)

A bemutatott példák és adatok a kiberbiztonsági trendeket csak nagy vonalakban ábrázolják, azonban a bevezetőben leírt dinamikus növekedést, a kibertér hódítását és a kihívások párhuzamos növekedését jól alátámasztják. Az egyre nagyobb kitettség következtében új szegmensek jönnek létre a különböző iparágakon belül, amelyre jó példa az egyelőre főként nagyvállalati környezetben terjedő kiberbiztosítás. Az egyik legújabb biztosítási piac lényege, hogy a vállalatok az egyre jobban elterjedő digitalizált folyamatok következtében olyan veszélyekkel és veszteségekkel szemben is szeretnének fedezetet, amelyek a kibertérből érkeznek. A kibertámadások személyre, iparágra, nemzetre való tekintet nélkül mindenkit fenyegetnek, az összes kapcsolódó kihívás áttekintése jelen esetben a teljes tankönyv határain is nagyságrendekkel túlmutatna, így a rendelkezésre álló kereteket a legfontosabb és leginkább aktuális nemzetközi biztonságpolitikai vonatkozású kiberbiztonsági kihívások bemutatására használjuk fel.

3. Lokális folyamatokat érintő kiberbiztonsági kihívások

Sokakban valószínűleg már az alcím olvasása közben felmerül a kérdés, hogyan kerülhetnek lokális folyamatok egy alapvetően nemzetközi biztonságpolitikai kihívásokat tárgyaló fejezetbe. A kérdés jogos, és egyszerű rá a felelet: a választások külföldi befolyásolása. A fejlett nemzetek számára – választási rendszertől függetlenül – a demokratikus választás és annak külső behatás nélkül történő lebonyolítása az államiság egyik alapját jelenti. De az államok belügyeibe történő külső beavatkozás nemcsak a demokratikus elvek mentén működő államok problémája. Bármely állam számára a 21. század első felének egyik legnagyobb kihívása, hogy a belső politikai folyamatait miként óvja meg a külső befolyásolástól. A befolyásolás nem új keletű a nemzetállamok között, régóta működik szabályozott és szabályozatlan keretek között egyaránt. Ami az újdonságot jelenti, az a kibertér szerepének jelentős megnövekedése. Az említett befolyásolásnak egy új dimenzióját láthatjuk napjainkban, az Amerikai Egyesült Államokban lezajlott 2016-os választásokat követően, illetve a 2017-es francia választások közben. Nagy valószínűséggel az elkövetkező évek során nem lesz olyan választás, amit ne érintene valamilyen szinten a kibertérből érkező kihívás. Legyen szó a választási adatok megváltoztatásáról, a választási kampányba történő beavatkozásról, vagy a szemben álló felek politikai ellehetetlenítéséről, a legtöbb állam egyelőre csak keresi azokat a megoldásokat, amelyek segítségével a kibertérből érkező kihívásokat minimalizálni lehetne a választásokkal összefüggésben.

Az Amerikai Egyesült Államokban lezajlott legutóbbi választások során a kibertérnek, illetve a kibertérből érkező fenyegetéseknek igen nagy jelentőséget tulajdonítottak az egész világon. Mivel az USA továbbra is az első számú katonai hatalom, szerte a világon nagy figyelemmel kísérték a választási kampányt és az azt megelőző eseményeket. Bár a mai napig több „kibertámadásként” emlegetett esemény bizonyítatlan, illetve a részletek ismeretlenek, a befolyásolásra utaló jelek mértéke akkora, hogy nem lehet őket figyelmen kívül hagyni. 2016. június közepén hozták nyilvánosságra az első olyan információkat, amelyek arra utaltak, hogy a választásokat is érintő kiberbiztonsági incidens történt a Demokrata Nemzeti Bizottságnál (Democratic National Committee, a továbbiakban DNC). Rövid időn belül a feltételezett tetteseket is bejelentik, miszerint az elkövetők az orosz kormányhoz köthető Fancy Bear, illetve Cozy Bear néven ismert hackercsoportok. Néhány nappal később a Wikileaks portál mintegy 20 000 DNC szerverekről származó e-mailt hoz nyilvánosságra, amire válaszként az Amerikai Egyesült Államok Szövetségi Nyomozó Irodája (Federal Bureau of Investigation, a továbbiakban FBI) nyomozást indít. Néhány héttel később, 2016. augusztus közepén a DNC vezetőinek adatai szivárognak ki, majd a nyár hátralevő része kölcsönös nyilatkozatháborúba fullad az orosz fél, illetve a két amerikai elnökjelölt és stábjaik között. Már javában fut az amerikai elnökválasztási kampány, amikor újabb 58 000 üzenet kerül nyilvánosságra a Wikileaks jóvoltából, egyenesen a demokrata jelölt kampányfőnökétől. 2016 őszére az amerikai hatóságok egybehangzóan Oroszországot nevezik meg a választások körül kialakult helyzet okozójaként, azonban a motiváció

tekintetében bizonytalanság mutatkozik. Az elindított vizsgálatoknak köszönhetően kiderül, hogy a DNC sorozatos hibákat követett el és nem az elvárható módon reagált a kiberbiztonsági incidensekre, ami hozzájárulhatott a támadások sikeréhez. A választások körül kialakult botrány következtében végül az USA szankciókat vezet be Oroszországgal szemben, és 35 orosz diplomatát 72 órás határidővel kiutasítanak az országból. A titkosszolgálatok vizsgálati eredményei alapján a választásokat közvetlenül nem befolyásolták, a szavazógépek és a szavazások lebonyolításához használt számítógépek nem kompromittálódtak.

A 2017-es franciaországi választások során is történt olyan esemény, amely a választások kibertámadásokkal szembeni kitettségére hívja fel a figyelmet. 2017. április 25-én a Trend Micro nevű cég elemzői bejelentették, hogy bizonyítékokkal rendelkeznek arra vonatkozóan, hogy a francia elnökválasztási kampány egyik jelöltjét és stábját támadja a Fancy Bear (APT28) néven ismert hackercsoport. A támadás kapcsán kiadott jelentés szerint célzott adathalász e-maileket kaptak a kampánystáb tagjai, amelyek a politikai mozgalom honlapja helyett fertőző oldalakra irányították a felhasználókat. A támadók figyeltek arra is, hogy a támadáshoz használt weboldalakhoz az eredeti oldalak címeihez hasonló neveket használjanak. Ezt követően május 6-án több ezer e-mail vált nyilvánosan elérhetővé az En Marche! mozgalom belső levelező rendszeréből. A mozgalom közleménye szerint a kampánystáb egy kiterjedt és összehangolt hackertámadás áldozatává vált, aminek következtében számos belső információ került be a közösségi médiába. Az áldozatok külön kiemelték, hogy több dokumentum is úgy terjed a világhálón, hogy az eredeti szövegrészeket fiktív elemekkel keverték össze, így alkalmassá téve azokat a megtévesztésre és a súlyos dezinformáció terjesztésére.

A választások befolyásolására irányuló kísérletek minden jel szerint a következő évek velejárói lesznek, ezért fontos lenne, hogy a problémával nemzetközi szinten foglalkozzanak az érintett felek. 2017-ben tartanak még egy Európai Uniós viszonylatban jelentősnek számító választást Németországban, 2018-ban pedig Magyarországon is választások lesznek. Németország jelentős erőkkel készül a választások kibertámadásokkal szemben történő megvédésére, aminek egyik publikus jele, hogy a német Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz, a továbbiakban BfV) vezetője nyíltan beszélt egy konferencián a befolyásolásról és az egyre agresszívabbá váló kiberkémkedési tevékenységről. A német hatóságok ellehetetlenítik, szükség esetén működésképtelenné teszik azokat a szervereket, amelyeknek az üzemeltetői, illetve tulajdonosai nem képesek garantálni, hogy azokat ne használják fel kibertámadásokhoz. (Rettmann, 2017) Amennyiben a német választásokat valóban kibertámadás éri valamilyen formában, és a német hatóságok a bejelentésnek megfelelően járnak el, ez lehet az első olyan nyilvános eset, ahol egy állam támadóképességeket vet be és visszatámad (hackback) a kibertérben.

Az elmúlt időszak lokális folyamatait érintő kiberbiztonsági kihívásai kapcsán jól kirajzolódik, hogy még az olyan állami belügynek számító eseményeknél is, mint a demokratikus választások, gyakran elmosódik a határ a nemzetállami szint és a nemzetközi dimenzió között.

4. Regionális folyamatokat érintő kiberbiztonsági kihívások

Általánosságban elmondható, hogy egyre inkább jellemző az, hogy a konfliktusok által sújtott régiókban az egymással szemben álló felek a kibertérben is aktív tevékenységet folytatnak. A biztonságpolitikai elemzők az elsők között szokták említeni a 2008-ban Oroszország és Grúzia között lezajlott fegyveres összecsapást, amelynek nemcsak az előkészítése során, hanem a katonai műveletek ideje alatt és azt követően is jelentős szerep jutott a kibertérben folytatott műveleteknek. A fegyveres harcokhoz képest hetekkel korábban megindultak az elosztott szolgáltatásmegtagadással (Distributed Denial of Service, a továbbiakban DDoS) járó támadások, számos honlap és szerver vált hosszabb-rövidebb időre elérhetetlenné és erősen akadozott a kommunikáció az érintett területeken. A támadók gyakorlatilag információs blokád alá vették Grúziát. 2008-ban a grúz kormány a támadások elkövetésével az

oroszokat vádolta meg, azonban az orosz kormány szóvivője a vádakat azzal hárította, hogy lehetnek olyan hazafias magánszemélyek Oroszországban, akik így nyilvánítják ki véleményüket. A Torontói Egyetem egyik szakértője az eseményeket követően azt nyilatkozta, hogy „méretét és a nemzetközi dimenziókat figyelembe véve mérföldkő a támadás". (Hart, 2008) Korábbról valóban nem tudunk olyan példát felhozni, amikor egy reguláris erőkkel vívott küzdelmet az előkészítéstől a lezárást követő időszakig ilyen volumenű kibertevékenység kísér. Egy biztosan látszott már a 2008-as eseményeket követően is: a kibertámadások olcsón és egyszerűen kivitelezhetők, néhány száz számítógép és pár képzett hacker elegendő ahhoz, hogy egy országot blokád alá vonjanak a kibertérben. Szintén jól kirajzolódott, hogy nem pusztán a kommunikáció bénítása volt a támadók célja, hanem a kommunikáció kontrollja is, vagyis ebben az esetben az orosz támadásokat előkészítő és segítő propaganda terjesztése. Bár jó esély van arra, hogy soha nem derül ki teljes bizonyossággal a támadók kiléte, a konfliktusok legalapvetőbb szabálya, hogy mind a támadó, mind a védő fél egyértelműen azonosítsa a másik felet. A fegyveres konfliktusokat szabályozó hadijog mindezt részletesen kifejti, azonban olyan időket élünk, amikor a felek azonosítása nemcsak a fizikai világban válik egyre nehézkesebbé a gerilla-hadviselés, illetve a terrorista módszerek elterjedése miatt, de a kibertér sajátosságaiból fakadóan szinte lehetetlen meghatározni, hogy egy-egy kibertámadás mögött egy másik nemzet, egy politikai csoportosulás, vagy esetleg bűnszervezet áll-e. 2008 óta ez a terület szinte érintetlen maradt, nem igazán sikerült sem technikai, sem szabályozói oldalról olyan megoldásokat kidolgozni, amelyek a kibertámadások elkövetőinek felelősségre vonását és a bizonyítást elősegítenék.

Ugyanakkor nem feltétlenül kell egy konfliktusnak a fegyveres összecsapásokig jutniuk ahhoz, hogy valamelyik fél kibertámadáshoz folyamodjon. Kiváló példa erre a bő egy évvel korábban, 2007 tavaszán történt észtországi kiberkonfliktus, amelynek kirobbantásával szintén Oroszországot vádolták meg. A kibertérben végrehajtott műveleteket 2007. április 27-én az észt fővárosban, Tallinnben kitört zavargások előzték meg, amelyek egy szovjet hősi emlékmű elköltöztetése miatt alakultak ki. Ebben az esetben is DDoS támadások játszották a főszerepet, amelyek néhány nappal a tüntetéseket követően kezdődtek és alapvetően észt kormányzati hivatalokat, minisztériumokat és a parlamentet vették célba. Ugyanakkor számos pénzügyi intézmény, telekommunikációs vállalat és médiacég szerverei is megbénultak. Akkoriban a célpontok kiválasztása, a támadások előkészítettsége és precíz végrehajtása, valamint volumene egyformán arra utalt, hogy átlagos hackereknél komolyabb erők állnak a háttérben, vagyis egy nemzetállam által támogatott támadásról volt szó, ami a tallinni események nyomán leginkább az oroszoknak állhatott érdekében. Bár a világon a sajtó mindenütt úgy tálalta az események következményeit, mintha azok katasztrofálisak lennének az észt társadalomra nézve, ha Tallinnben járunk, és egy kicsit utánakérdezünk, hamar kiderül, hogy az átlagemberek életében korántsem okozott akkora fennakadást a támadássorozat, mint azt kívülállóként gondolnánk. A nagyjából két hét alatt 128 túlterheléses támadást regisztráltak, amelyek között volt, amelyik csak néhány óráig tartott, és volt, amelyik napokig, továbbá számtalan oldalt feltörtek és módosították azt jellemzően valamilyen oroszbarát tartalommal. Mivel Észtország ekkor már négy éve a NATO tagja volt, viszonylag gyorsan felmerült a kérdés, hogy katonai akciónak minősíthető-e a kibertérben végrehajtott támadás, és ilyen esetben is érvénybe léptethető-e a NATO 5. cikkely szerinti segítségnyújtás a többi tagállam részéről. De akkoriban nem mutatkozott egyetértés ebben a kérdésben, így a NATO-szakértők nem minősítették katonai támadásnak az esetet.

Nem kérdéses azonban a jelenlegi ukrán konfliktus kapcsán, hogy katonai műveletekről van szó. Az orosz fél érintettsége itt is erőteljes, azonban Oroszország hivatalosan nem ismeri el, hogy katonai hírszerzőkön kívül komolyabb erőt alkalmazna egy másik állam területén. Bár a 2015 végén az ukrán energetikai rendszer ellen elkövetett kibertámadások széles körben ismertté váltak, az Ukrajnában zajló fegyveres konfliktusról kevésbé ismert, hogy a grúz esethez hasonlóan aktív kiberműveletek zajlanak a háttérben. A 2014-es ukrán választásokig nyúlnak vissza az ismét Oroszország számlájára írt kibertámadások, amelyek elsőként a választási bizottságot célozták annak érdekében, hogy az eredményeket befolyásolni lehessen. Az akkori hírek szerint a támadás olyan sikeres volt, hogy még a biztonsági mentéseket is sikerült tönkretenni. Végül a szavazást segítő rendszerek működtek, de

a választási bizottság honlapján a támadóknak sikerült meghamisított eredményeket elhelyezniük, amelyeket azután a média is átvett. Mindez persze a választás eredményét végül nem befolyásolta, azonban a kormányzat és a közigazgatási szervek integritását, valamint a beléjük vetett bizalmat jelentősen rombolta. A választások támadását követően az ukrán bankrendszert, a vasúthálózatot és több bányaipari céget is támadás ért. Az ukrán vezetés mindvégig Oroszországot tette felelőssé a kibertámadásokért, az oroszok pedig szokás szerint tagadták a vádakat. Felmerült az is, hogy Oroszország a katonai műveletek során olyan hatékonyan alkalmazta kibertámadási képességeit, hogy az Ukrán hadsereg tüzérségének jelentős veszteségei is ennek köszönhetők. A bizonyítás itt is elmarad, ráadásul a szakértők között sincs egyetértés abban, hogy az ukránok súlyos tüzérségi veszteségei és az oroszok által a kibertérben folytatott műveletek között valóban összefüggés mutatható ki. Egyes elemzők szerint az Ukrajna ellen bevetett kiberfegyvereket ugyanaz az orosz állami támogatással működő és az orosz katonai titkosszolgálathoz kötődő Fancy Bear (APT28) néven ismert csoport alkalmazza, amelynek az Amerikai Egyesült Államokban a DNC megtámadását is tulajdonítják. Pro és kontra számos érvvel találkozhatunk, azonban a támadó kilététől függetlenül is kijelenthető, hogy az ukrán konfliktusban jelentős szerephez jutott ismét a kibertér, illetve az ott folytatott műveletek.

Idő közben, 2016 nyarán a NATO elismerte a kiberteret a háború, illetve a hadviselés ötödik dimenziójaként, ami jelentős előrelépés több tekintetben is. Egyfelől a szövetség keretein belül ezentúl a kiberképességek fejlesztésére a többi dimenzióhoz (szárazföld, tenger, levegő, világűr) hasonlóan lehet célzott fejlesztéseket kialakítani és forrásokat allokálni, másfelől a kibertérből érkező támadások katonai akcióként történő elismerése egyértelműbb. Ha a kibertérből érkező támadás akár emberélet, akár gazdasági károk tekintetében felér egy fizikai támadással, akkor előfordulhat, hogy arra válasz is érkezik, és adott esetben nemcsak a kibertérben, hanem fizikai csapás formájában. Bár nem a NATO hajtotta végre, de a kibertérben zajló folyamatokra adott fizikai válaszokra jó példa az Iszlám Állam első számú hackereinek az USA által történő felkutatása és likvidálása drónok segítségével.

A biztonságpolitikai elemzők számára kirajzolódó trendek azt mutatják, hogy a folyamatos kapacitás és képességbővülés a kibertérben nagyon élénkké vált az utóbbi években. Sok esetben hosszú évek fejlesztései és ráfordításai kezdenek láthatóvá válni és egyre több azoknak az államoknak a száma, amelyek a kibervédelmi képességek mellett támadóképességeket is fejlesztenek. Ilyen tekintetben jelenleg a top 5 ország között találjuk Oroszországot, Kínát, Iránt, Észak-Koreát és az USA-t, de egyre meghatározóbb képességekre tesz szert Izrael, Pakisztán, illetve India is. A folyamatok egyértelműen azt mutatják, hogy egyfajta kiber fegyverkezési verseny van folyamatban, ami természetesen nem az utóbbi néhány év eredménye. Pusztán arról van szó, hogy a felhalmozott képességek nyílt bevetése és alkalmazása nyomán többé már a felszín alatt zajlanak ezek a folyamatok.

A kiberbiztonság különböző szegmenseit tárgyalva észre kell vennünk a kapcsolódási pontokat az adatvédelem területéhez, ahol szintén komoly regionális folyamatok zajlanak elsősorban az Európai Uniónak köszönhetően. Az EU-ban már eddig is számos rendelkezés biztosította a személyes adatok védelmét, de 2018. május 25-től új szintre emelkedik az adatvédelem az EU területén. Az új adatvédelmi szabályozás megalkotásának egyik oka az volt, hogy az érvényben lévő szabályozás egyre kevésbé alkalmazható a rohamos léptekben fejlődő információs társadalomban zajló folyamatokra. Az új szabályozás kialakításának másik oka az volt, hogy az EU döntéshozói meg kívánták erősíteni a magánszemélyek online szolgáltatásokba vetett bizalmát, illetve az online környezettel jobban harmonizáló, korszerű adatvédelmi jogszabályt szerettek volna létrehozni.

Az EU Általános Adatvédelmi Rendelete (General Data Protection Regulation, a továbbiakban GDPR) minden tagállamban, így hazánkban is adatvédelmi reformmal jár együtt és minden személyes adatot kezelő szervezetre kiterjed. Többek között a GDPR-nak köszönhetően módosul hazánkban az adatvédelmi törvény, a Kiberbiztonsági Stratégia, valamint az Információbiztonsági törvény, és azok a vonatkozó részletszabályok, amelyek nincsenek összhangban az EU-rendelettel. A rendelet szövege szerint a hatálybalépést követően minden ügyfél élhet az adatok hordozhatóságához és a felejtéshez fűződő jogával, ami azt jelenti, hogy egyfelől kérhetik szolgáltatójukat, hogy adataikat adja át másik szolgáltatónak, másfelől jogosultak a személyes adatok indokolatlan késlekedés nél-

küli törlését kérni. További újdonság az úgynevezett profilalkotás tiltásának joga, továbbá 2018-tól biztosítani kell az ügyfél számára a betekintés jogát. A rendelet egyik fontos és az elmúlt évek tömeges felhasználói adatlopásait figyelembe véve (gondoljunk csak az OPM, vagy a Yahoo botrányra), kiberbiztonsági szempontból is jelentős passzusa, hogy a személyes adatot álnéven kell tárolni pont azért, hogy a felhasználói adatokat tartalmazó adatbázis kompromittálódása esetén a személyiségi jogok ne sérülhessenek. A rendelet megalkotói megelőző intézkedéseket is előírnak, így minden olyan szervezet köteles adatvédelmi hatástanulmányt készíteni, amely jelentős mennyiségű személyes adatot kezel, illetve amelynél az érintettek adatai veszélyben lehetnek. Lényeges pont, hogy 2018-tól a szervezetek kötelesek az adatvédelmet, illetve a felmerülő költségeket beépíteni az üzleti folyamataikba és a rendszerek tervezésébe egyaránt. Szintén az elmúlt évek milliós és milliárdos nagyságrendű adatvesztéseinek egyik sajátosságát kívánják a rendelet megalkotói felszámolni azzal, hogy incidens esetén arról legkésőbb 72 órán belül értesíteni kell a nemzeti adatvédelmi hatóságokat. Az érintettekre nézve jelentős kockázat esetén azokat is kötelező tájékoztatni, akiknek az adatait az incidens érinti. Az EU súlyos szankciókat helyezett kilátásba bírság formájában, amelyek egységes mértékűek lesznek mindenütt és a legsúlyosabb incidensek esetén elérhetik a társaság árbevételének 4%-át, amit 20 millió euróban maximalizáltak.

Összességében a GDPR az egyik legfontosabb eleme az Európai Unió kiberbiztonság terén tett erőfeszítéseinek, hiszen olyan egységes, minden tagállamra kiterjedő, a személyes adatokat védő rendeletet alkotott, amely egyértelműen a felhasználók védelmében született és erős kényszerítő hatást fejt ki az adatkezelők irányába az általuk tárolt személyes adatok biztonságának növelése érdekében. A korábban említett tömeges adatlopások nagy valószínűséggel ettől még nem fognak megszűnni, azonban jó esély van arra, hogy egyre kevesebb kockázatos incidens történik az EU területén a felhasználókkal. Az EU rendeletbe foglalt adatvédelmi törekvései regionális szinten hatékony nemzetközi választ jelenthetnek az aktuális kiberbiztonsági kihívásokra, de csak akkor, ha az implementáció sikeres lesz és azon kis- és középvállalkozások számára is elfogadható mértékű lesz a rendeletből fakadó plusz költségek mértéke, amelyek jelenleg a leginkább kitettek a kibertámadásokkal szemben.

5. Globális folyamatokat érintő kiberbiztonsági kihívások

Általánosságban elmondható, hogy globális szinten egyre több a kibertámadás, amelyek egyre szofisztikáltabbak is, ugyanakkor azoknak a támadásoknak is meredeken emelkedik a száma, amelyekhez nem szükséges különösebb technikai tudás. A tudástranszfer következtében ma már minimális beruházással és minimális informatikai tudással is lehet valakiből támadó. A kiberbiztonsági fenyegetések és kihívások kapcsán fontos forrásnak tekinthetők az ezen a területen működő, jelentős ügyfélkörrel rendelkező biztonsági cégek, nagy tekintélyű kutatóközpontok és egyéb kiberbiztonsági szakembereket tömörítő szakmai szervezetek, amelyek időszakos felmérésekkel, beszámolókkal, éves jelentésekkel és rendszeres adatmegosztással segítik egymás és a kiberbiztonsági közösség munkáját.

A rendelkezésre álló legfrissebb adatok alapján csökkent a különböző rosszindulatú szoftverek által megfertőzött számítógépek átlagos helyreállítási költsége, ugyanakkor nőtt a kiberbűnözők által okozott kár. A Kaspersky Cybersecurity Index alapján 2016-ban a második fél évben a felmérésben résztvevők 74%-a vélte úgy, hogy őt nem érinthetik az online fenyegetések, 39%-uk egyáltalán nem használt védelmi megoldást, 29% volt azok aránya, akik valamilyen kárt szenvedtek kibertámadás következtében. A korábbi 2016-os index ugyanebben a sorrendben 79, 40, 29%-os arányt mutatott, ami azt jelenti, hogy az első fél évben több ember gondolta úgy, hogy nem eshet kibertámadás áldozatául és maradt védtelen. Szakértők szerint mindez arra utal, hogy bár nem túl gyorsan, de pozitívan változik az emberek hozzáállása az internetes biztonsághoz, és még ha lassan is, de folyamatosan nő azok száma, akik aggódnak a kibertérből érkező fenyegetések miatt és tudatosan szeretnék megvéde-

ni magukat a kibertámadásoktól. A Kaspersky felmérése alapján 2016 második fél évében 22%-ról 20%-ra esett azoknak a felhasználóknak az aránya, akik valamilyen kártékony programmal találkoztak. Nőtt azonban azoknak a száma, akik egyéb, más típusú fenyegetések áldozataivá váltak, például zsarolóprogramok, adathalászat, adatlopás és adatszivárgás károsultjai lettek.

A Symantec éves jelentése alapján 2016-ban több egyedülálló támadásra is sor került. Volt példa több millió dollár eltulajdonításával járó virtuális csalásra, az USA választási folyamatába történő beavatkozásra, és nem szabad megfeledkeznünk az eddigi egyik legnagyobb DDoS támadásról sem, amit IoT eszközökből alkotott gigantikus botnet segítségével hajtottak végre az elkövetők. Miközben a kibertámadások korábban nem látott mértékben zavarták meg a rendszerek működését, a támadók egyre gyakrabban használnak egyszerű eszközöket és taktikákat annak érdekében, hogy minél nagyobb hatást válthassanak ki. A 0. napi sérülékenységekkel és a szofisztikált malware-ekkel a támadók egyre inkább takarékoskodnak és gyakran támaszkodnak a célzott adathalászatra, vagy más egyéb nemegyszer legitim eszköz nem rendeltetésszerű használatára. 2016-ban öt éves csúcsot döntött a malware-t tartalmazó e-mailek aránya: 131 elküldött e-mailből egy biztosan tartalmazott kártékony elemet. A zsarolóvírusok továbbra is töretlenül szedik áldozataikat, a Symantec mérései alapján 2016-ban 36%-kal nőtt a zsarolóvírusos fertőzések száma és az átlagos 300 dollár körüli váltságdíj több mint háromszorosára, 1077 dollárra nőtt. Korábban viszonylag ritka volt azoknak a kártevőknek a megjelenése, amelyek kifejezetten destruktív céllal működnek, azonban 2016 ebben a tekintetben is negatív tendenciát mutat. Két egymástól független esetben is kimutatható volt a szabotázs szándéka kibertámadások során. Az egyik esetben az ukrán energiaellátó rendszereket támadták meg év elején és év végén is a Black Energy névre keresztelt kártékony szoftverrel, míg Szaud-Arábiában a Shamoon tűnt fel újra különböző ipari és közigazgatási rendszerekben.

A globális kiberbiztonsági fenyegetések és kihívások további részletezése szükségtelen, hiszen a változás rendkívül dinamikus, így érdemes a fenti adatokat is minden esetben a legfrissebb, rendelkezésre álló adatokkal behelyettesíteni. Ugyanakkor a bemutatott információkból is kirajzolódik, hogy a legtöbb kiberbiztonsági kihívás vagy az érintett felhasználók száma, vagy az okozott kár nagysága, esetleg a megtámadott rendszer jellege miatt nemzeti és nemzetközi szinten is jelentőséggel bír. Egy a kibertérben jelen levő állam ma már nem engedheti meg magának, hogy ne foglalkozzon a kiberbiztonsággal és ne allokáljon forrásokat a biztonság szavatolására. Több kimutatás is azt bizonyítja, hogy a kiberbiztonságra költött összegek világszerte növekednek szektoroktól függetlenül, azonban a károk is egyre nagyobbak. Az International Data Corporation (IDC) 2020-ra szóló előrejelzése alapján több mint 100 milliárd dollárt költ a világ kiberbiztonsági szolgáltatásokra, szoftverekre és hardverekre. Az előrejelzés alapján ennek az összegnek közel a harmadát, mintegy 31 milliárd dollárt az USA fog elkölteni különböző kiberbiztonsági eszközökre és szolgáltatásokra, míg a második helyen Nyugat-Európa áll 19 milliárd dolláros becsült költésével. Összességében a 2016-os évhez képest 38%-os a növekedés a kiberbiztonsági kiadások terén, de az nem derül ki, hogy ez milyen arányban oszlik el a 2020-ig hátralevő időszakban. Ehhez képest a kiberbűnözők számlájára írható kár nagysága már 2015-ben is elérte a 3 billió dollárt világszerte. Az érdekes az, hogy a 2016-os Cybercrime Report előrejelzése alapján 2021-re a kiberbűnözésből fakadó károk nagysága világszinten megduplázódik, és eléri a 6 billió dollárt. Ez magában foglalja a sérült és megsemmisült adatokat, az ellopott pénzt, a termeléskiesést, a szellemi termékek eltulajdonítását, a személyes és pénzügyi adatok ellopását, a sikkasztást, csalást, a törvényszéki nyomozást és helyreállítást, valamint a reputációban keletkezett károkat. Az IDC adataihoz képest a 2016-os Cybercrime Report nagyságrendbeli különbséget mutat a kiberbiztonsági termékekre és szolgáltatásokra vonatkozó kiadások tekintetében, mivel azt több mint tízszeresére becsüli. Bárhogy is történjen, a következő néhány évben továbbra is folyamatos és dinamikus növekedés várható a kiberbiztonságra költött források, illetve a kibertámadásokból fakadó károk terén, és várhatóan az aránytalanság is fennmarad. A kiberbiztonsági kiadások a következő években továbbra is elmaradnak a kívánatostól, illetve jelentős problémát okoz a források nem megfelelő, illetve nem kellően hatékony elköltése is, ami elvezet egy másik globális szintű kiberbiztonsági kihíváshoz. A kiberbiztonsági munkaerőpiacon az utóbbi időben egyre jelentősebbé

váló anomáliákat az eddigi kihívásokhoz képest azok összetettsége miatt részletesebben mutatjuk be több tanulmány alapján.

2014 nyarán a RAND Corporation kiadott egy tanulmányt 'H4CKER5 WANTED' címmel, amely alapvetően az Amerikai Egyesült Államok kiberbiztonsági munkaerőhelyzetével foglalkozott. Ha azonban elfogadjuk azt, hogy az Egyesült Államokat érintő infokommunikációs technológiákkal összefüggő folyamatok – ha némi késleltetéssel is, de – érzékelhetőek a világ más régióiban is, akkor a tanulmány megállapításai hasznosak lehetnek bármely ország számára. A tanulmány szerzői több korábbi jelentés és felmérés eredményét is feldolgozták, mint például az amerikai Kormányzati Ellenőrzési Hivatal (U. S. Government Accountability Office – GAO), az amerikai kormányzat számára tanácsadói tevékenységet folytató Booz-Allen Hamilton (BAH) vállalat, az amerikai Védelmi Minisztérium (Department of Defense – DoD), vagy a Belbiztonsági Tanácsadó Testület (Homeland Security Advisory Council – HSAC). A GAO az azóta a történelem egyik legjelentősebb adatlopási incidensét elszenvedő kormányzati Személyzeti Irodával (Office of Personnel Management – OPM) közösen megfogalmazott több követendő gyakorlatot is a kiberbiztonsági munkaerő utánpótlásával kapcsolatban. A GAO munkatársai felhívták a figyelmet a nemzetbiztonsági átvilágításokból fakadó anomáliákra, amelyek miatt akár egy évig is elhúzódhatott egy felvételi procedúra, és listázták azokat a kormányzati kezdeményezéseket, amelyek a különböző állami szervezetek számára nyújtanak segítséget a megfelelő kiberbiztonsági munkaerő megtalálásában és képzésében. (Libicki, 2014, 14–17.)

Az OPM-hez hasonlóan ismerős lehet a Booz-Allen Hamilton vállalat neve is, mivel ez volt az a cég, amelyik munkaerő-kölcsönzés keretében kiközvetítette Edward Snowdent az amerikai Nemzetbiztonsági Szolgálathoz (National Security Agency – NSA), és aminek következtében 2013-ban Snowdennek lehetősége nyílt leleplezni az amerikai titkosszolgálatok tömeges megfigyelési gyakorlatát. A BAH vállalat is készített korábban egy gyakran hivatkozott tanulmányt arról, hogy milyen elvek és módszerek mentén lehetne erősíteni az amerikai szövetségi hivatalok kiberbiztonsági munkaerő-állományát. A tanulmány szerzői többek között megállapították, hogy az amerikai kormányzati kiberbiztonsági munkaerőprogramok széttagoltak, az OPM tevékenysége nem megfelelő, az alkalmazási szabályok túl komplexek, miközben a megbízásos szerződéssel történő alkalmazás jóval egyszerűbb. A szolgálatért kapott ösztöndíjprogramok sem jártak teljes sikerrel, az állami szervezetek pedig egymás elől vették el a kiberbiztonsági szakembereket, miközben továbbra sem jutott elegendő pénz kiberbiztonsági képzésre és humánerőforrás-fejlesztésre. (Libicki, 2014, 17–19.)

A Stratégiai és Nemzetközi Tanulmányok Központ (Center for Strategic and International Studies – CSIS) kiberbiztonsági munkaerővel foglalkozó elemzése alapvetően nem pénzügyi problémákat állapított meg az amerikai kormányzat szakemberhiányával kapcsolatban, sokkal inkább a menedzsment alacsony hatékonyságát hibáztatta a kialakult helyzetért. A legfontosabb javaslatok között szerepelt az amerikai Belbiztonsági Minisztérium (Department of Homeland Security – DHS) számára a kibertérhez kapcsolódó kormányzati szerepkörök és szakismeretek rendszertanának kialakítása, az amerikai Nemzeti Szabványügyi és Technológiai Intézet (National Institute of Standards and Technology) és más szereplők számára az engedélyezési követelményrendszer létrehozása, valamint az OPM számára a karrierstruktúra javítása. (Libicki, 2014, 19–22.)

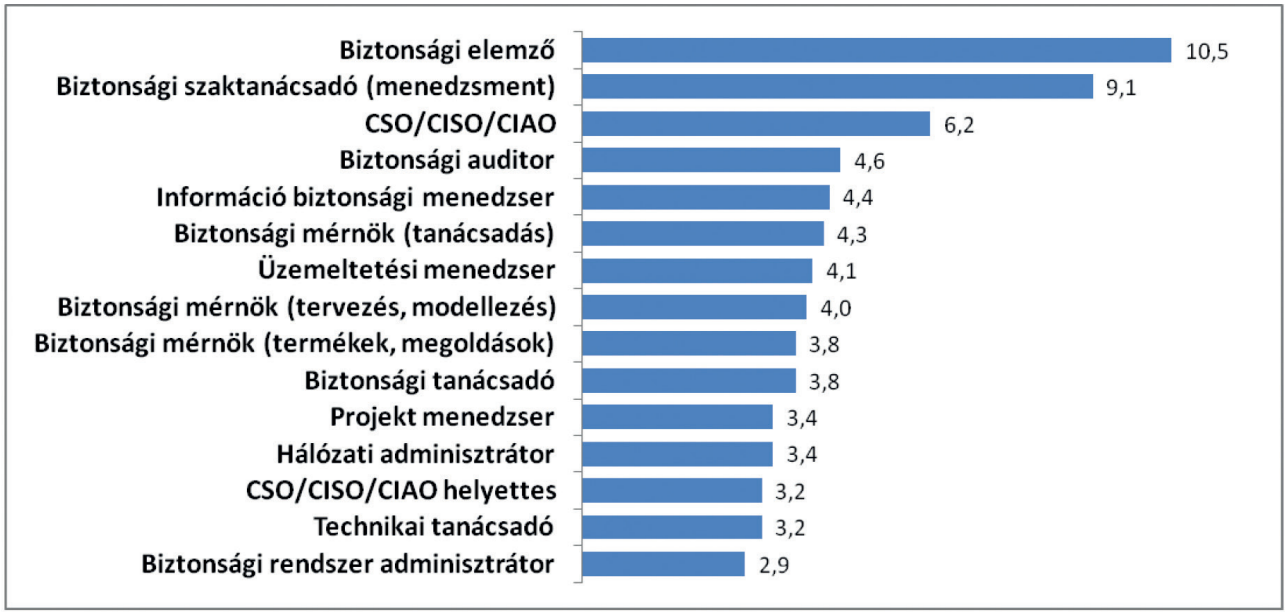
Az amerikai Védelmi Minisztérium (DoD) jelentése a kiberműveletek személyi állományáról jelentős hiányt mutatott ki a létszámban, illetve felhívta a figyelmet arra, hogy a különböző szolgálati ágak és haderőelemek eltérő igényekkel rendelkeznek a kiberbiztonsági szakértelem terén. Azért, hogy a DoD alá tartozó szervezetekben csökkenteni lehessen a kiberbiztonsági szakemberek hiányát, a minisztérium több programot is indított, amelyek elsősorban a képzési feltételek javítását és a pénzügyi körülmények fejlesztését szolgálták, például az iCollege program létrehozásával, vagy a szakmai tanúsítványokért járó bónuszrendszer kialakításával. (Libicki, 2014, 22–24.)

A Belbiztonsági Tanácsadó Testület (HSAC) létrehozott egy munkacsoportot, aminek olyan kiemelkedő személyiségek is tagjai voltak, mint például a DEF CON hackerkonferencia alapítója, Jeff Moss vagy a SANS Intézetet vezetője, Alan Paller. A testület arra jutott, hogy a Belbiztonsági Minisztérium (DHS) versenyképtelenné vált a munkaerőpiacon, mivel nem volt képes kellően érdekes

és kihívásokkal teli munkát kínálni a kiberbiztonsági szakemberek számára. Az amerikai kormányzat számára megfogalmazott legfontosabb javaslatok:

- Irányadó lista elkészítése a kritikus kormányzati kiberbiztonsági feladatokról;
- Gyakorlati forgatókönyvek és értékelési modell kifejlesztése;
- Dedikált tanácsadó testület felállítása a kiberbiztonsági munkaerő fejlesztésére;
- A veteránok bevonása és kiberbiztonsági tartalékos program kialakítása. (Libicki, 2014, 24–25.)

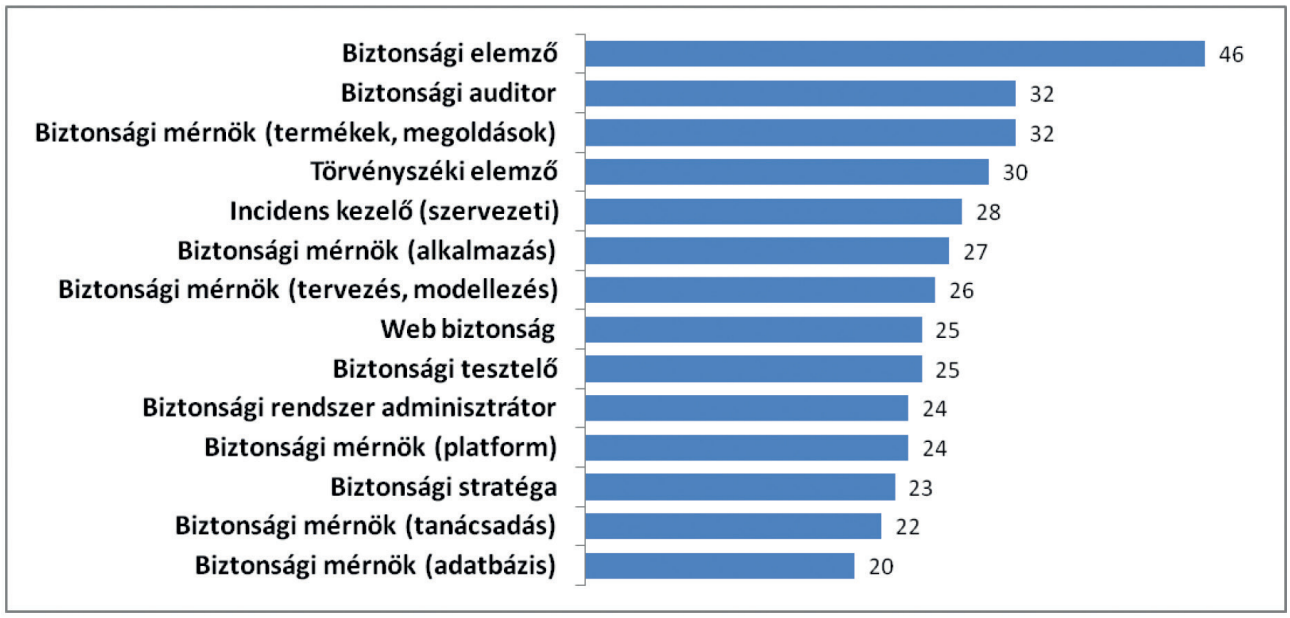
A kiberbiztonsági feladatokat és a kapcsolódó munkaköröket általában egy kategóriába sorolva emlegetik, azonban rendkívül szerteágazó tevékenységet fednek le a kiberbiztonsági pozíciók, így a szükséges szaktudás is eltérő. Bizonyos munkakörök betöltéséhez elengedhetetlen az erős technikai háttér, adott esetben a mérnöki végzettség, míg más esetekben inkább menedzsmentismeretekre és vezetői képességekre van szükség. Az (ISC)[2] a világ legnagyobb, információs és szoftverbiztonsági szakembereket tömörítő szervezete, amely több mint 160 országból 100 000-nél is több taggal rendelkezik. A szervezet által készített felmérés szerint 2015-ben a kiberbiztonság területén dolgozók több mint 10%-a biztonsági elemző volt, 9% körül alakult a biztonsági tanácsadók aránya, illetve meghaladta a 6%-ot a biztonsági és információbiztonsági vezetők aránya.



2. ábra: A Frost & Sullivan 14 000 válaszadóval készített felmérést az (ISC)2 számára, amelyből következtetni lehet a globális viszonyokra is2

A felmérés készítői arra is kíváncsiak voltak, hogy azoknál a szervezeteknél, ahol a válaszadók dolgoznak, milyen kiberbiztonsági szakmákban van hiány, illetve mely pozíciók feltöltése okozza a legnagyobb kihívást. Az eredmények azt mutatják, hogy bár a válaszadók között is jelentős számban vannak a biztonsági elemzők, még többre lenne szükség. A legnagyobb, közel 50%-os igény a biztonsági elemzők iránt mutatkozik, de egyformán keresettek a biztonsági auditorok és azok a mérnökök, akik a biztonsági termékek és megoldások tervezéséért felelősek.

[2] Az eredeti forrás felhasználásával szerkesztette és fordította a szerző. Az eredeti grafikon elérhető: isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf (utolsó letöltés: 2015. május 21.).

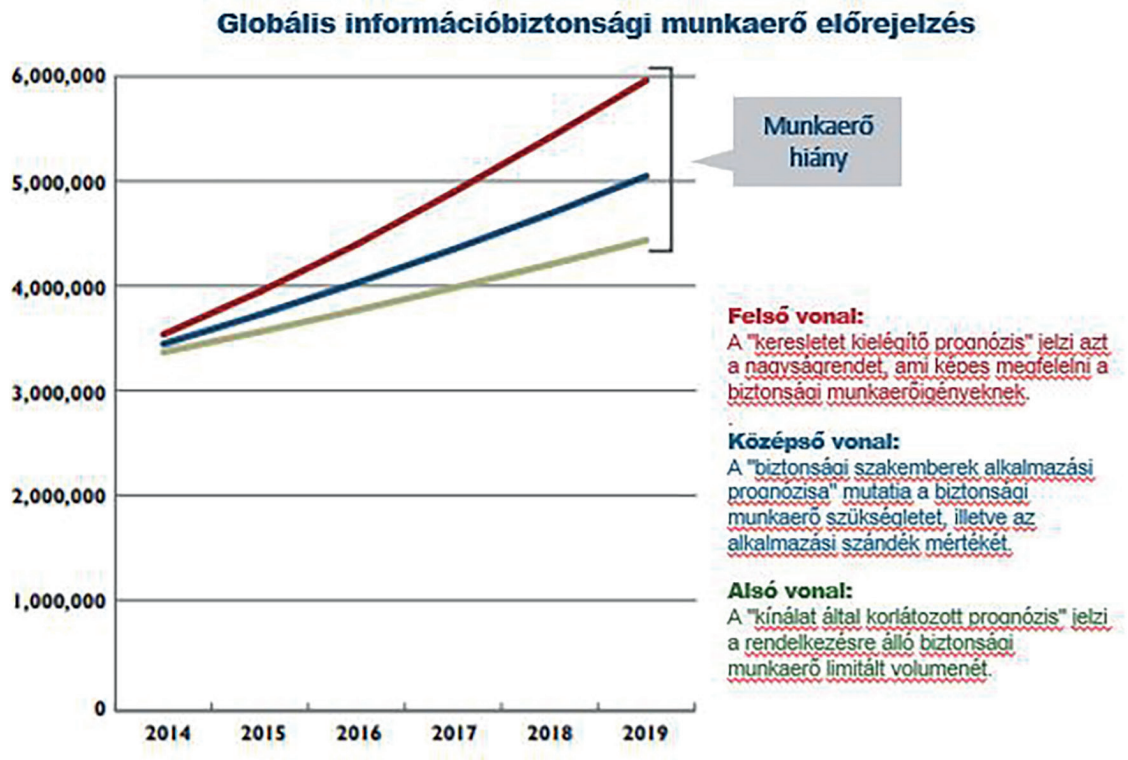


3. ábra: Az (ISC)2 számára készült 2015-ös felmérés alapján a legkeresettebb kiberbiztonsági szakmák sorrendje[3]

A válaszokból kitűnik, hogy jelentős igény van törvényszéki, illetve nyombiztosító elemzőkre, incidensek kezelésében jártas szakemberekre, de keresettek a biztonsági tesztelők, illetve az adatbázisok, az alkalmazások és a különböző platformok biztonságához értő mérnökök is.

A 2015-ös felmérés alapján a készítők egy 2014-2019 közötti időszakra vonatkozó becslést is elvégeztek, amiből jól látszik, hogy a nagyjából 3,5 milliós szakemberlétszám 2019-re 4,5 millió körülire bővül, azonban az igények ennél jóval nagyobb mértékben fognak növekedni és a kereslet várhatóan eléri a 6 millió főt globális szinten. A mintegy 1,5 millió fős különbség olyan kihívást jelent humán oldalról a kiberbiztonságban, amelyre ma még nem tudjuk biztosan a válaszokat. Amit viszont már most is biztosan tudunk, hogy erre a kihívásra nem lesz képes egyetlen ember vagy szervezet válaszokat adni. A kiberbiztonsági közösségnek és minden a kibertérrel kapcsolatba kerülő szervezetnek, nemzetállamnak közre kell működnie abban, hogy a biztonság nagyobb figyelmet kapjon az átlagos felhasználók körében éppúgy, mint a pályaválasztás előtt álló fiatalok esetében. A szükséges lépések késése vagy elmaradása csak ronthat a helyzeten.

[3] Az eredeti forrás felhasználásával szerkesztette és fordította a szerző. Az eredeti grafikon elérhető: isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf (utolsó letöltés: 2015. május 21.).



4. ábra: A kiberbiztonsági munkaerő várható alakulása 2014 és 2019 között. A zöld vonal jelöli azt a létszámot, amely biztosan megjelenik kínálati oldalon, a kék vonal mutatja az alkalmazási szándék várható alakulását, míg a vörös vonal azt jelzi, hogy mekkora lesz a teljes munkaerőigény a kiberbiztonság terén[4]

Jól látható, hogy miközben a kiberbiztonsági munkaerőhiány minden szektort érint, még az Amerikai Egyesült Államok kormánya számára is komoly nehézségeket okoz a helyzet megoldása. Az USA kormányának rendszerszintű problémákkal kell szembenéznie, és bár a munkát más országok kormányaihoz képest jóval korábban megkezdték, úgy tűnik 2015-ben még mindig rendkívül súlyos a helyzet. Elég csak a korábban már említett OPM adatlopási botrányra gondolni, amelyet 2015 júniusában fedeztek fel az illetékesek, és több mint 22 millió főt, az Egyesült Államok lakosságának 7%-át érintette az ügy. (Zengerle–Cassella, 2015) Szintén jelentős problémákra utal – még ha a forrás miatt fenntartásokkal is kell kezelnünk a hírt –, hogy az amerikai biztonsági rendszerek sérülékenységének napi szintű gyarapodásával még az ország legnagyobb riválisa, Kína sem tud lépést tartani, mert nem képes elég kiberbiztonsági szakembert biztosítani a felfedezett sérülékenységek kihasználásához. (Sz .n., 2015) Szintén beszédes adatokat rejt a Raytheon amerikai védelmi ipari vállalat támogatásával az amerikai Nemzeti Kiberbiztonsági Szövetség (National Cyber Security Alliance – NCSA) által készített felmérés, amely elsősorban az Y-generáció tagjai között vizsgálta a kiberbiztonsági szakma iránti érdeklődést. A felmérési eredményekből kitűnik, hogy a Közel-Keletet leszámítva minden régióban, illetve globálisan is 60% felett van azoknak a fiataloknak a száma, akik számára soha senki nem vetette fel annak lehetőségét, hogy kiberbiztonsági karriert építsenek. Ugyanakkor a válaszadók 38%-a szeretne többet tudni a kiberbiztonsági karrier lehetőségéről. Szintén rendszerszintű problémára mutat rá, hogy globális szinten a fiatalok 58%-a nem részesült kiberbiztonsággal kapcsolatos formális oktatásban. (Sz. n., 2016)

[4] Az eredeti forrás felhasználásával szerkesztette és fordította a szerző. Az eredeti grafikon elérhető: isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf (utolsó letöltés: 2015. május 21.).

A kiberbiztonsági munkaerőhiány kapcsán még 2015-ben napvilágot látott adatok szerint az Európai Unióban az ICT szektor évente 120 ezer új munkahelyet teremt. Azonban a magas munkanélküliség ellenére is, a képzett munkaerő hiánya miatt 2020-ra mintegy 900 ezer ICT állás maradhat betöltetlen az EU-ban. Tovább árnyalja a képet, hogy az EU lakosságának 20%-a soha nem használta az internetet, míg közel 40%-a nem rendelkezik megfelelő digitális képességekkel. Az EU lakóinak 14%-a pedig semmilyen digitális képességgel nem rendelkezik. (Ansip, 2015) Az önmagában alacsonynak tűnő érték valójában több mint 70 millió ember. A még csak kialakulóban lévő helyzetre nincs azonnali megoldás. Bár sokan hisznek abban, hogy néhány év múlva a legtöbb kiberbiztonsági területen az emberek szerepét átveszi a gépi tanulás és a mesterséges intelligencia alkalmazása, ezeknek a megoldásoknak a széles körű elterjedése 2020 előtt nem várható, és azután sem lehet majd mindent funkciót gépekre bízni. A következő években nem várható, hogy hirtelen nagy számban jelennének meg kiberbiztonságban jártas, képzett munkavállalók a piacon és ebben a tekintetben a bevándorlás és az agyelszívás sem megoldás. Az egyetlen előremutató, hosszú távon is eredményt hozó megoldás az oktatás és képzés, amihez nemzetközi összefogás szükséges annak érdekében, hogy a sokszor nagyon magas költségekkel képzett munkaerő ne hagyja el az adott országot vagy régiót. Jelenleg a nemzetközi kiberbiztonsági képzési és oktatási együttműködések meglehetősen fejletlenek, egy-két kivételtől eltekintve.

A nemzetközi együttműködések kapcsán gyakran felmerülő kihívás a terminológia kérdése. Bár elsőre nem tűnik komoly problémának, de ha jobban megvizsgáljuk a nemzetközi rendszer működésének alapjait és a különböző kooperatív kezdeményezéseket, hamar kiderül, hogy a kiberbiztonsági kihívások hatékony nemzetközi kezeléséhez nagy szükség lenne egy közös, egyezményes terminológia kialakítására. Ilyen azonban nem létezik, a kiberbiztonságnak nincs általánosan elfogadott meghatározása. Például az Európai Unió kiberbiztonsági stratégiája szerint a „kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket. A kiberbiztonság célja a hálózatok és az infrastruktúra rendelkezésre állásának és integritásának, valamint a benne lévő információk titkosságának megőrzése.” (EU, 2013, 3.) Az ENSZ mellett működő Nemzetközi Távközlési Egyesület (ITU) két meghatározása is érvényben van a kiberbiztonságra vonatkozóan. A rövidebb meghatározás szerint az adatok és rendszerek védelmét jelenti azokon a hálózatokon, amelyek az internethez kapcsolódnak. A tömör definíció helyett érdemesebb inkább az ITU hosszabb meghatározását figyelembe venni, amely szerint a kiberbiztonság olyan eszközök, politikák, biztonsági koncepciók, útmutatások, kockázatkezelési törekvések, intézkedések, képzések, legjobb gyakorlatok és technológiák együttese, amelyek alkalmasak a kibertér, illetve a kibertérben működő szervezetek és személyek tulajdonának védelmére. A meghatározás kitér arra is, hogy a szervezetek és felhasználók tulajdona alatt kell érteni minden a kibertérrel kapcsolatban álló eszközt, infrastruktúrát, alkalmazást, szolgáltatást, telekommunikációs rendszert és az összes küldött és tárolt információt. Az ITU meghatározása magába foglalja az információbiztonság három alapelvét is: bizalmasság, sértetlenség, rendelkezésre állás. (Mauer–Morgus, 2014) Bizalmasság vagy titkosság alatt azt értjük, hogy az információhoz csak az előírt módon és csak olyan személyek férhetnek hozzá, akiket erre feljogosítottak. A sértetlenség vagy más néven integritás nem más, mint az adat és információ eredetisége és épsége, illetve az információs rendszer hiteles és pontos állapota. Egyszerűbben fogalmazva, az adatokat és információkat csak azok módosíthatják, akik erre jogosultak és véletlen változás nem fordulhat elő. A rendelkezésre állás szintén egy állapotot határoz meg, amely egyfelől állandóságot jelent, másfelől az adatok és információk meghatározott időben történő elérhetőségét. A rendelkezésre állást értelmezhetjük úgy is, hogy a felhasználót semmi nem akadályozza abban, hogy az adatokhoz és információkhoz hozzáférjen, amikor azokra szüksége van. Ha már az euroatlanti szövetségi rendszer szóba került, érdemes megnézni a világ legerősebb katonai szervezeteként számon tartott NATO kiberbiztonsághoz kapcsolódó kifejezéseit. Katonai szervezet lévén a NATO által alkalmazott terminológia alapvetően a védelem és a kiber kifejezéseket társítja, de szintén több meg-

határozás van használatban párhuzamosan. Az egyik meghatározás szélesebb információbiztonsági környezetet foglal magában, ahol a kommunikációs és információs rendszerek biztonsága a bizalmasság, az integritás és a rendelkezésre állás megfelelő védelmének képességét jelenti. Ugyanakkor a NATO a kibervédelem kifejezés alatt olyan képességet ért, amellyel egy műveleti kommunikációs és információs rendszer szolgáltatásai megvédhetők a kibertérből érkező rosszindulatú tevékenységekkel szemben. (Klimburg, 2012) Már az említett meghatározások nyomán is jól látható, hogy az egyes kiberbiztonsági definíciók között eltérés mutatkozik attól függően, hogy melyik szervezetről vagy intézményről van szó. A helyzet csak tovább bonyolódik, ha az egyes államok szintjén vizsgáljuk a kiberbiztonság meghatározását, mivel a legtöbb ország saját megfogalmazást, egyedi definíciót alkalmaz. Ezen a szinten az eltérések sokszor jelentéktelenek, de gyakran előfordulnak komoly különbségek is. Mivel a fejezetnek nem célja a terminológiai hasonlóságok és eltérések részletes bemutatása, az állami definíciók közül csak a magyar meghatározást ismertetjük. A 2013-ban megjelent Nemzeti Kiberbiztonsági Stratégia (NKBS) 5. pontja az alábbiak szerint definiálja a kiberbiztonság fogalmát. A stratégia szerint a „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.” (MK, 2013, 6339.) A bemutatott meghatározások alapján jól látható, hogy a kiberbiztonság egyfelől leginkább egy állapotként írható le, amelynek három alapvető összetevője az adatok és információk bizalmassága, integritása és rendelkezésre állása, másfelől viszont egy olyan eszközrendszer illetve képesség, amely a kibertérből eredő kockázatokat elfogadható szinten tudja tartani. Fontos megjegyezni, hogy a fizikai világhoz hasonlóan a kibertérben sem érhető el abszolút biztonság.

6. Kiberbiztonság a nemzetközi béke és biztonság tükrében

Az államok az 1990-es évek óta foglalkoznak az információs és telekommunikációs technológiák nemzetközi békére és biztonságra gyakorolt hatásaival. Az azóta eltelt időszakban számos jelentős kiberbiztonsági incidens történt, amelyeknek köszönhetően a kormányok új stratégiákat és szervezeteket kezdtek el kialakítani a kibertér katonai célú felhasználásával összefüggésben. Ennek eredményeként jelenleg is aktív vita folyik arról, hogy milyen nemzetközi normák mentén lehetne irányítani a kiberteret, és milyen módon lehetséges a bizalomépítés ebben a dimenzióban. Fontos lenne a stabilitás növelése, illetve az államok számára olyan kiberbiztonsági képességek kialakítása, amelyek segítségével hatékonyan léphetnek fel a kibertérből érkező kihívásokkal szemben saját határaikon belül és kívül egyaránt. Az elmúlt évek trendjei alapján számos ország kezdte el a kiberbiztonsági kérdéseket beépíteni a nemzeti biztonsági és védelmi stratégiákba, illetve a fejlett államok mára már önálló stratégia keretén belül foglalkoznak a kibertér biztonságának garantálásával. A politika legfelső szintjeire eljutó kiberbiztonsági kérdések nyomán nemzeti beruházások indulnak annak érdekében, hogy kibervédelmi vagy éppen támadóképességeket alakítsanak ki a kihívások és sérülékenységek kezelésére. A fokozott érdeklődésnek és beruházásoknak köszönhetően újabb kérdések merülnek fel például a hagyományos biztonsági koncepciók alkalmazhatóságával, a kibertérre vonatkozó joggal és a kibertér irányítási struktúrájával kapcsolatban. A kialakult párbeszédek fókuszában jellemzően a nemzetközi jog alkalmazhatósága, a kibertérre vonatkozó normák és az államok kibertérben tanúsított magatartási formái állnak. Ezen a téren az egyik meghatározó politikai irány a tömegpusztító fegyverek leszereléséhez kapcsolódó bizalom és biztonságerősítő intézkedések nyomán próbálja meg a kiberteret biztonságosabbá tenni és az ehhez szükséges kibervédelmi kapacitásokat kialakítani. A fizikai világra alkalmazott nemzetközi jog, illetve az annak részét képező hadijogi alapelvek kapcsán fontos kérdések merülnek fel azzal kapcsolatban, hogy a megkülönböztetés vagy az arányosság elve

miként alkalmazható a kibertérben. A megkülönböztetés koncepciója szerint a hadviselő feleknek különbséget kell tenniük civil és katonai célpontok között, ami szinte egyáltalán nem kivitelezhető a kibertérben jelenleg. Hasonlóan problémás terület az arányosság elve, amelynek értelmében a támadással okozott pusztításnak arányban kell lennie a katonai előnnyel, amelyre a támadás következtében tesz szert valamely hadviselő fél. Tekintettel arra, hogy ezek az elvek nehezen vagy csak megkötésekkel alkalmazhatók a kibertérre, több olyan javaslat is napvilágot látott, amelyek értelmében a kibertérben megnövekedne az állam szerepe az információk ellenőrzése terén. Ezek az erőfeszítések azonban jelentős veszélyeket hordoznak magukban elsősorban a szólásszabadság vonatkozásában. Ez az egyik oka annak, hogy az információbiztonság és kiberbiztonság meghatározása és a kapcsolódó, egységes terminológia kialakítása során fontos emberi jogi kérdésekre is tekintettel kell lenni. Szintén fontos, hogy ezeknek a jelentős kérdéseknek a megvitatása korábban a nemzetállamok kiváltsága volt, a kibertérben azonban a társadalmi szereplőknek nemcsak közvetett módon lehet nagy hatása a nemzetközi békére és biztonságra. A kiberbiztonság aktualitásairól számos fórumon értekeztek már a nemzetközi béke és biztonság perspektíváit szem előtt tartva, azonban a kibertér védelmét és biztonságát erősíteni hivatott nemzetközi együttműködések a mai napig gyerekcipőben járnak. A kooperatív kezdeményezések túlnyomó részt egyetlen régióra vagy valamilyen problémakörre próbálnak megoldást találni. Kérdés, hogy a fragmentáltság a hatékonyságot milyen mértékben befolyásolja egy olyan határok nélküli közegben, ahol minden mindennel összefügg.

7. Irodalomjegyzék

Anglia Ruskin University Library (2008): Harvard System of Referencing Guide. libweb.anglia.ac.uk/referencing/harvard.htm (utolsó letöltés: 2017. 01. 06.)

Ansip, Andrus (2015): Digital skills, jobs and the need to get more Europeans online., 2015. Elérhetőség: ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/digital-skills-jobs-and-need-get-more-europeans-online_en (utolsó letöltés: 2017. 04. 02.)

Berzsenyi, Dániel – Ványi, Rajmond (2015): Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei. Nemzet és Biztonság, 2015. Elérhetőség: http://nemzetesbiztonsag.hu/cikkek/nb_2015_3_12_berzsenyi-vanyi_-_egy_katonapolitikai_dontes_lehetseges_kiberbiztonsagi_kovetkezmenyei_iszlam_allam.pdf (utolsó letöltés: 2015. 12. 27.)

Evans, Dave (2011): The Internet of Things., How the Next Evolution of the Internet Is Changing Everything? Cisco 2011. Elérhetőség: blogs.cisco.com/diversity/the-internet-of-things-infographic (utolsó letöltés: 2014. 04. 21.)

Hart, Kim (2008): Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar., Washington Post, 2008. Elérhetőség: washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html?hpid=topnews (utolsó letöltés: 2017. 04. 02.)

ITU (2012): Overview of the Internet of Things., 2012. itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (utolsó letöltés: 2014. 04. 21.)

ITU: ICT Facts and Figures 2016. itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf (utolsó letöltés: 2016. 10. 19.)

ITU: Measuring the Information Society, 2012. Elérhetőség: itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf (utolsó letöltés: 2016. 10. 22.)

Klimburg, Alexander edt. (2012): National Cyber Security Framework Manual. 2012. Elérhetőség: ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (utolsó letöltés: 2013. 12. 02.)

Kovács László – Krasznay Csaba (2017): Mert övék a hatalom., SVKK Elemzések. 2017. Elérhetőség: netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-9-az-internet-politikat-is-befolyasolo-hatasa-a-2016-os-amerikai-elnokvalasztas-soran-kovacs-l-krasznay-cs.original.pdf (utolsó letöltés: 2017. 05. 05.)

KSH: Rendszeres internethasználók aránya (2005–-2016). Elérhetőség: ksh.hu/docs/hun/eurostat_tablak/tabl/tin00091.html (utolsó letöltés: 2016. 10. 19.)

Libicki, Martin C. – Senty, David – Pollak, Julia (2014): H4CKER5 WANTED, An Examination of the Cybersecurity Labor Market. RAND Corporation, 2014. Elérhetőség: rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf (utolsó letöltés: 2014. 07. 23.)

Magyar Közlöny (2013), Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 2013. Elérhetőség: kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf (utolsó letöltés: 2013. 04. 03.)

Maurer, Tim – Morgus, Robert (2014): Compilation of Existing Cybersecurity and Information Security Related Definitions. 2014: Elérhetőség: na-production.s3.amazonaws.com/documents/compilation-of-existing-cybersecurity-and-information-security-related-definitions.pdf (utolsó letöltés: 2015. 02. 19.)

Mészáros Csaba (2016): Fenyegetések Internete. Computerworld, 2016. Elérhetőség: computerworld.hu/computerworld/fenyegetesek-internete.html (utolsó letöltés: 2017. 01. 12.)

Rettman, Andrew (2017): German spy chief warns Kremlin on election hack. Euobserver. 2017. Elérhetőség: euobserver.com/foreign/137788 (utolsó letöltés: 2017. 05. 06.)

Symantec Internet Security Threat Report, 2017. Elérhetőség: symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (utolsó letöltés: 2017. 05. 04.)

Sz. n. (2015): China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U. S. Security Systems. The Onion, 2015. Elérhetőség: theonion.com/article/china-unable-recruit-hackers-fast-enough-keep-vuln-51719 (utolsó letöltés: 2015. 10. 26.)

Sz. n. (2015): Securing Our Future: Closing the Cybersecurity Talent Gap., Raytheon. Elérhetőség: staysafeonline.org/download/datasets/16847/Securing%Our%Future%Closing%the%Cybersecurity%Talent%Gap.pdf (utolsó letöltés: 2016. 10. 30.)

The Economic Times: IoT: Hottest technology to watch out for in 2015. The Economic Times, 2015. Elérhetőség: economictimes.indiatimes.com/news/industry/jobs/iot-hottest-technology-to-watch-out-for-in-2015/articleshow/45807138.cms (utolsó letöltés: 2015. 10. 08.)

The Internet of Everything: 2014 [Slide Deck], Business Insider. Elérhetőség: businessinsider.com/the-internet-of-everything-2014-slide-deck-sai-2014-2#-11 (utolsó letöltés: 2016. 10. 22.)

UN: Word Population Prospects The 2015 Revision, 2015. Elérhetőség: esa.un.org/unpd/wpp/publications/files/key_findings_wpp_2015.pdf (utolsó letöltés: 2016. 10. 19.)

Wirtz, James J. (2015): Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. CCDCOE 2015. Elérhetőség: ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf (utolsó letöltés: 2016. 11. 02.)

Zengerle, Patricia –- Cassella, Megan (2015): Millions more Americans hit by government personnel data hack. Reuters, 2015. Elérhetőség: reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709 (utolsó letöltés: 2015. 07. 10.)

II. ZÁMBÓ NÓRA: BIZTONSÁGI ESEMÉNYKEZELÉSSEL KAPCSOLATOS ELVÁRÁSOK A HAZAI ÉS NEMZETKÖZI JOGBAN

1. Bevezető gondolatok

A mai modern társadalmak és a gazdasági szektorok egyre nagyobb mértékben használják a digitális infrastruktúrák kínálta előnyöket, ezzel egyidejűleg azonban megjelentek az ebből fakadó biztonsági kockázatok is. A megszaporodó adatlopások, a kritikus infrastruktúrákkal szembeni támadások és zsarolóvírusok megjelenése az Európai Unió szintjén is nyilvánvalóvá tették az összehangolt fellépés szükségességét, mivel a biztosági incidensek és az azokkal érintett szolgáltatások gyakran határon átnyúló jelleget öltenek. Hosszú évekig tartó előkészítő munka után 2016-ban hatályba léptek az uniós információbiztonsági rendszer két pillérének tekinthető jogszabályok: az Európai Unió általános adatvédelmi rendelete (GDPR), valamint a hálózati és információs rendszerek biztonságáról szóló irányelv (NIS). Mindkét jogszabály célja egy olyan közös minimumrendszer kidolgozása, amely a biztonsági előírások mellett eseménykezelési, incidensbejelentési kötelezettséget határoz meg. Mind az adatvédelem, mind a kiberbiztonság területén indokolt volt a korábbi hazai szabályozás felülvizsgálata, és szükséges a harmonizációja a GDPR rendeletben és a NIS irányelvben foglaltakhoz. Jelen tananyag áttekintést ad a NIS irányelv és a GDPR rendelet minimumszabályairól, továbbá az eseménykezelést érintő hatályos hazai szabályozásról. A tananyag összeállításakor cél volt továbbá annak igazolása, hogy az uniós és hazai szabályozás az együttműködés révén együttesen képes biztosítani az érintett szereplők számára a hatékony eseménykezelés hátterét.

2. Eseménykezelés a NIS irányelv tükrében

2.1. A NIS irányelv és ami mögötte van

2.1.1. Előzmények, út a hálózati és információs rendszereknek az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelvig

A 2008-ban kirobbant pénzügyi és gazdasági világválság következményeinek kezelése új kihívások elé állította az Európai Unió vezetőit. Nyilvánvalóvá vált, hogy az előttünk álló időszaknak az erőteljes modernizációból és globalizációból eredő kihívásait csak a fenntartható fejlődés elveit szem előtt tartva lehet kezelni, ami többek között hosszú távú stratégiai tervdokumentumok megalkotását

is feltételezi. A 2020-ig tartó időszak intézkedéseinek alapdokumentumaként született meg az *Europa 2020 foglalkoztatási és növekedési stratégia* (a továbbiakban Europa 2020 stratégia).[5]

Az Europa 2020 stratégia keretében hét kiemelt kezdeményezés indult, amelyek esetében az Uniónak és a tagállami hatóságoknak össze kell hangolniuk intézkedéseiket. Az egyik ilyen kiemelt kezdeményezés az Intelligens növekedés[6] célrendszerén belül az *Európai digitális menetrend*, amelynek célja, hogy a digitális technológia előnyei az európai polgárok és vállalkozások számára minél szélesebb körben elérhetőek legyenek.

Az Európai digitális menetrend keretében tervezett intézkedések:

a) az egységes digitális piac megteremtése (az online tartalmakhoz való jogszerű hozzáférés, valamint az elektronikus fizetés és számlázás megkönnyítése);
b) *az uniós adatvédelmi szabályozási keret felülvizsgálata;*
c) távközlési szolgáltatások egységesítése;
d) *fokozott interoperabilitás és szabványok;*
e) készülékek, alkalmazások, adattárolók, szolgáltatások és hálózatok átjárhatóságának növelése*;*
f) *bizalom és az internetes biztonság megerősítése;*
g) nagy sebességű és szupergyors internet-hozzáférés mindenki számára;
h) befektetés a kutatásba és az innovációba;
i) digitális jártasság, a digitális készségek és a digitális integráció előmozdítása;
j) a technológia intelligens használatából eredő előnyök kiaknázása a társadalom számára.

Az Európai Digitális Menetrend hét beavatkozási területe közül a Bizalom és biztonság intézkedési területen az alábbi célokat határozták meg:

a) *javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra;*
b) a számítógépes támadások elleni gyors reagálású európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok (CERT) hálózatának létrehozása, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepének megerősítése;
c) javaslattétel olyan tagállami forróvonalak létrehozására, ahol a gyermekek és szüleik bejelentést tehetnek a jogellenes internetes tartalmakról;
d) tudatosságnövelés, így többek között az internetes védelem iskolai oktatása;
e) egyebek mellett a gyermekbántalmazással, a személyazonosság-lopással és számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozása;
f) a magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten és azon kívül egyaránt.

---

[5] A 2010-ben elfogadott Europa 2020 stratégia célja, hogy megteremtse az intelligens (hatékonyabb oktatási, kutatási és innovációs beruházások, valamint a digitális társadalom fejlesztése), fenntartható (erőforrás-hatékonyabb, környezetbarátabb és versenyképesebb gazdaság) és inkluzív (a gazdasági, szociális és területi kohéziót előmozdító, magas foglalkoztatási arányt biztosító gazdaság) növekedés feltételeit. Az Europa 2020 stratégia címzettjei az európai uniós intézmények, a tagállamok és a szociális partnerek, az ő közös és összehangolt munkájuk eredményeként valósulhatnak meg a célkitűzések.

[6] Az Europa 2020 „Intelligens növekedés" pillére a tudás és az innováció erősítését célozza. Ehhez szükség van a K+F kiadások nagyarányú növelésére, az oktatás, képzés és az élethosszig tartó tanulás motiválására annak érdekében, hogy a munkerőpiaci igényekhez igazodó szakképzett munkavállalók járuljanak hozzá Európa fejlődéséhez. Az információs és kommunikációs technológiák iránti keresletnek csak egy elhanyagolható része köthető az európai vállalkozásokhoz, holott az innováció széles körben történő elterjesztése nagyban hozzájárulhat a digitális társadalom és az oktatás minőségének és teljesítmények növeléséhez.

A kiberbiztonság korábban szinte csak büntetőjogi vetülete okán szerepelt az uniós döntéshozók napirendjén. Elsőként az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága által jegyzett, *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* című uniós stratégiáról szóló 2013-ban közzétett közös közlemény vállalkozott a témakör átfogó áttekintésére (a továbbiakban uniós stratégia).[7] Az uniós stratégia az alábbi kihívásokat azonosítja:

a) *az információs rendszerek kibertámadásokkal szembeni ellenálló képességének megteremtése;*
b) a kiberbűnözés drasztikus visszaszorítása;
c) a kibervédelmi politika kidolgozása és a közös biztonság- és védelempolitikát érintő képességek fejlesztése;
d) a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése;
e) az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése.

Az uniós stratégia egyik fő eleme és egyfajta intézkedési terve az Európai Parlament és a Tanács 2016/1148 irányelve (2016. július 19.) a *hálózati és információs rendszereknek az egész Unióban egységesen magas szintjét biztosító intézkedésekről* (a továbbiakban NIS irányelv).[8] Jelen fejezet további részében az irányelv rendelkezéseit vesszük sorra.

2.1.2. A NIS irányelv megalkotásának indokai, célrendszere

A belső piac működése szempontjából az irányelv alapvetőnek tekinti a hálózati és információs rendszerek és szolgáltatások megbízhatóságát és biztonságát, mivel kiemelt szerepük van az áruk, szolgáltatások és személyek határokon átnyúló mozgásának elősegítésében. A határon átnyúló jellegükből adódóan a rendszerek jelentős zavara nemcsak az egyes tagállamokra lehet kihatással, hanem több tagállamra vagy akár az egész Európai Unióra, a cselekmény irányultságától függetlenül.

A NIS irányelv bevezető része kitér arra, hogy a biztonsági események nagyságrendje, gyakorisága és hatása növekszik, ami súlyos fenyegetést jelent a hálózati és az információs rendszerek működésére, ugyanis a működés akadályozására vagy megszakítására irányuló szándékos és ártalmas cselekmények a rendszereket sérülékeny célponttá teszik. Az ilyen események hátrányos kihatással vannak az Unió gazdaságára, jelentős pénzügyi veszteségeket, a felhasználói bizalom elvesztését és súlyos károkat okozhatnak.

A biztonsági események megelőzésére, kezelésére a tagállamok eltérő módon vannak felkészülve, ezért az irányelv célja, hogy kialakítsa az Európai Unióban a hálózati és információs rendszerek biztonságának általános szintjét, és egyenlő versenyfeltételeket biztosítson az összes uniós országra vonatkozó harmonizált szabályozás bevezetésével.

A NIS irányelv 2016. július 19-én jelent meg az Európai Unió hivatalos lapjában, és 2016. augusztus 8-án lépett hatályba. A NIS irányelv, mint uniós jogi norma sajátossága az, hogy az elérendő célt tekintve valamennyi címzett tagállamot kötelez, de a nemzeti hatóságok szabadon dönthetnek arról, hogy milyen módszerek és eszközök alkalmazásával teszik annak szabályait a nemzeti jog részévé. A NIS irányelv rendelkezéseit 2018. május 9-ig kell átültetni a tagállami jogrendszerbe, azaz ezen időpontig szükséges a vonatkozó hazai jogi szabályozást áttekinteni és harmonizálni azt az irányelvben foglaltakhoz.

---

[7] Lásd: register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (utolsó letöltés: 2019. április 20.)

[8] Lásd: eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&qid=1490464106404&from=-HU (utolsó letöltés: 2019. április 20.)

2.1.3. A NIS hatálya

Figyelemmel a NIS biztonsági intézkedésekre vonatkozó átfogó, mégis differenciált megközelítésére, érdemes röviden megvizsgálni a NIS irányelv alanyi hatályt szabályozó egyes rendelkezéseit.

A NIS irányelv hatálya alá tartozó szereplőket két csoportra lehet osztani. A valamennyi lényeges biztonsági eseményre[9] és kockázatra[10] kiterjedő szabályozás érdekében az irányelv hatálya kiterjed *az alapvető szolgáltatásokat nyújtó szereplőkre* és a *digitális szolgáltatókra,* amelyek szolgáltatásait az alapvető szolgáltatók is igénybe veszik, ezért biztonságos, folyamatos és megbízható működésük nélkülözhetetlen ahhoz, hogy az alapvető szolgáltatók zavartalanul szolgál.

Alapvető szolgáltatásokat nyújtó szereplőnek kell tekinteni azt az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és -elosztás, valamint a digitális infrastruktúra ágazatában működő – tagállami szinten kijelölt – közjogi vagy magánjogi szervezetet, amely megfelel az alábbi kritériumoknak:[11]

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

A fenti kitételeknek való megfelelésből következően tehát a NIS irányelv szabályozása nem vonatkozik valamennyi alapvető szolgáltatásokat nyújtó szereplőre, hanem csak azokra, amelyek kiesése komoly társadalmi vagy gazdasági károkat okozna.

A hatályos hazai szabályozással való összehasonlítás érdekében megjegyzendő, hogy a NIS irányelv csak az alapvető szolgáltatásokat nyújtó szereplőként azonosított közigazgatási szervekre alkalmazandó. A NIS irányelv hatálya alá nem tartozó közigazgatási szervek hálózati és információs rendszereinek biztonságáról a tagállamoknak kell gondoskodniuk.

Digitális szolgáltatónak minősül a NIS irányelv szempontjából minden digitális szolgáltatást nyújtó szereplő, amely szolgáltatása ugyan nem nélkülözhetetlen, de társadalmi szempontból kiemelt jelentőséggel bír. Digitális szolgáltatásnak tekinti az irányelv az online piacteret, az online keresőprogramot és a felhőalapú számítástechnikai szolgáltatást.[12]

Nem terjed ki a NIS irányelv hatálya:

- a mikro- és kisvállalatokra;
- más EU-szintű IT-biztonságot érintő ágazati szabályozás hatálya alá (is) tartozókra (például kritikus infrastruktúra);
- a nemzeti ágazati kijelölési kritériumokat nem teljesítő alapvető szolgáltatást nyújtó szereplőkre;
- hardvergyártókra, szoftverfejlesztőkre.

---

9 NIS irányelv 4. cikk 7 pont: „biztonsági esemény”: minden olyan esemény, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára.

10 NIS irányelv 4. cikk 9. pont: „kockázat”: minden olyan ésszerűen azonosítható körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerek biztonságára.

11 NIS 4. cikk, 4 pont; 5. cikk, 2. pont.

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

A NIS irányelv védett jogi tárgya az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók hálózati és információs rendszere,[13] amely:

- a 2002/21/EK irányelv[14] 2. cikkének a) pontja szerinti elektronikus hírközlő hálózat;
- 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
- az általuk működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

Az alapvető szolgáltatásokat nyújtó szereplőknek és a digitális szolgáltatóknak, továbbá a tagállami és uniós szereplőknek meg kell hozniuk azokat a védelmi intézkedéseket, amelyek révén garantálható a hálózati és információs rendszerek biztonsága. A NIS irányelv a hálózati és információs rendszerek biztonságának a hálózati és információs rendszer arra való képességét tekinti, hogy adott bizonyossággal ellenálljon az olyan cselekményeknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított vagy kezelt adatok, vagy az említett hálózati és információs rendszeren nyújtott vagy rajta keresztül elérhető kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát.[15]

Az eredménytelen védelmi intézkedések olyan biztonsági esemény bekövetkezéséhez vezethetnek, amely jelentős zavart okoz egy adott szolgáltatás nyújtásában, és amely megfelelő eljárásrend kidolgozását igényli tagállami és uniós szinten egyaránt.

2.2. A NIS eszközrendszere

A NIS irányelv alapelvként rögzíti, hogy az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó követelményeknek arányosaknak kell lenniük az adott hálózati és információs rendszert érintő kockázatokkal. Figyelemmel arra, hogy a kritikus társadalmi és gazdasági tevékenységek fenntartásához elengedhetetlen alapvető szolgáltatásokat nyújtó szereplők tekintetében jelentkező kockázatok mértéke magasabb, mint a digitális szolgáltatók esetében, ezért az alapvető szolgáltatásokat nyújtó szereplőkre vonatkozóan az irányelv alapján szigorúbb biztonsági követelményeket szükséges előírni.

Az irányelv egy olyan többszintű rendszert kíván kialakítani, amelyben az alapvető szolgáltatásokat nyújtó szereplőkön és a digitális szolgáltatókon túl a tagállami hatóságokra és az uniós szervekre is egymással összefüggő és egymásra épülő kötelezettségeket, feladatokat határoz meg.

Az alapvető szolgáltatást nyújtó szereplőkre a NIS irányelv az alábbi biztonsági követelményeket állapítja meg:[16]

- megfelelő és arányos műszaki és szervezési intézkedések megtétele a működésük során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében olyan módon, hogy az intézkedéseknek biztosítaniuk kell a felmerülő kockázatnak megfelelő biztonsági szintet;
- az alapvető szolgáltatások folytonosságát biztosító intézkedések megtétele a szolgáltatások nyújtása során alkalmazott hálózati és információs rendszerek biztonságát érintő biztonsági események megelőzésére és azok hatásainak csökkentésére;
- az alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági események indokolatlan késedelem nélküli bejelentése az illetékes hatóságnak.

---

13 NIS 4. cikk, 1. pont.

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

15 NIS irányelv 4. cikk, 2. pont.

16 NIS irányelv 14. cikk, (1)–(3) bekezdés.

A digitális szolgáltatók vonatkozásában az alábbi – az adott hálózati és információs rendszert érintő kockázatokkal arányos – biztonsági követelményeket kell számba venni,[17] amelyek a mikro- és kisvállalkozásokra nem alkalmazandók:

- az Unión belüli szolgáltatásnyújtás során használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése során olyan egzakt és a kockázattal arányos műszaki és szervezési intézkedéseket szükséges meghatározni és megtenni, amelyek biztosítják a felmerülő kockázatnak a megfelelő biztonsági szintet, és figyelembe veszik a következő tényezőket:

a) a rendszerek és a létesítmények biztonsága,
b) a biztonsági események kezelése,
c) üzletmenetfolytonosság-menedzsment,
d) monitoring, ellenőrzés és vizsgálat,
e) a nemzetközi szabványoknak való megfelelés;

- szolgáltatásaik folytonosságát biztosító intézkedések megtétele annak érdekében, hogy megelőzzék és csökkentsék a hálózati és információs rendszereik biztonságát érintő biztonsági események a szolgáltatásokra gyakorolt hatásokat;
- a szolgáltatásaik folytonosságára jelentős hatást gyakorló biztonsági események indokolatlan késedelem nélküli bejelentése az illetékes hatóságnak.

A NIS irányelv azonban nemcsak arra vonatkozóan tartalmaz előírásokat, hogy az érintett szereplőknek milyen, a kockázatokkal arányos mértékű hálózat- és rendszerbiztonságot kell garantálniuk, hanem a biztonsági incidens kezelésére is. Amennyiben a biztonsági követelmények ellenére ugyanis olyan esemény következik be, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára,[18] szükséges lefolytatni ezen biztonsági esemény észlelését, elemzését és elszigetelését, valamint a rájuk való reagálást támogató eljárásokat.[19]

A fent ismertetett követelményrendszerből látható, hogy a jelentős zavart okozó biztonsági események bejelentési kötelezettségét írja elő az irányelv. A biztonsági eseményt okozó zavar jelentőségének meghatározása a tagállamok feladata lesz, amelyek ágazatközi és ágazatspecifikus tényezőket vesznek figyelembe.

Ágazatközi tényezőknek minősülnek az alábbiak:

- az érintett szervezet által nyújtott szolgáltatásra támaszkodó felhasználók száma (akár közvetlenül, akár közvetetten – például digitális szolgáltatón keresztül – közvetítőn keresztül veszik igénybe az adott szolgáltatást);
- az adott szolgáltatást nyújtó szereplők függése a jelentős zavart okozó biztonsági eseménnyel érintett szervezet által nyújtott szolgáltatástól;
- a biztonsági események hatása – mértéküket és időtartamukat tekintve – a gazdasági és társadalmi tevékenységekre vagy a közbiztonságra;
- a jelentős zavart okozó biztonsági eseménnyel érintett szervezet piaci részesedése;
- az adott biztonsági esemény által esetlegesen érintett terület földrajzi kiterjedése;
- a jelentős zavart okozó biztonsági eseménnyel érintett szervezet jelentősége a szolgáltatás elégséges szintjének fenntartásában, figyelembe véve az adott szolgáltatás nyújtásához rendelkezésre álló egyéb lehetőségeket is.[20]

Ágazatspecifikus tényezőket is szükséges figyelembe venni annak vizsgálatakor, hogy a biztonsági esemény jelentős zavart okoz-e egy adott szolgáltatás nyújtásában. Ilyen tényező lehet például az egészségügyi ágazat tekintetében az, hogy a biztonsági eseménnyel érintett szolgáltató évente hány

[17] NIS irányelv 16. cikk (1)–(3) bekezdés.
[18] NIS irányelv 4. cikk, 7. pont.
[19] NIS irányelv 4. cikk, 8. pont.
[20] NIS irányelv 6. cikk, (1) bekezdés.

beteget lát el, vagy a vízszektort illetően az, hogy a szolgáltató kiknek (egyének, szervezetek számára) és milyen földrajzi kiterjedéssel szolgáltat.

A jelentős zavart okozó biztonsági esemény tekintetében tehát bejelentési kötelezettség terheli a szolgáltatót az illetékes hatóság felé. A tagállam által kijelölendő ezen nemzeti illetékes hatóság (amely akár több hatóság is lehet, és már létező hatóság is megbízható ezzel a feladattal) felel a hálózati és információs rendszerek biztonságáért,[21] és lehet egyúttal nemzeti szinten az egyedüli kapcsolattartó pont. Ilyen minőségében összekötő feladatokat lát el a tagállami hatóságok között és a többi tagállam érintett hatóságaival, az uniós szintű együttműködési csoporttal, valamint a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) hálózatával.[22]

Ha felmerül annak gyanúja, hogy a biztonsági esemény hátterében bűncselekmény húzódik meg, úgy az illetékes hatóságoknak és az egyedüli kapcsolattartó pontnak fel kell vennie a kapcsolatot és együtt kell működnie az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal.

Ugyanezen együttműködési kötelezettség áll fenn a személyes adatok biztonsági eseményekből eredő bármely megsértése esetén az adatvédelmi hatóságokkal.

A NIS irányelv alapján kialakítandó nemzeti intézményrendszer részét képezik a tagállamok által kijelölt, számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek vagy a Magyarországon használatos megnevezés szerint CERT-ek),[23] amelyek a kockázatok és a biztonsági események kezeléséért felelnek.

A CSIRT-ek feladatkörébe tartozik:

- a biztonsági események nemzeti szintű monitoringja;
- a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára;
- reagálás a biztonsági eseményekre;
- dinamikus kockázat- és eseményelemzés, valamint helyzetkép nyújtása;
- a CSIRT-ek hálózatában való részvétel.

A nemzeti intézmények kötelesek együttműködni egymással, így például amennyiben a CSIRT-ek nem kapják meg közvetlenül a biztonsági eseményekről szóló bejelentéseket, úgy hozzáférést kell biztosítani számukra az alapvető szolgáltatásokat nyújtó szereplők, illetve a digitális szolgáltatók által bejelentett biztonsági események adataihoz.

Az irányelv céljára figyelemmel az együttműködés nemcsak tagállami, hanem uniós szinten is meg kell, hogy valósuljon. A konzultatív jellegű együttműködést (például stratégiai iránymutatás, jó gyakorlatok megosztása) szolgálja a tagállamok, az Európai Bizottság és az ENISA képviselőiből álló együttműködési csoport,[24] míg az operatív közös munka (például a biztonsági eseményre vonatkozó információk megosztása) a CSIRT-ek hálózatán[25] belül valósul meg.

Fontos kitérni arra, hogy a NIS irányelv hatálya alá nem tartozó szervezeteknél is felmerülhet olyan biztonsági esemény, amely jelentős zavart okozhat az általuk nyújtott szolgáltatásokban. A NIS irányelv ebben az esetben is biztosítja a lehetőséget a biztonsági esemény önkéntes bejelentésére, ha a szervezet megítélése alapján a bejelentés közérdeket szolgál. A bejelentéseket az illetékes hatóságoknak vagy a CSIRT-eknek kell feldolgozniuk, ha az nem jelent aránytalan vagy indokolatlan terhet az érintett tagállamok számára.

---

21 NIS irányelv 8. cikk, (1) bekezdés.
22 NIS irányelv 8. cikk, (3)–(5) bekezdés.
23 NIS irányelv 9. cikk.
24 NIS irányelv 11. cikk.
25 NIS irányelv 12. cikk.

A fentieket összegzendő a NIS irányelv:

a) valamennyi tagállam számára kötelezettségként rögzíti a hálózati és információs rendszerek biztonsága nemzeti stratégiájának elfogadását;
b) előírja egy nemzeti hatóság kijelölését, amely felügyeli a NIS átültetését és végrehajtását;
c) előírja annak meghatározását, hogy ágazatonként milyen kritériumok alapján kerül egy-egy szolgáltató az irányelv hatálya alá, és ezt követően ezen szolgáltatók kijelölését;
d) biztonsági és bejelentési követelményeket állapít meg az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára;
e) létrehoz egy együttműködési csoportot a tagállamok közötti stratégiai együttműködés és információcsere támogatása és elősegítése, valamint a közöttük lévő bizalom erősítése céljából;
f) létrehozza a számítógép-biztonsági eseményekre reagáló csoportok, a CSIRT-ek hálózatát a tagállamok közötti bizalom erősítéséhez való hozzájárulás, valamint a gyors és hatékony operatív együttműködés előmozdítása céljából;
g) a tagállamok számára kötelezettségeket állapít meg arra vonatkozóan, hogy a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására jelöljenek ki nemzeti illetékes hatóságokat, egyedüli kapcsolattartó pontokat, valamint CSIRT-eket.

Az eseménykezeléssel érintett hazai és uniós hatóságok által kibocsátásra kerülő iránymutatások az irányelvben foglalt minimumszabályok kifejtésével, részletezésével segíthetik a jogalkalmazás hatékonyságát.

3. Eseménykezelési elvárások a GDPR szabályozásában

3.1. Fogalomrendszer

Az Európai Unió Általános Adatvédelmi Rendeletének értelmezése megköveteli az adatvédelem és az információbiztonság alapfogalmainak rögzítését.

Az *adat* közlésre, megjelenítésre vagy további feldolgozásra alkalmas entitás, amely számos formában megjelenhet (például alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása. Az *információ* valamilyen megfigyelés, tapasztalat vagy ismeret, amely által következtetések vonhatók le és döntések alapjául szolgálhat, azaz jelentéssel felruházott adat.[26]

Az *adatvédelem* központjában az adatkezelés jogszerűségét biztosító – főként szabályozási – tevékenységek állnak, elsősorban a védelmet biztosító szabályok és eljárások, valamint az adatkezelési eszközök és módszerek összessége. Ehhez képest az *adatbiztonság* meghatározása alatt alapvetően az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összessége értendő. 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.

Az *információvédelem* körébe tartozó tevékenység például az információt hordozó entitások (személyek és eszközök) védelme, azaz az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelme, az irat- és dokumentumvédelem, valamint a személyi védelem is. Az információvédelem célja – hasonlóan az adatvédelemhez – a jogosulatlan hozzáférés, módosítás vagy megsemmisítés elleni védelem és az információk folyamatos rendelkezésre állásának biztosítása.

[26] Vesd össze: Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz. Budapest, Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, 2016. április. 21. oldal.

Az *információbiztonság* olyan követelményrendszer, amelynek középpontjában a bizalmasság, sértetlenség és rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen formában és milyen adathordozón jelenik meg. Az információbiztonság a biztonsági események megelőzése, kezelése kapcsán jellemzően az IT-üzemeltetés területén jelenik meg, ahol a gyakorlatban az adatok, információs rendszerek fizikai, logikai, adminisztratív védelmén van a hangsúly. Érzékelhető, hogy ebben a szabályozási környezetben nem az adatvédelem és az adatbiztonság az először vizsgált elem.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban BM rendelet) 1. melléklete szerinti biztonsági osztályba sorolásánál, illetve a szervezet 2. melléklet szerinti biztonsági szintjének meghatározásánál már jelentősége van a személyes adatok vagy azok különleges típusai kezelésének, ami utal a kapcsolódó adatvédelmi előírásokra.

A hazánkban jelenleg hatályos adatvédelmi szabályok szintén tartalmaznak adatbiztonsági követelményeket, így az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban Infotv.) is. Az Infotv. 25/I. § (3) bekezdésében rögzíti a személyes adatot kezelő vagy feldolgozó személy kötelezettségeit, feladatait, amelyekkel biztosítja a személyes adatok megfelelő szintű biztonságát és az érintettek alapvető jogainak érvényesülését. Annak érdekében, hogy az adatokkal végzett tevékenységek, műveletek jól körülhatárolhatók legyenek, az Infotv. mintegy gyűjtőfogalomként meghatározza, mi minősül adatkezelésnek[27] és adatfeldolgozásnak.[28]

Az Infotv. rögzíti továbbá az adatkezelő[29] és az adatfeldolgozó[30] fogalmát.

Az Infotv. meghatározza az adatvédelmi incidens[31] fogalmát is. Eszerint adatvédelmi incidensnek kell tekinteni az adatbiztonság olyan sérelmét, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Ez a fogalommeghatározás összhangban áll az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban Ibtv.) által alkalmazott biztonsági esemény fogalmával, így ezek együttes értelmezésével az elektronikus információs rendszerek által kezelt személyes adatokra vonatkozóan bekövetkezett jogsértések azonosítása – jogi szempontból – könnyebben elvégezhető.

Az Infotv. rögzíti, hogy az adatkezelőnek az érintett részére a törvényben meghatározott esetekben nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal kell teljesítenie.[32] Ezen kívül meghatározásra kerül számos további, az érintettet megillető jogosultság is (például hozzáféréshez, helyesbítéshez, törléshez való jog stb.).

---

27 Infotv. 3. § 10. pontja: „Az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése."

28 Infotv. 3.§ 17. pontja: „Az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége."

29 Infotv. 3.§ 9. pontja: „Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja."

30 Infotv. 3.§ 18. pontja: „Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel."

31 Infotv. 3. § 26. pont.

32 Infotv. 15.§ (1) bekezdés.

Mindemellett az Infotv. rendelkezik még többek között a személyes adatok kezelése jogalapjainak általános feltételeiről, az adattovábbítással kapcsolatos előírásokról, az adatkezelői, illetve adatfeldolgozói nyilvántartásról, valamint az elektronikus napló és az adatvédelmi hatásvizsgálat lefolytatásának alapvető szabályairól is. Továbbá rögzíti az adatbiztonsági intézkedéseket, és az adatvédelmi tisztivelőre vonatkozó előírásokat is.

A fentieket összefoglalva rögzíthető, hogy adatbiztonság alatt az Infotv. a személyes adatok információbiztonságát érti.[33]

Személyes adatok kezelése és feldolgozása során az Infotv. tovább pontosítja az adatbiztonsági elvárásokat. Rögzíti, hogy az adatkezelő és tevékenységi körében az adatfeldolgozó szervezési és műszaki intézkedésekkel biztosítja:

> a) az adatkezeléshez használt eszközök (a továbbiakban: adatkezelő rendszer) jogosulatlan személyek általi hozzáférésének megtagadását;
> b) az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását;
> c) az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozását;
> d) az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozását;
> e) azt, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá;
> f) azt, hogy ellenőrizhető és megállapítható legyen, hogy a személyes adatokat adatátviteli berendezés útján mely címzettnek továbbították vagy továbbíthatják, illetve bocsátották vagy bocsáthatják rendelkezésére;
> g) azt, hogy utólag ellenőrizhető és megállapítható legyen, hogy mely személyes adatokat, mely időpontban, ki vitt be az adatkezelő rendszerbe;
> h) a személyes adatoknak azok továbbítása során vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozását;
> i) azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen; valamint
> j) azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével se lehessen megváltoztatni.[34]

Emellett az Infotv. általános jelleggel kötelezi az adatkezelőt vagy adatfeldolgozót, hogy az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor figyelembe veszi a tudomány és a technológia mindenkori állását, az intézkedések megvalósításának költségeit, az adatkezelés jellegét, hatókörét és céljait, továbbá az érintettek jogainak érvényesülésére az adatkezelés által jelentett változó valószínűségű és súlyosságú kockázatokat..[35]

---

[33] A NAIH adatvédelmi szótára szerint az adatbiztonság „az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere”. Adatvédelmi szótár naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2017. április 20.).

[34] Infotv. 25/I. § (3) bekezdés.

[35] Infotv. 25/I. § (2) bekezdés.

3.2. GDPR alapok

A már említett Digitális Menetrend *Bizalom és biztonság* című intézkedési területén az Európai Bizottság számára meghatározott feladatok keretében alkották meg, és lépett hatályba 2018. május 25-től valamennyi Európai Uniós tagállamban egységesen és közvetlenül alkalmazandó Általános Adatvédelmi Rendelet[36] (angolul General Data Protection Regulation, a továbbiakban GDPR), amely közvetlen alkalmazhatósága miatt az irányelv rendelkezéseit átültető tagállami adatvédelmi jogszabályok, közöttük az Infotv. GDPR-ban már szabályozott tárgyköreinek lép a helyébe. Ennek következtében az Infotv. közérdekű és közérdekből nyilvános adatokra vonatkozó rendelkezései, valamint egyes, a GDPR által nem rendezett adatvédelmi előírások továbbra is hatályban maradnak (például az eljáró hatóságra vonatkozó szabályok).

A GDPR a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 95/46/EK irányelvet (a továbbiakban Adatvédelmi irányelv) váltja fel. Az adatvédelmi reform kiemelt célja az volt, hogy a személyes adatok védelme és az információbiztonsági követelmények egységesen magas szintje és koherenciája biztosított legyen, ezáltal növekedjen a felhasználók új technológiákba és az online térbe vetett bizalma, felgyorsuljon az egységes európai digitális tér létrejötte.[37]

A GDPR a személyes adatokat kezelő szervezetek számára átfogó adatbiztonsági előírásokat tartalmaz, a megfelelőség bizonyítását széles körű és részletes dokumentációhoz köti, továbbá már az adatok kezelésének megkezdése előtt kockázatalapú[38] tervezést és az adatvédelmi garanciák számba vételét várja el az adatkezelőtől. Az új szabályozás kiemelt figyelmet fordít az adatkezelési műveletekhez kapcsolódó technológiára (például titkosítás), és rögzíti, hogy minden adatkezelő köteles dokumentálni, bizonyos esetekben bejelenteni, valamint az érintetteket is tájékoztatni a személyes adatokat érintő incidensekről.

3.3. Adatbiztonság és adatvédelmi incidens a GDPR-ban és a kapcsolódó szabályok

A GDPR a fentiekben említett célok elérése és a kihívásoknak való megfelelés érdekében számos változást tartalmaz mind az adatvédelem, mind az adatbiztonság területén az Adatvédelmi irányelv és az Infotv. korábbi változatának előírásaihoz képest, ezért a szabályoknak történő megfelelésre két év felkészülési időt adott a jogalkotó. 2018. július 26-án hatályba lépett az Infotv. átfogó módosítása, így ennek eredményeként a törvény összhangba került az általános adatvédelmi rendelettel.

Az adatbiztonság 2018 májusáig hatályos általános megfogalmazását[39] kiegészíti a kockázatok értékelésével és a védekezés költségeinek mérlegelésével – „a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.”

---

36 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 (általános adatvédelmi rendelet) – (a továbbiakban: GDPR).

37 Digitális Menetrend: A Bizottság akcióterve az európai jólét fellendítésére. Brüsszel, 2010. május 19. europa.eu/rapid/press-release_IP-10-581_hu.htm (utolsó letöltés: 2017. április 20.)

38 A GDPR 32. cikkének megfogalmazása szerint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével kell kialakítani az adatbiztonsági intézkedéseket.

39 Adatvédelmi irányelv 17. cikk.

A GDPR az adatbiztonság területén elvárt védelmi intézkedéseket is felsorolja és rögzíti, hogy ahol szükséges és lehetséges, ott:

a) alkalmazni kell a személyes adatok álnevesített (pszeudonim) kezelését;[40]
b) alkalmazni kell a személyes adatok technológiai titkosítását;
c) biztosítani kell az adatkezelőnek vagy adatfeldolgozónak, hogy a személyes adatok kezelésére használt rendszerekben és szolgáltatásokban folyamatos védelmi intézkedések működjenek;
d) biztosítani kell, hogy fizikai vagy műszaki incidens esetén rendelkezésre álljon a biztonsági mentés vagy tartalék rendszer;[41]
e) a védelmi intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást kell az adatkezelőnek kialakítania.[42]

A GDPR rögzíti az adatvédelmi incidens fogalmát, amely szerint az „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”.[43]

A fentiekből eredően adatvédelmi incidensnek csak azon információbiztonsági események tekinthetőek, amelyek a személyes adatok biztonságát sértik. További megállapításként az is rögzíthető, hogy minden olyan biztonsági esemény, amely akár csak egyetlen természetes személy adatát is hátrányosan érinti, már adatvédelmi incidensnek minősül, még akkor is, ha annak minimális az érintett magánszférájára gyakorolt hatása. A tág fogalmi rendelkezésből következően emberi vagy technikai hibákra, téves adatkezelési műveletekre (például tévesen címzett személyes adatokat tartalmazó e-mail) visszavezethető eseményekre is kiterjed a fogalom hatálya.

A GDPR Preambuluma kimondja, hogy megfelelő és jól időzített védelmi intézkedések hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat az adatvédelmi incidens az adatalanyoknak. A Preambulum ide sorolja „a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.”[44]

Azon adatvédelmi incidensekről, amelyek „valószínűsíthetően magas kockázatot” jelentenek a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek az érintettet indokolatlan késedelem nélkül tájékoztatnia kell, amelyben rögzíteni kell annak leírását, hogy milyen jellegű az adatvédelmi incidens, valamint az érintettnek a természetes személynek szóló, a lehetséges hátrányos hatások enyhítését célzó javaslatait. Az indokolatlan késedelem nélküli tájékoztatás célja, hogy az értesítés hatására olyan védelmi intézkedéseket tehessen az érintett adatainak védelme érdekében – például jelszavának megváltoztatása annak kompromittálódása esetén, vagy elektronikus fizetőeszközének letiltatása – amelyekkel csökkentheti az incidens által okozott károkat.[45]

---

40 A GDPR 4. cikk 5. pontja meghatározása szerint az álnevesítés „a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.”

41 A GDPR 32. cikk (1) c) pontja megfogalmazásában „az arra való képesség, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani.”

42 GDPR 32. cikk (1) a)–d).

43 GDPR 4. cikk 12. pont.

44 GDPR Preambulum (85).

45 GDPR Preambulum (86).

Az adatvédelmi incidensek bejelentési kötelezettségét előíró szabályozás célja és lényege, hogy a megtett bejelentés alapján:

a) a nemzeti hatóság a szükséges intézkedéseket megtegye és a bejelentések tartalmából akár egyes adatkezelői csoportokra, szolgáltatási területekre nézve is adatot szerezhessen az adatbiztonság tényleges helyzetére vonatkozóan;
b) az adatkezelő a személyes adatokat ért incidenseket felismerje, körülményeit felmérje, azokat megfelelően dokumentálja, ami alapján tervezhetővé válnak a szükséges védelmi intézkedések;
c) az adatkezelő – a jó hírnevét is veszélyeztető incidensek és a hozzájuk kapcsolódó értesítési kötelezettségek előfordulásának minimalizálása érdekében – jelentős erőforrásokat fordítson az adatbiztonság szintjének növelésére, az incidenssel érintettek számának vagy a potenciális károknak a csökkentésére.[46]

Az adatvédelmi incidensek hatékony kezelése érdekében a GDPR 33. cikke előírja, hogy az adatvédelmi incidens bekövetkezését az adatkezelő indokolatlan késedelem nélkül – ha lehetséges, legkésőbb 72 órával az után, hogy az a tudomására jutott – köteles bejelenteni az illetékes felügyelő hatóságnak.[47] A GDPR a bejelentés főbb tartalmi elemei között előírja, hogy a bejelentésben rögzíteni kell:

a) az adatvédelmi incidens jellegét (körülményei), és ha az lehetséges, az arra vonatkozó adatokat (érintettek köre és száma, az incidenssel érintett adatok köre);
b) az adatvédelmi tisztviselő vagy kapcsolattartó személyének nevét és elérhetőségeit;
c) az incidens várható hatását, következményeit;
d) az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket.[48]

Ha az adatkezelő az bejelentésre előírt 72 órás maximális határidőt elmulasztja, akkor a bejelentéséhez mellékelni köteles a késedelem igazolására szolgáló indokokat is.

Nem kell bejelentenie az adatkezelőnek a hatóság részére azokat az adatvédelmi incidenseket, amelyek „valószínűsíthetően nem jár[nak] kockázattal a természetes személyek jogaira és szabadságaira nézve."[49]

Ha az adatvédelmi incidens „valószínűsíthetően magas kockázattal jár" a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül köteles tájékoztatni az érintetteket is az adatvédelmi incidensről,[50] kivéve, ha korábban mások számára értelmezhetetlenné tette az incidenssel érintett adatokat, vagy az incidenst követően olyan további intézkedéseket tett, amelyekkel a kockázatokat érdemben csökkentette.[51]

A GDPR az adatfeldolgozó kötelezettségeként írja elő az adatvédelmi incidensek felismerését és jelzését azzal, hogy köteles indokolatlan késedelem nélkül tájékoztatást adni a biztonsági eseményről, annak érdekében, hogy az adatkezelő a szükséges intézkedéseket megtegye.[52]

Az adatvédelmi incidensekről az adatkezelő részére nyilvántartási kötelezettséget is előír a GDPR, amely szerint az adatkezelőnek nyilvántartásban rögzítenie kell:

a) az adatvédelmi incidenshez kapcsolódó tényeket és annak hatásait;
b) az adatvédelmi incidens orvoslására tett intézkedéseket

azzal, hogy a nyilvántartásnak lehetővé kell tennie, hogy a felügyeleti hatóság ellenőrizhesse a

46 Szőke Gergely László (2017): Értesítési kötelezettség az adatvédelmi incidensek esetén – elméleti és gyakorlati kérdések. JURA, 2017/1. 140–153.
47 GDPR 33. cikk (1) bekezdés.
48 GDPR 33. cikk (3) bekezdés.
49 GDPR 33. cikk (1) bekezdés.
50 GDPR 34. cikk (1) bekezdés.
51 GDPR 34. cikk (3) bekezdés.
52 GDPR 33. cikk (2) bekezdés.

bejelentési követelményeknek való megfelelést.[53] Ez a nyilvántartási kötelezettség minden adatvédelmi incidensre kiterjed, és az elszámoltathatóság elve[54] alapján az adatkezelő köteles igazolni az incidensek bejelentéséről vagy az érintett tájékoztatásának szükségességéről hozott döntését.

A felügyeleti hatóság a nyilvántartást áttekintve ellenőrizheti, hogy az adatkezelő helyesen mérlegelte-e az adatvédelmi incidens kockázatát.[55]

A bejelentési és nyilvántartási kötelezettségének megsértése esetén az eljáró adatvédelmi hatóság az adatkezelőt vagy feldolgozót 10 millió euróig terjedő összegű közigazgatási bírsággal, vagy vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeggel sújthatja, azzal, hogy a két összeg közül mindig a magasabbat kell kiszabnia a hatóságnak.[56]

Fentiek ismertetésével összefüggésben szükséges megjegyezni, hogy az általános, minden adatkezelőre kiterjedő nyilvántartási és bejelentési, illetve értesítési kötelezettség a GDPR egyik legjelentősebb változása. Emellett azt is ki kell emelni, hogy az adatvédelmi incidensekre vonatkozó előírások nem a GDPR-ban jelentek meg először az Európai Unió adatvédelmi jogában, ahogy az átültetéssel járó kodifikációs eredmények is helyet kaptak már a nemzeti jogban.

Az elektronikus hírközlési ágazatban 2009 óta vonatkoznak előírások arra az esetre, ha a személyes adatok biztonsága sérülne.[57] Az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban Eht.) ültette át az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK (2002. július 12.) az Európai Parlament és a Tanács irányelvének (a továbbiakban EU e-hírközlési adatvédelmi irányelv) incidensekre vonatkozó előírásait. Az EU e-hírközlési adatvédelmi irányelve 2. cikk i) pontja szerint személyes adatok megsértése „a biztonság olyan megsértése, amely a Közösségben nyilvánosan elérhető hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítését, elveszítését, módosítását, jogosulatlan felfedését vagy az azokhoz való jogosulatlan hozzáférést eredményezi". Ezen szabályozásban is megjelenik a jogellenes magatartási formák felsorolása, azzal, hogy itt egy szűkebb adatkezelői kör, a hírközlési szolgáltatók a jogalanyok és egyes magatartási formák hiányoznak (például véletlen vagy jogellenes adatkezelés, vagy feldolgozás).

Az Eht. előírásai szerint az „előfizetői személyes adatok megsértését jelenti a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt, vagy más egyéb módon kezelt vagy feldolgozott személyes adatok véletlen, vagy jogellenes kezelése vagy feldolgozása, így különösen megsemmisítése, elvesztése, módosítása, jogosulatlan felfedése, nyilvánosságra hozatala, vagy az azokhoz való jogosulatlan hozzáférés."[58]

Az Eht. hatálya alá tartozó hírközlési szolgáltatók kötelesek a személyes adatok megsértése esetén haladéktalanul, de legkésőbb 24 órán belül bejelentést tenni a Nemzeti Média- és Hírközlési Hatóságnak (a továbbiakban NMHH).[59]

A hírközlési szolgáltatókra vonatkozó rendelkezések szerint, ha egy incidens várhatóan hátrányosan érinti az előfizető vagy más magánszemély személyes adatait vagy magánéletét, akkor erről az előfizetőt vagy magánszemélyt is indokolatlan késedelem nélkül értesítenie kell a szolgáltatónak. Ezen kötelezettség alól csak akkor mentesülhet, ha igazolni tudja, hogy végrehajtotta a megfelelő technikai védelmi intézkedéseket (például technológiai titkosítás), illetve, hogy ezen intézkedéseket alkalmazták is az incidenssel érintett adatok tekintetében, és ezzel értelmezhetetlenné teszik azokat

53 GDPR 33. cikk (5) bekezdés.

54 GDPR Preambulum (85), valamint az 5. cikk (2) bekezdésében foglaltak szerint.

55 GDPR 33. cikk (5) bekezdés és 34. cikk (1) bekezdés.

56 GDPR 83. cikk (4) bekezdés a) pontja alapján.

57 Az Európai Parlament és a Tanács az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK (2002. július 12.) irányelv (a továbbiakban EU elektronikus hírközlési adatvédelmi irányelv) rendelkezései közé a 2009/136/EK irányelv ültette át a kötelezettséget.

58 Az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban Eht.) 156. § (2) bekezdés.

59 Eht. 156. § rendelkezései alapján.

az adatokhoz jogosulatlanul hozzáférő számára.[60] Ezt a rendelkezés a GDPR azon előírásával szükséges összevetni, amely szerint az érintettet nem kell indokolatlan késedelem nélkül tájékoztatni, ha „az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat".[61] A hírközlési szolgáltató az Infotv. nyilvántartási előírásához képest az Eht. rendelkezése szerint speciális, azt helyettesítő incidensnyilvántartást köteles vezetni annak érdekében, hogy az NMHH ellenőrizni tudja, hogy a szolgáltató megfelelően értesítette-e az érintetteket, vagy az értesítés mellőzése esetén helyesen mérlegelte-e az incidens következményeit, illetve alkalmazta-e a technikai és védelmi intézkedéseket.[62]

Összegzésként rögzíthető, hogy az adatvédelmi incidens fogalmi meghatározása alapján (ideértve az Infotv. és az Eht. rendelkezéseit is) a személyes adatok megsértése jogellenes – célhoz kötöttség elvét figyelmen kívül hagyó vagy tévesen meghatározott jogalappal történő – adatkezelés vagy a tájékoztatási kötelezettség elmulasztása révén valósítható meg, ami az Ibtv. szerinti biztonsági vagy súlyos biztonsági esemény meghatározására figyelemmel nem azonosítható egyértelműen a bizalmasság, sértetlenség, rendelkezésre állás követelményeinek együttes vagy egyenkénti megsértésével. A fogalmi összhang és a gyakorlati egységesítés a GDPR 2018-as kötelező alkalmazásától várható.

Az ismertetett rendelkezésekből gyakorlati következtetésként levonható, hogy a GDPR:

a) általános, a magas kockázatot nem jelentő biztonsági eseményekre is kiterjedő nyilvántartási kötelezettséget ír elő valamennyi adatvédelmi incidensre és tevékenységtől vagy szektortól függetlenül valamennyi adatkezelő részére;

b) az adatkezelő részére az incidens bejelentésére nyitva álló határidőt maximalizálja a tudomásszerzéstől számított legfeljebb 72 órában, ami az eddigieknél gyorsabb reagálási képességet követel meg az érintettektől.

Fontos kiemelni továbbá, hogy mind az adatkezelőknek, és mind az adatfeldolgozónak úgy kell megterveznie, kialakítania és szerveznie adatkezelési rendszereit, ügyviteli folyamatait, és úgy kell biztosítania az üzletmenet folytonosságát, hogy az adatvédelmi incidens(eke)t képes legyen felismerni annak érdekében, hogy azokat nyilvántartásba vehesse, majd mérlegelhesse az érintettre vonatkozó várható kockázat mértékét, és még határidőben eleget tehessen az esetleges bejelentési és értesítési kötelezettségének. Mindezt úgy, hogy természetesen az incidens elhárításának és az ebből eredő károk kezelésének is eleget tegyen. Ehhez szükséges, hogy a szervezet belső szabályaiban az incidensek észlelésére és nyilvántartására vonatkozó felelősségi szabályokat, valamint a munkatársak feladatait rögzítse. Szükséges továbbá, hogy a prevenció jegyében továbbképzések, figyelemfelhívó üzenetek útján tájékoztassa a munkatársakat az adatvédelmi elvekről és alapfogalmakról, hogy a munkatársak képesek legyenek az esetleges adatvédelmi incidensek azonosítására. Az érintettek értesítésére vonatkozó kötelezettségek miatt indokolt a technikai titkosítás és az álnevesítés alkalmazása a személyes adatokat tartalmazó adatbázisaikon. Ezek jelentős könnyítést eredményezhetnek a szervezet részére a GDPR értesítési kötelezettsége alóli mentesülés miatt.

60 Eht. 156. § (5) bekezdés.
61 GDPR 34. cikk (3) bekezdés a) pont.
62 Eht. 156. § (4) bekezdés.

4. Eseménykezelés az Ibtv. és végrehajtási szabályai tükrében

4.1. Alapfogalmak

Az információs hálózatok és elektronikus információs rendszerek[63] biztonságának eléréséhez és fenntartásához a védelmi rendszer megfelelő állapotát szükséges biztosítani, ahol a *védelem* a fenyegetések ellen hozott tevékenységek és intézkedések összessége.

Fenyegetés alatt az Ibtv. értelmében olyan lehetséges műveletet vagy eseményt kell érteni, „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."[64]

Ezek a fenyegetések részben érkezhetnek a globális[65] és/vagy a magyar kibertérből,[66] amely fenyegetések elkerülése érdekében kiemelt kormányzati és társadalmi érdek a közigazgatás és a társadalom működését lehetővé tevő informatikai infrastruktúrák és a nemzeti adatvagyon védelme, az úgynevezett kiberbiztonság[67] és az úgynevezett kibervédelem[68] megerősítése.

A 2013 márciusában elfogadott Magyarország Nemzeti Kiberbiztonsági Stratégiája[69] (a továbbiakban Kiberstratégia) is tartalmazza azokat az elérendő nemzeti célokat, amelyek hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességek kiépítését szorgalmazzák a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás ellen. Azaz a Kiberstratégia nemzeti céljai meghatározzák a kiberbiztonság és kibervédelem állami eszközeit.

A Kiberstratégiában rögzített célok és cselekvési területek a magyar kibertérre terjednek ki, ugyanakkor a feladatok hatékony megvalósításával Magyarország hozzájárul a globális kibertér védelméhez. Nemzeti cselekvési területként és ahhoz igazodó kormányzati intézkedésként rögzítették a Kiberstratégiában a szakosított intézmények létrehozását és működtetését, amelyek körébe tartoznak azok a speciális szakértelemmel és hatáskörrel rendelkező szervezetek, amelyek a kibervédelem területén kiemelt szerepet töltenek be.[70]

Az Ibtv. az elektronikus információs rendszer biztonságának azt az állapotot tekinti, amelyben a védelem az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelke-

---

63 Ibtv. 1. § (1) bekezdés 14b. pont: Elektronikus információs rendszer: elektronikus információs rendszernek tekinthető az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; valamint minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; továbbá ezen elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

64 Ibtv. 1. § (1) bekezdés 19. pont.

65 Ibtv. 1. § (1) bekezdés 22. pont: „Globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese."

66 Ibtv. 1. § (1) bekezdés 35. pont: „Magyar kibertér a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne."

67 Ibtv. 1. § (1) bekezdés 26. pont: „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."

68 Ibtv. 1. § (1) bekezdés 27. pont: a kibertérből jelentkező fenyegetések elleni védelem.

69 1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

70 Lásd részletezve: Az eseménykezelésben részt vevő szervezetek köre című alfejezetben.

zésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[71] Azaz a védelem megvalósítása során az összes számításba vehető fenyegetést kell figyelembe venni, azzal, hogy a védelem az elektronikus információs rendszer valamennyi elemére kiterjed és folyamatában megvalósul, továbbá költségei arányosak a fenyegetések által okozható károkkal. Ezt tekintjük a zárt,[72] folytonos,[73] teljes körű[74] és kockázatokkal arányos védelem[75] elvének. Ezen elv érvényesítésének támogatására az Ibtv. az alábbi védelmi formákat határozza meg:

a) az adminisztratív védelmet, amely a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések összessége, és az oktatás;[76]

b) a fizikai védelmet, amely a fizikai térben megvalósuló fenyegetések elleni védelem, ide sorolva a természeti csapás elleni és a mechanikai, az élőerős védelmet, az elektronikai jelzőrendszert, a beléptető- és a megfigyelőrendszert, a tápáramellátást, a sugárzott és vezetett zavarvédelmet, a klimatizálást és a tűzvédelmet;[77]

c) a logikai védelmet, amely az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.[78]

Ha a fenyegetések ellen felépített védelmi intézkedések a kívánt hatást nem érik el, vagy azok sérülnek – meghibásodás vagy vis maior, illetve szándékosság esetén –, olyan események vagy eseménysorozatok következnek be, amelyek kezelése eltérő működést kíván mind az elektronikus információs rendszer üzemeltetése, mind az egyén, mind a szervezet oldalán, akkor a működést – különleges szerepe miatt – a szabályozási oldalról (is) szükséges kezelni.

4.2. AZ Eseménykezeléssel összefüggő szabályok

A fenti védelmi intézkedések célja a biztonsági események bekövetkezésének elkerülése. Az Ibtv. értelmében biztonsági esemény az a 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.[79]

---

71 Ibtv. 1. § (1) bekezdés 15. pont.

72 Ibtv. 1. § (1) bekezdés 48. pont: „Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem."

73 Ibtv. 1. § (1) bekezdés 21. pont: „Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem."

74 Ibtv. 1. § (1) bekezdés 44. pont: „Teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem."

75 Ibtv. 1. § (1) bekezdés 31. pont: „Kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével."

76 Ibtv. 1. § (1) bekezdés 6. pont.

77 Ibtv. 1. § (1) bekezdés 20. pont.

78 Ibtv. 1. § (1) bekezdés 34. pont.

79 Ibtv. 1. § (1) bekezdés 9. pont.

A biztonsági esemény fogalmának az értelmezéséhez segítséget nyújt, hogy az Ibtv.-ben önálló fogalomként jelenik meg a *bizalmasság,*[80] a *sértetlenség,*[81] a *rendelkezésre állás.*[82] Az értelmező rendelkezések rögzítik, hogy:

a) Bizalmasságnak az elektronikus információs rendszer azon tulajdonságát kell érteni, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.

b) Sértetlenségnek az adat azon tulajdonságát kell érteni, amely szerint:

ba) az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyeznek, az adat az elvárt forrásból származik, azaz hiteles, és

bb) az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága is, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

c) Rendelkezésre állás alatt annak biztosítását kell érteni, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek, és az abban kezelt adatok felhasználhatóak.

A hatályos szabályozási környezet megkülönbözteti a biztonsági esemény fogalmát a súlyos biztonsági esemény fogalmától. Súlyos biztonsági eseménynek[83] kell tekinteni azt az informatikai eseményt, amely bekövetkezése esetén:

a) az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet;

b) emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;

c) súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben;

d) alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.

---

80 Ibtv. 1. § (1) bekezdés 8. pont.

81 Ibtv. 1. § (1) bekezdés 39. pont.

82 Ibtv. 1. § (1) bekezdés 38. pont.

83 Ibtv. 1. § (1) bekezdés 41.a pont.

*Kritikus adat*nak[84] az Infotv. értelmező rendelkezései által meghatározott személyes adat, különleges adat[85] vagy valamely jogszabállyal védett adat tekinthető. Utóbbi védett adatok körébe tartozik például a bűnügyi személyes adat[86] vagy a minősített adat védelméről szóló 2009. évi CLV. törvény értelmező rendelkezései által meghatározott nemzeti vagy külföldi minősített adat.[87]

Itt szükséges megjegyezni, hogy a BM rendelet 1. mellékletének 2. pontja szerint az 5. biztonsági osztályba sorolt elektronikus információs rendszer esetében kiemelkedően nagy káresemény következhet be, ha:

a) kiemelten nagy mennyiségű különleges személyes adat sérülhet;
b) emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
c) a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
d) az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
e) a lehetséges társadalmi-politikai hatás következtében súlyos bizalomvesztés lép fel az érintett szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
f) az üzlet- vagy ügymenet szempontjából nagy értékű, üzleti titkot vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
g) a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

A fentiekből az a következtetés vonható le, hogy súlyos biztonsági esemény bekövetkezésével a legmagasabb, 5-ös biztonsági osztályba sorolt elektronikus információs rendszer esetében kell számolni.

Egy adott biztonsági esemény bekövetkezését követően az esemény által kiváltott hatásnál figyelembe kell venni, hogy az milyen időtartamban állt fenn, milyen kiterjedésű volt – adott esetben

---

84 Ibtv. 1. § (1) bekezdés 32. a pont.

85 Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 2. és 3. pontja.
2: „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.”
3: „Különleges adat:
a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.”

86 Infotv. 3. § 4. pont: „Bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.”

87 A minősített adat védelméről szóló 2009. évi CLV. törvény 3. § 1. pontja:
„a) nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti, és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;
b) külföldi minősített adat: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.”

földrajzi értelemben is – milyen mértékű problémát, zavart okozott (adott esetben az elektronikus információs rendszer működésén túl az állam, a társadalom és a gazdaság tevékenységére), hány felhasználót és/vagy szolgáltatást érintett. A kiváltott hatás befolyásolja a választott eseménykezelést.

Az Ibtv. a biztonsági esemény kezelését fogalmi szinten határozza meg, ide sorolja:

a) a dokumentálást,
b) a következmények felszámolását,
c) a bekövetkezés okainak és felelőseinek megállapítását,
d) a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet.[88]

Bármely biztonsági esemény bekövetkezésekor intézkedni kell annak azonnali és hatékony kezelésével kapcsolatban. Az eseménykezelés történhet:

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

azzal, hogy a tevékenység járuljon hozzá az újbóli vagy megismételt biztonsági események bekövetkezése valószínűségének csökkentéséhez és a bekövetkezhető kár minimalizálásához.

Ennek érvényesítése érdekében az Ibtv. alapvető követelményként rögzíti,[89] hogy az intézkedéseknek a biztonsági események kezelése mellett – a PreDeCo (Preventive-Detective-Corrective) elvet alapul véve – támogatniuk kell:

a) a megelőzést, azaz a fenyegetés által okozható hatás bekövetkezésének elkerülését,[90]
b) a korai figyelmeztetést, azaz olyan aktív szervezeti cselekvést, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni,[91]
c) az észlelést, azaz a biztonsági esemény bekövetkezésének felismerését,[92]
d) a reagálást, amely a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedéseket foglalja magában.[93]

Az elektronikus információs rendszerek védelmének körében – a fentebb már említett – külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedések is tartalmaznak az eseménykezelésre vonatkozó közvetlen rendelkezést.

A BM rendelet 2. melléklete[94] a 4. biztonsági szervezeti szint követelményei között előírja:

a) az azonnali és eredményes, előre meghatározott biztonsági intézkedések bevezetését a feltárt vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges vagy bekövetkezett biztonsági esemény kezelését is, valamint
b) az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrásból származó,

88 Ibtv. 1. § (1) bekezdés 10. pont.
89 Ibtv. 6. §.
90 Ibtv. 1. § (1) bekezdés 36. pont.
91 Ibtv. 1. § (1) bekezdés 32. pont.
92 Ibtv. 1. § (1) bekezdés 17. pont.
93 Ibtv. 1. § (1) bekezdés 37. pont.
94 Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet 2. melléklet 4.1. alpontjának 4.1.3. és 4.1.6. alpontjai.

potenciális vagy valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárás vagy biztonsági ellenőrzés elvégezését.

A BM rendelet 3. melléklete[95] az adminisztratív védelmi intézkedések között rögzíti a biztonsági események kezelésére vonatkozóan követelményeket. Az intézkedések az adott elektronikus információs rendszer biztonsági osztályba sorolt értékének növekedésével arányosan szigorodnak, magasabb osztályba sorolt érték esetén egyre összetettebb cselekvést igényelnek a szervezet részéről. A BM rendelet az eseménykezelésre vonatkozóan az 1. és 2. biztonsági osztályt illetően nem rögzít önálló adminisztratív védelmi intézkedéseket, a 3. biztonsági osztálytól kezdődően az alábbi intézkedések[96] megtétele kötelező a szervezet vagy szervezeti egység számára.

A BM rendelet 4. mellékletének 3. alcíme *(Védelmi intézkedési katalógus)* az adminisztratív, fizikai és logikai védelmi intézkedések között is rögzít biztonsági események kezelésére vonatkozó részletszabályokat, így például informatikai biztonsági szabályzat elkészítését, fizikai biztonsági esemény (például fizikai behatolás) észlelésére és reagálására, valamint annak naplózására vonatkozó feladatok ellátását, biztonsági riasztások és tájékoztatások kezelését.

A BM rendeletben rögzített minden védelmi intézkedési forma tartalmaz előírást arra vonatkozóan, hogy az Ibtv.-ben meghatározott zárt, teljes körű, folytonos és a kockázatokkal arányos védelem előírásai a szabályozás és a gyakorlat szintjén egyaránt megvalósuljanak.

4.3. Az eseménykezelésben részt vevő nemzeti szervezetek

Az alábbiakban bemutatjuk az Ibtv.-ben nevesített és meghatározott azon szervezeteket, amelyek az eseménykezeléssel összefüggő feladatot látnak el.

Az Ibtv. a hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét a Kormány által kijelölt hatóság (a továbbiakban Hatóság) látja el.[97] A hatósági feladatokat jelenleg a Nemzetbiztonsági Szakszolgálat mint kijelölt Nemzeti Elektronikus Információbiztonsági Hatóság látja el.[98]

A Hatóság feladata[99] az eseménykezeléssel összefüggésben és ahhoz kapcsolódóan:

a) a biztonsági eseményekkel kapcsolatos bejelentések kivizsgálására irányuló hatósági eljárás megindítása,

b) az eseménykezelő központokkal való kapcsolattartás,

c) a biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott értesítések nyilvántartása és kezelése.

---

95 BM rendelet 3. melléklet 2. alcíme alatt szereplő táblázat 3.1. alpontjának 3.1.5. alpontja.

96 BM rendelet 4. melléklet 3.1.5. alcím alapján.

97 Ibtv. 14. § (1) bekezdés.

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

99 Ibtv.14. § (2) bekezdése és 15. § (1) bekezdés.

A Hatóság a biztonsági esemény kivizsgálására kötelezheti a szervezetet, ha pedig a szervezet a kötelezést nem teljesíti, bírságot szabhat ki.[100] A biztonsági esemény bekövetkezésének elhárítására fordított költségének megtérítésére kötelezi a szervezet, ha a szervezet:

a) a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére vonatkozó hatósági felszólítást figyelmen kívül hagyja, vagy

b) a Hatóság által javasolt védelmi intézkedéseket önhibájából nem teljesíti és ennek következtében az elektronikus információs rendszert olyan súlyos biztonsági esemény éri, vagy annak közvetlen bekövetkezése fenyegeti, amely a szervezet működéséhez szükséges alapvető információk vagy személyes adatok sérülésével jár.[101]

A Hatóság jogosult véleményezési jogot gyakorolni a kormányzati eseménykezelő központnak az ágazatok közötti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban.[102]

Az Ibtv. rögzíti,[103] hogy biztonsági esemény kivizsgálását a szervezet a Hatóság felhívása nélkül is kezdeményezheti – zárt célú elektronikus információs rendszerek, európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemek, valamint nemzetbiztonsági védelem alá eső szervezetek kivételével – a kormányzati eseménykezelő központnál vagy telephely biztonsági tanúsítvánnyal, továbbá a feladat ellátásához szükséges szakértelemmel és infrastrukturális feltételekkel rendelkező gazdálkodó szervezetnél.

A Kormány eseménykezelő központként (a továbbiakban: Központ) a Nemzetbiztonsági Szakszolgálatot jelöli ki. A Központ ellátja az alábbi feladatokat:

a) a biztonsági események nemzeti szintű nyomon követése;

b) a kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatás, korai előrejelzés, riasztás, bejelentéstétel és információterjesztés az érdekeltek számára;

c) reagálás a biztonsági eseményekre;

d) dinamikus kockázat- és eseményelemzések, valamint a biztonsági eseményekkel kapcsolatos helyzetkép készítése;

e) sérülékenységvizsgálat lefolytatása.[104]

A Központ a biztonságiesemény-kezelési feladatkörében felelős a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítéséért, a biztonsági eseményekről nyilvántartás vezetéséért, valamint a külön kormányrendelet szerinti korai figyelmeztető rendszer működtetéséért.[105]

---

100 Ibtv. 18. § (1) bekezdés.

101 Ibtv. 16. § (6) bekezdés.

102 Ibtv. 16. § (1) bekezdés.

103 Ibtv. 18. § (2)–(9) bekezdés.

104 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól, 3. § (6) bekezdés.

105 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól, 4. §.

5. Intézkedési terv a biztonsági események kezelésére

Az Ibtv. a szervezet vezetőjének felelősségi körébe tartozóan rögzíti,[106] hogy a szervezet elektronikus információs rendszereinek védelme körében:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését;
b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését;
c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg;
d) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot;
e) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról;
f) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak;
g) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről;
h) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről;
i) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek;
j) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek;
k) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért;
l) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.[107]

Az Ibtv. szerint, ha a biztonsági osztályba és a biztonsági szintbe sorolás alkalmával az adott elektronikus információs rendszerre vonatkozóan hiányosságot állapítanak meg, vagy a szervezet biztonsági szintje alacsonyabb, mint az előírt biztonsági alapszint, akkor a vizsgálatot követő 90 napon belül cselekvési tervet kell készíteni a hiányosság megszüntetésére és az előírt biztonsági szint elérésére.[108] A cselekvési terv készítése az elektronikus információs rendszer biztonságát érintő változás vagy új elektronikus információs rendszer bevezetésekor elvégzett soron kívüli felülvizsgálat esetén is kötelező, amennyiben a felülvizsgálat eredménye alapján meghatározott biztonsági szint alacsonyabb, mint a szervezetre vagy szervezeti egységre előírt biztonsági alapszint.[109]

[106] Ibtv. 11. § (1) bekezdés.
[107] Ibtv. 11. § (1) bekezdés.
[108] Ibtv. 8. § (5) bekezdés és 10. § (2) bekezdés.
[109] Ibtv. 10. § (7) bekezdés.

A NIS irányelv és a GDPR rendelet nem nevesíti az eseménykezeléssel (legyen az adatvédelmi incidens vagy biztonsági esemény) kapcsolatban a cselekvési vagy az intézkedési terv készítését. Erre vonatkozó tételes norma az Ibtv. szabályai között lelhető fel.

6. Irodalomjegyzék

Digitális Menetrend: A Bizottság akcióterve az európai jólét fellendítésére. Brüsszel, 2010. május 19. Elérhetőség: europa.eu/rapid/press-release_IP-10-581_hu.htm (utolsó letöltés: 2017. november 03.)

Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz felhasználásával –. Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest, 2016. április. Elérhetőség: nhit.hu/dokumentum/172/Feher_konyv_megalapozo_tanulmany_201607.pdf (utolsó letöltés: 2017. november 03.)

Nemzeti Adatvédelmi és Információszabadság Hatóság adatvédelmi szótára. Elérhetőség: naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2017. 11. 03.)

Szőke Gergely László (2017): Értesítési kötelezettség az adatvédelmi incidensek esetén – elméleti és gyakorlati kérdések. JURA, 2017/1. 140–153.

7. Jogszabálytár

- 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

net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500185.kor

- A minősített adat védelméről szóló 2009. évi CLV. törvény

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

- A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 95/46/EK irányelv

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

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

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

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

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

- Az elektronikus hírközlésről szóló 2003. évi C. törvény

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

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

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

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

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

- 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

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

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

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

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

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

kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf

- Az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet

https://net.jogtar.hu/jogszabaly?docid=A1800271.KOR

FOGALOMTÁR

Fogalom	Definíció
(FIRST) CSIRT	Forum of Incident Response and Security Teams. Számítógép-biztonsági Incidenskezelő Csoport – Computer Security Incident Response Team.
(TI) CSIRT	Trusted Introducer. Számítógép-biztonsági Incidenskezelő Csoport – Computer Security Incident Response Team.
ACPI	Advanced Configuration and Power Interface, az APM felváltására készült energiagazdálkodási rendszer. Az utóbbival ellentétben itt nem a BIOS irányítja a folyamatokat, hanem az operációs rendszer.
ACT	Allied Command Transformation – Szövetséges Transzformációs Parancsnokság.
Adatbiztonság	Az adatok fizikai biztonságát szolgáló eljárások.
Adatvédelem	A személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.
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.
Advise	Tanácsadás.
AMT	Intel Active Management Technology.
APWG	Anti-Phishing Working Group.
ASF	Advanced Streaming Format – a Microsoft által szabadalmazott digitális audio/digitális videócsomagoló (konténer), amit különösen a médiafolyamok továbbítására szántak.
ATP	Advanced Persistent Threat: fejlett támadás.
BAH	Booz-Allen Hamilton.
Bejelentés (logging)	A hívást és a hibakezelő rendszerben való rögzítést is jelenti, és nem különböztetik meg a felhasználókat.
BfV	Német Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz).
Bizalmasság	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.
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.
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.

Biztonságmenedzsment információs rendszere (security management information system)	Azon segédeszközök, adatok és információk összessége, amelyet az információbiztonság-menedzsment támogatására használnak.
CA	Certification Authority – Hitelesítésszolgáltató.
CC	Common Criteria – Közös Követelmények.
CCD CoE	Cooperative Cyber Defence Centre of Excellence – Kooperatív Kibervédelmi Kiválósági Központ.
CDMA	Cyber Defence Management Authority.
CDMB	Cyber Defence Management Board.
CECSP	Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform).
CERT	Számítógép-vészhelyzet Kezelő Csoport – Computer Emergency Response Team.
CERT/CC	Számítógép-vészhelyzet Kezelő Csoport – koordinációs központ (Computer Emergency Response Team – Coordination Center).
CERT/CC	CERT Competence Center.
CFIA	Component Failure Impact Analysis.
Címtár	Azonosítja és hitelesíti a szervezet felhasználóit, meghatározva alapvető jogosultságukat. A felhasználók és munkaállomások tevékenysége központilag korlátozható, a biztonsági házirendek központilag definiálhatók.
CIP CSIRT	Kritikusinfrastruktúra-védelemért felelős csoport – Critical Infrastructure Protection.
CIS	Center of Internet Security.
CMS	Content Management System.
COBIT	Control Objectives for Information and Related Technologies.
COBIT	Control Objectives for IT and Related Technology.
Code of Practice	Magatartási kódex.
Cookie	Egy információcsomag, amelyet a szerver küld a böngészőnek, majd a böngésző visszaküld a szervernek minden, a szerver felé irányított kérés alkalmával. Segíti a böngészést, de biztonsági kockázata is van.
COSI	Európai Unió Belső Biztonsági Állandó Bizottsága.
CRAMM	Risk Analysis and Management Method.
CVSS	Common Vulnerability Scoring System.
Cyberbullying	Elektronikus zaklatás.
CSA	Cloud Security Alliance
CSIRT	Számítógép-biztonsági Incidenskezelő Csoport – Computer Security Incident Response Team.
CSIS	Stratégiai és Nemzetközi Tanulmányok Központ –Center for Strategic and International Studies.
DDoS	Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás.
Dead analízis	A lefoglalt anyagokat (disk image, memória image, számítógép) analizálja.
DENSEK projekt	Distributed ENergy SEcurity Knowledge.
Disaster recovery site	Egy olyan része az informatikai rendszernek, amely attól fizikailag elkülönülő helyen üzemel, és az éles rendszer minden elemét és adatát tartalmazza.
DLP	Adatszivárgást megelőző eszköz.
DMZ	A demilitarizált zóna a hálózat egy olyan része, amely mind az internet irányából, mind pedig a munkahelyi hálózatról csak speciális tűzfalszabályokon keresztül érhető el.

DNS szerver	Domain Name System.
DoD	Department of Defense.
DoS	Denial of Service – szolgáltatásmegtagadással járó támadás.
Dump file	Egy pillanatfelvétel az alkalmazásról.
EC3	European Cybercrime Centre – Europol-Számítástechnikai Bűnözés Elleni Központ.
EDR	Endpoint Detection and Response.
EE-ISAC	European Energy-Information Sharing Analysis Centre.
EMPACT Program	Európai Multidiszciplináris Platform a bűnügyi fenyegetés ellen – European Multidisciplinary Platform against Criminal Threats.
ENISA	Európai Uniós Hálózat- és Információbiztonsági Ügynökség – European Union Agency for Network and Information Security.
Eredendő ok (root cause)	Egy incidens vagy probléma mögöttes vagy eredeti oka.
Esemény (event)	Olyan állapotváltozás, amelynek jelentősége van egy konfigurációs elemben vagy az IT szolgáltatás menedzsmentjében.
Észlelés (detection)	A kiterjesztett incidens életciklusának egy szakasza. Az észlelés hatására az incidens ismertté válik a szolgáltató számára.
Európai digitális menetrend	Célja, hogy a digitális technológia előnyei az európai polgárok és vállalkozások számára minél szélesebb körben elérhetőek legyenek.
EUROPOL	Európai Rendőrségi Hivatal.
Failover	Az eszközöknek egy olyan felhasználása, amikor az informatikai rendszer azonos funkciójú elemeiből két vagy több példány folyamatosan működik a rendszerben, de egy időben mindig csak egy érhető el belőle.
FAIR	Fejlesztéspolitikai Adatbázis és Információs Rendszer.
Fancy Bear	Hackercsoport.
FI-ISAC	European Financial Institutes – Information Sharing and Analysis Centre.
Forensics	A bizonyítékokat olyan minőségben, és azoknak az alapelveknek a betartásával gyűjtsük össze és analizáljuk, amelyek garantálják, hogy akár egy bírósági tárgyaláson is elfogadhatóak lesznek.
Forrótartalék (hot start, hot standby)	Olyan létesítmény, amelyben az eszközök azonnal képesek a szoftverek, archivált adatok feltöltésére és futtatására.
FTA	Fault Tree Analysis – hibafaelemzés.
FTK	The Forensic Toolkit, képes többek között disk- és memóriaimagelésre is.
GAO	U. S. Government Accountability Office.
GDPR	Európai Unió Általános Adatvédelmi Rendelete – General Data Protection Regulation.
GovCERT	Kormányzati Eseménykezelő Központ.
GPT	Guid Partition Table – partícióeloszlás-táblázat.
Hálózati szegmentáció	A különböző funkciójú infrastruktúraelemeket egymástól hálózati eszközök segítségével választják el.
Hash függvény	Olyan, az informatikában használt eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le.
Hiba (error/fault)	Tervezési hiányosság vagy helytelen működés, amely meghibásodást okoz egy vagy több konfigurációelemben vagy IT-szolgáltatásban.
Hidegtartalék (cold start, cold standby)	Olyan hordozható vagy helyhez kötött létesítmény, amelyben alapinfrastruktúrával (kábelezés, áramellátás) rendelkező számítógépközpont van.

Hívás (call)	Telefonhívás a felhasználótól az ügyfélszolgálatra.
HSAC	Homeland Security Advisory Council – Belbiztonsági tanácsadó testület (USA).
Hun-CERT	Két önkéntes alapon működő CSIRT.
Iaas	Azonnal elérhető számítási infrastruktúra.
IBSZ	Informatikai biztonsági szabályzat.
IDC	International Data Corporation.
IDF	Behatolás-detektáló rendszer.
Incidens	Egy IT szolgáltatás be nem tervezett megszakadása, vagy az IT szolgáltatás minőségének csökkenése.
Információbiztonság-menedzsment (information security management)	Ez a folyamat felelős azért, hogy egy szervezet eszközeinek, információinak, adatainak és IT-szolgáltatásainak bizalmassága, integritása és rendelkezésre állása megfeleljen a megállapodott üzleti igényeknek.
IoC	Indicator of Compromise.
IPS	Behatolásmegelőző rendszer.
IPS/IDS rendszer	A külső támadások elleni védelem eszközei, a forgalom folyamatos elemzését végzik, szükség esetén riasztanak és képesek az adott folyamatot letiltani.
IRT	Incidenskezelő csapat.
ISACA	Információrendszer-menedzserek és ellenőrök nemzetközi szakmai szervezete.
Ismert hiba (known error)	Olyan probléma, amelynek van dokumentált eredendő oka és megkerülő megoldása.
ITGI	IT Governance Institute
ITIL	Nemzetközi szabvány, informatikai rendszerek üzemeltetésére és fejlesztésére vonatkozó ajánlás, módszertan.
ITIL	Information Technology Infrastructure Library.
ITILv3	Legfirssebb szabványverzió.
IWWN	Nemzetközi kiberbiztonsági fórum.
Katasztrófa (disaster)	Olyan hirtelen, nem tervezett, szerencsétlen esemény, amely jelentős kárt vagy veszteséget okoz.
Katasztrófa-elhárítási Terv (Disaster Recovery Plan – DRP)	Azoknak az eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes a káresemények következtében kiesett szolgáltatásait a normál működési szintre visszaállítani.
KEF	Közbeszerzési és Ellátási Főigazgatóság.
Kibertér	A számítógéprendszerek és -hálózatok által alkotott metaforikus tér, amelyben elektronikus adatok tárolódnak és online adatforgalom, valamint kommunikáció zajlik.
KNBSZ	Katonai Nemzetbiztonsági Szolgálat.
Különleges személyes adat	A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, valamint a kóros szenvedélyre vonatkozó és a bűnügyi személyes adat.
Live analízis	A futó számítógép vizsgálata.
LMS	Learning Management System.
Load ballancing	Az eszközöknek egy olyan felhasználása, amikor az informatikai rendszer azonos funkciójú elemeiből két vagy több példány folyamatosan működik a rendszerben,és folyamatosan elérhetőek a felhasználók számára.
LRLIBEK	Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ.

Malware	Rosszindulatú program.
Meghibásodás (failure)	Annak a képességnek az elvesztése, hogy valami előírás szerint működjön vagy a kívánt eredmény előálljon.
Megkerülő megoldás (workaround)	Olyan incidens vagy probléma hatásának csökkentése vagy kiküszöbölése, amelyre teljes megoldás még nincs (például egy meghibásodott konfigurációelem újraindítása).
Megoldás (resolution)	Intézkedés egy incidens vagy probléma eredendő okának kijavítására vagy egy megkerülő megoldás megvalósítására.
Microsoft event log	Microsoft naplózási protokoll.
MILCERT	honvédelmi/katonai CERT.
Minőség (quality)	Egy termék, szolgáltatás vagy folyamat képessége arra vonatkozóan, hogy a tervezett értéket nyújtsa (például egy hardverkomponenst jó minőségűnek kell tekinteni, ha az elvárások szerint működik és nyújtja az elvárt megbízhatóságot).
MOF	Microsoft Operations Framework.
MTA SZTAKI	Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézet.
Működésfolytonossági Terv (MFT), (Business Continuity Plan – BCP)	Azoknak az információknak és eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes váratlan káreseményekre hatékonyan reagálni és kritikus üzleti folyamatait egy elfogadható szinten fenntartani. MFT-nek nevezik azt a keretrendszert, amely átfogja a működésfolytonosság tervezési, megvalósítási és ellenőrzési fázisait.
NAC	Network Access Control – Hálózati Hozzáférés Felügyelet.
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság.
NCSC	Nemzeti Kiberbiztonsági Központok – National Cyber Security Center.
NEIH	Nemzeti Elektronikus Információbiztonsági Hatóság.
Nemzeti adatvagyon	A Magyarországgal kapcsolatos vagy a tulajdonában lévő hozzáférhető adatok összessége.
NIIF-CSIRT	Nemzeti Információs Infrastruktúra Fejlesztés.
NIIFI-CSIRT	Két önkéntes alapon működő CSIRT.
NIST	Nemzeti Szabvány és Technológiai Intézete – National Institute of Standards and Technology.
NKI	Nemzeti Kibervédelmi Intézet.
NMHH	Nemzeti Média- és Hírközlési Hatóság.
NMHH-OIHF	Nemzeti Média- és Hírközlési Hatóság, Országos Informatikai és Hírközlési Főügyelet.
NMSDB	Network Management System Database.
Nulladik napi fenyegetés	Egy biztonsági fenyegetés, amely valamely számítógépes alkalmazás olyan sebezhetőségét használja ki, amit még nem publikáltak, a szoftver fejlesztője nem tud róla, vagy nem érhető még el az azt foltozó biztonsági javítás.
OECD	Gazdasági Együttműködési és Fejlesztési Szervezet.
ORFK NEBEK	Országos Rendőr-főkapitányság Nemzetközi Bűnügyi Együttműködési Központ.
OSCE	Organization for Security and Co-operation in Europe – Európai Biztonsági és Együttműködési Szervezet (EBESZ).
PaaS	Azonnal elérhető platform
PDCA elv	Plan-Do-Check-Act – Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás.
PKI	Public key infrastructure – közösségi kulcs infrastruktúra.
PreDeCo elv	Preventive-Detective-Corrective – Megelőzés-Felderítés-Korrigálás.

Problémamenedzsment (Problem Management)	A szolgáltatás üzemképtelenségének minimalizálása a fő célja.
Proxy	Helyettesítő/kiváltó.
Ransomware	Zsarolóvírus.
Rendelkezésre állás	Az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek, és az abban kezelt adatok felhasználhatóak.
Reporting	Gyakorlatok megosztása.
Rootkit	Olyan szoftvereszközök, amelyek segítségével egy cracker könnyen visszatérhet a „tett színhelyére”, ha már korábban beférkőzött a rendszerbe, hogy bizalmas adatokat gyűjtsön a fertőzött számítógépről.
SaaS	Azonnal elérhető szoftver.
Sandbox	Olyan ellenőrzött – valós világhoz közeli – informatikai környezet, ahol megfigyelhető egy állomány futtatása során annak tevékenysége úgy, hogy az ne jelentsen veszélyt a teljes informatikai rendszerre.
SECaaS	Azonnal elérhető biztonsági szolgáltatás.
SEM	Security Event Management – Biztonsági Eseménykezelő.
SERT	Security Emergency Response Team – Sürgősségi Reagáló Biztonsági Csapat.
Sértetlenség	Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyeznek, az adat az elvárt forrásból származik, azaz hiteles és származása ellenőrizhető.
SIEM	Security Information and Event Management – Biztonsági Információ és Eseménykezelő Csoport.
SIM	Security Information Management – Biztonsági információkezelés.
SLA	Service Level Agreement – Szolgáltatásiszint-megállapodás.
SNMP	Simple Network Management Protocol – Egyszerű hálózatkezelő protokoll.
SOA	Szolgáltatásorientált architektúra (Service Oriented Architecture).
SOAR	Biztonsági eseménykezelő rendszer.
SOC	Biztonsági Üzemeltetési Központok – Security Operation központok.
Social engineering	Támadási forma, ahol a hozzáféréssel rendelkezőket zsarolják vagy befolyásolják, esetleg bizalmába férkőzve kihasználják hiszékenységét.
SSO	Single Sign-On – egyszeri bejelentkezési módszer.
Stuxnet	Annak a rosszindulatú programnak a neve, amelyet célzottan csak az iráni urándúsító létesítmény ellen terveztek, és amely csak azt támadta meg, annak ellenére, hogy több százezer számítógépen is megtalálták később.
SWOT analízis	A stratégiaalkotás folyamatának egyik lépése. Strengths – erősségek; Weaknesses – gyengeségek; Opportunities – lehetőségek; Threats – veszélyek.
SYN Flood	Elárasztásos támadás.
Syslog	Linux naplózási protokoll.
Szolgáltatás helyreállítása (restoration of service)	Intézkedés egy IT-szolgáltatás javítás és visszaállítás utáni visszaadásáról a felhasználóknak.
Szolgáltatásstratégia (Service Strategy)	A folyamat azonosítja azokat a piaci lehetőségeket, amelyeket új szolgáltatások bevezetésével ki lehetne aknázni.
Szolgáltatástervezés (Service Design)	A folyamat eredményeként projektterv készül az előző lépésben kidolgozott stratégia által felvázolt szolgáltatás konkrét megvalósítására.

TARANSITS	Egy európai projekt, amelynek célja az új CSIRT-ek létrehozásának és a már működő CSIRT-ek bővítésének, fejlesztésének támogatása speciális tanfolyamok által.
TCO	Total Cost of Ownership –Teljes Bekerülési Érték.
TI	Fenyegetettségi információszolgáltatást.
Tivoli Security Policy Manager	Leválasztja a biztonsági irányelveket az alkalmazásokról, lehetővé téve az alkalmazásjogosítványok központosítását és leegyszerűsítését, valamint az adathozzáférés részletes szabályozását.
TPM	Trusted Platform Module.
Tűzfal	A külső támadások ellen védik a szervezeti infrastruktúra elemeit.
Üzleti hatáselemzés (Business Impact Analysis – BIA)	Eljárás, amely során a szervezet meghatározza a kritikus üzleti folyamatok megszakadásának következményeit és a normál működési állapotra való visszaállás elvárásait.
Üzletmenet-folytonosság menedzsment (Business Continuity Management – BCM)	Az a folyamat, amelynek során egy szervezet felkészül a kritikus üzleti folyamatok megszakadására, vagy kiesése esetén a folyamatok visszaállítására.
Vis maior	Váratlan, nem befolyásolható esemény.
Volatility	Változékonyság.
Volatility	Memória dump analizáló eszköz.
VPN	Virtual private network – virtuális magánhálózat.
Warning	Riasztás.
WARP	Warning, Advise and Reporting Points.
WBEM	Web-Based Enterprise Management.
WMI	Windows Management Interface.
Worm attack	Féregtámadás.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Dékán

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Császár-Biró Anna

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-091-9

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

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE