Bodó Attila Pál – Haddad Richárd –
Marsi Tamás – Pongrácz Péter

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME

Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára

Nemzeti Közszolgálati Egyetem, Budapest

A Nemzeti Közszolgálati Egyetem kiadványa

Szerkesztő:
Deák Veronika

Szerzők:
© Dr. Bodó Attila Pál
© Haddad Richárd
© Marsi Tamás
© Pongrácz Péter

Szakmai lektor:
Dr. Buttyán Levente

2022-ben a hatályosítást végezte:
Legárd Ildikó, hatályosításért felelős szakmai szakértő
Mikula Fanni

A hatályosított kézirat lezárásának dátuma:
2022. február 25.

Eredeti megjelenés éve:
2019

Kiadja:
© Nemzeti közszolgálati Egyetem, 2022
Közigazgatási Továbbképzési Intézet

Felelős kiadó:
Prof. Dr. Kis Norbert
rektorhelyettes

TARTALOM

I. Bodó Attila Pál: Újdonságok a magyar kibervédelmi szabályozásban és a kritikus információs infrastruktúrák szabályozása 6

1. Bevezető gondolatok 6
2. Változások a kibervédelem stratégiai szintjén 6
   - *2.1. A NIS-irányelv és hatása 7*
   - *2.2. Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája 11*
3. Főbb változások a magyar kibervédelmi szabályozásban 16
   - *3.1. Az Ibtv. változásai 17*
   - *3.2. A végrehajtási rendeletek változásai 19*
4. A kritikus infrastruktúrával kapcsolatos nemzeti szabályozás 28
   - *4.1. Az Lrtv. szerinti ágazatok és alágazatok 28*
   - *4.2. A javaslattevő és a kijelölő hatóságok 30*
   - *4.3. Az Lrtv. szerinti azonosítási eljárás 32*
   - *4.4. Az Lrtv. szerinti kijelölési eljárás 33*
   - *4.5. Horizontális és ágazati kritériumok 36*
   - *4.6. Hatósági feladatok 38*
   - *4.7. Ellenőrzési feladatok 40*
   - *4.8. Szankció 41*
   - *4.9. Biztonsági összekötő 42*
   - *4.10. Üzemeltetői feladatok és az üzemeltetői biztonsági terv 43*
   - *4.11. Ágazati szabályok 45*
   - *4.12. Uniós kötelezettségek 45*
5. Mellékletek 46
6. Irodalomjegyzék 55

II. Marsi Tamás: Incidenskezelés kritikus információs infrastruktúrák esetén 56

1. Bevezetés 56
2. A kritikus infrastruktúra fogalma incidenskezelési szempontból 57
   - *2.1. Általános megközelítés 57*
   - *2.2. Európai megközelítés 57*
   - *2.3. A magyar szabályozás 59*
3. Incidenskezelésben érintett hazai szervezet felépítése és feladatai 60
   - *3.1. Esemény- és incidenskezelésben érintett szervek 60*
   - *3.2. Szolgáltatási területek 60*
   - *3.3. A hatóság 65*
4. Biztonsági események bejelentése 68
5. Incidenskezelési sajátosságok kritikus infrastruktúrák esetén 69

6. Incidens esettanulmányok 70
6.1. Útválasztó kompromittálás 70
6.2. Ransomware egy kritikus infrastruktúrában 71
6.3. Illetéktelen elérés. 71
6.4. Tanulságok levonása 72
7. Incidensek keletkezésének megelőzése 72
8. Irodalomjegyzék 73

III. Haddad Richárd: Okoseszközök a kritikus információs infrastruktúrákban, villamosenergetikai fókusszal 74

1. Bevezetés 74
2. IoT/IIoT a villamosenergetikában 75
2.1. AZ IoT és AZ IIoT fogalma 75
2.2. Az IoT- és az IIoT-rendszerek elemei 75
2.3. Az IoT/IIoT-rendszer kialakításának kérdései 77
3. Smart Energy – okos megoldások a villamosenergetikában. 78
3.1. Okos Hálózatok (Smart Grid) 78
3.2. Okos Mérés (Smart Metering) 80
3.3. OkosOtthon (Smart Home) 86
4. Háztartási villamosenergia-rendszerek és informatikai rendszereik. 88
4.1. Vezetékes informatikai rendszerek 88
4.2. Vezeték nélküli informatikai rendszerek 93
4.3. Rövid hatótávolságú vezeték nélküli rendszerek 98
5. Rövidítésjegyzék 108
6. Irodalomjegyzék 110

IV. Pongrácz Péter: Kibertámadások villamosenergetikai környezetben 111

1. Bevezetés 111
2. Eltérések az IT és az OT világai között 111
3. Ismert sebezhetőségek a villamosenergetikai környezet informatikai rendszereiben. 112
4. IT- és OT-védelem kibertámadások ellen 115
4.1. Fenyegetéselemzés és információgyűjtés 117
4.2. Eszközleltár és hálózatbiztonsági monitoring 118
4.3. Incidenskezelés 119
4.4. Fenyegetés és környezet kezelése. 122
5. Kiberbiztonsági műszaki megfelelőségi követelmények villamosenergia-környezetben 123
5.1. Jogszabályi követelmények 123
6. Konkrét kibertámadások és azok tanulságai 125
6.1. Korai kibertámadások ICS-rendszerek ellen 125
6.2. Stuxnet 125
6.3. Havex/Dragonfly 126
6.4. Kibertámadás ukrán áramszolgáltatók ellen 127
6.5. Industroyer/CrashOverride 128
6.6. Támadások az USA villamosenergia-rendszere ellen. 129

7. Számítógép-alapú Social Engineering-technikák bemutatása 129
7.1. Általában a Social Engineering-kockázatokról 129
7.2. Jellemzők ICS-környezetekben. 130
7.3. Supply chain-támadások veszélyei ICS-rendszerekre. 131
8. Villamosenergia-irányító rendszerek kibertámadásának hálózati és informatikai következményei, teendői. 131

Jogszabálytár 134

1. Magyar jogszabályok. 134
2. Európai uniós jogi aktusok. 136
3. Külföldi jogi aktusok 137

Fogalomtár 138

A fogalmak forrásjegyzéke 149

I. BODÓ ATTILA PÁL: ÚJDONSÁGOK A MAGYAR KIBERVÉDELMI SZABÁLYOZÁSBAN ÉS A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK SZABÁLYOZÁSA

1. Bevezető gondolatok

Az elmúlt években a kibervédelem szabályozása az Európai Unióban (a továbbiakban: Unió) és a nemzetállamokban egyaránt jelentős változáson ment keresztül. Az általános szabályozási keretek kezdeti megalkotását követően megjelentek a speciális, az egyes részterületekre összpontosító szabályozási elemek, amelyek hatása a végrehajtás szintjén is jelentkezik. Ugyanakkor egyre erőteljesebbé vált az a törekvés, hogy a szakterületi kidolgozottság mellett az egységes, komplex szabályok gyakorlati alkalmazása is érvényesüljön, és területi korlátok nélkül érvényesíthető legyen. Jelen jegyzetben a szabályozási környezetben bekövetkezett változásokat vizsgáljuk, alapvetően két szempontból. Az egyik az Unió stratégia- és jogalkotása területét érintő speciális szakkérdés, a hálózatbiztonság és az ebből eredő, nemzetállami szinten megjelenő kötelezettségek köre, a másik az önálló, szuverén államok által végzett jogalkotási tevékenység Magyarországra adaptálva. Ezen két megközelítés mellett jelen tananyag külön fejezetben ismerteti a kritikus infrastruktúrákkal kapcsolatos nemzeti szabályozási környezetet, figyelemmel arra, hogy az alapvető szolgáltatók kijelölése tekintetében kapcsolódik az uniós szabályozáshoz. Továbbá ezen témakör főbb elemeinek áttekintése a fent említett változások hatására szükségszerű ahhoz, hogy az információbiztonsággal foglalkozó szakember aktuális és rendszertani elméleti ismereteket szerezzen feladata szakszerű ellátásához és a jó gyakorlatok alkalmazásához.

2. Változások a kibervédelem stratégiai szintjén

A kibervédelem területére vonatkozó stratégiaalkotás uniós és nemzetállami szintje egymással szoros összefüggésben van. Az uniós irányok, adott esetben nemzetállami jogalkotási kötelezettségeket keletkeztető irányelvek, rendeletek, meghatározzák a kibervédelem aktuális mérföldköveit, biztosítva az egységes kereteket. Az Európát ért változó jellegű és mértékű kibertámadások hatására a sebezhetőség, az ellenálló és a reagáló képesség kérdésköre politikai szintre emelkedett, a kibervédelem aktualitása központi témává vált az Unió felsővezetői szintjén is. Ezzel összefügg, hogy az Európai Bizottság elnökének minden év szeptemberében az Európai Parlament előtt az Unió helyzetéről elmondott beszédében is megjelenik a kibervédelem témaköre, mivel az „évértékelés" tájékoztatást ad az elmúlt év eredményeiről és bemutatja a következő év kiemelt feladatait, kiemelve az Európai Bizottság és az Európai Unió előtt álló legfontosabb kihívásokat. Az évértékelő beszédeknek – különös tekintettel a 2017-es tallinni digitális csúcstalálkozó és az azzal párhuzamosan kiadott, *„Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése"* című Európai Parlamenti és a Tanácsi közös közleményre – visszatérő eleme lett a kibervédelem kérdésköre, amely fókuszpontjában az együttműködésen alapuló és komplex kiberbiztonság kialakításának szorgalmazása áll. A 2018-as évértékelés részét képező szándéknyilatkozatban a kibervédelem korábbi beszédekből már ismert, több eleme ismételten megjelenik, így újból előkerül a főbb kezdeményezések között

az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítésére vonatkozó javaslat (2. prioritás). Új elemként jelenik meg az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról szóló rendelet tervezetének (2. prioritás), valamint a kiberbiztonsági eseményekkel szembeni védelemről szóló bizottsági ajánlás (7. prioritás) tervezetének elfogadtatása. Ezen véglegesítés előtt álló szabályozási eszközök mellett az „Erős kiberbiztonság kialakítása Európában" című bizottsági bejelentés központi elemként jeleníti meg a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016. július 6-i 2016/1148/EU európai parlamenti és tanácsi irányelv (a továbbiakban: NIS-irányelv) hatékony végrehajtását és támogatását. A NIS-irányelv alapvetését és hatását – rendelkezéseinek részletes ismertetése nélkül – az alábbiakban tárgyaljuk.[1]

2.1. A NIS-irányelv és hatása[2]

Az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága 2013 februárjában közzétett közös közleménye, *„Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér"* című uniós stratégiában meghatározott prioritásokhoz[3] kapcsolódóan került megalkotásra az első uniós kiberbiztonsági jogszabály, a NIS-irányelv[4]. Az irányelv mint uniós jogi norma sajátossága, hogy az elérendő célt tekintve valamennyi címzett tagállamot kötelezi a végrehajtásra úgy, hogy a nemzeti hatóságok szabadon dönthetnek arról, hogy az uniós szabályokat milyen módszerek és eszközök alkalmazásával teszik a nemzeti jog részévé. A NIS-irányelv a hatálybalépést követően az átültetési kötelezettség teljesítésére 21 hónapot írt elő[5], így minden tagállamnak a nemzeti jogi környezetének áttekintését és az irányelv előírásaival való összhang meg-

[1] A szakanyag lezárást követően a Tanács **2019. április 9-én** elfogadta azt a **kiberbiztonsági jogszabályként** is ismert rendeletet, amely lehetővé teszi az EU számára, hogy célzott korlátozó intézkedéseket vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek külső fenyegetést jelentenek az EU vagy annak tagállamai számára: AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály"))

2020 decemberében az Európai Bizottság és az Európai Külügyi Szolgálat (EKSZ) **új uniós kiberbiztonsági stratégiát** terjesztett elő (Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér; http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001). E stratégia célja, hogy:

- megerősödjön Európa kiberfenyegetésekkel szembeni rezilienciája,
- minden polgár és vállalkozás megbízható szolgáltatásokat és digitális eszközöket vehessen igénybe, és ezek előnyeit teljes mértékben ki tudja használni,
- megőrizze a globális és nyílt internetet, biztosítékot nyújtva ugyanakkor arra, hogy a biztonság mellett az európai értékek és a mindenkit megillető alapvető jogok is védelmet élvezzenek.

[2] 2021. november 26-án az Európai Unió Tanácsa elfogadta az EU egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekkel kapcsolatos álláspontját, amely intézkedések célja, hogy tovább javuljon mind az állami, mind a magánszektornak, illetve az Unió egészének kiberrezilienciája és a kiberbiztonsági eseményekre való reagálási képessége. Elfogadását követően az **új, „NIS 2" elnevezésű irányelv** a hálózati és információs rendszerek biztonságáról szóló jelenlegi irányelv (NIS-irányelv) helyébe lép. Bővebben ld.: https://www.consilium.europa.eu/hu/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/

[3] A stratégia prioritásai:

a) kibertámadásokkal szembeni ellenálló képesség megteremtése;
b) a számítástechnikai bűnözés és a kibertámadások visszaszorítása;
c) kibervédelmi politika kidolgozása és a kiberképességek fejlesztése;
d) a kiberbiztonsághoz szükséges ipari és technológiai erőforrások biztosítása;
e) a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése;
f) számítógépes bűnözéssel foglalkozó nemzeti kiválósági központok hálózatának kialakítása és finanszírozása.

[4] Hatálybalépés: 2016. augusztus 8.

[5] NIS-irányelv 25. cikk (1) bekezdés.

teremtését ezen határidőig el kellett végeznie. Az irányelv rendelkezéseit 2018. május 10-től kezdve kötelező alkalmazni.

A NIS-irányelv alapvetése[6], hogy a hálózati és információs rendszerek és szolgáltatások megbízhatósága és biztonsága kiemelt jelentőségű a gazdaság és a társadalom működése szempontjából, mivel ezen információs rendszerek és szolgáltatások az Unió belső piacának működését tekintve létfontosságúnak minősülnek, alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló mozgásának biztosításában. Ezért a működési zavarok, szélsőséges esetben részleges vagy teljes szolgáltatáskiesések az egyes tagállamok mellett akár az egész Unióra is kihatással lehetnek. Ennek megakadályozása érdekében az irányelv célja, hogy:

a) harmonizált szabályozás bevezetésével megteremtse a hálózati és információs rendszerek biztonságának általános szintjét az Unióban, továbbá
b) a tagállamok kibervédelmi felkészültségének egyenszilárdságát támogassa és
c) a kiberbiztonság általános javítása érdekében valamennyi tagállam számára kötelezettségeket és konkrét intézkedéseket állapítson meg.

Fentiek érdekében – mintegy nemzeti keretként – a NIS-irányelv[7]:

a) a tagállamok számára előírja a hálózati és információs rendszerek biztonsága nemzeti stratégiájának kidolgozását és elfogadását azzal, hogy ezen nemzeti stratégiának a célkitűzések mellett a végrehajtandó konkrét szakpolitikai intézkedéseket is meg kell határoznia és rögzíti annak főbb tartalmi elemeit[8];
b) a tagállamok közötti stratégiai, illetve operatív együttműködés támogatása, a gyors és hatékony információcsere előmozdítása és elősegítése, valamint a közöttük lévő bizalom erősítése céljából:
  ba) együttműködési csoport létrehozását rendeli el a tagállamok, az Európai Bizottság és az ENISA képviselőivel a tagállamok közötti stratégiai együttműködés, tapasztalat- és információcsere támogatása és elősegítése céljából[9];
  bb) létrehozza a számítógép-biztonsági eseményekre reagáló csoportok hálózatát[10] (a továbbiakban: CSIRT-ek), amely a tagállamok CSIRT-jei és a CERT-EU képviselőiből áll és leírja a CSIRT-ek hálózatának feladatait[11];
c) biztonsági és bejelentési követelményeket állapít meg az alapvető szolgáltatásokat nyújtó szereplők[12] és a digitális szolgáltatók[13] számára;
d) a tagállamok részére kötelezettségként írja elő, hogy jelöljenek ki:
  da) a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására nemzeti illetékes hatóságokat[14], amelyek felügyelik a NIS-irányelv átültetését és végrehajtását;

---

[6] NIS-irányelv bevezető (1)–(3) bekezdések.
[7] NIS-irányelv 1. cikk (2) bekezdés.
[8] NIS-irányelv 7. cikk.
[9] NIS-irányelv 11. cikk.
[10] Computer Security Incident Response Teams.
[11] NIS-irányelv 12. cikk.
[12] Alapvető szolgáltatásokat nyújtó szereplőnek minősül az energia, a közlekedési, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és -elosztás, valamint a digitális infrastruktúra ágazatában működő – tagállami szinten kijelölt – közjogi vagy magánjogi szervezet, amely megfelel az alábbi kritériumoknak:
  a) kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt;
  b) az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ;
  c) az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában.
NIS-irányelv 4. cikk 4 pont; 5. cikk 2. pont.
[13] Digitális szolgáltatónak minősül a NIS-irányelv szempontjából az online piactér, az online keresőprogram és a felhőalapú számítástechnikai szolgáltatás. – NIS-irányelv 4. cikk, 6. pont, III. melléklet.
[14] NIS-irányelv 8. cikk (1) bekezdés.

db) olyan, a hálózati és információs rendszerek biztonságáért felelős egyedüli kapcsolattartó pontokat, amelyek összekötő feladatokat látnak el a tagállami hatóságok és más tagállamok, továbbá az unió illetékes intézményei felé[15], valamint

dc) CSIRT-eket[16].

e) előírja a tagállamok részére ágazatonként és alágazatonként az alapvető szolgáltatók azonosítását és kijelölését, az alapvető szolgáltatókról jegyzék összeállítását[17].

A NIS-irányelv előírja[18], hogy a tagállamoknak biztosítaniuk kell, hogy jól működő CSIRT-ekkel rendelkezzenek, amelyek megfelelnek a biztonsági események és kockázatok kezeléséhez szükséges hatékony és kompatibilis képességek garantálására, valamint az eredményes uniós szintű együttműködés biztosítására vonatkozó alapvető követelményeknek azzal, hogy az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók minden típusa tekintetében el kell végezni a CSIRT-ek kijelölését. Ezen előírás alapján Magyarországon nemzeti CSIRT-ként a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete került kijelölésre, aki egyben a nemzeti egyedüli kapcsolattartó pont is[19]. A CSIRT-ek kötelezettségeit és feladatait meghatározó azon alapvetéseket, melyeket a nemzeti szabályozásnak tartalmaznia kell, a NIS-irányelv 1. melléklete tartalmazza, amelyek az alábbiak.

A CSIRT-ek kötelezettsége:

a) biztosítani a hírközlési szolgáltatásaik magas szintű elérhetőségét a kritikus hibapontok kiküszöbölése által,

b) folyamatosan több eszközt fenntartani elérhetőségük és a kapcsolattartás céljára,

c) egyértelműen meghatározni a kommunikációs csatornákat a felhasználók és a partnerek megismertetésével együttesen,

d) hivatali helyiségei és a támogató információs rendszerei biztonságos helyszíneken történő elhelyezése,

e) az üzletmenet-folytonosság biztosítása, amely érdekében:

ea) megfelelő rendszerrel kell rendelkeznie a megkeresések kezelésére és továbbítására,

eb) feladatellátását elegendő létszámú személyi állománnyal kell elvégeznie a folyamatos készenlét biztosításához,

ec) redundáns rendszereket és tartalék munkaterületet kell fenntartania.

A CSIRT-ek feladata:

a) a biztonsági események nemzeti szintű monitoringja,

b) a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés,

c) reagálás a biztonsági eseményekre,

d) dinamikus kockázat- és eseményelemzés, továbbá helyzetkép nyújtása,

e) a CSIRT-ek hálózatában való részvétel,

f) együttműködési kapcsolatok kialakítása a magánszférával,

g) közös vagy szabványosított gyakorlatok elfogadásának és alkalmazásának támogatása a biztonsági események és a kockázatok kezelésére vonatkozó eljárások, valamint a biztonsági események, kockázatok és információk osztályozására szolgáló rendszerek tekintetében.

[15] NIS-irányelv 8. cikk (3) bekezdés.

[16] NIS-irányelv 9. cikk.

[17] NIS-irányelv 5. cikk (1)–(3) bekezdései.

[18] NIS-irányelv bevezetés (34) bekezdés.

[19] 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 (a továbbiakban: hatósági rendelet) 29/A. § (1) bekezdése.

A NIS-irányelv átültetését és végrehajtását felügyelő nemzeti illetékes hatóságnak 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 a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságát (a továbbiakban: BM OKF) jelölte ki[20]. 2018-ban azonban az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet 2. § (1) bekezdése, valamint az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól a 271/2018. (XII. 20.) Korm. rendelet 3. § (1) b) pontja a bejelentés-köteles szolgáltatást nyújtókkal kapcsolatos hatósági, valamint eseménykezelési feladatok ellátására a Nemzetbiztonsági Szakszolgálatot (NBSZ) jelölte ki.

A NIS-irányelv szerint az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó biztonsági követelményeknek arányosaknak kell lenniük az adott hálózati és információs rendszert érintő kockázatokkal, ezért kötelező biztonsági és bejelentési követelményeket állapít meg[21]. Ezek a biztonsági követelmények az alapvető szolgáltatóknál magasabb szintűek, mivel működőképességük alapfeltétel a kritikus társadalmi és gazdasági tevékenységek fenntartásához.

A digitális szolgáltatók esetében a biztonsági követelmények az alábbiak[22]:

a) megfelelő és arányos műszaki és szervezési intézkedések meghatározása és megtétele azzal, hogy az intézkedéseknek biztosítaniuk kell a felmerülő kockázatoknak megfelelő biztonsági szintet és figyelembe kell venniük a következő tényezőket:
  aa) a rendszerek és a létesítmények biztonságát,
  ab) a biztonsági események kezelését,
  ac) az üzletmenet-folytonosság menedzsment követelményét,
  ad) a monitoring, az ellenőrzés és a vizsgálat követelményét,
  ae) a nemzetközi szabványoknak való megfelelést;

b) a digitális szolgáltatásaik folytonosságát biztosító intézkedések megtétele annak érdekében, hogy megelőzzék és csökkentsék a hálózati és információs rendszereik biztonságát érintő biztonsági eseményeknek a digitális szolgáltatásokra gyakorolt hatásait;

c) a digitális szolgáltatásaik folytonosságára jelentős hatást gyakorló biztonsági események indokolatlan késedelem nélküli bejelentése az illetékes hatóságnak vagy a CSIRT-nek. A jelentős hatás meghatározása során:
  ca) az érintett felhasználók számát, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását,

d) a biztonsági esemény időtartamát,

e) a biztonsági esemény által érintett terület földrajzi kiterjedését,

f) a szolgáltatás működésében támadt zavar mértékét és

g) a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértékét

kell elsősorban figyelembe venni.

Az alapvető szolgáltatást nyújtó szereplőkre vonatkozó biztonsági követelmények az alábbiak[23]:

a) megfelelő és arányos műszaki és szervezési intézkedések megtétele a működés során használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében, azzal, hogy az intézkedéseknek biztosítaniuk kell a felmerülő kockázatok alapján azonosított biztonsági szintet;

[20] Hatósági rendelet 25. § (5) bekezdés, melyet .hatályon kívül helyezett a 375/2020. (VII. 30.) Korm. rendelet 73. § f). Hatálytalan: 2020. VII. 31-től.

[21] NIS-irányelv 14–17. cikkek.

[22] NIS-irányelv 16. cikk (1)–(4) bekezdés.

[23] NIS-irányelv 14. cikk (1)–(4) bekezdés.

b) az alapvető szolgáltatások folytonosságát biztosító intézkedések megtétele a szolgáltatásnyújtáshoz igénybe vett és alkalmazott hálózati és információs rendszerek biztonságát érintő biztonsági események megelőzésére és azok hatásainak csökkentésére;
c) az alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági események indokolatlan késedelem nélküli bejelentése az illetékes hatóságnak vagy a CSIRT-nek. A jelentős hatás meghatározása során:
  ca) az alapvető szolgáltatás zavara által érintett felhasználók számát,
  cb) a biztonsági esemény időtartamát és
  cc) a biztonsági esemény által érintett terület földrajzi kiterjedését kell elsősorban figyelembe venni.

A NIS-irányelv a digitális szolgáltatókra és az alapvető szolgáltatást nyújtó szereplőkre egyaránt elsődlegesen a jelentős zavart okozó biztonsági események bejelentési kötelezettségét írja elő azzal, hogy a zavar jelentőségének meghatározásához a tagállamoknak ágazatközi tényezőket kell figyelembe venniük. Ágazatközi tényezőknek minősülnek legalább az alábbiak:
a) a szolgáltatásokat igénybe vevő felhasználók száma (akár közvetlenül, akár közvetetten – pl. szolgáltatón mint közvetítőn keresztül – veszik igénybe az adott szolgáltatást),
b) az adott szolgáltatást nyújtó szereplők függelmi helyzete a jelentős zavart okozó biztonsági eseménnyel érintett más szervezet által nyújtott szolgáltatástól,
c) a biztonsági események hatása – mértéküket és időtartamukat tekintve – a gazdasági és társadalmi tevékenységekre vagy a közbiztonságra,
d) a jelentős zavart okozó biztonsági eseménnyel érintett szervezet piaci részesedése,
e) az adott biztonsági esemény által esetlegesen érintett terület földrajzi kiterjedése,
f) 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[24].

Fentiekben felsorolt, a NIS-irányelv által előírt kötelezettségek közül a nemzeti stratégia készítésére és az alapvető szolgáltatók kijelölésére vonatkozó részletszabályok a következő fejezetekben kerülnek ismertetésre.

2.2. Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája

A hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia (a továbbiakban: nemzeti stratégia) olyan keret, amelyben a hálózati és információs rendszerek biztonságára vonatkozóan nemzeti szinten stratégiai célkitűzéseket és prioritásokat állapít meg.[25] A NIS-irányelv[26] rendelkezik arról, hogy valamennyi tagállamnak kötelező elkészítenie és elfogadnia a nemzeti stratégiáját, amelyben az alapvető szolgáltatásként érintett ágazatokra (energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvízellátás és -elosztás, digitális infrastruktúra) és a digitális szolgáltatókra (online piactér, online keresőprogram, felhőalapú számítástechnikai szolgáltatás) vonatkozóan meg kell határozni:
a) a stratégiai célokat, valamint
b) a hálózati és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges szakpolitikai és szabályozási intézkedéseket.

[24] NIS-irányelv 6. cikk (1) bekezdés.
[25] NIS-irányelv 4. cikk 3. pont.
[26] NIS-irányelv 7. cikk (1) bekezdés.

A nemzeti stratégiának az alábbiakat kell tartalmaznia[27]:

a) a stratégiai célokat és prioritásokat, valamint ezek teljesítését szolgáló irányítási keretrendszert, ideértve a kormányzati szervek és egyéb érintett szereplők szerepkörét és felelősségét is,
b) a felkészültségre, a reagálásra és a helyreállításra vonatkozó intézkedések azonosítását, ideértve a köz- és a magánszféra közötti együttműködést is,
c) a kapcsolódó oktatási, tájékoztató és képzési programok, valamint a kutatási és fejlesztési tervek megjelölését,
d) a kockázatok feltárására szolgáló kockázatértékelési tervet,
e) a végrehajtásába bevont szereplők jegyzékét.

A nemzeti stratégiát, annak elfogadást követő 3 hónapon belül, meg kell küldeni a Bizottságnak.

Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat (a továbbiakban: Korm. határozat) 1. pontja alapján, a Kormány elfogadta Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiáját (a továbbiakban: Stratégia).[28] A Stratégia célja[29]:

a) a szabad, biztonságos és innovatív kibertér megteremtése,
b) Magyarország versenyképességének növelése,
c) az innovációk, az új technológiai megoldások biztonságos módon történő bevezetése, illetve adaptálása,
d) a digitalizálódott államigazgatási, kormányzati és gazdasági területeken, a biztonságosabb elektronikus közigazgatási rendszer létrehozása, illetve az állami szolgáltatások innovatív fejlesztése, valamint
e) a kiberbiztonság, a tudatosság növelése, a felkészültség szintjének emelése a társadalom minden területén.

A Stratégia célkitűzései között 3 fő prioritás szerepel:

a) a digitális környezet iránti bizalom erősítése,
b) a digitális infrastruktúra-védelem és
c) a gazdasági szereplők támogatása.

Ezen fő prioritások 12 témakörben kerültek kibontásra, 56 darab intézkedés nevesítésével együtt, amelyek végrehajtásához külön intézkedési tervet kell kidolgoznia a nemzeti stratégia megalkotásáért felelős szervezetnek.

A *digitális környezet iránti bizalom erősítése* prioritáshoz tartozó témakörök és intézkedések az alábbiak[30]:

1. A szakmai együttműködés erősítése, különös tekintettel a biztonsági kérdésekkel, a biztonsági események kezelésének kérdéskörével kapcsolatban, mivel az érintettek közötti megfelelő kommunikáció és információcsere a záloga annak, hogy hatékony reagálásra és védelmi intézkedések meghozatalára kerüljön sor. A már meglévő együttműködési formák erősítése és új együttműködési csatornák kialakítása érdekében előírt intézkedések (7 darab) a következők:
    a) felül kell vizsgálni a kormányzati, piaci, oktatási és civil szereplők együttműködésének hatékonyságát;

[27] NIS-irányelv 7. cikk (1) bekezdés.
[28] A nemzeti stratégia ismertetésére a www.kormany.hu oldalon található normaszöveg felhasználásával kerül sor, egyes esetekben információbiztonsági alapvetések kiegészítésével.
[29] Nemzeti stratégia 1. oldal.
[30] Nemzeti stratégia 11–13. oldalak.

b) biztosítani kell azt a fórumot, ahol lehetőség nyílik a társadalmi párbeszédre és a széleskörű tájékoztatásra, az etikus hackerek szerepének, illetve a társadalom és az etikus hackerek viszonyának tisztázására;
c) azonosítani kell, hogy mely területen szükséges javítani a meglévő együttműködésen;
d) létre kell hozni a hatóságok, az állami és civil szervezetek, valamint az eseménykezelő központok közötti információmegosztás, illetve a kölcsönös segítségnyújtás érdekében az összehangolt megelőzési, feltárási, mérséklési és reagálási mechanizmusokat;
e) ösztönözni kell a „Hibavadász" programok használatát az informatikai rendszerek gyengeségeinek feltárása és a biztonsági hibákra való figyelmeztetés érdekében;
f) időszakos kiberbiztonsági gyakorlatokat kell tartani a reagáló és védekezési képesség továbbfejlesztése érdekében;
g) támogatni és ösztönözni kell a köz- és magánszféra közös felelősségvállalásának tudatosítását.

2. A biztonságtudatosság növelése, az állampolgárok, szervezetek, a társadalom és a gazdaság szereplői irányába a kibertér és a digitális világ (digitális eszközök és elektronikus szolgáltatások) biztonságos használatával és kiberbiztonsággal összefüggésben. Az intézkedések (3 darab) kiemelt célja, hogy a lakosság és a gazdasági szereplők legyenek tudatában annak, hogy hol juthatnak hiteles információhoz és hova fordulhatnak segítségért, amellyel összefüggésben szükséges, hogy hiteles adatok álljanak rendelkezésre a lakosság és a gazdasági szereplők tájékozottságáról, tudatosságáról, felkészültségéről, fenyegetettségi helyzetéről. Előírás, hogy olyan ösztönzők kidolgozására kerüljön sor, melyek segítségével a kis- és középvállalkozási szektorban az információbiztonsági politikával rendelkező szervezetek aránya növekszik.
3. A kiberbűnüldözés fejlesztése, a felderítési hatékonyság növelésével, valamint a preventív intézkedések megtételével a károk mérséklésének érdekében, ideértve az elkövetők jövőbeni jogsértő magatartásának visszaszorítását. Ennek érdekében az intézkedések (2 darab) előírják, hogy:
   a) fejleszteni kell a rendvédelem és az igazságszolgáltatás kiberbűncselekmények elleni fellépési képességét,
   b) aktív együttműködés és információmegosztás szükséges a kiberbűncselekmények elleni hazai, valamint nemzetközi szervezetek között.
4. A szakmai irányító intézményrendszer fejlesztése, amely érdekében Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat (a továbbiakban: NKS) által létrehozott szakosított intézményrendszert, annak feladat- és hatásköre felülvizsgálatát kell elvégezni. Az előírt intézkedések (4 darab) a következők:
   a) ki kell jelölni a NIS-irányelvben megfogalmazott követelményeknek megfelelően a szükséges nemzeti szakosított intézményeket (CSIRT-ek és hatóságok);
   b) ki kell alakítani a nemzeti stratégiában megfogalmazott céloknak megfelelő szervezeti rendszert;
   c) fejleszteni kell a létfontosságú rendszerek, létesítmények és szolgáltatások információbiztonsági hatósági rendszerét az irányelvben megfogalmazott követelmények ágazatokon átívelő érvényesítése érdekében;
   d) létre kell hozni – a meglévő szabályozás figyelembevételével – a nemzeti eseménykezelő központot a nemzeti kibertér használóinak szélesebb köre számára elérhető kiberbiztonsági szolgáltatások nyújtása érdekében.

A *digitális infrastruktúra-védelem* prioritáshoz tartozó témakörök és intézkedések az alábbiak[31]:

1. Az informatikai fejlesztések minőségmenedzsmentjének kialakítása, amely során már a fejlesztés tervezési szakaszában meg kell határozni a kiberbiztonsági kritériumokat és azok mérési mutatóit. A minőségbiztosítási folyamat tervezéséhez előírt intézkedések (4 darab) rögzítik, hogy:
   a) kerüljön kialakításra egy könnyen elérhető, érthető és használható információs bázis,
   b) kerüljenek kidolgozásra a különböző komplexitású informatikai projektekhez, modulárisan felépülő módszertani útmutatók,
   c) kerüljenek kialakításra ingyenes segédletek a belső minőségbiztosítási folyamathoz,
   d) kerüljön kialakításra egy magyar–angol kétnyelvű, ingyenes, modulárisan felépülő, nyilvánosan elérhető kiberbiztonsági minőségmenedzsment tudástár.

2. A kormányzati elektronikus szolgáltatások biztonságának növelése, amely során tovább kell emelni a közigazgatás belső folyamatainak, illetve a közigazgatási szolgáltatásoknak elektronizálását, valamint az állami érdekkörbe tartozó információk és tartalmak digitalizációját és nyilvánosságát. Ezen törekvések végrehajtása során kiemelt figyelmet kell fordítani a hálózatok, rendszerek, folyamatok és felhasználói adatok biztonságára. A célok elérésére előírt intézkedések (7 darab) rögzítik, hogy:
   a) garantálni kell a kormányzati IT üzembiztos és biztonságos működését,
   b) meg kell valósítani a nemzetbiztonsági szempontból, illetve a közigazgatás belső működése és az elektronikus közigazgatási szolgáltatások elérhetősége szempontjából létfontosságú információs infrastruktúrák, rendszerek és külső alkalmazások, valamint az ezekben tárolt és kezelt adatok maximális védelmét,
   c) biztosítani kell a közigazgatás belső rendszereit és külső szolgáltatásait kiszolgáló hálózatok, informatikai infrastruktúra és alkalmazások maximális védelmét,
   d) meg kell valósítani az ágazati sajátosságok figyelembevételével a közigazgatást átfogó, annak valamennyi alrendszerét érintő biztonsági felügyeletet,
   e) elő kell írni, hogy a kormányzati támogatásban részesülő informatikai fejlesztések teljesülése a biztonsági előírások megvalósulásához legyen kötve,
   f) el kell készíteni a meglévő e-közszolgáltatások esetében az előírt biztonsági szint eléréséhez szükséges intézkedési tervet,
   g) szigorítani kell a meglévő szabályozást és gyakorlatot az informatikai fejlesztések egységes biztonsági követelményrendszerének kötelező előírásával.
3. A nemzetközi együttműködés erősítése a stratégiai és operatív szintű regionális és nemzetközi kibervédelmi gyakorlatok tervezésében és végrehajtásában, kiváltképp az Unió, a NATO és a közép-kelet-európai régió keretein belül történő kiberbiztonsági együttműködésekben, a kapcsolódó nemzetközi elvárások és szabályozások megfogalmazásában. Emellett aktív részvétel szükséges a szektorális együttműködést biztosító közösségekkel és központokkal (ISAC-ok, szektorális CSIRT-ek). A kölcsönös bizalmon alapuló együttműködés kialakítása érdekében előírt intézkedések (4 darab) előírják, hogy:
   a) erősíteni kell az együttműködést a NIS-irányelvben meghatározott uniós és a kijelölt hazai intézmények között,
   b) összehangolni és fokozni kell a hazai intézmények nemzetközi együttműködését,
   c) részt kell venni nemzetközi szintű kiberbiztonsági gyakorlatokon a nemzetközi együttműködés előmozdítása és a nemzetközi szintű reagáló és védekezési képesség továbbfejlesztése érdekében,
   d) hangsúlyosan kell képviselni Magyarország érdekeit és értékeit a kibertérrel kapcsolatos külkapcsolati tevékenység során.

[31] Nemzeti stratégia 14–17. oldalak.

4. Az alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák és szolgáltatásaik védelme, amely kiemelt célja, hogy azon alapvető szolgáltatást nyújtó szereplők, valamint a digitális szolgáltatók, amelyek kijelölt létfontosságú rendszerek és létesítmények, üzemeltető szinten kiemelten kezeljék a hálózati és információs rendszereik kockázatokkal arányos, zárt, teljes körű és folytonos védelmének megteremtését és fenntartását. A célok eléréshez előír intézkedések (7 darab) között rögzítésre került, hogy ki kell alakítani egy olyan kockázatértékelési, elemzési módszertant, amely lehetővé teszi az adatok korrelált gyűjtését, a szolgáltatáskiesés hatásainak dinamikus becslését és a kötelező évenkénti jelentést a szervezetek számára. Mindezt ágazati szinten kell megvalósítani. A további intézkedések rögzítik, hogy:
    a) hozzáférhetővé kell tenni a biztonsági célok elérésére vonatkozóan az ágazatközi, illetve ágazatspecifikus ajánlásokat és jó gyakorlatokat,
    b) elő kell mozdítani az állami intézmények és a magánszektor szereplőinek kölcsönös bizalmon alapuló együttműködésének kialakítását és fenntartását,
    c) hozzáférhetővé kell tenni a kritikus infrastruktúrák üzemeltetői részére a védelmet kiegészíteni képes, egységes szolgáltatáscsomagot,
    d) biztosítani szükséges a célzott pályázati lehetőségeket az üzemeltetők, a szolgáltatást nyújtók, az érintett hatóságok és az eseménykezelő központok működésének fejlesztésére a létfontosságú rendszerek, létesítmények és szolgáltatások fizikai és kiberbiztonsága területén a hatékony megelőzés és gyors reagáló képesség fejlesztésére,
    e) fokozni kell a létfontosságú rendszerek, létesítmények és szolgáltatások üzemeltetőinek irányába az információbiztonsági tudatosítási tevékenységet az érintett hatóságok és szervezetek részvételével,
    f) be kell vonni a nemzeti és nemzetközi védelmi gyakorlatokba a létfontosságú infrastruktúrák üzemeltetőit.
5. A védekező, elhárító és reagáló kiberképességek fejlesztése, amely során alapvető célként került meghatározásra, a meglévő infrastruktúra passzív és aktív eszközeinek széleskörű kialakítása és alkalmazása. Az intézkedések (5 darab) rögzítik, hogy:
    a) fejleszteni kell azon észlelési, feldolgozási (elemzés) és felderítési képességeket, amelyek lehetővé teszik a fenyegetések és támadások felismerését, osztályozását és forrásának megállapítását,
    b) meg kell teremteni az ágazati szinten egységes és ágazatok közötti koordináción alapuló irányítást és menedzsmentet,
    c) ki kell alakítani a gyors helyzetfelismerés, az értékelés és a kockázatelemzés rendszerét, ki kell fejleszteni a különböző fokozatú reagálás eszközrendszerét,
    d) meg kell teremteni a lehetőségét annak, hogy különleges esetekben civil, polgári területen dolgozó szakemberek is részt tudjanak venni a nemzeti kibervédelemben.

A *gazdasági szereplők támogatása* prioritáshoz tartozó témakörök és intézkedések az alábbiak[32]:

1. A kutatóközpontokkal való együttműködés, valamint a kutatás és fejlesztés szerepének erősítése, amely során szükséges a felsőoktatási és tudományos kutatóműhelyekkel a stratégiai együttműködés kialakítása, valamint az ilyen irányú K+F feladatok és források kutatóbázisokhoz történő összpontosítása. A célok elérésére előírt intézkedések (5 darab) rögzítik, hogy:
    a) biztosítani kell a mérnökök, kutatók képzéséhez és a kiemelkedő tehetségek gondozásához, illetve magyarországi tevékenységükhöz szükséges feltételeket,
    b) létre kell hozni egy kiberbiztonsági szakterületet érintő kutatási stratégiát, melynek célja a magyar fejlesztésű kiberbiztonsági eszközök, szoftverek és termékek alkalmazásának fokozása, amely stratégiának kiemelten kell kezelnie az Unió 2021–2027

[32] Nemzeti stratégia 18–20. oldalak.

között meghirdetésre kerülő Kutatás+Fejlesztés+Innováció felhívásainak témáit, a magyar szervezetek nemzetközi projektekben való részvétele céljából,

c) azonosítani kell a kapcsolódó kutatás-fejlesztési témaköröket azzal, hogy meg kell teremteni az ehhez szükséges állami ösztönzési lehetőségeket, beleértve a magyar korai fázisú vállalkozások ösztönzését is,

d) támogatni kell a gazdaságdiplomáciai tevékenységek során a kiberbiztonsággal foglalkozó magyar szolgáltató- és fejlesztőközpontok megjelenését.

2. A hazai digitális innováció támogatása, támogatási konstrukciók kialakítása, koordinációs feladatok ellátása, amelyhez kapcsolódóan előírt intézkedések (2 darab) rögzítik, hogy:
   a) ki kell alakítani az államilag támogatott kibervédelmi szolgáltatáscsomagokat a szektor vállalkozásainak a nehezen elérhető, drága megoldások beszerzésének és bevezetésének elősegítése érdekében,
   b) biztosítani kell a vállalkozások számára a támogatott formában elérhető oktatási, képzési programokat biztonsági üzemeltetési, biztonsági megfelelőségi és audit témában.
3. A versenyképes hazai tudásbázis létrehozása, amely érdekében a kiberbiztonsági oktatás, képzés, valamint a kutatási és fejlesztési lehetőségek fejlesztése mellett a digitális kompetenciák, a tudatosság és tájékozottság, illetve az információbiztonságot elősegítő oktatási és szakképzési szakterületek fejlesztését kell elvégezni. Ezzel összefüggésben az előírt intézkedések (6 darab) rögzítik:
   a) át kell tekinteni az aktuális problémákat és meg kell fogalmazni az azonosított problémák kezelésére vonatkozó javaslatokat a kiberbiztonsági munkacsoportnak,
   b) biztosítani kell, hogy az érintett oktatási és szakképzési végzettségek adjanak megbízható alapot a munkaerőpiaci versenyben,
   c) meg kell teremteni és hozzáférést kell biztosítani az érintetteknek egy közös informatikai tudásbázishoz,
   d) biztosítani kell az információbiztonsági képzéshez való hozzájutást és a képesítés szerzésének lehetőségét a társadalom széles köre számára,
   e) ki kell dolgozni az alapvető szolgáltatók személyi állományát érintően az információbiztonságra vonatkozó képzettségi követelményeket és a képzési programokat,
   f) támogatni kell azokat az egységes minőségi követelmények mellett megtartott helyi és országos kiberbiztonsági gyakorlatokat és versenyeket, melyek a közép- és felsőoktatásban tanuló fiatalok bevonását és tudásnövelését célozzák meg.

A kormányhatározat 2. pontja felhívja a belügyminisztert, hogy az érintett miniszterek bevonásával, a Stratégiában szereplő 56 darab intézkedés végrehajtása érdekében 2019. március 31-ig intézkedési tervet készítsen. (Az intézkedési terv elkészítése jelen jegyzet kéziratának lezárásánál még folyamatban volt a kijelölt szerv által.)

3. Főbb változások a magyar kibervédelmi szabályozásban

A 2018. évben a nemzeti szabályozás főáramát a NIS-irányelvből eredő átültetési kötelezettség határozta meg. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és végrehajtási rendeletei tekintetében minden esetben sor került a jogharmonizációs klauzula beépítésére, amely átültetési kötelezettségből eredő szabályváltozások főként 2019. január 1-vel kerültek hatálybaléptetésre. További számottevő változás a törvényi szintet nem érintette, de új végrehajtási rendeletek megalkotására vonatkozó felhatalmazó szabályok megalkotására sor került.

3.1. Az Ibtv. változásai

Az Ibtv.-nek az Ákr.[33] hatálybalépésével összefüggő és az E-ügyintézési tv.[34] végrehajtásához kapcsolódó módosításai mellett – a NIS-irányelv szerinti jogharmonizációs klauzula beépítésén kívül – a 2018. évben érdemi módosítása csak a biztonsági szintbe sorolást érintően volt. A módosítás azt a kiegészítő szabályt[35] érintette, amely szerint, ha a szervezet vagy szervezeti egység biztonsági szintje az 1. szintet nem éri el, az 1. szint eléréséhez szükséges intézkedéseket 6 éven belül meg kell valósítani. Ezt a kiegészítő szabályt a törvény hatálybalépése óta többször[36] módosították, azonban a szabály újabb módosítására 2021-ben is sor került, amely következtében az 1. biztonsági szint eléréséhez szükséges maximum időtartamot 8 évről 10 évre emelték.

2019-ben az Ibtv. módosításának első lépéseként az értelmező rendelkezések január 1-jei kiegészítésére került sor. Meghatározásra került a NIS-irányelvvel összhangban az alapvető szolgáltatásokat nyújtó szereplő és a bejelentésköteles szolgáltatás[37] fogalma, mindkét esetben utaló szabály alkalmazásával az ágazati jogszabályra. Alapvető szolgáltatásokat nyújtó szereplőnek a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 2/A. §-a alapján kijelölt szolgáltató minősül[38] (ezen törvény a 4. fejezetben kerül ismertetésre). Bejelentésköteles szolgáltatásnak[39] minősülnek az információs társadalommal összefüggő szolgáltatások – ide nem értve az Ibtv. személyi hatálya alá tartozó szervek[40] számára adatkezelést végzők és a nemzeti adatvagyon körébe tartozó nyilvántartások adatfeldolgozói által nyújtott szolgáltatásokat – közül:

a) az online piactér[41],
b) a keresőszolgáltatás[42] és
c) a felhőalapú számítástechnikai szolgáltatás[43].

Változott továbbá az elektronikus információs rendszer fogalma[44] is, amely igazodik a NIS-irányelv hálózati és információs rendszer fogalmához[45]. Az új meghatározás alapján elektronikus információs rendszernek minősül:

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat[46];

---

[33] Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény.

[34] Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény

[35] Ibtv. 10. § (3) bekezdés.

[36] 2015-ben 1 évről 2 évre, 2016-ban 2 évről 4 évre, 2017-ben 4 évről 5 évre, 2018-ban 5 évről 6 évre, 2019-ben 6 évről 8 évre.

[37] Ibtv. 1. § (1) bekezdés 7a. pont.

[38] Ibtv. 1. § (1) bekezdés 6a. pont.

[39] Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § j) pontjában meghatározott szolgáltatások.

[40] Ibtv. 2. § (1) bekezdés.

[41] Olyan szolgáltatás, amely a fogyasztói jogviták alternatív rendezéséről, valamint a 2006/2004/EK rendelet és a 2009/22/EK irányelv módosításáról szóló, 2013. május 21-i 2013/11/EU európai parlamenti és tanácsi irányelv szerinti fogyasztók, illetve kereskedők számára lehetővé teszi, hogy az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi vagy szolgáltatási szerződéseket kössenek.

[42] Olyan szolgáltatás, amely információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára.

[43] Olyan szolgáltatás, amely távoli hozzáférést tesz lehetővé a többek között hálózati funkciókat, adattárolást, alkalmazások, szolgáltatások futtatását biztosító számítástechnikai megoldásokhoz.

[44] Ibtv. 1. § (1) bekezdés 14b. pont.

[45] NIS-irányelv 4. cikk 1. pont.

[46] Elektronikus hírközlő hálózat jelek vezetékes vagy vezeték nélküli úton elektronikus hírközlő eszközökkel történő továbbítását lehetővé tevő, állandó infrastruktúrán vagy központilag adminisztrált kapacitáselosztáson alapuló rendszerek, továbbá adott esetben kapcsoló vagy útválasztó eszközök, valamint más erőforrások, beleértve a nem aktív hálózati elemeket is. Elektronikus hírközlő hálózat különösen a műholdas hálózat, a helyhez kötött – vezetékes vagy vezeték nélküli – hálózat és a mobil rádiótelefon-hálózat; az energiaellátó kábelrendszerek olyan mértékben, amennyiben azokat a jelek továbbítására használják, valamint a műsorterjesztő hálózat. – 2003. évi C. törvény).

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi vagy
c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

A létfontosságú rendszerelemek ágazati szabályozásával összefüggően rögzítésre került a honvédelmi célú elektronikus információs rendszer fogalma[47], valamint az Unió Általános Adatvédelmi Rendelete[48] és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) módosítása miatt a kritikus adat fogalma[49].

Az Ibtv. személyi hatálya alá tartozó szervek esetében alaprendelkezés, hogy az általuk kezelt adatok csak a Magyarország területén üzemeltetett és tárolt elektronikus információs rendszerekben, valamint honvédelmi, diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetők. Ez alól kivételt képez a Magyar Nemzeti Bank által a monetáris politika végrehajtásával és a devizatartalék kezelésével kapcsolatos kockázatértékelési és portfóliókezelési tevékenysége keretében kezelt adatok köre. Ez a kivétel vonatkozik az EGT-államok területén belül üzemeltetett elektronikus információs rendszerekben történő, hatósági engedélyen alapuló rendelkezésre is[50].

Kiegészítésre került továbbá a Nemzetbiztonsági Szakszolgálat, mint az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság (a továbbiakban: Hatóság)[51], jogköre az elektronikus információs rendszer védelmére vonatkozó intézkedések terén. Ez alapján a Hatóság jogosult az eljárása során független, képesített ellenőrt igénybe venni és az általa végzett ellenőrzés eredményét megállapításainál figyelembe venni[52].

2019. január 1-től új hatósági jogkör a költségvetési szervek esetében történő – a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat megsértése esetén – a bírság kiszabása[53], amely részletszabályait az Ibtv. végrehajtási rendelete tartalmazza (lásd: 3.2 fejezet).

---

[47] Ibtv. 1. § (1) bekezdés 23. pont: honvédelmi célú elektronikus információs rendszer:
a) a honvédelmi szervezetek, a honvédelemért felelős miniszter fenntartói irányítása alá tartozó, honvédségi szervezetnek nem minősülő többcélú szakképző intézmény, a honvédelemért felelős miniszter tulajdonosi joggyakorlása alá tartozó gazdasági társaságok, az állami vagyonról szóló 2007. évi CVI. törvény 3. § (2) bekezdés *c)* pontja szerinti gazdasági társaságok, valamint jogszabály szerint a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok zárt célú elektronikus információs rendszereinek, valamint egyéb – funkciója, rendeltetése, feladatellátása szerint – nyílt elektronikus információs rendszereinek összessége, amely ágazatspecifikus módon támogatja a honvédelmi ágazaton belüli és ágazatok közötti működést,
b) a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló kormányrendelet alapján kijelölt ágazaton belüli honvédelmi létfontosságú rendszerelemek elektronikus információs rendszerei,
c) az illetékes ágazatban ki nem jelölt, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvényben meghatározott ágazaton kívüli honvédelmi rendszerelem elektronikus információs rendszerei, valamint
d) a honvédelmi ágazat hatáskörébe tartozó nemzetbiztonsági védelem alá eső szervek elektronikus információs rendszere.

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

[49] Ibtv. 1. § (1) bekezdés 32a. pont – kritikus adat: a személyes adat vagy valamely jogszabállyal védett adat.

[50] Ibtv. 3. §. (1) és (3) bekezdései, hatályosak 2019. január 1-től.

[51] Hatósági rendelet 2. §-a.

[52] Ibtv. 4. §-a és 16. §. (1) bekezdés h) pont, hatályosak 2019. január 1-től.

[53] Ibtv. 16. §. (1) bekezdés h) pont, hatályos 2019. január 1-től.

Európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemek szervezetei tekintetében a Hatóság előzetes engedélyezési jogköre megszűnt az adott szervezetre irányadó besorolási szintnél alacsonyabb szintű besorolás megállapítása esetén, az indokolási kötelezettség azonban megmaradt[54].

Kiegészült az Eseménykezelő Központ jogköre a sérülékenységvizsgálatok elvégzésével kapcsolatban, mivel már saját hatáskörben a Központ is indíthat és lefolytathat sérülékenységvizsgálatot regisztrált felhasználói jogosultság birtokában vagy ennek hiányában, ha erre külön jogszabály felhatalmazza[55].

A NIS-irányelvből adódó kötelezettségek végrehajtása érdekében az Ibtv. eseménykezelő központokra vonatkozó rendelkezései szintén módosultak. A kormány által kijelölt eseménykezelő központ (a továbbiakban: Központ)[56]:

a) az alapvető szolgáltatást nyújtó szolgáltatók, valamint a bejelentésköteles szolgáltatást nyújtó szolgáltatók elektronikus információs rendszereit (kivéve a honvédelmi célú elektronikus információs rendszereket és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit), valamint

b) az európai vagy nemzeti létfontosságú rendszerelemmé törvény[57] alapján kijelölt rendszerelemek elektronikus információs rendszereit

érintően a Nemzetbiztonsági Szakszolgálat irányítása alatt működő Nemzeti Kibervédelmi Intézet lett. Az Intézet feladatai kiegészültek az azonnali figyelmeztetések közzétételével a kritikus hálózatbiztonsági fenyegetettségekről és ezek magyar nyelvű megjelenítésével, valamint a nemzetközileg publikált sérülékenységek honlapján történő hozzáférhetővé tételével[58].

Módosult az Ibtv. adatvédelmi rendelkezése is. A Hatóság és az eseménykezelő központok a hatósági döntés véglegessé válását, a sérülékenységvizsgálat lezárását, valamint a biztonsági esemény vizsgálatának lefolytatását követő öt évig jogosultak adatkezelésre, amely lejártát követően kötelesek az elektronikus információs rendszereikből és adathordozóikról az adatokat törölni. Módosult továbbá a munkatársakra vonatkozó titoktartási kötelezettség szabálya is, amely a minősített adatok tekintetében azok érvényességi idejének végéig, személyes adatok tekintetében időkorlát nélkül fennmarad.[59]

2022. július 1-től az Ibtv. hatálya kiterjed a poszt-kvantumtitkosítás vonatkozásában kizárólag a poszt-kvantumtitkosítás alkalmazásra kötelezett szervezetre is.[60] A poszt-kvantumtitkosítás alkalmazásának szabályairól az Ibtv. III/B. fejezete rendelkezik.

3.2. A végrehajtási rendeletek változásai

2018-ban – figyelemmel a NIS-irányelvben meghatározott határidőre – sor került az Ibtv. végrehajtási rendeletei vonatkozásában a NIS-irányelvnek való megfelelés céljából a jogharmonizációs klauzula beépítésére. Jelen tananyag a végrehajtási rendeletek közül kizárólag a kormányrendeletek változását tárgyalja, a miniszteri rendeleti szintű háttérszabályok ismertetésére nem tér ki, mivel azok módosítására 2019-ben nem került sor. A Korm. rendeletek közül a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok

[54] Ibtv. 9. §. (6) bekezdés.

[55] Ibtv. 18. §. (2a) bekezdés, hatályos 2019. január 1-től.

[56] Ibtv. 19. §. (1) bekezdés, hatályos 2019. január 1-től.

[57] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.).

[58] Ibtv. 20. §. (1) bekezdés, hatályos 2019. január 1-től.

[59] Ibtv. 22. §. (2)–(3) bekezdései, hatályosak 2019. január 1-től.

[60] Ibtv. 2. §. (9) bekezdés

létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet módosítására nem került sor.[61] A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet 2019. január 1-től hatályos minimális szövegcserés módosítására az Ibtv. Hatóság és Központ elnevezésének és feladatkörének változása miatt került sor, kodifikációs pontosítások átvezetése mellett.

1. 2019-ben az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 187/2015. (VII. 13.) Korm. rendelet (a továbbiakban: hatósági rendelet) változásait a Hatóság feladatellátásával összefüggő módosítások alkották. Alapvetésként bekerült a szabályozásba a Hatóság függetlenségét deklaráló rendelkezés, amely szerint hatósági eljárása során és hatósági döntéseinek tartalmával összefüggésben – a feladat elvégzésére vagy a mulasztás pótlására irányuló utasítás kivételével – nem utasítható[62].

   Az Ibtv. változásával összhangban, amely szerint a Hatóság jogosult az eljárása során független, képesített ellenőrt igénybe venni és az általa végzett ellenőrzés eredményét megállapításainál figyelembe venni, a hatósági rendelet is módosításra került. Az ellenőrzési jogosultság kiterjed minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedésre, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek[63].

   A Hatóság feladatai közül – az Ibtv. fent említett változásaival való összhang megteremtése érdekében – néhány törlésre került[64], illetve új feladatként jelentek meg az alábbiak[65]:

   a) hatósági ellenőrzés keretében lefolytatja a fizikai, logikai és adminisztratív védelmi ellenőrzéseket,

   b) a Központtól kapott, biztonsági eseményekkel kapcsolatos értesítéseket nyilvántartja és honlapján közzéteszi azokat,

   c) az elektronikus információs rendszerek biztonságáért felelős nemzetközi szervezetekben ellátja Magyarország képviseletét.

   A NIS-irányelv átültetésének és végrehajtásának felügyeletére kijelölt nemzeti hatóság a BM OKF, amely egyben ellátja az alapvető szolgáltatásokat nyújtó szolgáltatók hálózati és információs rendszerei biztonságának felügyeletét is. Szükség szerint konzultációt folytat és együttműködik a bűnüldöző szervekkel, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósággal (a továbbiakban: NAIH).

---

[61] 2021-ben a korm.rendelet számos módosításon esett át, melyek körül a lényegesebbek:
- 1. § (1)A Nemzeti Kiberbiztonsági Koordinációs Tanács elnöke a Nemzetbiztonsági Szakszolgálat vezetője. A Tanács elnökét – akadályoztatása esetén – az e-közigazgatásért felelős miniszter által megbízott kiberkoordinátor (a továbbiakban: kiberkoordinátor) helyettesíti.
- 1. § (3) A Tanács tagja – a (2) bekezdésben meghatározottakon túl – a Szabályozott Tevékenységek Felügyeleti Hatósága elnöke vagy az általa delegált személy, a Katonai Nemzetbiztonsági Szolgálat főigazgatója és a kiberkoordinátor.
- 2. § A Tanács által felkért egyetemi, kutatói, szakmai, gazdasági és más nem kormányzati szereplőkből álló Kiberbiztonsági Fórum vezetését a Tanács elnöke, a Fórum munkájának szakmai koordinálását a kiberkoordinátor látja el.

Változtak a 3. §-ban szabályozott Kiberbiztonsági Munkacsoportokra vonatkozó rész is: A Tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását a Nemzeti Kibertér Munkacsoport és a Nemzetközi és Európai Uniós Kibertér Munkacsoport (a továbbiakban: Kiberbiztonsági Munkacsoportok) segíti.

[62] Hatósági rendelet 2. § (2) bekezdése.

[63] Hatósági rendelet 5/A. §.

[64] Hatósági rendelet 6. § (1) bekezdés i)–n) pontok, hatályos 2019. január 1-től.

[65] Hatósági rendelet 6. § (1) bekezdés f)–h) pontok, hatályos 2019. január 1-től.

A Hatóság, mint egyedüli kapcsolattartó pont, feladatai az alábbiak:

a) biztosítja a hatóságok és az érintett EGT-tagállamok hatóságai között folytatott együttműködést,

b) együttműködik a NIS-irányelvnek való megfelelés vizsgálata érdekében a Központtal, a BM OKF-fel, valamint a Hatósággal[66],

c) az azonosított alapvető szolgáltatásokat nyújtó szolgáltatók elektronikus információs rendszerei esetében a megfelelés vizsgálatával összefüggő adatokat[67], valamint a vizsgálat eredményét megküldi az Európai Bizottság részére,

d) tájékoztatja az érintett tagállamokat az azonosított alapvető szolgáltatásokat nyújtó és a bejelentésköteles szolgáltatást nyújtó szolgáltatók elektronikus információs rendszereiben bekövetkezett biztonsági eseményről, ha az jelentős zavart okozott a szolgáltatás nyújtásában,

e) az Unió e feladatra létrehozott Együttműködési csoportja részére összefoglaló jelentést küld a d) pont szerinti biztonsági eseményekről,

f) együttműködik a magyar és a nemzetközi hálózatbiztonsági szervekkel, különösen az Együttműködési csoporttal és a NIS-irányelv által létrehozott CSIRT-ek hálózatával,

g) szükség szerint konzultációt folytat és együttműködik a rendvédelmi szervekkel, illetve a NAIH-val[68].

Az Ibtv. módosításához igazodva változtak a Hatóság által alkalmazható jogkövetkezményekre vonatkozó szabályok. A bírság kiszabása, mint szankció, már költségvetési szerv esetén is alkalmazható. Az új eljárási lépések az alábbiak[69].

a) A Hatóság vagy a Központ értesítése esetén megfelelő határidő tűzése mellett a Hatóság felszólítja az érintett szervezetet a jogszabálysértő tevékenység vagy a jogsértő állapot megszüntetésére, ennek keretében különösen bejelentési, adatszolgáltatási, együttműködési kötelezettségének teljesítésére.

b) Ha a költségvetési szerv a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be – a jogkövető magatartás betartására vonatkozó eredménytelen felszólítás, illetve a felügyelő szerv eredménytelen közreműködése esetén –, az eset összes körülményeinek mérlegelésével, bírságot szabhat ki. A kiszabható bírság ötvenezer forinttól ötmillió forintig terjedhet, amelyet a határozat véglegessé válását követő 8 napon belül kell befizetni a Hatóság Magyar Államkincstárnál vezetett számlájára.

c) Az eljárás akadályozása, illetve az adatszolgáltatás nem vagy nem megfelelő teljesítése esetén a Hatóság hárommillió forintig terjedő bírsággal sújthatja – ismételt jogsértés esetén sújtani köteles – a jogsértő vezető tisztségviselőjét is.

---

[66] Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 6/B. § (3) bekezdése szerinti hatóság.

[67] A megküldött adatok köre:

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

b) a kritikus társadalmi, gazdasági tevékenységek fenntartásához nyújtott alapvető szolgáltatások jegyzéke,

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

d) az adott szolgáltatásra támaszkodó felhasználók száma vagy az alapvető szolgáltatásokat nyújtó gazdasági szereplő ellátási szintje,

e) az eseménykezelő központok hatásköréről és a biztonsági események kezelésére szolgáló eljárásról szóló tájékoztatás.

Hatósági rendelet 29/A. § (2) bekezdés, hatályos 2019. január 1-től.

[68] Hatósági rendelet 29/A. § (1) bekezdés, hatályos 2019. január 1-től.

[69] Hatósági rendelet 13. § (4)–(6) bekezdései, hatályosak 2019. január 13-tól.

	A jogszabálysértés megnevezése	Legkisebb mérték	Legnagyobb mérték
1.	Regisztráció elmulasztása	50 000 Ft	100 000 Ft
2.	Adatváltozás bejelentésének elmulasztása	50 000 Ft	500 000 Ft
3.	Kockázatelemzés készítésének elmulasztása	200 000 Ft	500 000 Ft
4.	Kockázatokkal arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása	300 000 Ft	5 000 000 Ft
5.	Kockázatelemzés és a szükséges biztonsági intézkedések biztonsági eseményt követő haladéktalan, egyéb esetben évente dokumentált felülvizsgálatának elmulasztása, a felülvizsgálat során feltárt hiányosságok alapján a szükséges módosítások végrehajtásának elmulasztása	200 000 Ft	2 000 000 Ft
6.	Biztonsági esemény bejelentésének elmulasztása	300 000 Ft	5 000 000 Ft
7.	Hatóság végleges, végrehajtandó határozatában foglalt kötelezésének nem teljesítése	400 000 Ft	5 000 000 Ft

1. táblázat: Az egyes jogszabálysértések esetén kiszabható bírság mértéke
(Forrás: Hatósági rendelet 1. melléklet.)

2. Főbb változást 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 (a továbbiakban: Rendelet) hozott, amely 2019. január 1-jén lépett hatályba. A Rendelet hatályon kívül helyezte 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. rendeletet [a továbbiakban: 185/2015. (VII. 13.) Korm. rendelet], amely a NIS-irányelvvel való összhang megteremtésére vonatkozó, átfogó módosítására még 2018. május 10-ei határnappal sor került. A Rendelet normaszövege a 185/2015. (VII. 13.) Korm. rendelet korábbi felépítésén és normaszövegén alapul, az Ibtv. fent említett változásai és a NIS-irányelv, valamint a végrehajtásához szükséges rendelkezéseket megállapító bizottsági rendelet[70] miatt abba új részek is bevezetésre kerültek.

   Az értelmező rendelkezések között meghatározásra került az alapvető szolgáltatást nyújtó szolgáltató[71] és a bejelentésköteles szolgáltatást nyújtó fogalma[72], amely összhangban áll a NIS-irányelv és az Ibtv. vonatkozó rendelkezéseivel. Új fogalomként került rögzítésre a CSIRT-ek hálózata, mint a NIS-irányelv által létrehozott hálózat[73], valamint a közvetítő szolgáltató[74] meghatározása. Közvetítő szolgáltató olyan, az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely:

[70] A hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról szóló, 2018. január 30-i (EU) 2018/151 bizottsági végrehajtási rendelet.

[71] Alapvető szolgáltatást nyújtó szereplő: a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján alapvető szolgáltatást nyújtóként azonosított szolgáltató. – Rendelet 1. § 2. pont.

[72] Bejelentésköteles szolgáltatást nyújtó: az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) 2. § j) pontja szerinti szolgáltatást nyújtó szolgáltató. – Rendelet 1. § 4. pont.

[73] Rendelet 1. § 8. pont.

[74] Rendelet 1. § 11. pont – Közvetítő szolgáltató: az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § l) pontja szerint Rendelet 1. § 11. pont.

a) egyszerű adatátvitel és hozzáférés-biztosítást,
b) gyorsítótárolást,
c) tárhelyszolgáltatást,
d) keresőszolgáltatást,
e) alkalmazásszolgáltatást,
f) videómegosztóplatform-szolgáltatást
biztosít.

Új sérülékenységvizsgálati módszerként került meghatározásra a pszichológiai manipuláció[75] és fogalma[76], amely olyan tevékenységi forma, technikák és módszerek összessége, amely az emberek befolyásolására alapozva teszi lehetővé bizalmas információk megszerzését vagy kártékony program terjedését és működését. A vizsgálat lefolytatásának határideje 90 nap[77].

A Központ feladatai jelentősen átalakultak. Az új, megváltozott feladatokat a Rendelet az alábbiak szerint határozza meg[78]. A Központ kezeli

a) az Ibtv. hatálya alá tartozó szervek[79] – kivéve a honvédelmi célú és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit – nyílt,
b) a bejelentésköteles szolgáltatók,
c) az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők (kivéve honvédelmi célú rendszerelemek),
d) a központosított informatikai és elektronikus hírközlési szolgáltató elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket.

Az eseménykezelés céljából a Központot együttműködési kötelezettség terheli:

a) az elektronikus információs rendszerek felügyeletére kijelölt hatóságokkal,
b) a honvédelmi célú és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereinek eseménykezelő központjaival,
c) a rendvédelmi szervekkel,
d) a Nemzeti Média- és Hírközlési Hatósággal és az általa működtetett Országos Informatikai és Hírközlési Főügyelettel,
e) az elektronikus hírközlési szolgáltatókkal, a központosított informatikai és elektronikus hírközlési szolgáltatóval,
f) az Lrtv.80 szerinti üzemeltetőkkel, kijelölő és javaslattevő hatóságokkal, valamint
g) a NAIH-val.

A Központ a biztonsági eseményre vagy fenyegetésre utaló tevékenységek kivizsgálását követően, szükség esetén figyelmeztetést ad ki:

a) a felhasználók,
b) az eseménykezelő központok,
c) az elektronikus információs rendszerek felügyeletét ellátó hatóságok,
d) a Hatóság mint egyedüli kapcsolattartó pont (akit tájékoztat a biztonsági események kezelésére vonatkozó, jogszabályban nem részletezett eljárásrendjéről),
e) az Ibtv. hatálya alá tartozó szervek,
f) a bejelentésköteles szolgáltatók,

[75] Rendelet 24. § (1) bekezdés d) pont.
[76] Rendelet 1. § 15. pont.
[77] Rendelet 24. § (3) bekezdés c) pont.
[78] Rendelet 3. § (1)–(7) bekezdései.
[79] Ibtv. 2. §.
[80] Lrtv.

g) az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők, valamint
h) a központosított informatikai és elektronikus hírközlési szolgáltatók felé.

A Központ feladatellátása során:
a) végzi a biztonsági események nemzeti szintű nyomon követését,
b) ellátja a kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatást az érdekeltek számára,
c) végzi a korai előrejelzéssel, a riasztással, a bejelentéstétellel és az információterjesztéssel kapcsolatos feladatokat,
d) reagál a biztonsági eseményekre,
e) dinamikus kockázat- és eseményelemzéseket, valamint a biztonsági eseményekkel kapcsolatos helyzetképet készít,
f) sérülékenységvizsgálatot végez,
g) a hatáskörébe tartozó elektronikus információs rendszerek tekintetében részt vesz a CSIRT-ek hálózatának tevékenységében,
h) meghatározza a biztonsági események és kockázatok kezelésére vonatkozó eljárásokat, valamint a biztonsági események, kockázatok és információk osztályozására szolgáló eljárásokat és szabályokat.

Változtak a biztonsági események bejelentésére vonatkozó előírások. A Rendelet 8. §-a szerint a Központ felé bejelentési kötelezettség terheli az Ibtv. hatálya alá tartozó szerveket[81] – kivéve a honvédelmi célú és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit – nyílt rendszereiket ért biztonsági események tekintetében, valamint a közvetítő szolgáltatókat. A honvédelmi célú elektronikus információs rendszert érintő biztonsági eseményt és fenyegetést a Katonai Nemzetbiztonsági Szolgálat felé kell bejelenteni.

A Rendelet szerint a bejelentésnek tartalmaznia kell legalább[82]:
a) a biztonsági esemény rövid leírását és státuszát,
b) a szolgáltatás működésében támadt zavar mértékét,
c) az esemény kezelésére az üzemeltető által kijelölt kapcsolattartó személy és szervezet elérhetőségeit,
d) a biztonsági esemény hatását meghatározó szempontokat, valamint
e) közvetítő szolgáltató igénybevétele esetén a közvetítő szolgáltató megnevezését, elérhetőségét.

A biztonsági események bejelentése elsődlegesen elektronikus úton történik, ha azonban az elektronikus információs rendszer oly mértékben sérül, hogy az nem lehetséges, a bejelentés bármely más módon megvalósítható[83].

Az alapvető szolgáltatást nyújtó szolgáltatókra további külön szabályok vonatkoznak[84]. A szolgáltatás folytonosságára jelentős hatást gyakorló biztonsági eseményeket indokolatlan késedelem nélkül kötelesek bejelenteni a Központnak. A jelentős hatás meghatározása érdekében a bejelentésnek az alábbi adatokat kell tartalmaznia:
a) az alapvető szolgáltatás zavara által érintett felhasználók száma,
b) a biztonsági esemény időtartama,
c) a biztonsági esemény által érintett terület földrajzi kiterjedése.

[81] Ibtv. 2. §.
[82] Rendelet 11. §.
[83] Rendelet 11. §.
[84] Rendelet 9. §.

Ha az alapvető szolgáltatás nyújtása harmadik fél bejelentésköteles szolgáltatóra alapozott, akkor ezen szolgáltatónak is be kell jelentenie minden olyan esetet, amikor a bejelentésköteles szolgáltatót érintő biztonsági esemény jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára.

További kiegészítő szabályok vonatkoznak a bejelentésköteles szolgáltatást nyújtóra is, akinek haladéktalanul be kell jelentenie a Központ részére az elektronikus információs rendszerein bekövetkezett azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Unión belül kínált, bejelentésköteles szolgáltatás nyújtására. A jelentős hatás meghatározása érdekében a bejelentésnek az alábbi – külön jogszabályban meghatározott – adatokat kell tartalmaznia[85]:

a) a biztonsági esemény által érintett felhasználók számát, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását,
b) a biztonsági esemény időtartamát,
c) a biztonsági esemény által érintett terület földrajzi kiterjedését,
d) a szolgáltatás működésében támadt zavar mértékét,
e) a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértékét.

A Központ az alapvető szolgáltatást, valamint a bejelentésköteles szolgáltatást nyújtók bejelentései alapján vizsgálja a jelentős hatást gyakorló biztonsági események határon átnyúló hatását, és közvetlenül vagy az egyedüli kapcsolattartó pont útján indokolt esetben tájékoztatja az Unió érintett tagállamait. A tájékoztatás során gondoskodnia kell arról, hogy ne sérüljenek a szolgáltatók kereskedelmi érdekei és a bejelentésben foglalt információk bizalmassága[86].

Új szabályozási elemként megjelent a biztonsági események kezelése tekintetében az önkéntes bejelentés[87] lehetősége az alapvető szolgáltatónak nem minősülő ágazati szereplők részére, kivéve azon rendszerelemeket, amelyek létfontosságú rendszerelemként kijelölésre kerültek. A Központ felé történő bejelentést olyan biztonsági események esetében alkalmazhatják, amelyek jelentős hatást gyakorolnak az általuk nyújtott szolgáltatások folytonosságára. Az online piactért, a keresőszolgáltatást és a felhőalapú számítástechnikai szolgáltatást biztosító bejelentésköteles szolgáltató önkéntes alapon bejelenthet minden olyan eseményt, amelyek számára addig ismeretlen jellemzőkkel bírnak, ideértve különösen a sérülékenységet kihasználó új módszereket, a kihasználásra vonatkozó adatokat, sebezhető pontokat vagy fenyegetéseket. A Központnak ezeket a bejelentéseket csak akkor kell feldolgoznia, ha az nem jelent aránytalan vagy indokolatlan terhet.

A biztonsági eseménnyel érintett szervezet a biztonsági esemény kivizsgálása során köteles együttműködni a Központtal, amely együttműködés kiterjed:

a) a bejelentéssel kapcsolatos információk átadására,
b) a biztonsági eseményben érintettek (támadó/támadott) beazonosításához szükséges műszaki, technikai adatok átadására,
c) a Központ szakembereit illetően:
  ca) a biztonsági esemény következményei elhárítása érdekében tett intézkedésekről, illetve a biztonsági esemény vizsgálata során, az infrastruktúrával kapcsolatos beállításokról történő tájékoztatásra,
  cb) az incidensben érintett infrastruktúrához való hozzáférés biztosítására, valamint

[85] Az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet 6. §-a.
[86] Rendelet 12. §.
[87] Rendelet 13. §.

cc) az általuk végzett kockázatelemzés alapján szükségesnek ítélt korai figyelmeztető- vagy csapdarendszerek, szenzorok telepítésére,
cd) alapvető szolgáltatást nyújtó szolgáltatók esetében az incidensben érintett infrastruktúrával kapcsolatos, speciális, ágazati sajátosságok megosztására.[88]

A biztonsági eseményekkel érintett szerv – a bejelentésköteles szolgáltató kivételével – köteles a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a Központ rendelkezésére bocsátani[89].

Kiegészítő szabály, hogy a bejelentésköteles szolgáltatók, valamint az alapvető szolgáltatást nyújtó internetszolgáltatók az incidensben érintett előfizetőkkel kapcsolatban a Központ kérésére kötelesek szükség szerint tiltásokat bevezetni, illetve (felhasználói, előfizetői) hozzáféréseket korlátozni, felfüggeszteni vagy megszüntetni.[90]

A bejelentésköteles szolgáltatóra vonatkozóan további kiegészítő szabályok kerültek megalkotásra az alábbiak szerint[91]:

a) Ha a Központtal való együttműködéshez szükséges adatok összegyűjtésére bármely okból nem képes a Központ képviselője helyszíni tanácsadás keretein belül, az érintett szervezet szakértőinek bevonásával javaslatot tesz a szükséges adatok összegyűjtésének és biztosításának módjára, azzal, hogy a szolgáltatást nyújtó köteles gondoskodni az adatokhoz való hozzáférés biztosításáról.
b) Kötelezettsége a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat tartalmazó, bitazonos másolatokat a Központ rendelkezésére bocsátani.
c) A biztonsági esemény felszámolásához szükséges intézkedéseket a Központ támogatásával ki kell dolgoznia és haladéktalanul végre kell hajtania.
d) Az esemény felszámolását követően felül kell vizsgálja az elektronikus információs rendszerei kockázatelemzésének, kockázatkezelésének teljeskörűségét, és a szükséges módosításokat végre kell hajtania.

A közvetítő szolgáltatókra[92] vonatkozó kiegészítő szabályok[93]:

a) A biztonsági események kivizsgálása során a Központnak jogosultsága van szükség szerint megismerni a különböző szolgáltatás- vagy üzletmenet-folytonosságot biztosító szabályzókat, eljárásrendeket, ideértve különösen az üzletfolytonossági tervet és a katasztrófa-helyreállítási tervet.
b) A konkrét biztonsági esemény kezelése érdekében a Központ kérésére:
  ba) a biztonsági eseményben érintettek, a támadó és a támadott beazonosításához szükséges, adatait átadja,
  bb) az incidensben érintett előfizetőkkel kapcsolatban szükség szerint tiltásokat vezet be, felhasználói, illetve előfizetői hozzáféréseket korlátoz, függeszt fel vagy szüntet meg.
c) Veszélyesnek vagy károsnak ítélt szolgáltatás biztosítása esetén a Központ kötelezést adhat ki az adott szolgáltatás tiltására.

[88] Rendelet 16. § (1)-(2) bekezdései.
[89] Rendelet 17. § (4) bekezdés.
[90] Rendelet 16. § (3) bekezdés.
[91] Rendelet 17. § (3) és (5) bekezdése, valamint (7)–(8) bekezdései.
[92] Vö. 28–29. oldalak fogalommeghatározása.
[93] Rendelet 19. § (1)–(4) bekezdések.

Kiegészítő szabály került megalkotásra a nyilvántartásba felvett, sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetre[94] vonatkozóan, amely szerint a gazdálkodó szervezetnek a felvételt követő minden második évben ismételten meg kell küldenie[95] az Alkotmányvédelmi Hivatal részére – a feltételek teljesülésének ismételt ellenőrzése céljából – a tevékenyég végzéséhez szükséges okiratokat[96]. A kötelezettség elmulasztása a nyilvántartásból való törlést eredményezi.

A Központ részére a Központ által saját hatáskörében indított sérülékenységvizsgálat végrehajtása érdekében, az érintett szervezetek[97] kötelesek bejelenteni a webes szolgáltatások, weboldalak és webszerverek elérhetőségére vonatkozó egyedi technikai adatokat azzal, hogy a bekövetkezett változásokat 3 napon belül be kell jelenteni. A Központ tájékoztatja az érintett szervezetet a vizsgálathoz használt IP-címről vagy más egyedi technikai azonosítóról, amelyet az érintett szervezet nem tilthat ki a webes szolgáltatás eléréséből. [98]

3. Az Ibtv. felhatalmazó rendelkezései[99] között 2019. január 1-től megjelent három új szabály, amely az alábbi rendeletek megalkotását írja elő a Kormány részére:
   a) a korai figyelmeztetés részletes szabályairól, így különösen annak rendszerét, a rendszer üzemeltetőjének kijelölését, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét előíró rendelet (ennek működtetése a Központ feladat- és hatáskörébe került[100]),
   b) az Ibtv. 16. § (1) bekezdése szerinti független, képesített ellenőr igénybevételével kapcsolatos eljárásrendet tartalmazó rendelet,
   c) a honvédelmi célú elektronikus információs rendszerre vonatkozóan a korai figyelmeztetés részletes szabályait, így különösen annak rendszerét, a rendszer üzemeltetőjének kijelölését, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét előíró rendelet.

A 2019. január 1-jei módosítást követően az Ibtv. felhatalmazói rendelkezései között újabb szabályok jelentek meg, amelyek további rendeletek megalkotását írják elő a Kormány számára.[101] Az Ibtv. 24. § (1a) pontja értelmében felhatalmazást kap a Kormány, hogy kijelölje a 22/B. § (1) bekezdés b) pontja szerinti – a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kormány által kijelölt hatóság – tanúsító hatóságot.

94 Rendelet 22. § (5) bekezdés.
95 Rendelet 22. § (11)–(13) bekezdései.
96 Rendelet 22. § (4) és (7) bekezdései.
97 Rendelet 22. § (1) bekezdése alapján a nemzetbiztonsági védelem alá eső állami és önkormányzati szervek elektronikus információs rendszerei, az Ibtv. 2. § (1) bekezdése szerinti szervezetek létfontosságú rendszerelemmé kijelölt elektronikus információs rendszerek, valamint a zárt célú elektronikus információs rendszerek. A Katonai Nemzetbiztonsági Szolgálatot a bejelentési kötelezettség saját illetékes eseménykezelő központja felé terheli.
98 Rendelet 27. § (1)–(2) bekezdése. A Katonai Nemzetbiztonsági Szolgálatot a bejelentési kötelezettség saját illetékes eseménykezelő központja felé terheli.
99 Ibtv. 24. § (1) bekezdés d), l), m) pontok.
100 Rendelet 4. § c) pont.
101 Ibtv. 24. § b), e), i), k), n), o) és p) pontok.

4. A kritikus infrastruktúrával kapcsolatos nemzeti szabályozás

Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv (a továbbiakban: EKI-irányelv) volt az Unió részéről az első olyan szabályozás, amely intézkedéseket tartalmazott az európai kritikus infrastruktúrák védelmére vonatkozóan és rögzítette, hogy a védelmi intézkedések kialakítása során figyelembe kell venni az ember által okozott technológiai veszélyeket, a természeti katasztrófákat és a fokozott terrorveszélyt. Az EKI-irányelv megállapította, hogy az európai kritikus infrastruktúrák védelmének felelőssége a tagállamokat és az infrastruktúrák tulajdonosait/üzemeltetőit terheli, akiknek valamennyi kijelölt kritikus infrastruktúra esetében gondoskodni kell arról, hogy rendelkezzenek üzemeltetői biztonsági tervvel, vagy ezzel egyenértékű olyan intézkedések kerüljenek bevezetésre, amelyek magukban foglalják a jelentős eszközök meghatározását, a kockázatértékelést, valamint az ellenintézkedések és -eljárások meghatározását, kiválasztását és rangsorolását. Az EKI-irányelv kimondja, hogy valamennyi kijelölt kritikus infrastruktúra tekintetében gondoskodni kell biztonsági összekötő tisztviselő kijelöléséről a kritikus infrastruktúrák védelméért felelős nemzeti hatóságokkal való együttműködés és kapcsolattartás megkönnyítése érdekében. Rögzíti továbbá, hogy a tagállamoknak az európai kritikus infrastruktúrák védelmével foglalkozó kapcsolattartó pontot kell kialakítaniuk a koordináció és a végrehajtás érdekében. Az EKI-irányelvnek való megfelelés érdekében a tagállamoknak 2011. január 12-ig kellett meghozni a szükséges intézkedéseket. Az EKI-irányelvnek való megfelelést Magyarország a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.), valamint a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (a továbbiakban: Lrtv. vhr.) megalkotásával biztosította, amelyek NIS-irányelv szerinti megfeleltetésére is sor került 2018-ban. Jelen fejezet az Lrtv. és az Lrtv. vhr. 2019. január 1-től hatályos főbb rendelkezéseit rögzíti és a főbb rendelkezések tekintetében utal a kapcsolódó ágazati szabályokra is.

4.1. Az Lrtv. szerinti ágazatok és alágazatok

Az Lrtv., mint a nemzeti jogrendbe átültetett létfontosságú rendszerelemekre vonatkozó szabályozás, meghatározza a nemzeti és az európai létfontosságú rendszerelemmé történő kijelölés főbb eljárási lépéseit, a kijelöléssel érintett ágazatokat és alágazatokat, valamint a NIS-irányelvvel összhangban az alapvető szolgáltatásokat nyújtó szereplők kijelölésére és nyilvántartására vonatkozó rendelkezéseket.

Létfontosságú rendszerelemnek az Lrtv. 1. mellékletben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatás tekinthető, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.[102] A kijelölt rendszerelem üzemeltetője egyben – a NIS-irányelvvel összhangban – alapvető szolgáltatásokat nyújtó szereplőnek is minősül, ha az alágazat megfeleltethető a NIS-irányelv szerinti ágazatnak vagy alágazatnak (az alapvető szolgáltatások jegyzékében szereplő szolgáltatást nyújt), a szolgáltatás nyújtása elektronikus információs rendszerektől függ és a bekövetkezett biztonsági esemény jelentős zavart okozna a szolgáltatás biztosításában.[103]

[102] Lrtv 1. § j) pont.
[103] Lrtv 2/A. § (2) bekezdés.

Az Lrtv. szerinti, valamint a NIS-irányelv szerinti megfeleltetés alapján azonosított ágazatokat és alágazatokat az alábbi felsorolás tartalmazza[104]:

a) Energiaágazat és alágazatai, melyek mindegyike a NIS-irányelv szerinti megfeleltetés alapján azonosításra került, az alábbiak:
  aa) a villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek),
  ab) a kőolajipar,
  ac) a földgázipar és
  ad) a távhő.

b) Közlekedési ágazat és alágazatai, melyek a logisztikai központok kivételével a NIS-irányelv szerinti megfeleltetés alapján azonosításra kerültek, az alábbiak:
  ba) a közúti közlekedés,
  bb) a vasúti közlekedés,
  bc) a légi közlekedés,
  bd) a vízi közlekedés és
  be) a logisztikai központok.

c) Agrárgazdasági ágazat alágazatai (NIS-irányelv szerinti megfeleltetésükre nem került sor):
  ca) a mezőgazdaság,
  cb) az élelmiszeripar és
  cc) az elosztó hálózatok.

d) Egészségügyi ágazat és alágazatai, melyek a laborok és a gyógyszer-nagykereskedelem kivételével a NIS-irányelv szerinti megfeleltetés alapján, mint egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is) azonosításra kerültek, az alábbiak:
  da) az aktív fekvőbeteg-ellátás,
  db) a mentésirányítás,
  dc) az egészségügyi tartalékok és vérkészletek,
  dd) a magas biztonsági szintű biológiai laboratóriumok és
  de) a gyógyszer-nagykereskedelem.

e) Társadalombiztosítási ágazat, azon belül a társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások. NIS-irányelv szerinti megfeleltetésére nem került sor.

f) Pénzügyi ágazat és alágazatai, melyek a készpénzellátás kivételével a NIS-irányelv szerinti megfeleltetés alapján azonosításra kerültek, az alábbiak:
  fa) a pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei (NIS-irányelv szerint pénzügyi piaci infrastruktúrák),
  fb) a bank- és hitelintézeti biztonság (NIS-irányelv szerint banki szolgáltatások) és
  fc) a készpénzellátás.

g) Infokommunikációs technológiák ágazata és alágazatai, melyek közül egy került a NIS-irányelv szerinti megfeleltetés alapján azonosításra, az alábbiak:
  ga) az internet-infrastruktúra és internethozzáférés-szolgáltatás (NIS-irányelv szerint digitális infrastruktúra),
  gb) a vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok,
  gc) a műsorszórás,
  gd) a postai szolgáltatások és
  ge) a kormányzati elektronikus információs rendszerek.

[104] Lrtv 1. § f) pont és az Lrtv. 1. melléklete.

h) Vízágazat és alágazatai, melyek közül egy került a NIS-irányelv szerinti megfeleltetés alapján azonosításra, az alábbiak:
  ha) az ivóvíz-szolgáltatás (NIS-irányelv szerint ivóvízellátás és -elosztás),
  hb) a felszíni és felszín alatti vizek minőségének ellenőrzése,
  hc) a szennyvízelvezetés és -tisztítás,
  hd) a vízbázisok védelme és
  he) az árvízi védművek és gátak.
i) A közbiztonság és védelem ágazata, azon belül a rendvédelmi szervek infrastruktúrái (NIS-irányelv szerinti megfeleltetésükre nem került sor).
j) A honvédelem ágazata, azon belül a honvédelmi rendszerek és létesítmények (NIS-irányelv szerinti megfeleltetésükre nem került sor).

4.2. A javaslattevő és a kijelölő hatóságok

A létfontosságú rendszerelem kijelölésére vonatkozó eljárás során javaslattevő hatóságként jár el:
a) a BM OKF, a közrend, a közbiztonság, a lakosságvédelem, az alkotmányvédelem, a nemzetbiztonság és a terrorelhárítás szempontjai esetében[105],
b) a BM OKF, a Büntetés-végrehajtás Országos Parancsnoksága, az Országos Rendőr-főkapitányság azon rendvédelmi rendszer, létesítmény vonatkozásában, melynek üzemeltetőjét irányítja, felügyeli[106],
c) az agrárgazdasági ágazat tekintetében – az üzemeltetőn kívül – a Nemzeti Élelmiszerlánc-biztonsági Hivatal az élelmiszerlánc-biztonsági és állategészségügyi hatósági hatáskörében, illetve a növény- és talajvédelmi hatósági hatáskörében eljáró megyei kormányhivatal bevonásával is kezdeményezheti[107],
d) az ivóvíz-szolgáltatás, a szennyvízelvezetés és -tisztítás, valamint az árvízvédelmi létesítmény vonatkozásában a területi vízügyi igazgatóság a vízágazat tekintetében[108],
e) az egészségügyi ágazatot érintően
  ea) az aktív fekvőbeteg-ellátás esetében az Állami Egészségügyi Ellátó Központ,
  eb) a mentésirányítás esetében az Országos Mentőszolgálat,
  ec) az egészségügyi tartalékok vonatkozásában az Állami Egészségügyi Ellátó Központ,
  ed) a vérkészletek vonatkozásában az Országos Vérellátó Szolgálat,
  ee) a magas biztonsági szintű biológiai laboratóriumok esetében az országos tisztifőorvos,
  ef) a gyógyszer-nagykereskedelem esetében az Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet[109],
f) a pénzügyi közvetítőrendszer felügyeletével kapcsolatos feladatkörében eljáró Magyar Nemzeti Bank a pénzügyi ágazat tekintetében[110],

[105] Lrtv. vhr. 3. §.

[106] Az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet (a továbbiakban: Rendvédelmi vhr.) 1. § (3) bekezdés.

[107] A létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 540/2013. (XII. 30.) Korm. rendelet (a továbbiakban: Agrár vhr.) 1. § (1) bekezdés.

[108] A létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendelet (a továbbiakban: Víz vhr.) 1. § (1) bekezdése.

[109] Az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet (a továbbiakban: Eü. vhr.) 2. §-a.

[110] A pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet (a továbbiakban: Pénzügy vhr.) 2. §-a.

g) a Honvédelmi Minisztérium a honvédelmi ágazat tekintetében[111],
h) a postai szolgáltatások tekintetében a postaügyért felelős miniszter[112].

A létfontosságú rendszerelem kijelölésére vonatkozó eljárás során ágazati kijelölő hatósági feladatokat lát el:

a) Az energiaágazat vonatkozásában[113]:
  aa) a villamosenergia-rendszer tekintetében a Magyar Energetikai és Közműszabályozási Hivatal,
  ab) a kőolaj-feldolgozás és kőolajtermék-tárolás kivételével a kőolajipar és a földgázipar tekintetében a bányafelügyelet,
  ac) a kőolaj-feldolgozás és kőolajtermék-tárolás tekintetében első fokon a fővárosi és megyei kormányhivatal mérésügyi feladatkörében eljáró megyeszékhely szerinti járási (fővárosi kerületi) hivatala.
b) A rendvédelmi ágazat vonatkozásában[114]:
  ba) az Alkotmányvédelmi Hivatal, a Nemzetbiztonsági Szakszolgálat, a Terrorelhárítási Információs és Bűnügyi Elemző Központ, a Büntetés-végrehajtás Országos Parancsnoksága és szervei, a Nemzeti Védelmi Szolgálat, az Országos Rendőr-főkapitányság és szervei, valamint a Terrorelhárítási Központ vonatkozásában a BM OKF üzemeltető telephelye szerinti területi szerve,
  bb) a BM OKF és szervei vonatkozásában az általános rendőrségi feladatok ellátására létrehozott szervnek az üzemeltető telephelye szerinti területi szerve.
c) Az agrárgazdasági ágazat tekintetében a Nemzeti Élelmiszerlánc-biztonsági Hivatal[115].
d) A vízágazat tekintetében a közcélú ivóvíz-szolgáltatást biztosító vízilétesítmény – ideértve a vonatkozó ivóvíz célú kitermelésre szánt felszíni és felszín alatti vizek minőségének ellenőrzését biztosító vízilétesítményt és a vonatkozó ivóvízbázis-védelmet biztosító vízilétesítményt –, valamint a szennyvízelvezetést és -tisztítást szolgáló vízilétesítmény és árvízvédelmi létesítmény tekintetében az illetékes vízügyi hatóság[116].
e) Az egészségügyi ágazat vonatkozásában az egészségügyért felelős miniszter, akit feladatainak ellátásában döntés-előkészítő bizottság segít[117].
f) A pénzügyi ágazat tekintetében a pénz-, tőke- és biztosítási piac szabályozásáért felelős miniszter, akit feladatainak ellátásában döntés-előkészítő bizottság segít[118].
g) A honvédelmi ágazat tekintetében a Honvédelmi Minisztérium[119].
h) Az infokommunikációs technológiák vonatkozásában a Nemzeti Média- és Hírközlési Hatóság Hivatala, amelyet feladatellátásában döntés-előkészítő bizottság segít[120], kivéve a kormányzati informatikai, elektronikus hálózatokat, ahol a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter[121].

---

111 A honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló 359/2015. (XII. 2.) Korm. rendelet (a továbbiakban: Honvédelmi vhr.) 3. §-a.
112 Az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet (a továbbiakban: Infokom. vhr.) 5. § (1) bekezdés.
113 Az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet (a továbbiakban: Energia vhr.) 2. §-a.
114 Rendvédelmi vhr. 1. § (1) bekezdés.
115 Agrár vhr. 1. § (2) bekezdés.
116 Víz vhr. 1. § (2) bekezdés.
117 Eü. vhr. 3. §.
118 Pénzügy vhr. 3. §.
119 Honvédelmi vhr. 3. § (1) bekezdés.
120 Infokom. vhr. 3. § (1) bekezdés és (4) bekezdés.
121 Infokom. vhr. 6. § (1) bekezdés.

4.3. Az Lrtv. szerinti azonosítási eljárás

A létfontosságú rendszerelem kijelölését megelőzi az üzemeltető által elvégzett azonosítás[122] folyamata, amely során a lehetséges létfontosságú rendszerelemeket kockázatelemzés[123], valamint az ágazati és horizontális kritériumok alapján határozzák meg. Üzemeltetőnek az a természetes, jogi személy vagy jogi személyiség nélküli szervezet minősül, aki vagy amely az eszköz, létesítmény, rendszer rendszerelemének tulajdonosa, engedélyese, rendelkezésre jogosultja vagy napi működéséért felelős[124].

Az azonosítási eljárás eredményéről az üzemeltető azonosítási jelentést készít, amely tartalmazza[125]:

a) a vizsgált lehetséges létfontosságú rendszerelem megnevezését, elhelyezkedésének beazonosíthatóságát biztosító helyadatokat, a kockázatelemzést, valamint annak eredményét és a nemzeti vagy európai létfontosságú rendszerelemmé történő kijelölésre irányuló javaslatot vagy a kijelölés visszavonására vagy a kijelölés fenntartására vonatkozó javaslatot,

b) az üzemeltetőnek az azonosítási jelentés teljességére vonatkozó nyilatkozatát, valamint

c) az azonosítási vizsgálat kezdő- és zárónapját,

d) az Lrtv. 2/A. § (2) bekezdésében meghatározott szempontrendszerre vonatkozó elemzést, ha a lehetséges rendszerelem tekintetében megállapítható, hogy az Lrtv. 1. mellékletében meghatározott azon alágazatba tartozik, amely a 3. melléklet alapján megfeleltethető a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és tanácsi irányelv szerinti valamely ágazatnak vagy alágazatnak,

e) az üzemeltető neve, székhelye, levelezési címe, cégjegyzékszáma, statisztikai számjele és adóazonosító száma, képviselőjének neve, telefonszáma, e-mail-címe,

f) a nemzeti létfontosságú rendszerelemek, szolgáltatások megnevezése és címe, valamint azon európai létfontosságú rendszerelemek, szolgáltatások megnevezése és címe, amelyek esetében Magyarország érintett fél.

Az azonosítási jelentést első alkalommal az adott ágazatra vonatkozó ágazati kritériumokat megállapító jogszabály hatálybalépését[126] követő 180 napon belül kellett az üzemeltetőnek elkészítenie és benyújtania az ágazati kijelölő hatóságnak. Ha az üzemeltető határidőn belül kötelezettségét nem teljesíti, az ágazati kijelölő hatóság határidő tűzésével felszólítja az azonosítási jelentés elkészítésére és benyújtására. Ha a felszólítás eredményeképpen az üzemeltető egyetlen rendszerelemet sem azonosított lehetséges létfontosságú rendszerelemként, ebben az esetben is be kell nyújtani az azonosítási jelentést.[127] Az ágazati kijelölő hatóság az azonosítási jelentést véleményezés céljából megküldi a javaslattevő hatóságnak, aki a jelentés beérkezésétől számított 30 napon belül megvizsgálja az azonosítási jelentést és a kockázatelemzéssel kapcsolatos javaslatait megküldi az ágazati kijelölő hatóságnak.[128]

---

122 A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (a továbbiakban: Lrtv. vhr.) 1. § 1. pont.

123 *Kockázatelemzés:* fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából. – Lrtv. vhr. 1. § 3) pont.

124 Lrtv. 1. § l) pont.

125 Lrtv. vhr. 2. § (1)–(2) bekezdései.

126 Az Lrtv. felhatalmazó rendelkezése alapján minden ágazatnak önálló Korm. rendeletet kellett készítenie végrehajtás céljából.

127 Lrtv. vhr. 2. § (3)–(4) bekezdései.

128 Lrtv. vhr. 2. § (5) bekezdése.

Az üzemeltető további kötelezettsége, hogy minden olyan a tevékenységében bekövetkezett változásról, amely érinti a létfontosságú rendszerelem azonosítását, 8 napon belül írásban értesítse az ágazati kijelölő hatóságot, illetve a kijelölésre vonatkozó döntés véglegessé válásától számított 5 év elteltével új azonosítási jelentést kell készítenie.[129]

További részletszabályokat az ágazati végrehajtási rendeletek tartalmaznak (vö. *4.11. Ágazati szabályok* alcím).

4.4. Az Lrtv. szerinti kijelölési eljárás

Az Lrtv. szerint nemzeti létfontosságú rendszerelem[130] a kijelölési eljárás során kijelölt olyan létfontosságú rendszerelem, amelynek kiesése, a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt, jelentős hatással lenne Magyarországon. Európai létfontosságú rendszerelem[131] a kijelölési eljárás során kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra.

Az Lrtv. szerint létfontosságú rendszerelem egy szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna, illetve, amely az Lrtv. 1. mellékletében meghatározott ágazatok valamelyikébe tartozik.

Ahhoz, hogy a fentiekben felsorolt valamely ágazat alágazatába tartozó eszköz, létesítmény vagy rendszer rendszereleme nemzeti létfontosságú rendszerelemként kerüljön kijelölésre vagy a NIS-irányelv szerinti megfeleltetés esetén alapvető szolgáltatást nyújtó szereplőkként kerüljön azonosításra, az ún. ágazati kijelölő hatóságnak kijelölési eljárást kell lefolytatnia[132].

Az ágazati kijelölő hatóság eljárását hivatalból folytatja le, az üzemeltető[133] által elkészített azonosítási jelentés benyújtását követően, az ún. javaslattevő hatóság javaslata alapján, szakhatóság bevonásával, amely során előzetes szakhatósági állásfoglalásnak nincs helye[134].

Az eljárás során az ágazati kijelölő hatóság, az ágazati és horizontális kritériumok alapján, az azonosítási jelentés kézhezvételétől számított 70 napon belül[135]:

a) határozatban dönt a nemzeti létfontosságú rendszerelemmé történő kijelöléséről és egyidejűleg rendelkezik az üzemeltető felvételéről az alapvető szolgáltatásokat nyújtó szereplők jegyzékébe[136] vagy dönt a kijelölés visszavonásáról és ezzel egyidejűleg rendelkezik az üzemeltető törléséről az alapvető szolgáltatásokat nyújtó szereplők jegyzékéből[137],

b) meghatározza az üzemeltetői biztonsági terv kidolgozásának határidejét, valamint

[129] Lrtv. vhr. 2. § (7)–(8) bekezdései.

[130] Lrtv 1. § k) pont.

[131] Lrtv 1. § f) pont.

[132] Lrtv 2. § (1) bekezdés és 2/A. § (1) bekezdése.

[133] Lrtv. 1. § l) pont, üzemeltető: az a természetes, jogi személy vagy jogi személyiség nélküli szervezet, aki vagy amely az eszköz, létesítmény, rendszer rendszerelemének tulajdonosa, engedélyese, rendelkezésre jogosultja vagy napi működéséért felelős.

[134] Lrtv 2. § (1) bekezdés, Lrtv. vhr. 4. § (1) és (2) bekezdés.

[135] Lrtv 2. § (3)–(4) bekezdései, Lrtv. vhr. 4. § (1) bekezdés.

[136] Lrtv. 2/A. § (3) bekezdése.

[137] Lrtv. 2/A. § (5) bekezdése.

c) a létfontosságú rendszerelem védelmével[138] összefüggő, a rendszerelem egyedi sajátosságaihoz, környezetéhez, a rendszerelem által potenciálisan előidézhető veszély mértékéhez igazodó feltételeket írhat elő az üzemeltető részére.

Az ágazati kijelölő hatóság határozatában:

a) jóváhagyja az üzemeltető azonosítási jelentését és a rendszerelemet a hatósági nyilvántartásba történő felvétel elrendelése mellett nemzeti létfontosságú rendszerelemnek jelöli ki, feltéve, hogy az ágazati kritériumok közül és a szakhatóság állásfoglalása vagy a kijelölő hatóság döntése[139] alapján a horizontális kritériumok közül legalább egy-egy bekövetkezésének lehetősége fennáll,

b) jóváhagyja az üzemeltető azonosítási jelentését és a kijelölést visszavonja, valamint elrendeli a nyilvántartásból való törlést,

c) a kijelölésre, kijelölés visszavonására irányuló javaslatot elutasítja vagy legfeljebb 90 napos határidő tűzésével és a feltárt hibák, hiányosságok tételes megjelölésével új azonosítási jelentés benyújtását írja elő,

d) jóváhagyja, hogy az üzemeltető egyetlen rendszerelemet sem azonosított lehetséges létfontosságú rendszerelemként,

e) rendelkezik az üzemeltető felvételére vagy törlésére az alapvető szolgáltatásokat nyújtó szereplők jegyzékéből.[140]

A nemzeti létfontosságú rendszerelemmé történő kijelölés visszavonásáról az ágazati kijelölő hatóság a javaslatevő hatóság vagy az üzemeltető kérelmére – szakhatóság bevonásával, előzetes állásfoglalás mellőzésével – dönthet[141], amely döntés alapján a nyilvántartó hatóság törli az alapvető szolgáltatásokat nyújtó szereplők jegyzékéből az üzemeltetőt[142].

Európai létfontosságú rendszerelemmé történő kijelölési eljárást az ágazati kijelölő hatóság hivatalból folytatja le[143]:

a) az üzemeltető által lefolytatott azonosítási eljárás alapján elkészített azonosítási jelentés benyújtását követően,

b) EGT-állam kezdeményezése alapján vagy

c) a javaslattevő hatóság ágazati kijelölő hatóságnál tett kezdeményezése alapján.

A kezdeményezést és az üzemeltető által benyújtott azonosítási jelentést az ágazati kijelölő hatóság – *c)* pont kivételével – a javaslattevő hatóság bevonásával megvizsgálja és a szakmai álláspontjáról az ágazatért felelős miniszter útján a Belügyminisztert mint a katasztrófák elleni védekezésért felelős minisztert (a továbbiakban: Belügyminiszter) tájékoztatja. A Belügyminiszter az adott ágazat szerinti feladat- és hatáskörrel rendelkező miniszterrel együtt kezdeményezi az európai létfontosságú rendszerelemmé nyilvánítással kapcsolatos nemzetközi szerződés megkötését. A nemzetközi szerződés hatálybalépésétől számított 30 napon belül az ágazati kijelölő hatóság a kijelölésről határozatot hoz, amelyben meghatározza az üzemeltető kötelezettségeit, azok végrehajtásának határidejét és ellenőrzését.[144]

---

[138] Lrtv. 1. § i) pont, létfontosságú rendszerelem védelme: a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység.

[139] Ha kijelölő hatóságként a BM OKF központi, területi vagy helyi szerve jár el, a horizontális kritériumok teljesülése fennállásának a kérdését a hatósági eljárás során a kijelölő hatóság vizsgálja. – Lrtv. vhr. 4. § (1) bekezdés.

[140] Lrtv. vhr. 4. § (3) bekezdés.

[141] Lrtv 2. § (2) bekezdés, Lrtv. vhr. 4. § (2) bekezdés.

[142] Lrtv. 2/A. § (5) bekezdése.

[143] Lrtv 3. § (1) bekezdés.

[144] Lrtv 3. § (2)–(4) bekezdései.

Ha a Belügyminiszter nem ért egyet:

a) a javaslattevő hatóság európai létfontosságú rendszerelemmé történő kijelölésre irányuló kezdeményezésével, kiegészítésre visszaküldi, ha a vhr. 2. § (2) bekezdésében foglaltaknak nem felel meg, vagy nem támogatja, amennyiben az azonosítási jelentésben megfelelően nem igazolt legalább kettő, az Európai Gazdasági Térségről szóló megállapodásban részes más államra (a továbbiakban: EGT-állam) kiterjedően a nemzeti létfontosságú rendszerelem kiesésének jelentősége,

b) az Európai Gazdasági Térségről szóló megállapodásban részes más állam európai létfontosságú rendszerelemmé történő kijelölésre irányuló kezdeményezésével, erről tájékoztatja a kezdeményező államot[145].

Európai létfontosságú rendszerelemmé történő kijelölés visszavonásáról az ágazati kijelölő hatóság hivatalból, EGT-állam kezdeményezése alapján hivatalból vagy az üzemeltető nyilatkozata alapján dönthet[146]. Ha a Belügyminiszter egyetért az EGT-állam kezdeményezésével, illetve az üzemeltető kérelmével, az adott ágazat szerinti feladat- és hatáskörrel rendelkező miniszterrel együtt kezdeményezi az európai létfontosságú rendszerelemmé nyilvánítással kapcsolatos nemzetközi szerződés felbontását. Ez esetben a nemzetközi szerződés felbontását követően az ágazati kijelölő hatóság a kijelölésről határozatot hoz és a kijelölést visszavonja, valamint a feltételek fennállása esetén dönt a nemzeti létfontosságú rendszerelemmé történő kijelölésről. Ha a Belügyminiszter az üzemeltető kijelölés visszavonására vonatkozó kérelmével nem ért egyet, a kijelölő hatóság tájékoztatja az üzemeltetőt a kijelölés fenntartásáról. Ha a visszavonást EGT-állam kezdeményezi, a fenti szabályok alkalmazásával kezdeményezi a kijelölés fenntartását. [147]

Ha az európai létfontosságú rendszerelemmé történő kijelölés vagy a kijelölés visszavonása kérdésében az ágazatért felelős miniszter és a Belügyminiszter ellentétes álláspontot képvisel, a végleges álláspontról a Kormány dönt.[148]

Az ágazati kijelölő hatóság a kijelölésre és a kijelölés visszavonására vonatkozó, véglegessé vált határozatát haladéktalanul köteles megküldeni a BM OKF-nek mint nyilvántartó hatóságnak. A kijelölés visszavonására vagy elutasítására vonatkozó véglegessé vált határozatát pedig a kijelölési eljárásban érintett valamennyi hatóságnak meg kell küldenie[149].

Az ágazati kijelölő hatóság által lefolytatott kijelölési és kijelölés visszavonására vonatkozó hatósági eljárásban a hatóságok és a szakhatóságok részéről csak olyan személy vehet részt, akinek a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott nemzetbiztonsági ellenőrzését elvégezték és akivel szemben kockázati tényező nem merült fel. Ugyanez a szabály érvényes az európai létfontosságú rendszerelemekre vonatkozó azonosítási eljárás lefolytatása során az üzemeltető által igénybe vett közreműködő szervezet részéről igénybe vett személy esetén is[150].

A BM OKF központi, területi vagy helyi szerve ágazati kijelölő hatósági, illetve szakhatósági eljárásában:

a) a gazdasági hatás kritériuma teljesülésének kérdésében a Nemzeti Adó- és Vámhivatal központi szerve,

b) a társadalmi hatás kritériuma teljesülésének kérdésében az általános rendőrségi feladatok ellátására létrehozott szerv területi, illetve központi szerve, az Alkotmányvédelmi Hivatal központi szerve, a Terrorelhárítási Központ, a Terrorelhárítási Információs és Bűnügyi Elemző Központ, valamint az Országos Idegenrendészeti Főigazgatóság,

[145] Lrtv. vhr. 5. § (1)-(2) bekezdései.
[146] Lrtv 3. § (1a) bekezdés.
[147] Lrtv. vhr. 5. § (3)–(4) bekezdései.
[148] Lrtv. vhr. 5. § (6) bekezdése.
[149] Lrtv 5. § (3) és (6) bekezdései.
[150] Lrtv 4. § (1) bekezdése.

c) a politikai hatás kritériuma teljesülésének lehetősége tekintetében az illetékes kormánymegbízott,
d) a környezeti hatás kritériuma teljesülésének lehetősége kérdésében a területi környezetvédelmi hatóság, a területi vízügyi és vízvédelmi hatóság, az országos természetvédelmi és környezetvédelmi hatóság, valamint az országos vízügyi és vízvédelmi hatóság,
e) a védelem kritériuma teljesülésének kérdésében a hivatásos katasztrófavédelmi szerv területi szerve véleményét kérheti.

Ezek a szervek ellenőrzési tevékenységük során a kijelölés alapjául szolgáló körülmények változatlan fennállásán kívül vizsgálják:
a) a létfontosságú rendszerelemek,
b) a létfontosságú rendszerelemekhez tartozó közterületek, valamint
c) a létfontosságú rendszerelemeket felügyelő, működtető személyek
azon fizikai, humán és informatikai biztonsági feltételeinek meglétét, amelyek garantálják az azonosított kockázatokkal szembeni védelmet, a rendeltetésszerű működést, a szándékos és nem szándékos károkozás elkerülését[151].

További részletszabályokat az ágazati végrehajtási rendeletek tartalmaznak (vö. *4.11. Ágazati szabályok* alcím).

4.5. Horizontális és ágazati kritériumok

Az Lrtv. szerint horizontális kritériumnak[152] minősülnek azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének kiesése által kiváltott hatásra vonatkoznak és amelyek teljesülése esetén – figyelemmel a bekövetkező emberiélet-veszteségekre, az egészségre gyakorolt hatásra, a gazdasági és társadalmi hatásokra, a természetre és az épített környezetre gyakorolt hatásra – az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki attól függetlenül, hogy mely ágazatba tartozik.

Az Lrtv. vhr. 1. melléklete szerint horizontális kritériumnak minősül egyetlen vagy egymással közvetlenül összefüggő eseményekkel kapcsolatban Magyarország területén:
1. A veszteségek kritériuma:
   a) 24 óra leforgása alatt az áldozatok száma a 20 főt meghaladja vagy a súlyos sérültek száma legalább 75 fő, vagy
   b) 72 óra leforgása alatt az áldozatok száma a 40 főt meghaladja vagy a súlyos sérültek száma legalább 150 fő.
2. A gazdasági hatás kritériuma: a gazdasági veszteség mértéke vagy termékek és szolgáltatások romlásának mértéke, a rendszer és létesítmény fizikai sérüléséből, elvesztéséből fakadó közvetlen vagy közvetett károk, amelyek ötvenezer fő vonatkozásában meghaladják az egy főre eső bruttó nemzeti jövedelem bármely 30 napos időszakra vetített mértékének 25%-át.
3. A társadalmi hatás kritériuma: 300 fő/km^2-nél sűrűbben lakott területen a köznyugalom súlyos megzavarása, beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is.
4. A politikai hatás kritériuma: az állam és intézményei iránti közbizalom megszűnése, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete kritikus szint alá csökken.

[151] Lrtv. vhr. 11. § (1) és (3) bekezdés.
[152] Lrtv. 1. § h) pont.

5. A környezeti hatás kritériuma: az esemény vagy folyamat, amely miatt a természeti vagy épített környezetben, különösen:
   a) az infrastruktúrában bekövetkező sérülés vagy zavar, az épített vagy természetes környezet oly mértékű rongálódását idézi elő, amelynek következtében:
      aa) 10 000 fő kimenekítése vagy kitelepítése válik szükségessé, vagy
      ab) legalább 100 km^2 nagyságú terület tartósan szennyeződik, vagy
      ac) a felszín alatti vizek vagy azok természetes víztartó képződményei, a folyóvizek és természetes tavak, valamint ezek medre vagy élővilága szenved tartós károsodást,
      ad) az ország tájegységeiben, kiemelkedő földrajzi területeiben visszafordíthatatlan negatív változás következik be.
6. A védelem kritériuma: az infrastruktúrában bekövetkező sérülés, zavar, állapot, esemény vagy folyamat:
   a) amely következtében a rendszerelem ellátási láncban betöltött szerepét nem tudja ellátni,
   b) sérülése vagy megsemmisülése esetén a beavatkozás, mentés vagy kárfelszámolás ideje aránytalanul megnövekszik, vagy
   c) katasztrófák elleni védekezés, a károk felszámolása időlegesen ellehetetlenül.

A horizontális kritériumok értékeléséhez a BM OKF központi, területi vagy helyi szerve véleményt kérhet az 1. § (1) bekezdésben meghatározott szervektől, azonban az (1) bekezdésben megkeresett szervek véleménye a szakhatóságot döntése során nem köti.[153]

Ágazati kritériumnak[154] minősülnek azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének megzavarása vagy megsemmisítése (a továbbiakban együtt: kiesés) által kiváltott hatásra vonatkoznak és amelyek teljesülése esetén az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki azzal szoros összefüggésben, hogy mely ágazatba tartozik.

Az Lrtv. hatálya alá tartozó alágazatok ágazati kritériumait a végrehajtási rendeletek tartalmazzák, amelyek részletes ismertetése nem célja jelen tananyagnak. Az egyes szabályzók és az ágazati kritériumokat felsoroló jogszabályi rendelkezések az alábbiak:

a) az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet (a továbbiakban: Energia vhr.) 3–4. §-ai,
b) az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet (a továbbiakban: Rendvédelmi vhr.) 2. §-a,
c) a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 540/2013. (XII. 30.) Korm. rendelet (a továbbiakban: Agrár vhr.) 2–4. §-ai,
d) a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendelet (a továbbiakban: Víz vhr.) 2. és 4. §-ai,
e) az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet (a továbbiakban: Eü. vhr.) 4–11. §-ai,
f) a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet (a továbbiakban: Pénzügy vhr.) 6–7. §-ai,

[153] Lrtv. vhr. 11. § (2) bekezdés.
[154] Lrtv. 1. § a) pont.

g) a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló 359/2015. (XII. 2.) Korm. rendelet (a továbbiakban: Honvédelmi vhr.) 2. §-a,
h) az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet (a továbbiakban: Infokom. vhr.) 9–14. §-ai.

4.6. Hatósági feladatok

Az Lrtv. szerinti nyilvántartó hatósági feladatokat – kivéve a honvédelmi létfontosságú rendszerelemeket – a BM OKF[155] látja el, amely feladat- és hatáskörében eljárva nyilvántartja és kezeli[156]:

a) az üzemeltető nevét, székhelyét vagy lakcímét, levelezési címét, cégjegyzékszámát vagy az egyéni vállalkozói nyilvántartási számát, statisztikai számjelét és adóazonosító számát, képviselőjének nevét, telefonszámát, e-mail címét,
b) a biztonsági összekötő személy természetes személyazonosító adatait, telefonszámát, e-mail címét, szakirányú végzettségét, a végzettséget igazoló okirat sorszámát,
c) a nemzeti létfontosságú rendszerelemek, szolgáltatások megnevezését és címét, valamint azon európai létfontosságú rendszerelemek, szolgáltatások megnevezését és címét, amelyek esetében Magyarország érintett fél,
d) az üzemeltetői biztonsági tervet,
e) az ágazati kijelölő hatóságnak az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem kijelöléséről és a kijelölés visszavonásáról szóló határozatát,
f) a hatósági ellenőrzéssel összefüggő dokumentumokat,
g) *az informatikai biztonsági szabályzatot.

Ezen adatkezelés célja az azonosítási és a kijelölési eljárás, a kijelölés visszavonására vonatkozó eljárás lefolytatásának biztosítása, valamint a hatósági ellenőrzés biztosítása érdekében a létfontosságú rendszerelemek védelmével kapcsolatos kötelezettségek teljesítésének és a kijelölési eljárás során hozott határozatban előírt feltételeknek való megfelelésnek a vizsgálata. Az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem adatait a nyilvántartó hatóság, valamint a kijelölési eljárásban érintett valamennyi hatóság az ágazati kijelölő hatóság rendszerelem kijelölése visszavonásáról szóló határozatának véglegessé válása után 30 napon belül a nyilvántartásból törli és erről az üzemeltetőt írásban értesíti. Az ágazati kijelölő hatóság haladéktalanul köteles megküldeni

a) a kijelölés visszavonására vagy elutasítására vonatkozó véglegessé vált határozatot a kijelölési eljárásban érintett valamennyi hatóságnak,
b) a kijelölés visszavonására vonatkozó véglegessé vált határozatot a nyilvántartó hatóságnak. [157]

Fentiekben felsorolt alapadatokat tartalmazó hatósági nyilvántartásból az adatkezelési céllal összefüggésben a BM OKF adattovábbítást – az érintett szervek írásbeli, az adatigénylési cél meghatározásával és az átvenni kívánt adatok körének pontos megjelölésével ellátott kérelme alapján[158] – az alábbiak figyelembevételével végezhet[159]:

a) a kijelölési eljárásban, a kijelölés visszavonására irányuló eljárásban részt vevő hatóságok részére a kijelölési eljárás, a kijelölés visszavonására irányuló eljárás lefolytatásának biztosítása céljából,
b) az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem ellenőrzését koordináló szerv részére a koordinációs feladatok biztosítása céljából,

[155] Lrtv. vhr. 10. § (1) bekezdés.
[156] Lrtv. 5. § (1) és (2) bekezdései.
[157] Lrtv. 5. § (5)–(6) bekezdés.
[158] Lrtv. vhr. 10. § (3) bekezdés.
[159] Lrtv. 5. § (4) bekezdés.

c) az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem helyszíni ellenőrzését lefolytató szerv részére a helyszíni ellenőrzés lefolytatása céljából,
d) az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem hatósági ellenőrzésére jogszabály alapján feladat- és hatáskörrel rendelkező hatóságok részére a hatósági ellenőrzések lefolytatása céljából,
e) rendkívüli esemény bekövetkezése esetén az eseménykezelésben és a helyreállításban részt vevő szervek tevékenységének támogatása céljából,
f) a hivatásos katasztrófavédelmi szerv területi és helyi szervei részére hatósági, megelőzési, kapcsolattartási és tájékoztatási feladatai elvégzése, illetve rendkívüli esemény kezelése céljából,
g) az Ibtv. 2. § (5) bekezdése és 14. § (1) bekezdése szerinti hatóság, az Európai Parlament és a Tanács 2016. július 6-i (EU) 2016/1148 irányelve alapján kormányrendeletben kijelölt egyedüli kapcsolattartó pont, valamint az Ibtv. 19. § (1) és (2) bekezdése szerinti eseménykezelő központ részére feladataik ellátása céljából,
h) a honvédelmi ágazat javaslattevő hatósága részére a lehetséges honvédelmi létfontosságú rendszerelemek körének felmérése céljából,
i) különleges jogrend vagy honvédelmi veszélyhelyzet időszakában a honvédelmi ágazat javaslattevő hatósága részére a nemzeti létfontosságú rendszerelemek fokozott védelmének megszervezése céljából,
j) az egységes digitális rádiótávközlő rendszer (a továbbiakban: EDR) kormányzati célú hírközlési szolgáltatás biztosítása érdekében az EDR szolgáltatás biztosítójának,
k) nemzetbiztonsági, valamint terrorelhárítási érdekből, külön, a feladatellátásért felelős szerv által benyújtott, indokolt kérelem alapján.

A BM OKF-nek a szabályszerű adatszolgáltatást 15 napon belül teljesíteni kell.

Fenti nyilvántartási tevékenység végzése mellett az alapvető szolgáltatásokat nyújtó szereplők jegyzékét is a BM OKF, mint nyilvántartó hatóság vezeti[160].

A BM OKF – ideértve a helyszíni ellenőrzést lefolytató szervet is – az ellenőrzési tevékenysége során a biztonsági összekötő büntetlen előéletre vonatkozóan megismert személyes adatait – ha a hatósági ellenőrzése során azt állapítja meg, hogy a biztonsági összekötő e követelményének nem felel meg – további eljárás lefolytatása céljából átadja az ágazati kijelölő hatóságnak. A büntetlen előéletre vonatkozó személyes adatot:

a) a helyszíni ellenőrzést lefolytató szerv a helyszíni ellenőrzés, valamint az ágazati kijelölő hatóságnak történő adattovábbítás időtartamára,
b) a BM OKF a hatósági ellenőrzés, valamint az ágazati kijelölő hatóságnak történő adattovábbítás időtartamára,
c) az ágazati kijelölő hatóság a hiánypótlásra vonatkozó hatósági ellenőrzés időtartamára, valamint ezen határozat véglegessé válásáig

kezeli.[161]

Az üzemeltetői biztonsági tervben meghatározott rendkívüli esemény bekövetkezésekor a BM OKF[162]:

a) a hivatásos katasztrófavédelmi szerv központi szerve jogosult a hatáskörükben érintett hatóságoktól és szervektől a beavatkozáshoz és elhárításához szükséges adatokat beszerezni, azok közreműködését kérni;

[160] Lrtv. 2/A. § (4) bekezdése.
[161] Lrtv. 8. § (8)–(9) bekezdései.
[162] Lrtv. vhr. 11 § (6) bekezdés.

b) az *a)* pont szerinti adatszolgáltatást az érintett hatóság és szerv soron kívül köteles teljesíteni, az adatszolgáltatást a megkeresett nem tagadhatja meg;
c) a rendkívüli eseményre való reagálás, a mentés megszervezése, irányítása, továbbá a lakosság tájékoztatása, a károk felmérése, az eredeti állapot lehetőség szerinti helyreállítása a hivatásos katasztrófavédelmi szerv központi szervének koordinálásával történik;
d) a szükséges erők, eszközök bevonására az érintett kijelölő hatóság javaslatot tehet;
e) a kiváltó okok azonosításában, a tett intézkedések értékelésében az érintett kijelölő hatóság, a beavatkozást végző szervek és a biztonsági összekötő személy együtt vesz részt.

4.7. Ellenőrzési feladatok

1. Az Lrtv. szerint a BM OKF a kijelölt létfontosságú rendszerelemek hatósági ellenőrzése során mint kijelölt ellenőrzést koordináló szerv jár el[163], kivéve a honvédelmi létfontosságú rendszerelemeket. Ennek keretében a jogszabály alapján feladat- és hatáskörrel rendelkező hatóságok részére hatósági ellenőrzés lefolytatására vonatkozó javaslatot tesz, több társhatóság bevonásával együttes hatósági ellenőrzéseket szervez. Koordinációs feladatkörében eljárva – a NIS-irányelvvel összhangban – ellátja a létfontosságú rendszerelemek védelmével kapcsolatos információ- és hálózatbiztonsági intézkedések koordinációját, a hálózatbiztonság fenntartásának elősegítését, a hálózatbiztonsággal kapcsolatos események elemzését és értékelését is.[164]

A BM OKF-nek feladatellátásával összefüggésben[165]:
a) éves ellenőrzési tervet kell összeállítania a tárgyévet megelőző év december 31-ig, figyelemmel arra, hogy minden létfontosságú rendszerelemnek legalább 5 évente el kell végezni az ellenőrzését,
b) az ellenőrzési terv végrehajtásáról összefoglaló jelentést kell készítenie a tárgyévet követő év március 1-ig,
c) az ellenőrzések lefolytatása során az ellenőrzésben részt vevő szervektől eljárásaik kimeneteléről, a megállapított hiányosságok pótlásáról tájékoztatást kérhet, melyet a szervek haladéktalanul kötelesek teljesíteni.

Az éves ellenőrzési terv elkészítése érdekében az érintett hatóságok minden évben legkésőbb a tárgyévet megelőző év október 15. napjáig kötelesek megküldeni a BM OKF részére az ellenőrzési terv elkészítéséhez szükséges javaslataikat, melyeket a saját ellenőrzési rendszerükben is felhasználnak[166].

A BM OKF ellenőrzi[167]:
a) az általa, mint nyilvántartó hatóság által, nyilvántartott és kezelt adatok valódiságát,
b) az üzemeltetői biztonsági tervben foglalt, a létfontosságú rendszerelem teljes körű személyi, fizikai, adminisztratív védelmének, a folyamatos működést veszélyeztető kockázatoknak és kezelésüknek a teljeskörűségét.

[163] Lrtv. 8. § (1) és (4) bekezdése.
[164] Lrtv. 8. § (6) bekezdése.
[165] Lrtv. vhr. 8. § (1)–(3) bekezdései.
[166] Lrtv. vhr. 11. § (4) bekezdés.
[167] Lrtv. vhr. 8. § (4) bekezdése.

Honvédelmi létfontosságú rendszerelemek esetén az ellenőrzést koordináló szerv a Honvédelmi Minisztérium, kivéve a honvédelmi létfontosságú információs rendszerelemeket, ahol az ellenőrzést koordináló szerv feladatait a Katonai Nemzetbiztonsági Szolgálat látja el.[168]

A BM OKF és szervei létfontosságú rendszerei vonatkozásában az ellenőrzést koordináló szerv feladatait a Belügyminiszter az általa kijelölt, ellenőrzési feladatokat ellátó szervezeti egység útján látja el[169].

2. A helyszíni ellenőrzés lefolytatására jogosult szervek a BM OKF koordinálásával ütemezett módon, az általa készített éves ellenőrzési terv alapján végzik az ellenőrzéseket. Kötelezettségük, hogy a kijelölt rendszerelemet legalább két évente ellenőrizzék, amely vizsgálatot a nemzetbiztonsági szempontok figyelembevételével kell lefolytatniuk[170].

Helyszíni ellenőrzésre jogosult szervek:

a) a BM OKF és szervei létfontosságú rendszerei vonatkozásában a Belügyminiszter az általa kijelölt, ellenőrzési feladatokat ellátó szervezeti egység közreműködésével látja el a feladatot[171],

b) az egészségügyi ágazat vonatkozásában[172]:

ba) a kórházak és a laboratóriumok tekintetében a népegészségügyi feladatkörében eljáró fővárosi és megyei kormányhivatal,

bb) a mentésirányítást végző szervezet, az Állami Egészségügyi Tartalék kezelője, az állami vérkészletek kezelője és a gyógyszer-nagykereskedelem tekintetében az egészségügyért felelős miniszter, aki a minisztériumnak az általa kijelölt, ellenőrzési feladatokat ellátó szervezeti egysége közreműködésével látja el a feladatot.

A helyszíni ellenőrzést lefolytató szerv a hatósági ellenőrzés céljából adatot igényelhet a bűnügyi nyilvántartási rendszerből, amely kizárólag a biztonsági összekötő büntetlen előéletének megállapítására irányulhat.[173]

4.8. Szankció

Ha a létfontosságú rendszerelem üzemeltetője nem tesz eleget az Lrtv.-ben vagy a felhatalmazása alapján kiadott más jogszabályokban, illetve az ágazati kijelölő hatóság határozatában foglalt előírásoknak, az ágazati kijelölő hatóság határozatban:

a) kötelezi az üzemeltetői biztonsági terv módosítására vagy új üzemeltetői biztonsági terv készítésére,

b) bírságot szabhat ki.[174]

A *b)* pont szerint kiszabható bírság összege 100 000.- Ft-tól 10 000 000.- Ft-ig terjedhet, melyet a bírság kiszabásáról rendelkező döntés véglegessé válásától számított 15 napon belül kell megfizetni a kijelölő hatóság által megadott bírság letéti számla javára. A bírság kiszabását a létfontosságú rendszerelemmel kapcsolatos hatósági eljárásokban részt vevő hatóságok is kezdeményezhetik a kijelölő hatóságnál.[175]

168 Honvédelmi vhr. 3. §-a.
169 Rendvédelmi vhr. 3. §-a.
170 Lrtv. vhr. 8. § (1) bekezdés.
171 Rendvédelmi vhr. 3. §-a.
172 Eü. vhr. 15. §-a.
173 Lrtv. 8. § (7) bekezdés.
174 Lrtv. 9. §
175 Lrtv. vhr. 9. § (1)–(3) bekezdései.

4.9. Biztonsági összekötő

Az üzemeltető kötelezettsége az Lrtv. előírásai szerint, hogy gondoskodjon a biztonsági összekötő személy foglalkoztatásáról és folyamatosan biztosítsa a tevékenységéhez szükséges feltételeket. A biztonsági összekötő személy feladata a kapcsolattartás az üzemeltető és a kijelölési eljárásban részt vevő hatóságok, szakhatóságok között, valamint az üzemeltetői biztonsági terv kidolgozása.[176]

Biztonsági összekötőnek az a büntetlen előéletű személy jelölhető ki, aki az adott ágazatnak megfelelő szakirányú végzettség mellett az alábbiakban meghatározott képzettséggel rendelkezik[177]:

a) védelmi igazgatási, katasztrófavédelmi vagy rendészeti igazgatási szakon szerzett felsőfokú végzettséggel,
b) tűzvédelmi, iparbiztonsági, polgári védelmi szakmai irányú rendészeti szervezői szakképesítéssel vagy ezzel egyenértékű végzettséggel,
c) iparbiztonsági szaktanfolyami végzettséggel,
d) iparbiztonsági szakon szerzett felsőfokú végzettséggel vagy
e) a katasztrófavédelem hivatásos szerveinél legalább 5 év iparbiztonsági szakterületen szerzett gyakorlattal.

Az *a)–c)* pontjában előírt követelmények alól, a korábban rendvédelmi szerv által, a rendvédelmi szerv alaptevékenységébe tartozó feladatok ellátása körében legalább öt évig foglalkoztatott felsőfokú végzettségű személy mentesül. A mentesülés feltételeinek való megfelelést az érintettnek szükséges igazolnia.

Az adott ágazatra vonatkozó további képzettségi követelmények az alábbiak:

a) az energiaágazatban a fent felsorolt képzettségeken kívül szakirányú műszaki végzettséggel kell rendelkeznie[178],
b) az egészségügyi ágazatban[179] ágazati szakirányú végzettségnek minősül az orvosi végzettség, ezen felül:
  ba) laboratóriumban történő foglalkoztatás esetén a biológus végzettség, illetve a mikrobiológus végzettség,
  bb) gyógyszer-nagykereskedelemben történő foglalkoztatás esetén az orvosi végzettség helyett
    i. a gyógyszerek minőségbiztosítása érdekében meghatalmazott személy képesítési feltételeiről szóló miniszteri rendeletben meghatározott feltételeknek megfelelő végzettség, illetve
    ii. bármely műszaki, mérnöki, logisztikus, gépész, gyógyszerész, vegyész vagy informatikus szakon szerzett felsőfokú végzettség, csak akkor, ha az ott meghatározott végzettséggel rendelkező gyógyszer-kereskedelmi, illetve egyéb gyógyszeripari tevékenységet végző gazdasági társaságnál, vállalkozásnál vagy ilyen területen működő hatóságnál, intézetnél vagy más szervezetnél legalább 3 év gyakorlatot szerzett a végzettségének megfelelő tevékenységet végezve foglalkoztatásra irányuló vagy megbízási jogviszony keretében.
  bc) a gyógyszer-nagykereskedelemben történő foglalkoztatás kivételével az egészségügyi ágazatnak megfelelő szakirányú végzettségnek minősül továbbá minden egyéb felsőfokú végzettség, ha a felsőfokú végzettséggel rendelkező egészségügyi igazgatási feladatkörben legalább hároméves szakmai gyakorlatot szerzett foglalkoztatásra irányuló vagy megbízási jogviszony keretében.

[176] Lrtv. 6. § (7) bekezdés.
[177] Lrtv. vhr. 6. § (1)–(3) bekezdései.
[178] Energia vhr. 18. §.
[179] Eü. vhr. 13. §.

c) a pénzügyi ágazatban felsőfokú szakirányú közgazdasági vagy jogi végzettséggel kell rendelkeznie[180],
d) a honvédelmi ágazatban a katonai felsőfokú végzettséggel és az adott rendszerelem működtetésében legalább kétéves szakmai tapasztalattal kell rendelkeznie[181],
e) az infokommunikációs technológiák ágazat esetében[182]:
  ea) az üzemeltető által elismert felsőfokú végzettséggel,
  eb) az infokommunikációs technológiák ágazatban eltöltött legalább öt év munkaviszonnyal és okleveles védelmi igazgatási vagy azzal egyenértékű végzettséggel vagy
  ec) az Ibtv. szerinti elektronikus információs rendszer biztonságáért felelős személy tekintetében irányadó képzettséggel,
  ed) fentieken túl az egyetemes postai szolgáltatás esetében a jogi végzettséggel is.

A büntetlen előéletre vonatkozó követelmény teljesülését a biztonsági összekötő igazolja.[183]

4.10. Üzemeltetői feladatok és az üzemeltetői biztonsági terv

Az üzemeltető az ágazati kijelölő hatóság határozatában meghatározott határidőn belül – amely nem lehet rövidebb a kijelölő határozat közlésétől számított 60 napnál – köteles kidolgozni a döntésben meghatározott tartalmi és formai követelmények szerinti üzemeltetői biztonsági tervet, amelyben szerepeltetnie kell:

a) a létfontosságú rendszerelemeket és azt a szervezeti- és eszközrendszert, amely biztosítja azok védelmét,
b) azokat a biztonsági intézkedéseket, amelyek kialakítása és működtetése biztosítja a létfontosságú rendszerelem védelmét,
c) azokat az ideiglenes intézkedéseket, amelyeket a különböző kockázati és veszélyszinteknek megfelelően foganatosítani kell,
d) a létfontosságú rendszerelem védelmét szolgáló meglévő vagy kialakítás alatt álló biztonsági megoldásokkal kapcsolatos eljárást.

A hatósági döntés meghozatalánál figyelembevételre kerülő, az üzemeltetői biztonsági terv felépítésére, tartalmi és formai elemeire vonatkozó követelmények a 2. melléklet tartalmazza[184].

Soron kívül módosítani kell az üzemeltetői biztonsági tervet, ha olyan változás áll be, amely érinti a létfontosságú rendszerelem szolgáltatásának nyújtását, tevékenységét, működését vagy védelmét, ideértve a bekövetkezett rendkívüli eseménnyel összefüggő újonnan felmerülő kockázat kezelését is, ha azt korábban még nem vizsgálták[185]. Soron kívüli felülvizsgálatot kezdeményezhet a kijelölő hatóság vagy a kijelölő hatóságnál a BM OKF. Egyéb esetben az üzemeltető felelőssége az üzemeltetői biztonsági terv szükség szerinti módosítása és az elkészítést követő 2 év elteltével annak jegyzőkönyv felvétele mellett történő felülvizsgálata.[186]

Az üzemeltetői biztonsági tervben meghatározott rendkívüli esemény bekövetkezésekor az érintett ágazati kijelölő hatóság, a beavatkozást végző szervek és a biztonsági összekötő személy együtt vesz részt a kiváltó okok azonosításában és a megtett intézkedések értékelésében[187].

[180] Pénzügy vhr. 8. §.
[181] Honvédelmi vhr. 6. §.
[182] Infokom. vhr. 15. §.
[183] Lrtv. 6. § (7) bekezdés.
[184] Lrtv. vhr. 7. § (1) bekezdés és 2. melléklet.
[185] Lrtv. 6. § (1), (2), (3), (6) bekezdései.
[186] Lrtv. vhr. 7. § (2), (2a), (3) és (4) bekezdés.
[187] Lrtv. vhr. 11 § (6) bekezdés.

Ha az üzemeltetői biztonsági tervet módosítani szükséges, akkor annak módosítással érintett részét, vagy jelentős tartalmi módosítás esetén a módosításokkal egységes szerkezetbe foglalt üzemeltetői biztonsági tervet, az üzemeltetőnek haladéktalanul meg kell küldenie tartalmi és formai ellenőrzésre a kijelölő hatóságnak. Az ellenőrzés határideje a módosított üzemeltetői biztonsági terv kijelölő hatósághoz érkezésének napjától számított 30 nap. Ha a felülvizsgálat eredményeként nem szükséges az üzemeltetői biztonsági tervet módosítani, a felülvizsgálatról szóló jegyzőkönyvet az üzemeltető a felülvizsgálatot követően haladéktalanul másolatban megküldi a BM OKF-nek mint nyilvántartó hatóságnak és a kijelölő hatóságnak[188].

Ha az üzemeltető a kijelölés alkalmával rendelkezik olyan biztonsági dokumentummal, amely az üzemeltetői biztonsági terv tartalmi elemeit magában foglalja, akkor kérelmére az ágazati kijelölő hatóság rendelkezhet úgy, hogy a biztonsági dokumentum az üzemeltetői biztonsági tervet helyettesíti. Az üzemeltető kötelezettsége, hogy a létfontosságú rendszerelem működésének védelmét és folyamatosságát az üzemeltetői biztonsági tervvel összhangban szervezze meg és biztosítja az üzemeltetésében lévő létfontosságú rendszerelem működésének védelmét és folyamatosságát.[189]

Az üzemeltetőnek az üzemeltetői biztonsági tervet – ideértve a fenitek alapján módosított tervet is – papíralapon és elektronikus adathordozón is meg kell küldenie az ágazati kijelölő hatóságnak, aki a nyilvántartásba vételt megelőzően azt a döntésében foglaltak alapján formailag és tartalmilag ellenőrzi, hiányosság esetén az üzemeltetőt hiánypótlásra szólítja fel. Az ellenőrzött és megfelelő üzemeltetői biztonsági tervet az ágazati kijelölő hatóság a BM OKF-nek mint nyilvántartó hatóságnak és az üzemeltetőnek küldi meg.[190]

Az üzemeltetői biztonsági terv és mellékletei, vagy az azokat helyettesítő biztonsági dokumentum, nem nyilvánosak.

Az üzemeltető feladatkörébe tartozik továbbá[191]:

a) a biztonsági esemény bekövetkezését követően a Központ haladéktalan tájékoztatása,
b) soron kívül módosítja az üzemeltetői biztonsági tervet, ha olyan változás áll be, amely érinti a létfontosságú rendszerelem szolgáltatásának nyújtását, tevékenységét, működésének feltételeit vagy védelmét,
c) a nyilvántartott adatokban bekövetkezett változásokról a BM OKF 72 órán belül történő tájékoztatása,
d) katasztrófaveszély vagy katasztrófa esetén az ágazati kijelölő hatóság és a BM OKF haladéktalan értesítése, honvédelmi létfontosságú rendszerelem esetén a fentieken felül a Magyar Honvédség Központi Ügyeletét értesítése.

Az Lrtv. előírásai szerint az üzemeltetőt terhelik az alábbi költségek[192]:

a) üzemeltetői biztonsági terv elkészítésének, módosításának és gyakoroltatásának, a biztonsági összekötő személy foglalkoztatásának költségei,
b) az üzemeltetői biztonsági tervben foglalt, a létfontosságú rendszerelemek védelmét szolgáló szervezeti és eszközrendszerrel kapcsolatban felmerült költségek.

[188] Lrtv. vhr. 7. § (5)–(6) bekezdései.
[189] Lrtv. 6. § (3)–(4) bekezdések és Lrtv. vhr. 7. § (7) bekezdés.
[190] Lrtv. 6. § (1) és (6) bekezdései.
[191] Lrtv. 6. § Lrtv. vhr. 10 § (2) bekezdés és 11. § (5) bekezdés.
[192] Lrtv. 7. §.

4.11. Ágazati szabályok

Az Lrtv. felhatalmazása alapján az Lrtv. vhr. mellett több további Korm. rendelet is tartalmaz kiegészítő szabályokat az egyes ágazati szabályokra, specialitásokra vonatkozóan. Ezen rendelkezések fő szabályozási környezethez kapcsolódó elemei (pl. javaslattevő és ágazati kijelölő hatóságok, ágazati kritériumok, biztonsági összekötő képesítési követelményei) fentiekben már rögzítésre kerültek. A további részletszabályok tételes ismertetésére jelen jegyzet nem tér ki, néhány kiegészítő szabályt azok speciális jellegére vonatkozóan azonban kiemelni szükséges.

További ágazati végrehajtási szabályok:

a) Közbiztonság és védelem ágazata: Rendvédelmi vhr.,
b) Agrárgazdasági ágazat: Agrár vhr.,
c) Vízágazat: Víz vhr.,
d) Egészségügyi ágazat: Eü. vhr.,
e) Pénzügyi ágazat: Pénzügy vhr.,
f) Honvédelem ágazata: Honvédelmi vhr.,
g) Infokommunikációs technológiák ágazata: Infokom. vhr.,
h) Energiaágazat: Energia vhr.,
i) Közlekedési ágazat: Közlekedési vhr.

A társadalombiztosítási ágazatban még nincs kihirdetett végrehajtási rendelet.

4.12. Uniós kötelezettségek

Az Lrtv. előírja[193] Magyarország Kormánya részére, hogy évente jelentést nyújtson be az Európai Bizottságnak:

a) az európai létfontosságú rendszerelemnek kijelölt létfontosságú rendszerelemek ágazatonkénti számáról,
b) az Unió azon tagállamainak számáról, amelyek az európai létfontosságú rendszerelemektől függenek,
c) azon ágazatok sebezhetőségi pontjainak, az azokat fenyegető veszélyeknek és kockázatoknak típusairól, amelyekben európai létfontosságú rendszerelemet jelöltek ki.

Az Lrtv. emellett rögzíti a BM OKF kötelezettségeként, hogy kétévente a Kormány által az Európai Bizottságnak történő jelentést megelőzően felülvizsgálja és szükség szerint pontosítja az alapvető szolgáltatásokat nyújtó szereplők jegyzékét.[194]

[193] Lrtv. 13. §.
[194] Lrtv. 2/A. § (6) bekezdés.

5. Mellékletek

1. melléklet

AZ ÜZEMELTETŐI BIZTONSÁGI TERV FELÉPÍTÉSE
(az Lrtv. vhr. 2. mellékletével azonos tartalom)

1. Általános bemutatás

1.1. rendszerelem megnevezése
- 1.1.1. üzemeltetető neve
- 1.1.2. üzemeltetető székhelye
- 1.1.3. üzemeltetető lakcíme
- 1.1.4. üzemeltetető levelezési címe
- 1.1.5. üzemeltetető cégjegyzékszáma vagy az egyéni vállalkozói nyilvántartási száma
- 1.1.6. üzemeltetető adóazonosító száma
- 1.1.7. üzemeltetető képviselőjének neve
- 1.1.8. üzemeltetető telefon- és telefaxszáma
- 1.1.9. üzemeltetető e-mail-címe
- 1.1.10. pontos cím hiányában a kijelölt rendszerelem elhelyezkedésére vonatkozó más azonosító adat és földrajzi koordináta

1.2. biztonsági összekötő
- 1.2.1. biztonsági összekötő személy neve
- 1.2.2. biztonsági összekötő személy természetes személyazonosító adatait (családi és utóneve, születési családi és utóneve, születési helye, születési ideje, anyja születési családi és utóneve)
- 1.2.3. biztonsági összekötő személy telefon- és telefaxszáma
- 1.2.4. biztonsági összekötő személy e-mail-címe

1.3. szervezet általános bemutatása
- 1.3.1. szervezet tevékenysége
- 1.3.2. szervezet irányítási rendszere
- 1.3.3. kijelölt rendszerelem védelmével kapcsolatos fő célkitűzései
- 1.3.4. a horizontális és ágazati kritériumok teljesülésének, indokoltságának vizsgálata a rendszerelem tekintetében

1.4. szervezeti struktúra és üzemvezetés
- 1.4.1. szervezet felépítése, szervezeti ábra
- 1.4.2. szervezet vezetése, vezető tisztségviselők, felelősségi köreik

1.5. szervezet személyzet (saját munkavállalók, külső, szerződéses munkavállalók)
- 1.5.1. szervezet létszáma, dolgozók státusza szerinti bontásban
- 1.5.2. külső (harmadik féltől igénybe vett, kölcsönzött, bedolgozó, szerződéses vagy vállalkozó) dolgozók létszáma, státuszuk szerinti bontásban, a működés szempontjából kritikus folyamatok tekintetében

1.6. kijelölt rendszerelem tevékenységének, illetve működésének általános bemutatása, az elvárt, normális működés paraméterei
- 1.6.1. rendszerelem tevékenységének áttekintő bemutatása
- 1.6.2. rendszerelem normál működésének paraméterei (így különösen a termelésszám, a kapacitás, a lekötött tatalék, illetve az ellátott körzet)
- 1.6.3. beszállítói kör, illetve beszállítói lánc megjelölése, általános bemutatása, a működés szempontjából kritikus folyamatok tekintetében
- 1.6.4. ha a beszállítói lánc bármely eleme a kijelölt létfontosságú rendszerelem üzemszerű működését veszélyezteti
  - 1.6.4.1. beszállító cégadatai
  - 1.6.4.2. beszállító képviselőjének elérhetősége
  - 1.6.4.3. beszállítóval kötött megállapodás rendszerelem üzemfolytonos működését biztosító garanciái
  - 1.6.4.4. beszállítói audit szabályozottsága, annak megléte, eredménye, időszakossága, szankciói
- 1.6.5. azon ágazatok és alágazatok függőségeinek bemutatása, amelyben érintett rendszerelemek, szolgáltatások hatással lehetnek a működésre
- 1.6.6. rendszerelem meglévő és teljesített szabvány-megfelelőségei, ágazati követelményei
- 1.6.7. a rendszerelem működése szempontjából kritikus műveletek, technológiák, feltételek, szolgáltatások, folyamatok meghatározása

1.7. kijelölt rendszerelem elemeinek azonosítása és értékelése a teljesült ágazati és horizontális kritériumok alapján
- 1.7.1. ágazati kritériumok megjelölése
- 1.7.2. horizontális kritériumok megjelölése

1.8. belső audit és vezetőségi átvizsgálás
- 1.8.1. belső auditrendszer bemutatása (így különösen az auditorok személye, képzettsége, belső képzése)
- 1.8.2. belső auditok időszakossága, eredményei, dokumentáltsága
- 1.8.3. vezetői átvizsgálás rendszerének bemutatása
- 1.8.4. vezetői átvizsgálás időszakossága, eredményei, dokumentáltsága

1.9. a változtatások kezelése és annak követése.
- 1.9.1. a belső auditok és vezetői átvizsgálások eredménye következtében megvalósult változtatások és azok követése („change management”)

2. A kijelölt rendszerelem környezetének bemutatása

2.1. a kijelölt rendszerelemet környező területek jellemzése
- 2.1.1. a kijelölt rendszerelem természetbeni helye
  - 2.1.1.1. település
  - 2.1.1.2. utca
  - 2.1.1.3. házszám
  - 2.1.1.4. emelet, ajtó
- 2.1.2. a kijelölt rendszerelem helyrajzi száma
- 2.1.3. a kijelölt rendszerelem földrajzi fekvése (koordinátái)
- 2.1.4. a kijelölt rendszerelem és környezetének felülnézeti (műholdas) képe
- 2.1.5. a kijelölt rendszerelem környezetének légtere és sajátosságai

2.1.6. a kijelölt rendszerelem környezetében található, a működésére befolyással bíró veszélyes üzemek, gyárak, erőművek megnevezése, címe, tevékenységi köre
2.1.6.1. tevékenységére gyakorolt esetleges hatása
2.1.7. a természeti környezetre vonatkozó legfontosabb információk
2.1.7.1. a területre jellemző, a kijelölt rendszerelem sérülését eredményező és a következmények alakulására hatást gyakorló meteorológiai jellemzők
2.1.7.2. a helyszínt jellemző, a kijelölt rendszerelem biztonságos tevékenységére, üzemeltetésére, működésére hatást gyakorló legfontosabb geológiai és hidrológiai jellemzők
2.1.7.3. egyéb, a működésre befolyással bíró külső tényezők bemutatása

3. A kijelölt rendszerelem bemutatása

3.1. a kijelölt rendszerelem valamennyi elemének részletes bemutatása (így különösen a normál működési rend során a kijelölt rendszerelem működését garantáló eszközök, berendezések, technológiai és karbantartási folyamatok, műveletek menete, naplózása)
3.1.1. a rendeltetésszerű működés folyamatának bemutatása a működést biztosító berendezésekkel együtt
3.1.1.1. a rendeltetésszerű működés biztosításához szükséges erőforrások és kapacitásaik bemutatása
3.1.1.2. a rendeltetésszerű működés tartalék eszközeinek és szolgáltatásainak bemutatása
3.1.1.3. a tartalék eszközök és szolgáltatások normál működésbe történő beillesztésének időszükséglete
3.1.1.4. a tartalék berendezésről és szolgáltatásról, normál működésre való visszatérés folyamata, szabályai, időszükséglete
3.1.1.5. a tartalék berendezések és szolgáltatások időszakos tesztelése
3.1.1.6. a minimális működés folyamatának bemutatása a működést biztosító berendezésekkel együtt
3.1.1.7. a minimális működés biztosításához szükséges erőforrások és kapacitásaik bemutatása
3.1.2. valamennyi elemének méretarányos helyszínrajza, valamint hozzátartozó magyarázat, útmutató
3.1.3. a kijelölt rendszerelem működését releváns módon befolyásoló informatikai rendszerek, eszközök, hálózatok ismertetése
3.1.4. az informatikai rendszerek, eszközök, hálózatok kijelölt rendszerelem működésben betöltött szerepük leírása

3.2. a telephelyet kiszolgáló infrastruktúra
3.2.1. elektromos áramellátás biztosítása
3.2.1.1. elektromos áramellátás szolgáltatója
3.2.1.2. elektromos áramellátás területi ellátottsága
3.2.1.3. szolgáltató által végzett műszaki karbantartások és javítások bemutatása (így különösen a kapcsolattartás módja, rendje, időszakossága)
3.2.1.4. elektromos áramellátás becsatlakozási pontjainak bemutatása
3.2.1.5. belső elektromos áramellátás bemutatása
3.2.1.6. tartalék és alternatív elektromos rendszerbiztosítása
3.2.1.6.1. tartalék elektromos rendszer bemutatása
3.2.1.6.2. tartalék elektromos rendszer kapacitása
3.2.1.6.3. tartalék elektromos rendszer ellátási területe

3.2.1.6.4. tartalék elektromos rendszer műszaki karbantartásainak és javításainak bemutatása
3.2.1.6.5. alternatív elektromos rendszere bemutatása
3.2.1.6.6. alternatív elektromos rendszer kapacitása
3.2.1.6.7. alternatív elektromos rendszer ellátási területe
3.2.1.6.8. alternatív elektromos rendszer műszaki karbantartásainak és javításainak bemutatása
3.2.2. vezetékes gázellátás biztosítása
3.2.2.1. vezetékes gázellátás szolgáltatója
3.2.2.2. vezetékes gázellátás területi ellátottsága
3.2.2.3. szolgáltató által végzett műszaki karbantartások és javítások bemutatása
3.2.2.4. vezetékes gázellátás becsatlakozási pontjainak bemutatása
3.2.2.5. belső vezetékes gázellátás bemutatása
3.2.2.6. tartalék és alternatív gáz rendszer biztosítása
3.2.2.6.1. tartalék gáz rendszer bemutatása
3.2.2.6.2. tartalék gáz rendszer kapacitása
3.2.2.6.3. tartalék gáz rendszer ellátási területe
3.2.2.6.4. tartalék gáz rendszer műszaki karbantartásainak és javításainak bemutatása
3.2.2.6.5. alternatív gáz rendszere bemutatása
3.2.2.6.6. alternatív gáz rendszer kapacitása
3.2.2.6.7. alternatív gáz rendszer ellátási területe
3.2.2.6.8. alternatív gáz rendszer műszaki karbantartásainak és javításainak bemutatása
3.2.3. közüzemi ivóvízellátás biztosítása
3.2.3.1. közüzemi ivóvízellátás szolgáltatója
3.2.3.2. közüzemi ivóvízellátás területi ellátottsága
3.2.3.3. szolgáltató által végzett műszaki karbantartások és javítások bemutatása
3.2.3.4. közüzemi ivóvízellátás becsatlakozási pontjainak bemutatása
3.2.3.5. belső közüzemi ivóvízellátás bemutatása
3.2.3.6. tartalék és alternatív ivóvíz rendszer biztosítása
3.2.3.6.1. tartalék ivóvíz rendszer bemutatása
3.2.3.6.2. tartalék ivóvíz rendszer kapacitása
3.2.3.6.3. tartalék ivóvíz rendszer ellátási területe
3.2.3.6.4. tartalék ivóvíz rendszer műszaki karbantartásainak és javításainak bemutatása
3.2.3.6.5. alternatív ivóvíz rendszere bemutatása
3.2.3.6.6. alternatív ivóvíz rendszer kapacitása
3.2.3.6.7. alternatív ivóvíz rendszer ellátási területe
3.2.3.6.8. alternatív ivóvíz rendszer műszaki karbantartásainak és javításainak bemutatása
3.2.4. ivóvíz tisztítási eljárás (saját vízforrás esetén)
3.2.4.1. eljárás bemutatása
3.2.4.2. kapacitási adatai és karbantartása
3.2.5. közüzemi szennyvízelvezetés biztosítása
3.2.5.1. közüzemi szennyvízelvezetés szolgáltatója
3.2.5.2. közüzemi szennyvízelvezetés területi ellátottsága
3.2.5.3. szolgáltató által végzett műszaki karbantartások és javítások bemutatása
3.2.5.4. közüzemi szennyvízelvezetés becsatlakozási pontjainak bemutatása
3.2.5.5. belső közüzemi szennyvízellátás bemutatása

3.2.6. infokommunikációs hálózati ellátás
- 3.2.6.1. infokommunikációs szolgáltatás felsorolása
- 3.2.6.2. infokommunikációs szolgáltatás szolgáltató
- 3.2.6.3. szolgáltató által végzett műszaki karbantartások és javítások bemutatása
- 3.2.6.4. belső infokommunikációs rendszer bemutatása
- 3.2.6.5. belső infokommunikációs hálózat bemutatása
- 3.2.6.6. a létfontosságú rendszerelem működtetéséhez szükséges infokommunikációs rendszerek/alkalmazások bemutatása
- 3.2.6.7. a létfontosságú rendszerelem működtetéséhez szükséges, harmadik féltől igénybe vett infokommunikációs rendszerek, alkalmazások bemutatása
- 3.2.6.8. a létfontosságú rendszerelem infokommunikációs rendszerektől, alkalmazásoktól való függőségének, hatásainak bemutatása
- 3.2.6.9. a létfontosságú rendszerelem infokommunikációs rendszereinek, alkalmazásainak, hálózatainak függősége a kiszolgáló elektromos áramellátási rendszerektől
- 3.2.6.10. az infokommunikációs rendszerek üzemeltető által meghatározott szolgáltatási szintjeinek bemutatása (így különösen normál, csökkentett, minimális működés)
- 3.2.6.11. tartalék és alternatív infokommunikációs rendszer biztosítása
  - 3.2.6.11.1. tartalék infokommunikációs rendszer bemutatása
  - 3.2.6.11.2. tartalék infokommunikációs rendszer kapacitása
  - 3.2.6.11.3. tartalék infokommunikációs rendszer ellátási területe
  - 3.2.6.11.4. tartalék infokommunikációs rendszer műszaki karbantartásainak és javításainak bemutatása
  - 3.2.6.11.5. alternatív infokommunikációs rendszere bemutatása
  - 3.2.6.11.6. alternatív infokommunikációs rendszer kapacitása
  - 3.2.6.11.7. alternatív infokommunikációs rendszer ellátási területe
  - 3.2.6.11.8. alternatív infokommunikációs rendszer műszaki karbantartásainak és javításainak bemutatása

3.2.7. távhő ellátás
- 3.2.7.1. távhő szolgáltatás felsorolása
- 3.2.7.2. távhő szolgáltatás szolgáltató
- 3.2.7.3. szolgáltatás lefedettségi területe
- 3.2.7.4. szolgáltató által végzett műszaki karbantartások és javítások bemutatása
- 3.2.7.5. a távhő telephelyen történő feldolgozásának bemutatása
- 3.2.7.6. a távhő kiesése esetén igénybe vett alternatív, vagy tartalék rendszerek bemutatása
- 3.2.7.7. azon távhőrendszer-szolgáltatók felsorolása, amely a kijelölt létfontosságú rendszerelem üzemfolytonos működését biztosítja

3.2.8. egyéb
- 3.2.8.1. minden egyéb a rendszerelem működéséhez nélkülözhetetlen, üzletmenet folytonosságát befolyásoló szolgáltatás bemutatása az alábbi pontok részletezésével
- 3.2.8.2. igénybe vett szolgáltatási rendszer bemutatása
- 3.2.8.3. igénybe vett szolgáltatók bemutatása
- 3.2.8.4. alternatív szolgáltató, az azonos szolgáltatás biztosítása céljából
- 3.2.8.5. szolgáltatás kapacitás adatainak bemutatása
- 3.2.8.6. a rendeltetésszerű működéshez szükséges minimum szolgáltatási szint bemutatása
- 3.2.8.7. a szolgáltatás kiesésének működésre gyakorolt hatásának bemutatása

3.2.8.8. tartalék és alternatív igénybe vett szolgáltatási rendszer biztosítása
3.2.8.8.1. tartalék igénybe vett szolgáltatási rendszer bemutatása
3.2.8.8.2. tartalék igénybe vett szolgáltatási rendszer kapacitása
3.2.8.8.3. tartalék igénybe vett szolgáltatási rendszer ellátási területe
3.2.8.8.4. tartalék igénybe vett szolgáltatási rendszer műszaki karbantartásainak és javításainak bemutatása
3.2.8.8.5. alternatív igénybe vett szolgáltatási rendszere bemutatása
3.2.8.8.6. alternatív igénybe vett szolgáltatási rendszer kapacitása
3.2.8.8.7. alternatív igénybe vett szolgáltatási rendszer ellátási területe
3.2.8.8.8. alternatív igénybe vett szolgáltatási rendszer műszaki karbantartásainak és javításainak bemutatása

3.3. a kijelölt rendszerelem felépítésének, elemeinek, részletes tevékenységének, termelési, működési folyamatainak bemutatása, a tevékenységekre vonatkozó legfontosabb technológiai és karbantartási folyamatok, műveletek
3.3.1. a létfontosságú rendszerelem tevékenységének bemutatása, kapacitás adatokkal együtt
3.3.2. a tevékenységekre vonatkozó legfontosabb technológiai, műveleti, munka folyamatok bemutatása
3.3.2.1. a tevékenység célja
3.3.2.2. a rendeltetésszerű működéshez szükséges erőforrás
3.3.2.2.1. humán
3.3.2.2.2. technikai, technológiai
3.3.2.2.3. anyagi
3.3.2.2.4. harmadik féltől igénybe vett szolgáltatás
3.3.2.2.5. a kiszolgáló infrastruktúra és a technológiai, műveleti, munkafolyamatok kapcsolódási pontjainak részletes bemutatása
3.3.2.3. a rendeltetésszerű működéshez szükséges minimum erőforrás
3.3.2.3.1. humán
3.3.2.3.2. technikai, technológiai
3.3.2.3.3. anyagi
3.3.2.3.4. harmadik féltől igénybe vett szolgáltatás
3.3.2.3.5. a kiszolgáló infrastruktúra és a technológiai, műveleti, munkafolyamatok kapcsolódási pontjainak részletes bemutatása
3.3.3. a tevékenységekre vonatkozó legfontosabb karbantartási folyamatok bemutatása

3.4. a lehetséges veszélyt jelentő anyagok, berendezések megjelölése, mennyisége, tárolási adatai
3.4.1. a rendeltetésszerű működésre veszélyt jelentő anyagok bemutatása
3.4.2. a rendeltetésszerű működésre veszélyt jelentő anyagok kezelése, szállítása, tárolása
3.4.3. a rendeltetésszerű működésre veszélyt jelentő anyagok megsemmisítése, elszállítása
3.4.4. a rendeltetésszerű működésre veszélyt jelentő berendezések bemutatása
3.4.5. a rendeltetésszerű működésre veszélyt jelentő berendezések kezelése, szállítása, tárolása, karbantartása
3.4.6. a rendeltetésszerű működésre veszélyt jelentő berendezések megsemmisítése, elszállítása

3.5. belső és külső tájékoztatási rendszerek
3.5.1. a szervezet kommunikációs stratégiájának bemutatása
3.5.2. a szervezet kommunikációs eljárásrendjei
3.5.3. a szervezet válságkommunikációs stratégiájának bemutatása
3.5.4. a szervezet válságkommunikációs eljárásrendjei

3.5.5. belső tájékoztatási rendszerek, eszközök, szolgáltatások bemutatása
3.5.6. külső (harmadik féltől igénybe vett) tájékoztatási rendszerek, eszközök, szolgáltatások bemutatása

3.6. felügyeleti és biztonsági szervezetek, eszközrendszerük, működésük
3.6.1. biztonsági szolgálat bemutatása [ha kiszervezett, a harmadik féltől igénybe vett biztonsági szolgálat (ok) bemutatása]
3.6.2. elsősegélynyújtó és mentőszervezetek bemutatása (ha kiszervezett, a harmadik féltől igénybe vett biztonsági szolgálat bemutatása)
3.6.3. munkavédelmi szervezet bemutatása (ha kiszervezett, a harmadik féltől igénybe vett szolgáltatás bemutatása)
3.6.4. tűzvédelmi szervezet bemutatása (ha kiszervezett, a harmadik féltől igénybe vett szolgáltatás bemutatása)
3.6.5. környezetvédelmi szervezet bemutatása (ha kiszervezett, a harmadik féltől igénybe vett szolgáltatás bemutatása)
3.6.6. műszaki biztonsági szolgálat bemutatása (ha kiszervezett, a harmadik féltől igénybe vett szolgáltatás bemutatása)
3.6.7. katasztrófa elhárítási szervezet bemutatása (ha kiszervezett, a harmadik féltől igénybe vett szolgáltatás bemutatása)
3.6.8. távfelügyeleti és monitoring hálózat bemutatása (ha kiszervezett, a harmadik féltől igénybe vett szolgáltatás bemutatása), minimum elvárás a rendszerben lévő jelző és érzékelő eszközök tervrajzon való feltüntetése és a dokumentumhoz történő csatolása
3.6.9. laboratóriumi kapacitás bemutatása (ha kiszervezett, a harmadik féltől igénybe vett szolgáltatás bemutatása)
3.6.10. beléptető és behatolás jelző rendszer bemutatása, minimum elvárás a rendszer által védett helyszínek tervrajzon való feltüntetése és a dokumentumhoz történő csatolása
3.6.11. zárt láncú kamerás megfigyelő rendszer bemutatása, minimum elvárt a kamerák és diszpécserközpontok elhelyezési rajza, a kamerák által lefedett területek jelölésével
3.6.12. tűzjelző rendszer bemutatása, minimum elvárás a rendszer által védett helyszínek, eszközök és diszpécser központok tervrajzon való feltüntetése és a dokumentumhoz történő csatolása
3.6.13. tűzoltó rendszer bemutatása, minimum elvárás a rendszer által védett helyszínek, eszközök tervrajzon való feltüntetése és a dokumentumhoz történő csatolása
3.6.14. egyéb a rendszerelem biztonságát szavatoló eszköz, rendszer, szolgáltatás bemutatása (ha releváns, tervrajzon való feltüntetése és a dokumentumhoz történő csatolása)

4. Kockázatok azonosítása, értékelése, kezelése (az üzemeltető azonosítja, értékeli és kezeli a kijelölt rendszerelemmel összefüggő kockázatokat)

4.1. az üzemeltető által fenntartott kockázat menedzsment rendszer bemutatás
4.1.1. felelősségi körök bemutatása
4.1.2. kockázat kezelési módszertan bemutatása

4.2. kockázatok tételes azonosítása, értékelése különösen az alábbi elemek használatával:
4.2.1. meteorológia kockázatok
4.2.1.1. viharos szél
4.2.1.2. villámcsapás
4.2.1.3. rendkívüli hőmérsékleti körülmények (extrém magas/alacsony)
4.2.1.4. rendkívüli csapadék

4.2.2. geológiai kockázatok
- 4.2.2.1. földrengés
- 4.2.2.2. árvíz
- 4.2.2.3. belvíz

4.2.3. humán kockázatok
- 4.2.3.1. külső támadás
- 4.2.3.2. belső munkavállaló által elkövetett szándékos károkozás
- 4.2.3.3. belső munkavállaló által elkövetett gondatlan károkozás
- 4.2.3.4. szakképzettség hiánya
- 4.2.3.5. kritikus létszámhiány
- 4.2.3.6. külső munkavállaló által elkövetett szándékos károkozás
- 4.2.3.7. külső munkavállaló által elkövetett gondatlan károkozás
- 4.2.3.8. humán eredetű járványhelyzet
- 4.2.3.9. állati eredetű járványhelyzet

4.2.4. technikai kockázatok
- 4.2.4.1. villamosenergia-szolgáltatás kiesése
- 4.2.4.2. épületgépészeti meghibásodás
- 4.2.4.3. diszpécserközpont meghibásodása
- 4.2.4.4. vízszolgáltatás kiesése
- 4.2.4.5. távhőszolgáltatás kiesése
- 4.2.4.6. gázszolgáltatás kiesése
- 4.2.4.7. csőtörés létesítményen, épületen belül
- 4.2.4.8. csőtörés technológiai téren belül
- 4.2.4.9. redundáns áramellátás kiesése
- 4.2.4.10. klimatizálás kiesése

4.2.5. kommunikációs kockázatok
- 4.2.5.1. híradó technika meghibásodása
- 4.2.5.2. redundanciát nyújtó technika meghibásodása
- 4.2.5.3. kommunikációs csatornák meghibásodása
- 4.2.5.4. EDR meghibásodása
- 4.2.5.5. IP telefon meghibásodása
- 4.2.5.6. analóg telefon meghibásodása
- 4.2.5.7. internetszolgáltatás kiesése

4.2.6. tűzeset
- 4.2.6.1. létesítményben tűz
- 4.2.6.2. technológiai térben tűz
- 4.2.6.3. szerverhelyiségben tűz

4.2.7. informatikai kockázatok
- 4.2.7.1. szerver meghibásodása
- 4.2.7.2. használt szoftver meghibásodása
- 4.2.7.3. adatkapcsolat meghibásodása
- 4.2.7.4. munkaállomások meghibásodása
- 4.2.7.5. szünetmentes tápegység meghibásodása
- 4.2.7.6. hálózati meghibásodás
- 4.2.7.7. használt informatikai rendszer, alkalmazás meghibásodása (rendszerenként)
- 4.2.7.8. kibertámadás, kibertérből érkező támadás

4.2.8. veszélyes anyagokkal és technológiákkal kapcsolatos kockázatok
- 4.2.8.1. radiológiai veszély
- 4.2.8.2. veszélyes anyagokkal kapcsolatos veszély (tűz, túlnyomás, mérgezés)
- 4.2.8.3. biológiai veszély

4.2.9. egyéb, az adott ágazat szempontjából specifikus kockázatok

4.3. a kijelölt rendszerelem kölcsönösen függő (interdependens) kapcsolódásai és az azokból adódó kockázatok felmérése (azaz a kijelölt rendszerelem kiesése milyen más ágazatokra, szervezetekre, személyekre van hatással), és azokkal a kockázati lista kiegészítése

4.4. a kockázatok valószínűsíthető okainak feltárása, a bekövetkezéskor prognosztizálható negatív hatások meghatározása, keletkezett kárérték meghatározása

4.5. a felmerült kockázatok értékelése táblázat készítése a bekövetkezési valószínűség, a veszélyeztető hatások szintje és harmadik fél felé fennálló kitettség alapján
- 4.5.1. a bekövetkezési valószínűség lehet: nagyon ritka, ritka, alkalmankénti, gyakori, nagyon gyakori (1-5 skálán)
- 4.5.2. a veszélyeztető hatások szintje lehet: elhanyagolható, alacsony, közepes, magas, katasztrofális (1-5 skálán)
- 4.5.3. a harmadik fél felől fennálló kitettség lehet: harmadik féltől igénybe vett, vagy üzemeltető által saját hatáskörben nyújtott vagy nem értelmezhető (1-2 skálán) – ahol a „2” érték súlyozottan veendő figyelembe

4.6. Kockázatkezelés
- 4.6.1. a kockázatok értékelésére készített táblázat kiegészítése a kockázat kezelésére, elfogadására, áthárítására tett intézkedésekkel
- 4.6.2. a rendkívüli események meghatározása (minimum tartalmi követelmény: az esemény megnevezése, mértéke, bejelentési rend, alkalmazandó eljárásrend)

5. A kijelölt rendszerelem védelmének eszközrendszere rendkívüli esemény bekövetkezése esetén

5.1. a rendszerelem védelmét biztosító általános intézkedés bemutatása

5.2. a rendszerelem védelmét biztosító speciális intézkedés bemutatása a 4.2-4.5. szerint azonosított kockázatonként

5.3. a rendszerelem védelmét biztosító, a rendkívüli esemény során alkalmazandó eljárásrend bemutatása

5.4. rendkívüli esemény kezelésében résztvevő szervezeti egységek felsorolása

5.5. kijelölt rendszerelem védelmére rendszeresített felszerelések és a vezetéshez, a döntés-előkészítéshez szükséges folyamatok és infrastruktúrák bemutatása
- 5.5.1. a vezetői állomány rendkívüli esemény esetén történő értesítésének eszközrendszere
- 5.5.2. a vezetői állomány rendkívüli esemény esetén történő értesítésének eljárásrendje
- 5.5.3. a dolgozók rendkívüli eseménykori riasztásának eszközrendszere
- 5.5.4. a dolgozók rendkívüli eseménykori riasztásának eljárásrendje
- 5.5.5. a rendkívüli esemény következményeinek csökkentését végző saját eszközeinek és erőforrásainak alkalmazása
- 5.5.6. vezetői irányítás folyamata
- 5.5.7. döntési kompetenciák, felelősségek
- 5.5.8. üzemfolytonos működés minimum szintjéhez szükséges feltételek és intézkedések
- 5.5.9. üzemfolytonos működés normál szintjéhez szükséges feltételek és intézkedések
- 5.5.10. üzemfolytonos működés helyszíni, illetve távoli munkavégzéshez szükséges feltételek és intézkedések

6. Honvédelmi létfontosságú rendszerelem esetén a honvédelmi szervekkel történő kapcsolattartás és együttműködés rendje

6.1. Honvédelmi létfontosságú rendszerelem esetén a honvédelmi szervekkel történő kapcsolattartás rendje

6.2. Honvédelmi létfontosságú rendszerelem esetén a honvédelmi szervekkel történő együttműködés rendje

Formai követelmények

Az üzemeltetői biztonsági tervet a „Tartalmi követelmények" részben feltüntetettek szerinti tagolásban, írásban kell elkészíteni. A jóváhagyott üzemeltetői biztonsági tervet a kijelölő hatóság részére az üzemeltető és a biztonsági összekötő személy által aláírva, elektronikus úton kell benyújtani.

A térképeket elektronikus adathordozón is be lehet nyújtani. A térképvázlat vagy helyszínrajz tartalmazza a kijelölt rendszerelem egészét és olyan felbontású és formátumú legyen, amely a megfelelő eligazodást biztosítja.

6. Irodalomjegyzék

1. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.
URL: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu
Letöltés ideje: 2019. augusztus 22.

2. Az Unió helyzete 2018 Jean-Claude Juncker, az Európai Bizottság elnökének beszéde – 2018. szeptember 12.
URL: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-brochure_hu_0.pdf
Letöltés ideje: 2019. augusztus 22.

3. Erős kiberbiztonság kialakítása Európában
URL: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_hu.pdf
Letöltés ideje: 2019. augusztus 22.

II. MARSI TAMÁS: INCIDENSKEZELÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK ESETÉN

1. Bevezetés

Az informatika térhódításával a digitális információ szinte az élet minden területén megjelenik. Az internet használatával további lehetőségek nyílnak meg mindenki előtt, amelyre folyamatosan egyre több szolgáltatás épül. Ezeket a szolgáltatásokat pedig egyre többen és gyakrabban használjuk informálódásra, kapcsolattartásra, vásárlásra, ügyintézésre és még ezernyi másra. Az egyre növekvő méretű és egyre érzékenyebb információkat tartalmazó adatforgalom miatt azonban a kiberbűnözés is erősödik, ami mindig új kihívások elé állítja az internet biztonságáért küzdő szakembereket.

A mai változó és kiberfenyegetésekkel terhelt világunkban kiemelt figyelem hárul a kiberbiztonságra, és ebben a világban a kritikus szolgáltatások védelme elsődleges feladata a különböző szektoroknak és az államoknak is.

A hagyományos kritikus infrastruktúrák fokozatosan egyre inkább kapcsolódnak a modern, digitális technológiákhoz és hálózatokhoz. Gondoljunk csak Magyarországon a banki szektorban a netbankokra, melyek segítségével napi pénzügyeinket tudjuk kényelmesen és gyorsan intézni vagy esetleg az egészségügyben az Egységes Egészségügyi Szolgáltatási Térre (EESZT), ahol a korelőzményeink és a leleteink mellet ma már az orvosi vényeinkhez is hozzáférhetünk.

Ez a növekvő digitalizáció okosabbá teszi az infrastruktúrákat és lehetővé teszi a felhasználók számára, hogy jobban részesüljenek az innovatív szolgáltatások előnyeiből.

Ugyanakkor a digitalizálás jelentős kockázatokat hordoz, mivel a kibertámadások és a kiberbiztonsági események fokozott kitettsége potenciálisan veszélyeztetheti a szolgáltatások és az infrastruktúrák biztonságát és a személyes adatainkat is.

Manapság már országonként, sőt, európai uniós szinten is átfogó jogi keretet alakítottak ki a kiberbiztonságra vonatkozóan azonban a különböző szektorokban különböző típusú kihívásokkal szembesülnek a szakemberek. Egy azonban mindenképpen kimondható, az rendszerek és a felhasználók erősen függenek egymástól, így akár egyetlen rendszer kiesése is láncreakciót indíthat el, melynek nemzetgazdaságilag is súlyos következményei lehetnek.

Az első (jól dokumentált) villamosenergia rendszer elleni kibertámadás Ukrajnában zajlott, 2015 végén. A támadók három helyi energiaelosztó vállalat információs rendszerét támadták meg, melynek következtében Ukrajna egy részén, körülbelül 230 ezer ember maradt áram nélkül körülbelül 1-6 órán keresztül. A szofisztikált célzott támadás során célzott adathalász elektronikus leveket segítségével jutatták el a támadók a káros kódot, majd a rendszerbe jutva átvették a hatalmat több rendszer – például az ipari vezérlőrendszerek (SCADA), az informatikai infrastruktúra (energiaellátási és hálózati eszközök) – felett. [195]

Ebből is látszik, hogy nem csak a lehetőség, hanem a képesség és az igény is megjelent a kritikus infrastruktúrák elleni támadásokhoz, ezért erre kiemelt figyelmet kell fordítania a szektorok szereplőinek és az államoknak is az infrastruktúráik és végső sorok az állampolgáraik védelme érdekében. Az események észlelése és az incidensek hatékony menedzselése érdekében a szereplőknek új kihívásokkal kell szembesülniük, melyekre a válaszokat szervezetükön belül és a többi szereplővel való hatékony kooperációval tudják megfogalmazni.

[195] https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

A tananyag célja az elektronikus információbiztonsági vezetők részére egy áttekintés a kritikus infrastruktúra fogalmi hátteréről és az incidenskezelés jogszabályi hátteréről, az ezzel foglalkozó nemzetközi és hazai szervezetrendszer felépítéséről. A tananyag röviden kitér kritikus infrastruktúrákban feltárt incidens esettanulmányokra, valamint az incidenskezelés technikai kihívásaira is.

2. A kritikus infrastruktúra fogalma incidenskezelési szempontból

2.1. Általános megközelítés

A kritikus infrastruktúra fogalma országonként és szakterületenként eltér egymástól, ennek egzakt definíciója nehéz feladat.

Egy általános és egyszerű megfogalmazás szerint a kritikus infrastruktúrák társadalom és a gazdaság működéséhez nélkülözhetetlen eszközök Leggyakrabban az alábbi szektorok tartoznak ide:

- fűtés (földgáz, üzemanyag, távfűtés stb.),
- élelmiszer (élelmiszer-előállítás és -terjesztés),
- víz (ivóvíz, szennyvíz, felszín feletti vizek),
- egészségügy (kórházak és mentők),
- közlekedési rendszerek (üzemanyag-ellátás, vasúti hálózat, repülőterek, kikötők, belföldi hajózás),
- védelmi szolgáltatások (rendvédelem és haderő),
- energiatermelés, szállítás és elosztás (földgáz, kőolaj, szén és atomenergia),
- telekommunikáció (a sikeres üzemeltetéshez szükséges koordináció),
- ipari szektor (áruk és szolgáltatások, valamint pénzügyi szolgáltatások)[196].

A kilencvenes évek közepétől felismerték a nemzetállamok, hogy a kritikus infrastruktúráknak, társadalmi fontosságuk, kiemelt helyzetük miatt kiemelt védelemre van szükségük. Ez a kiemelt védelem, bár a fizikai és egyéb biztonságot követően, de a kiberbiztonságban is megjelent a 2010-es évek elején.

Könnyen belátható, hogy az infrastruktúráknak, fontosságuk okán szükségük van kiberbiztonságra és szükségük van mindenki által elfogadott incidenskezelési alapelvekre is.

A kiberbiztonsági védelmi mechanizmusokkal a rendszerek üzemeltetői elsősorban az incidensek megelőzésére törekszenek, ám sosem lehet olyan védelmet építeni, ami minden támadásnak ellenáll, különösen célzott támadásoknak, amiknek a kritikus infrastruktúrák fokozottan ki vannak téve. Ezért fel kell arra készülni, hogy lesznek sikeres támadások, és az ezekből származó incidenseket hatékonyan kell tudni kezelni mind a rendszerek üzemeltetőinek, mind az ezt segítő egyéb szervezeteknek (hatóság, CSIRT...). Ezért fontos kérdés és feladat az incidenskezelés, valamint annak alapelveinek és módszereinek a megértése és a gyakorlatban történő használata.

Ezek az alapelvek sztenderdek, és esetlegesen jogszabályok államonként vagy közösségenként eltérhetnek, azonban céljaikban hasonlítanak egymásra: megfelelni a kor kihívásának és hatékony választ megfogalmazni a kiberfenyegésekre.

2.2. Európai megközelítés

Az Európai Unióban 2016-tól hatályos hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv (NIS-irányelv), melynek

[196] https://en.wikipedia.org/wiki/Critical_infrastructure

egyik deklarált célja a hálózati és információs rendszerek biztonsági kihívásainak hatékony kezelése. Az irányelvben foglaltak alapján annak érdekében, hogy a szabályozás valamennyi lényeges biztonsági eseményre és kockázatra kiterjedjen, ezt az irányelvet mind az alapvető szolgáltatásokat nyújtó szereplőkre, mind a digitális szolgáltatókra is alkalmazni kell.[197]

Mint fent szerepel, az Európai Unió az alapvető szolgáltatások kifejezést használja. Alapvető szolgáltatásokat nyújtó szereplő az irányelv meghatározása alapján olyan szereplő, mely az alábbi kritériumoknak felel meg:

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

Az irányelv alapján tehát fontos kritérium az, hogy ha egy alapvető szolgáltatást nyújtó szereplőt biztonsági esemény ér, akkor annak szolgáltatásában fennakadás állna elő. Ez igen fontos és az incidens hatása felől közelítő kritérium.

Az irányelv megfogalmazása szerint a biztonsági esemény (avagy hálózatbiztonsági esemény) minden olyan esemény, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára, annak kezelése a biztonsági események észlelését, elemzését és elszigetelését, valamint a rájuk való reagálást támogató eljárások összessége.[198]

Ezenkívül az irányelv rögzíti a jelentős zavar fogalmát, a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) létrehozásának kötelezettségét, a CSIRT-ek nemzeti és Európai Unión belüli (CSIRT-ek hálózata) együttműködését, valamint az együttműködési csoport létrehozását is, melyeknek többek között célja szervezeti és szervezetközi keretek kialakításával az incidenskezelés hatékonyságának növelése.

Az irányelv ezeken kívül kitér a szereplők incidens-bejelentési kötelezettségére is, mely szerint az alapvető szolgáltatásokat nyújtó szereplők indokolatlan késedelem nélkül bejelentik az illetékes hatóságnak vagy a CSIRT-nek az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket.[199] Ezenkívül a szereplőknek egyéb információkat is a hatóság és a CSIRT rendelkezésére kell bocsátaniuk. [200]

A kommunikáció megkönnyítése és átláthatóságának biztosítása érdekében minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért felelős nemzeti egyedüli kapcsolattartó pontot (a továbbiakban: egyedüli kapcsolattartó pont vagy SPOC)[201] Az egyedüli kapcsolattartó pontnak kell ellátnia az összekötő feladatokat a tagállami hatóságok közötti és a többi tagállam érintett hatóságaival folytatott, határokon átnyúló együttműködés, valamint az együttműködési csoporttal és a CSIRT-ek hálózatával folytatott együttműködés biztosítása céljából.[202]

A NIS-irányelv hét különböző típusú szervezettípust határoz meg, melyekre épülő eseménykezelési struktúra kialakítását a tagállamokra bízza a jogalkotó:[203]

1. Energia
   a) Villamos energia
   b) Kőolaj

[197] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
[198] NIS-irányelv 4. cikk (7)–(8) bekezdés.
[199] NIS-irányelv 14. cikk (3) bekezdés.
[200] NIS-irányelv 14. cikk (5) bekezdés.
[201] NIS-irányelv 8. cikk (3) bekezdés.
[202] NIS-irányelv 8. cikk (4) bekezdés.
[203] NIS-irányelv II. melléklet.

   c) Földgáz
2. Közlekedés
   a) Légi közlekedés
   b) Vasúti közlekedés
   c) Vízi közlekedés
   d) Közúti közlekedés
3. Banki szolgáltatások
4. Pénzügyi piaci infrastruktúrák
5. Egészségügy, egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is)
6. Ivóvízellátás és -elosztás
7. Digitális infrastruktúra

2021. november 26-án az Európai Unió Tanácsa elfogadta az EU egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekkel kapcsolatos álláspontját amely intézkedések célja, hogy tovább javuljon mind az állami, mind a magánszektornak, illetve az Unió egészének kiberrezilienciája és a kiberbiztonsági eseményekre való reagálási képessége. Elfogadását követően az új, „NIS 2" elnevezésű irányelv a hálózati és információs rendszerek biztonságáról szóló jelenlegi irányelv (NIS-irányelv) helyébe lép.[204]

2.3. A magyar szabályozás

A magyar joganyagban a létfontosságú rendszerelem: a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény mellékleteiben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.[205]

A törvény az alábbi szektorokat azonosítja, melyek a törvény 1. mellékletében foglaltaknak alapján feleltethetőek meg a NIS-irányelvben foglaltaknak:

1. Energia
2. Közlekedés
3. Agrárgazdaság
4. Egészségügy
5. Társadalombiztosítás
6. Pénzügy
7. Infokommunikációs technológiák
8. Víz
9. Közbiztonság és védelem
10. Honvédelem

A magyar szabályozás ebben a tekintetben már összetettebb, mert nincs egy taxatív lista a kritikus infrastruktúra-szolgáltatókról. Ahhoz ugyanis, hogy valamely szereplő alapvető szolgáltatást nyújtó szolgáltató legyen, a kijelölő hatóságnak azonosítani és kijelölni szükséges az adott szereplőt. Ezt

[204] Bővebben ld.: https://www.consilium.europa.eu/hu/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/

[205] 2012. évi CLXVI. törvény 1. § j) pont.

Magyarországon jelenleg a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF) végzi erre a célra létrehozott kritériumrendszer mentén, hatósági eljárás keretében. Csak a BM OKF által kijelölt szereplőkre vonatkoznak a NIS-irányelvben megfogalmazott és fent röviden ismertetett kötelezettségek. A BM OKF a szereplőkről jegyzéket vezet.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) alapján az alapvető szolgáltatásokat nyújtó szolgáltató a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 2/A. §-a alapján kijelölt szolgáltató, tehát az a szolgáltató, akit a BM OKF azonosított és kijelölt, azaz szerepel a jegyzékben. Az Ibtv. végrehajtási rendelete 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 (az Ibtv. végrehajtási rendelete) ugyanígy fogalmaz.

3. Incidenskezelésben érintett hazai szervezet felépítése és feladatai

Az incidenskezelésben jelenleg kulcsfontosságú szerepet játszik a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete (NKI). Az NKI 2016-os létrehozása óta a Nemzetbiztonsági Szakszolgálat szervezeti egységeként működik, jelenleg a hatósági és egyéb feladatokat ellátó Hatósági Főosztály és a technikai tevékenységet ellátó öt, később bemutatásra kerülő, szolgáltatási terület szervezeti egységekkel.

A szakterületek többsége, bár más működési modellben, de korábban is létezett, működésüknek leírását a szerző már megtette jelen kötet korábbi kiadásaiban, így ezekről itt csak röviden és leginkább a változásokat hangsúlyozva lesz szó. Az NKI a változó világ igényei és jogszabályi kötelezettségei miatt több új tevékenységet is elkezdett végezni, ilyen az NKI eseményészlelési képesség, a sajtó- és tudatosító tevékenység fokozása és az egyedüli kapcsolattartó pont is. Ennek okán e szakterületek bemutatása a fentiekhez képest sokkal részletesebben fog megtörténni.

3.1. Esemény- és incidenskezelésben érintett szervek

Az Ibtv. végrehajtási rendelete az alapvető szolgáltatókkal kapcsolatosan illetékes eseménykezelő központnak a Nemzetbiztonsági Szakszolgálatot jelöli ki. Ez a gyakorlatban azt jelenti, hogy az incidenskezeléssel összefüggő feladatokat a Nemzeti Kibervédelmi Intézet látja el.[206] Ez a szabály 2019 év elejétől hatályos, korábban a feladatot a BM OKF látta el.

A tevékenysége során az eseménykezelő központ a feladatellátást a biztonsági események és fenyegetések kezelése céljából a Lrtv. szerinti üzemeltetőkkel, kijelölő és javaslattevő hatóságokkal szorosan együttműködve végzi.[207] Az esemény- és incidenskezelés technikai feladatát az NKI 2019-től öt szolgáltatási területe látja el.

3.2. Szolgáltatási területek

3.2.1. Nemzeti CSIRT

Az NKI rendeltetése az informatikai rendszerek informatikai biztonsági támogatása országosan, amely egyrészt megelőző jellegű, a szoftversérülékenységek és információbiztonsági fenyegetések

[206] 271/2018 Korm. rend 2. §.
[207] 271/2018 Korm. rend 3. § (2) bekezdés f) pont.

nyomon követésére és az IT-rendszereket üzemeltetők részére történő kommunikálására (sérülékenységmenedzsment), másrészt pedig reaktív jellegű, a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és a kezelésük koordinációjára irányul. Az NKI nem ellenőrzi az internetfelhasználást és nem tilt le semmilyen honlaphoz való hozzáférést, csupán figyelmeztet a veszélyes helyekre.

A sérülékenységmenedzsment során az NKI információkat gyűjt a szoftversérülékenységekről és káros szoftverekről, megvizsgálja azok ügyfélkörre vonatkozó relevanciáját és általános körben vagy célzottan tájékoztatja a fenyegetés kiváltotta biztonsági esemény megelőzése érdekében ezen rendszerek üzemeltetőit.

Az incidenskezelési tevékenység során folyamatosan fogadja az IT-rendszereket érő incidensek bejelentéseit, és megteszi az alapvető intézkedéseket (incidensek nyilvántartásba vétele, bejelentő visszatájékoztatása, alapvető információk azonosítása stb.). A bejelentett incidens felszámolása során a következő lépés a jogosultsággal és/vagy képességgel rendelkező szerv/személy tájékoztatása a teendőkről, szükség esetén kapcsolattartás a bejelentővel, valamint az érintett incidens felszámolásának nyomon követése, azaz az incidenskoordináció.

Amennyiben szükséges, az incidensre utaló jelek alapján összegyűjti az incidens felderítéséhez szükséges információkat (pl. naplóadatok), ezek elemzésével megkísérlik rekonstruálni az incidens kiváltó okait, egyúttal javaslatot tesz a hasonló incidensek megelőzését vagy az okozott kár enyhítését támogató informatikai védelmi intézkedésekre.

Az NKI CSIRT-szakterület az alábbi feladatokat látja el:

- biztonsági események kezelése,
- fenyegetésmenedzsment,
- ügyeleti szolgálat,
- kibervédelmi gyakorlatokon való részvétel, gyakorlatok szervezése,
- információvédelmi felelősök kijelölésének támogatása,
- biztonságiesemény-kezelés kapcsán együttműködés a központi szolgáltatóval (NISZ Zrt.) és az ügyfelekkel,
- rendszeres vezetői tájékoztatás, negyedéves jelentések készítése.

3.2.2. Incidenskivizsgálás

A Nemzeti Kibervédelmi Intézet incidenskivizsgálási szolgáltatása ellátja a biztonsági események kivizsgálásának támogatását, igény szerint kivizsgálását, ennek során elvégezheti a biztonsági események adatainak műszaki vizsgálatát, amelyhez adatokat és az adatokhoz elektronikus hozzáférést kérhet.

Az incidens felszámolása, azaz az incidens előtti állapot helyreállítása egy iteratív folyamat, melynek végrehajtása az érintett szerv feladata. Az NKI az incidens felszámolásban technikai támogatást nyújt, koordinál (bevonja az érintett feleket, közvetíti az információkat), dokumentál és javaslatokat tesz, opcionálisan elemzést végez.

A felszámolás folyamatának lépései:

- információk begyűjtése és elemzése,
- megoldási lehetőségek felkutatása,
- javaslat a végrehajtandó lépésekre,
- helyreállított állapot ellenőrzése.

Legfőbb tevékenységek:
- bekövetkezett biztonsági események elemzése,
- hordozható, asztali számítógépek és szerverek vizsgálata,
- hálózati kommunikáció- és adatforgalom-elemzés,
- adattárolók hiteles kezelése, másolat készítése,
- dokumentumok felkutatása, elemzése[208].

3.2.3. Sérülékenységvizsgálat

Az NKI 2015 szeptemberétől végez sérülékenységvizsgálati szolgáltatást az Ibtv.-ben foglalt bizonyos ügyfél, továbbá a nemzetbiztonsági védelem alá eső állami és önkormányzati szervek elektronikus információs rendszereinek vonatkozásában.

A sérülékenységvizsgálat, vagy más néven etikus hekkelés, az informatikai rendszer gyenge pontjainak (pl. potenciális szoftverhibák, gyenge jelszavak, hibás beállítások) feltárására irányul, ezzel is átfogóbb képet adva a vizsgált rendszer/rendszerelem aktuális biztonsági állapotáról, ami kiinduló információként szolgálhat a kockázatok kezeléséhez, illetve az informatikai támadások elleni védekezéshez.

A rosszindulatú támadók a biztonsági rések adta lehetőségeket kihasználva akár jelentős károkat is okozhatnak, ezért a vizsgálati eredményekről készülő jelentésben az NKI minden esetben javaslatot tesz az azonosított sérülékenységek kijavítására.

A szükséges intézkedések elvégzése által nagy eséllyel megelőzhető a bizalmas és nélkülözhetetlen szervezeti adatok elvesztése, ellopása, továbbá megakadályozható az ezekhez való illegális hozzáférés. Az NKI által végzett sérülékenységvizsgálati szolgáltatás teljes egészében térítésmentes.

A vizsgálati irányultságok az alábbiak lehetnek, zárójelben a jogszabály által meghatározott, a vizsgálat kezdetétől számított befejezési határidő található:
- külső vizsgálat (30 nap),
- belső vizsgálat (90 nap),
- webes vizsgálat (75 nap),
- vezeték nélküli hálózat vizsgálat (30 nap),
- pszichológiai manipuláció (90 nap)[209].

Új vizsgálati lehetőség az NKI sérülékenységvizsgálati palettáján a pszichológiai manipuláció módszerére épített vizsgálat, mely az elektronikus információs rendszerek leggyengébb pontját, az embert (felhasználót, rendszergazdát, vezetőt) célozza. A pszichológiai manipuláció olyan tevékenységi forma, technikák és módszerek összessége, amely az emberek befolyásolására alapozva teszi lehetővé bizalmas információk megszerzését vagy kártékony program terjedését és működését, tehát adathalász e-mailt küld vagy egy lehetetlen ajánlatot reklámoz és várja az emberek reakcióját.[210]

3.2.4. Biztonságirányítás

A támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról szóló 60/2014. (III. 6.) Korm. rendelet, a Nemzetbiztonsági Szakszolgálatot jelöli ki a FAIR, EMIR és IMIR 2014–2020 rendszerek informatikai biztonsági feladatainak ellátására. A Nemzetbiztonsági Szakszolgálat,

[208] 271/2018. Korm. rendelet 14–19. §.
[209] 271/2018. (XII. 20.) Korm. rendelet 22–29. §.
[210] 271/2018. (XII. 20.) Korm. rendelet 1. § 15. pont.

a Nemzeti Kibervédelmi Intézet biztonságirányítási szolgáltatásának keretében végzi a feladatkörébe rendelt információs rendszerek informatikai biztonsági feladatait. A feladatellátás során, az NKI szolgáltatási palettájából merítve biztosítják a szolgáltatást nyújtó szakemberek, a rendszereket érintő bejelentések fogadását, az incidenseket kezelését, a sérülékenységek feltárását, továbbá a szabályzókból, eljárásrendekből összetevődő dokumentációs környezet fejlesztésén keresztül támogatják a rendszerekért felelős információbiztonsági felelősök munkáját.

3.2.5. Eseményészlelés

Az Eseményészlelési Szakterület (Event Detection Team, EDT) intézmények közti megállapodás keretében a biztonság növelése érdekében folyamatosan monitorozza a hálózati forgalom különböző szegmenseit. A szakterület által végzett feladat preventív és detektív jellegű, hiszen alapvetően passzív adatforgalom-ellenőrzésről és annak elemzéséről van szó. A szisztematikusan összegyűjtött támadási kísérletek rendszerezett adatai alapján azonosíthatjuk a támadók által felhasznált internetes erőforrások címeit, másrészt – különböző elemző algoritmusok segítségével – felfedezhetjük a behatolási módszerek alkalmazási trendjeinek aktuális alakulását, valamint következtetéseket vonhatunk le az internetre épülő szolgáltatások hátterét nyújtó szoftverkörnyezet esetleges gyenge pontjairól, illetve sebezhetőségeiről. A támadási mintázatok elemzésének révén lehetségessé válik az eleddig ismeretlen támadási módszerek felismerése és ezen módszerek viselkedési szabályai, azonosítói (indikátorai) alapján további biztonsági intézkedések megtétele.

3.2.5.1. EWS

A Korai Figyelmeztető Rendszer (Early Warning System, EWS) működtetését a NIS-irányelv rója a tagállamokra.[211] Ezzel összhangban, jogszabályi felhatalmazás alapján[212] az NKI is megalkotta a saját informatikai biztonsági korai figyelmeztetőrendszerét. Az EWS az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának az ún. szenzorokkal történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményt.

A szenzor a Korai Figyelmeztető Rendszerbe integrált, hálózati forgalommonitorozó célhardver, amely dedikált hálózati kapcsolattal rendelkezik a védendő infrastruktúra felé, a védendő rendszer szempontjából logikailag egyirányú eszköz, amellyel az aktív beavatkozás lehetősége kizárt.

Az EWS jelzéseket, adatokat és ezekre épülő szolgáltatásokat nyújt az egyes védendő rendszerekre vonatkozóan azok fenntartó intézményeinek kijelölt munkatársai és az NKI számára.

Az EWS egyedülálló előnye, hogy a csatlakozó szereplőknek egységesen magas szintű kiegészítő védelmet nyújt és annak kihasználásához szükséges oktatást biztosít – mindezt megbízható kormányzati partnertől, központi finanszírozással.

Az EWS-rendszer szolgáltatásai az Ibtv., illetve az annak végrehajtásáról szóló 41/ 2015. (VII. 15.) BM rendelet (továbbiakban: BMr.) által előírtan az intézmény által önállóan megvalósításra kerülő védelmi intézkedések nyújtotta biztonságon felüli kiegészítő intézkedésként javítja a csatlakozó intézmény észlelési, felügyeleti, megfelelőségellenőrzési képességét és ezeken keresztül integritását.

Az EWS segítségével az intézmény számára hamarabb és nagyobb mértékben válhatnak láthatóvá, illetve ezáltal kezelhetővé a rendszert érintő támadások (pl. hálózati betörési kísérlet, adatlopás, weboldalrongálás), visszaélések, korrupciós cselekmények (pl. adatszivárogtatás, zsarolási kísérlet) és kockázatok (pl. sérülékeny vagy illetéktelen eszközök és szolgáltatások, lappangó kártevők).

[211] NIS-irányelv 2. melléklet (2) bekezdés a) pont ii. alpont.
[212] 271/2018. (XII. 20.) Korm. rendelet 4. § c) pont.

Az EWS nem más, mint tulajdonképpen egy nagy méretű, több felhasználóval működő behatolásjelző rendszer (IDS), melynek üzemeltetéséről és szakmai karbantartásáról (szignatúrákkal és szabályokkal való ellátásáról) egy harmadik fél gondoskodik, miközben az előnyeit a védett intézmény élvezi. Az EWS képes viselkedésalapú (pl. szolgáltatásmegtagadásos támadás) és szignatúraalapú (pl. káros kódok) káros tevékenység felismerésére is.

Az EWS csatlakozással az intézménynek csökkennek az incidens kivizsgáláshoz kapcsolódó adminisztratív terhei, mivel a tipikusan átadandó adatok egy része már eleve elektronikus formában az NKI rendelkezésére áll; valamint az NKI ezen adatok előzetes elemzésével és a védendő rendszer felépítésének ismeretében célzottabb javaslatot tud tenni a még szükséges műszaki adatok begyűjtésére, illetve az indokolt védelmi intézkedésekre vonatkozóan.

Az EWS bevezetésekor az NKI szakmai és integritás-tanácsadói képzést biztosít az intézmény kijelölt munkatársai számára térítésmentesen, így járulva hozzá az EWS nyújtotta lehetőségek lehető legnagyobb mértékű kihasználásához. Ezen szakmai továbbképzés, biztonságtudatos és antikorrupciós szemléletformálás eredményeként a munkatársak jobban hozzá tudnak járulni a védendő rendszerek által kezelt adatvagyon, illetve a nyújtott szolgáltatások biztonságához, az informatikai biztonsági incidensek kezeléséhez és a korrupció kockázatának csökkentéséhez.

Az EWS-rendszer tervezése során nagy hangsúlyt kapott az adatvédelem. Ennek érdekében szigorú, többlépcsős és többfaktoros bejelentkezés és szigorú jogosultságmenedzsment épült ki, melynek célja, hogy minden intézmény, minden szereplő kizárólag a saját adataihoz férjen hozzá.

3.2.5.2. Honeypot

A csapdarendszerek (honeypot) elsődleges célja az, hogy – valós működést szimulálva – elhitessék a támadókkal, hogy éles szolgáltatást nyújtó rendszert sikerült elérniük. Mindeközben azonban a jól felépített csapdarendszerek a támadó valamennyi tevékenységét letapogatják, módszeresen összegyűjtik, rögzítik és naplózzák. Tekintettel arra, hogy a csapdarendszer valójában nem működtet „igazi" szolgáltatást, a rajta észlelt valamennyi tevékenység jogtalannak minősíthető, azaz potenciális támadásként fogható fel. A csapdarendszerek tehát lényegében arra szolgálnak, hogy a támadók saját magukat leplezzék le egy olyan álcázott környezetben, ahol minden tevékenységük nyomot hagy.

A szisztematikusan összegyűjtött támadási kísérletek rendszerezett adatai alapján aztán egyrészt azonosíthatók és lekérdezhetők a támadók által felhasznált internetes erőforrások (számítógépek, illetve szerverek) forráscímei, másrészt pedig – különböző elemző algoritmusok segítségével – felfedezhető a behatolási módszerek alkalmazási trendjeinek aktuális alakulása, valamint következtetések vonhatók le az internetre épülő szolgáltatások hátterét nyújtó szoftverkörnyezet esetleges gyenge pontjairól, ill. sebezhetőségeiről.

A csapdarendszerek által feltárt információk esetenként közvetlenül, akár automatizáltan, is hasznosíthatók lehetnek. A csapda rendszer által rögzített adatok, támadási mintázatok elemzésének révén eleddig ismeretlen támadási módszerek is felismerhetők és megtanulhatók, ami elengedhetetlenül szükséges a további biztonsági intézkedések megtételéhez.

Az elosztott kormányzati IT-hálózatbiztonsági csapdarendszer (GovProbe) egy központi adatgyűjtő, kiértékelő elemből, valamint az azzal kapcsolatban álló, a külső támadó számára valósnak látszó hálózati szolgáltatásokat szimuláló célpont rendszerekből (szenzorok) áll, ami az aktív támadási próbálkozások során keletkező adatok és mintázatok rögzítését teszi lehetővé.

A rendszer által rögzített támadási adatok betekintést nyújtanak a rendszer által védett infrastruktúrákat érő kibertámadások előkészítési, információgyűjtési, valamint terjedési folyamataiba is. A rendszer segítségével felderíthetőek a hálózatokon belüli, illetve kívülről érkező letapogatási és zero day (a nyilvánosság számára ismeretlen) sérülékenységeket kihasználó aktivitások.

Speciális kiépítése és alapvetően passzív hálózati elhelyezése következtében a csapdarendszer olyan információkhoz juttatja a kiberbiztonsági incidensek feltárását végző elemzőket, melyek más, jellemzően vonalra épülő biztonsági rendszerek (például IDS/IPS, Network Tap) esetén természetszerűleg nem érhetők el.

3.3. A hatóság

3.3.1. Egyedüli kapcsolattartó pont

A Nemzetbiztonsági Szakszolgálat Nemzet Kibervédelmi Intézet Hatósági Főosztálya látja el továbbá az EU felé a nemzeti egyedüli kapcsolattartó pont (ún. SPOC) feladatát is.

A SPOC egyik feladata, hogy elősegítse a NIS-irányelv hatékony átültetését, hálózati és információs rendszerek biztonságával kapcsolatos kérdések koordinálásával. Ezt a nemzeti NIS-irányelv szerinti hatóságok és CSIRT-ek közötti koordináció és összekötő funkció ellátásával. A nemzeti egyedüli kapcsolattartó pont a nemzeti joggal összhangban, szükség szerint konzultálhat és együttműködhet az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal. A SPOC másik feladata az uniós szinten folytatott határokon átnyúló együttműködés biztosítása, többek között a CSIRT-ek hálózata és az Együttműködési Csoport feladatainak elősegítése, támogatása által.

Egy határon átnyúló természetű biztonsági incidens esetén, amely kritikus infrastruktúrák esetén még több koordinációt igényelhet, valamely nemzeti illetékes hatóság vagy CSIRT megbízhatja az egyedüli kapcsolattartó pontot azzal, hogy továbbítsa az eseményről küldött bejelentést más érintett tagállamok egyedüli kapcsolattartó pontjai részére és segítse a hatóságok közötti koordinációt, kommunikációt.

Az egyedüli kapcsolattartó pont évente egyszer összefoglaló jelentést nyújt be az együttműködési csoport számára az azon év során kapott NIS-irányelv szerinti incidensbejelentésekről (bejelentések száma, a bejelentett biztonsági események jellege, valamint a hozott intézkedések) anonimizált módon.[213]

3.3.2. Hatósági nyilvántartás

A hatósági nyilvántartási szakterület legfontosabb feladatai az osztályba sorolás és a biztonsági szint megállapításának ellenőrzése és az ellenőrzés eredménye alapján döntés meghozatala, javaslattétel a létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény szerinti ágazati kijelölő hatóság részére a nemzeti létfontosságú rendszerelem kijelölésére. Kiemelt feladat ezenkívül a kapcsolattartás az elektronikus információbiztonság területén a különböző szereplőkkel[214], valamint a hatósági nyilvántartás kezelése.[215]

A hatósági nyilvántartás az alábbi adatokat tartalmazza[216]:

- A szervezet azonosításához szükséges adatok.
- A szervezet elektronikus információs rendszereinek megnevezése, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolása, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatai, tehát NEIH-OVI és NEIH-SZVI űrlapok.

[213] https://nki.gov.hu/szolgaltatasok/tartalom/nemzeti-egyeduli-kapcsolattarto-pont/
[214] Ibtv. 14. §.
[215] Ibtv. 15. § (1) bekezdés.
[216] Ibtv. 15. §.

- A szervezet elektronikus információs rendszer biztonságáért felelős személyének természetes személyazonosító adatai, telefon- és telefaxszáma, e-mail-címe, az Ibtv. 13. § (8) bekezdésében meghatározott végzettsége és szakképzettsége.
- A szervezet informatikai biztonsági szabályzata.
- A biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott értesítések.
- A sérülékenységvizsgálatok eredménye, valamint a sérülékenységek megszüntetésére vonatkozó intézkedési tervek.

A Nemzeti Kibervédelmi Intézettel együtt részt vesz a Nemzeti Kiberbiztonsági Koordinációs Tanács által felügyelt információtechnológiai, hálózatbiztonsági, információmegosztási és incidenskezelési munkacsoportokban is.

3.3.3. Bejelentésköteles szolgáltatók hatósági nyilvántartásba vétele

A NIS-irányelv európai szintű végrehajtása és magyar jogrendbe történő átültetése megtörtént: kihirdetésre került a Bizottsági (EU) 2018/151 rendelet (a továbbiakban: EU rendelet), illetve módosult az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.). A rendelkezések 2018. május 10. napján hatályba léptek. A magyar jogszabályok a NIS-irányelvben használt „digitális szolgáltatás" terminológia megfelelőjeként a „bejelentésköteles szolgáltatás" elnevezést használják.

Az új szabályozások célja, hogy a bejelentésköteles szolgáltatást nyújtók az általuk használt hálózati és információs rendszerek biztonságát növeljék, az azokat érő biztonsági eseményeket megelőzzék, illetve hatásukat csökkentsék, ezáltal emelve az általuk nyújtott szolgáltatások biztonságát. A bejelentésköteles szolgáltatások elterjedtsége, illetve más fontos szolgáltatásokba történő beépülése miatt a megbízható, folyamatos működésükre alapvető gazdasági és társadalmi tevékenységek támaszkodhatnak. Az erre épülő célokat, illetve a kibertérbeli működés biztonságát és üzemfolytonosságát támogatja az eseménykezelő központ és a hatóság.

A kiberbiztonság érdekében az EU rendelet előírja a hálózati és információs rendszerek kockázatokkal arányos védelmét és az alkalmazandó biztonsági elemeket. Az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet (a továbbiakban: Vhr.) a bejelentésköteles szolgáltatást nyújtó szereplők számára előírja a hatóságnál történő regisztrációt, valamint a hálózati és információs rendszereikben bekövetkezett jelentős biztonsági események bejelentését az eseménykezelő központ számára. A Vhr. a bejelentésköteles szolgáltatást nyújtókkal kapcsolatos hatósági, valamint eseménykezelési feladatok ellátására a Nemzetbiztonsági Szakszolgálatot (NBSZ) jelölte ki.

3.3.4. Hatósági ellenőrzés

Az ellenőrzési szakterület feladata az éves ellenőrzési tervben előre meghatározott módon és ütemben az elektronikus információs rendszerek osztályba sorolására és a szervezetek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése, az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése és eredményességének ellenőrzése.[217] A hatóság az ellenőrzési tervben foglaltaktól eltérhet, ha olyan azonnali

[217] Ibtv. 14. §.

ellenőrzéseket vagy eljárásokat kell lefolytatnia, amelyek a magyar kiberteret, a nemzeti elektronikus adatvagyont, az állam és polgárai számára kiemelten fontos elektronikus információs rendszereket fenyegető súlyos biztonsági események elhárítását szolgálják.[218]

3.3.5. Bírságolás

A hatóság régebbről meglévő bírságolási jogköre 2019. január 1-től már a költségvetési intézmények felé is lehetséges, ezért a téma mélyebb feldolgozása szükséges.

A korábbi szabályozás szerint, ha a szervezet költségvetési szerv és a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a hatóság köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére.

Az új joganyag alapján a hatóság köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére. Ha ezek ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, az eset összes körülményeinek mérlegelésével bírságot szabhat ki, amely további nem teljesülés esetén megismételhető. Ezenkívül a hatóság jogosult bírságot kiszabni külön Korm. rendeletben meghatározottak szerint.[219]

A hatóság jogszabálysértés esetén az alábbiakban rögzített bírságot szabhat ki. A kiszabható bírság ötvenezer forinttól ötmillió forintig terjedhet, amelyet a hatóság határozatának véglegessé válását követő nyolc napon belül kell befizetni a hatóság Magyar Államkincstárnál vezetett számlájára:

- regisztráció elmulasztása: 50 000–100 000 Ft,
- adatváltozás bejelentésének elmulasztása: 50 000–500 000 Ft,
- kockázatelemzés készítésének elmulasztása: 200 000–500 000 Ft,
- kockázatokkal arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása: 300 000–5 000 000 Ft,
- kockázatelemzés és a szükséges biztonsági intézkedések biztonsági eseményt követő haladéktalan, egyéb esetben évente dokumentált felülvizsgálatának elmulasztása, a felülvizsgálat során feltárt hiányosságok alapján a szükséges módosítások végrehajtásának elmulasztása: 200 000–2 000 000 Ft,
- biztonsági esemény bejelentésének elmulasztása: 300 000–5 000 000 Ft,
- hatóság végleges, végrehajtandó határozatában foglalt kötelezésének nem teljesítése: 400 000–5 000 000 Ft.

A korábban is a hatóság rendelkezésére álló lehetőségeken (azonnali intézkedésre kötelezés, felszólítás stb.) túlmenően az eljárás akadályozása, illetve az adatszolgáltatás nem vagy nem megfelelő teljesítése esetén a hatóság hárommillió forintig terjedő bírsággal sújthatja – ismételt jogsértés esetén sújtani köteles – a jogsértő vezető tisztségviselőjét is.

A hatóság a jogkövetkezmények alkalmazása során jogszabályban meghatározottakon túl az alábbi szempontokat veszi figyelembe:

- az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelménynek a biztonsági osztályba sorolás és biztonsági szint szerinti súlyát,
- történt-e súlyos biztonsági esemény vagy fennállt-e ilyen esemény bekövetkeztének veszélye,

[218] 187/2015. (VII. 13.) Korm. rendelet 12. § (3) bekezdés.
[219] Ibtv. 16. § (3) bekezdés a), b) és d) pont.

- a biztonsági esemény hatását vagy lehetséges hatását az érintett szervezetre, vagy más szervezetekre,
- az érintett szervezet magatartását, hatósággal való együttműködését és
- az esemény egyedi vagy ismételt jellegét.[220]

3.3.6. Tudatosítás és sajtómegjelenés

Az NKI egyik kiemelt feladata a biztonságtudatosság növelése a felhasználók vonatkozásában. A kibervédelem legolcsóbb és leghatékonyabb módja a biztonságtudatos használat. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne a megfelelő szinten kialakítható. A tudatosítás számos formában megjelenhet, mint például szakmai anyagok és útmutatók készítése, közvetlenül kifejtett oktatási vagy képzési tevékenység, a kiberbiztonság hangsúlyának növelése a médiában.

A tudatosító tevékenység számos réteget céloz, ezek közt elsősorban kell említeni a döntéshozókat (szervezeti vezetőket, akik a rendszerek védelméért felelősek), az üzemeltetőket (akik ellátják a rendszerek működtetését, és tőlük várható el a védelmi intézkedések működtetése) és a felhasználókat, akiket meg kell tanítani az internet és az információs technológiák biztonságos használatára, saját és a rájuk bízott adatok felelős és szakszerű kezelésére.

4. Biztonsági események bejelentése

A biztonsági események bejelentésének kötelezettségét, az alapvető szolgáltatókkal kapcsolatos részletszabályokat a NIS-irányelven való megfeleltetés okán az Ibtv. végrehajtási rendelete tartalmazza.

A NIS-irányelv alapján a tagállamok biztosítják, hogy az alapvető szolgáltatásokat nyújtó szereplők indokolatlan késedelem nélkül bejelentik az illetékes hatóságnak vagy a CSIRT-nek az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket. A bejelentéseknek tartalmazniuk kell az ahhoz szükséges információkat, hogy az illetékes hatóság vagy a CSIRT meg tudja határozni az adott biztonsági esemény esetleges határon átnyúló hatásait. A bejelentés nem róhat többletfelelősséget a bejelentő félre.[221] Az információk megfelelő áramlása miatt az illetékes hatóságnak vagy CSIRT-nek az alapvető szolgáltatásokat nyújtó szereplőktől kapott bejelentésben foglalt információk alapján tájékoztatnia kell a többi érintett tagállamot, amennyiben a biztonsági esemény az adott tagállamban jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára.[222]

Az Ibtv. végrehajtási rendelete részletesen tartalmazza a biztonsági események bejelentésének szabályait.

Az alapvető szolgáltatást nyújtó szolgáltatók (kritikus infrastruktúrák) indokolatlan késedelem nélkül bejelentik az NKI CSIRT-szakterülete részére az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket.[223]

A biztonsági esemény hatása jelentőségének meghatározása és a kockázatelemzés megkönnyítése érdekében az alapvető szolgáltatást nyújtó szolgáltató tájékoztatásának tartalmaznia kell: az alapvető szolgáltatás zavara által érintett felhasználók számát, a biztonsági esemény időtartamát, a biztonsági esemény által érintett terület földrajzi kiterjedését.[224]

---

220 187/2015. (VII. 13.) Korm. rendelet 13. § és 1. számú melléklet.
221 NIS 14. cikk (3) bekezdés.
222 NIS 14. cikk (5) bekezdés.
223 271/2018 Korm. rendelet 9. § (1).
224 271/2018 Korm. rendelet 9. § (2).

Ha egy alapvető szolgáltatásokat nyújtó szolgáltató valamely, a kritikus társadalmi és gazdasági tevékenységek fenntartása szempontjából alapvetőnek tekintett szolgáltatás nyújtását egy harmadik fél bejelentésköteles szolgáltatóra alapozza, az említett szolgáltatónak be kell jelentenie minden olyan esetet, amikor a bejelentésköteles szolgáltatót érintő biztonsági esemény jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára.

A bejelentésköteles szolgáltatást nyújtó haladéktalanul bejelenti a Központ részére az elektronikus információs rendszerein bekövetkezett azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Európai Unión belül kínált bejelentésköteles szolgáltatás nyújtására.[225] Ez nagyon fontos kötelezettség az érintetteknek, ez alapján tud gyorsan és hatékonyan elindulni az EU-szintű egyeztetés.

A biztonsági események bejelentése a kialakult szokásoknak és a modern kor kihívásainak is megfelelve, valamint a hatékonyságot maximálisan szem előtt tartva, elsődlegesen elektronikus úton történik, ha azonban az elektronikus információs rendszer oly mértékben sérül, hogy az nem lehetséges, a bejelentés bármely más módon megvalósítható.[226]

A bejelentésnek minimálisan tartalmaznia kell a gyors megértés céljából a biztonsági esemény rövid leírását, státuszát, a súlyosság még pontosabb körbehatárolása miatt a szolgáltatás működésében támadt zavar mértékét és a biztonsági esemény hatását meghatározó szempontokat.

Ezeken kívül a kapcsolattartás megkönnyítése érdekében az esemény kezelésére az üzemeltető által kijelölt kapcsolattartó személy és szervezet elérhetőségeit, valamint közvetítő szolgáltató igénybevétele esetén a közvetítő szolgáltató megnevezését, elérhetőségét is bele kell foglalni a bejelentésbe.[227] Az NKI felkészült végponti titkosítással ellátott (PGP) elektronikus levelek fogadására, a levelezéshez szükséges publikus kulcs elérhető az NKI weboldalán. Ezek megléte nagyban segíti a CSIRT munkáját és hozzájárul az incidens hatékony kezeléséhez.

Az NKI a korábban leírtak alapján vizsgálja az alapvető szolgáltatást nyújtók szolgáltatásaira jelentős hatást gyakorló biztonsági események határon átnyúló hatását, és közvetlenül vagy az egyedüli kapcsolattartó pont útján indokolt esetben tájékoztatja a jelentős hatást gyakorló biztonsági eseményekről a többi érintett tagállamot.[228]

Nagyon fontos garanciális szabály az ügyfelek részére, hogy az NKI Nemzeti CSIRT-nek ezen tájékoztatás során biztosítania kell a szolgáltatók biztonságát, gondoskodnia kell arról, hogy ne sérüljenek a kereskedelmi érdekei és a bejelentésben foglalt információk bizalmassága.

5. Incidenskezelési sajátosságok kritikus infrastruktúrák esetén

Az incidenskezeléssel kapcsolatos korábbi szakanyagokban szereplő és a NIST incidenskezelési eljárását követő[229] megállapításai általánosan igaznak bizonyulnak a kritikus infrastruktúrákra vonatkozóan is, azonban szükséges hangsúlyossá tenni néhány információt ezzel kapcsolatban.

A kritikus infrastruktúrák nem kizárólag „hagyományos” rendszereket üzemeltetnek, hanem számtalan olyan felügyeleti és adatgyűjtő rendszert (SCADA, Supervisory Control and Data Acquisition) és azok alapvető működéséért felelős ipari vezérlőrendszert (PLC, programmable logic controller) működtetnek. A PLC-k valósítják meg a rendszerekben az logikai döntéseket a rendszerekben, tehát például egy vízerőműben a víz útját szabályozó eszközöket vezérelhetik.

[225] 271/2018 Korm. rendelet 10. §.
[226] 271/2018 Korm. rendelet 11. § (1).
[227] 271/2018 Korm. rendelet 11. § (2).
[228] 271/2018 Korm. rendelet 12. § (1).
[229] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

A PLC-k gyártóspecifikus speciálisan ezekre az eszközökre fejlesztett kommunikációs protokollokat használnak, melyek teljes mértékben különbözhetnek a szabványos protokolloktól, és melyekre az általános monitorozási, megelőzési és incidenskezelési eljárások nem vagy csak korlátozottan használhatóak, ezek megértéséhez és vizsgálatához speciális tudás szükséges. Az ezek leírásához való hozzáférés szintén nem olyan evidens, mint a szabványos protokoll leírások elérhetősége. Az eszközök, az azokon futó szoftverek, valamint a kommunikációs és egyéb protokollok ismerete pedig alapvető fontosságú az incidenskezelés szempontjából.

Ezeket a rendszereket és protokollokat még az internet általánossá válása előtt (10-15 évvel korábban vagy még régebben) fejlesztették ki. Az általánosan bevett eljárások szerinti cseréjük, frissítésük jóval nagyobb kihívás, sőt, sok esetben kompatibilitási okokból gyakorlatilag lehetetlen. Az ilyen rendszerek cseréje olyan költséggel járhat, melyet a termelőtevékenység nem, vagy csak nagyon nehezen termel ki.

Fontos kiemelni továbbá, hogy ezek a rendszerek gyakran kritikus folyamatokat menedzselnek, melyeknél a rendelkezésre állás olyan szinten hangsúlyos lehet, mely erős hatással van az informatikai biztonság többi szempontjára is.

6. Incidens esettanulmányok

6.1. Útválasztó kompromittálás

Egy incidensbejelentés szerint az érintett intézmény internetforgalmát kiszolgáló router eszközt valószínűleg ismeretlen személyek feltörték és működésképtelenné tették. A bejelentésben közöltek szerint a router eszköz működésképtelenségéből fakadóan nem voltak elérhetők az internetes honlapok, nem, vagy csak részben működtek bizonyos szakrendszerek, elérhetetlen volt a netbank. Az intézmény munkatársai az esetet több szervezetnek is bejelentették.

A router, hibás működését követően, eltávolításra került a hálózatból, az üzembiztonság fenntartása érdekében helyére egy másik, funkcionalitásban megegyező eszköz került. Tekintettel a működésképtelenség nem egyértelmű okára, az intézmény munkatársai az eszközt gyári alaphelyzetre állították, végül szakszervízbe is küldték. Megjegyzendő, hogy ez a lépés az incidenskezelési alapelveket sértette, mert ezt követően (ha az eszköz adattárolójáról nem készül hiteles másolat) nem lehetséges több vizsgálat elvégzése, például egy esetleges káros kód telepítésének megállapítása sem.

Az eszközben két nem odaillő scriptállomány is megtalálható volt, melyek egyértelműen nem a rendszer szabályos működése következtében keletkeztek, azokat külső támadó helyezhette el az eszköz feltörését követően. Bár a két script a gyári visszaállítás ellenére sem törlődött, a feltörés pontos módja – így a konkrét sérülékenység kihasználása – és ideje már nem megállapítható. Egyértelműen megállapítható, hogy a scriptállományok célja egy dedikált oldalon elhelyezett konfigurációs fájl letöltése, valamint az abban található konfigurációs tartalom importálása a feltört eszközön.

A router által letöltött konfigurációs állományból kiolvasható, hogy az kizárólag egyetlen beállítást módosít, melynek segítségével az internet irányából kiszolgálást biztosító PPPOE-interfészen a DNS-szolgáltatást letiltja. E beállítás – tekintettel arra, hogy az internet gyakorlatilag összes eszközének és szolgáltatásának döntő többsége DNS-névfeloldást használ a hivatkozások megkönnyítése érdekében – önmagában alkalmatlanná teszi az eszközt releváns internetforgalom kiszolgálására, előidézve mindazon tüneteket, melyeket a kórház munkatársai bejelentésükben tapasztaltak. A scriptállományok és -parancsok alapján a támadás célja az eszköz működésének és a kiszolgált internetforgalomnak a megzavarása volt, melyet a támadó sikeresen elért.

Az NKI munkatársai – a támadás feltárt céljától függetlenül – a megkapott tűzfal naplóállományokat ellenőrizték a nemzetközi kapcsolatrendszer segítségével megszerzett, azonos gyártmányú routereket fertőző, káros kampány indikátorait keresve. E kampányban a támadók egy bizonyos gyártmányú eszközöket törnek fel és fertőznek abból a célból, hogy a rajtuk átmenő forgalom módosítása által

valós kliens munkaállomásokon váljanak képessé kriptovaluta-bányász folyamatok és műveletek elindítására, illetőleg futtatására.

A tűzfal naplóállományok ellenőrzése rámutatott, hogy a kampányhoz köthető egyik vezérlőszerver IP-címe több napon is forgalmat generált az érintett eszközön.

A hivatkozott mintán megfigyelhető, hogy a megszólítások minden alkalommal DNS-névfeloldási lekérdezések voltak, egyéb generált forgalom nem volt tapasztalható. Az érintett router nem szerepelt a nemzetközi forrásból megszerzett, fertőzött eszközöket tartalmazó összesített listában, ugyanakkor a tapasztalt kezdetleges kommunikáció arra enged következtetni, hogy az a kampány szempontjából esetlegesen fertőzendő lehetett.

6.2. Ransomware egy kritikus infrastruktúrában

Az NKI egy káros kód (Dharma zsarolóvírus) fertőzést vizsgált egy kritikus infrastruktúra vonatkozásában. Az incidens következtében az intézmény bizonyos rendszerei nem voltak elérhetőek, az adatok kizárólag papíralapon álltak rendelkezésre. A fertőzés eredete nem volt megállapítható, mivel az intézmény és alvállalkozója közti kialakított vegyes üzemeltetésű infrastruktúrán a vizsgálat idején rendelkezésre álló adatok alapján ez már nem volt visszakövethető.

A vizsgálat során azonban megállapítást nyert, hogy a kliens és a központi szerver lemezeit azonos zsarolóvírus titkosította, mely a szerverről kiajánlott SMB-megosztás fertőzésével juthatott be a szerverre, mivel a káros kód önálló terjedésre nem volt képes.

Ezenkívül kiderült az is, hogy a kliens merevlemezen a Microsoft Volume Shadow Copy szolgáltatása tartalmazott árnyékmásolatokat, melyeket alkalmazva a felhasználó profilokban található állományok visszanyerhetők voltak, azokat a szervezet informatikai biztonsági vezetőjének az NKI eljuttatta. A központi szerver merevlemeze azonban egyáltalán nem tartalmazott VSS-árnyékmásolatokat, valamint a titkosított állományok a zsarolóvírusokkal foglalkozó releváns szakmai portálok bejegyzései szerint egyelőre nem visszafejthetők.

6.3. Illetéktelen elérés

Az NKI-hoz érkezett egy harmadik féltől tájékoztatás, melyben jelezték, hogy egy kritikus infrastruktúrák által használt szakrendszer weboldala bizonyos almappái bejelentkezés nélkül elérhetőek, továbbá egy „teszt” felhasználójaként bárki be tud jelentkezni a felületre.

A jelzett mappák elérhetőségének ellenőrzését követően az NKI munkatársai az illetéktelen hozzáférés lehetőségét jelezték ügyfélszolgálati e-mail-címen és telefonos megkeresésben is a fejlesztő és egyben üzemeltető cég felé, egyúttal kérve az illetéktelen hozzáférés lehetőségének mielőbbi megszüntetését.

Az incidenskezelés következtében az üzemeltető az említett hiányosságokat rövid időn belül orvosolta, ezt követően már nem lehetett érzékeny tartalmakhoz illetéktelenül hozzáférni a jelzett módon.

További intézkedésként az üzemeltető letiltotta a mappák tartalmának listázási lehetőségét, az érzékeny adatokat tartalmazó mappák kikerültek a webszerver fizikai elérhetőségi köréből, tehát ilyen fájl tartalmát még közvetlenül a teljes elérési útvonal, valamint a fájlnév ismeretében sem lehetett ezt követően megjeleníteni. Ezen túlmenően bármely olyan hozzáférési próbálkozás esetén, amely nem a portál által kínált menürendszeren vagy linken keresztül történik, a webszerver azonnal a portál kezdőlapját jeleníti meg, valamint megváltoztatták a rendszer üzemeltetői felhasználói fiókjainak jelszavait is.

6.4. Tanulságok levonása

Nagyon fontos tudatosítani a rendszerek üzemeltetői felé az incidenskezelés jelentőségét. Az üzemeltetés a klasszikus CIA-modell alapján hajlamos megfeledkezni a bizalmasság és a sértetlenség kérdéskörének vizsgálatáról, és az elérhetőség helyreállítására helyezik a hangsúlyt. Az incidenskezelés megnehezülhet, sőt, adott esetben el is lehetetlenülhet, ha nem fordítunk rá megfelelő figyelmet, és ez később még komolyabb incidensek kialakulásához vezethet.

Az incidens kialakulásának nemcsak a következményét kell felszámolni, hanem az okait is kellő körültekintéssel kell kezelni, fel kell tárni a biztonsági réseket, a rossz gyakorlatokat és folyamatosan tudatosítani szükséges a munkatársakat a megfelelő információbiztonsági tudatosság eléréséért.

Az incidensek kialakulásának minimalizálása érdekében alapvető lépések megtétele szükséges, mely a következő fejezetben kerül részletezésre.

7. Incidensek keletkezésének megelőzése

Az NKI a technikai kivizsgálásokat követően ajánlásokat, tanácsokat, javaslatokat fogalmaz meg az érintett szereplő részére a bekövetkezett esemény ismételt megelőzése vagy egyéb, az elemzést követően feltárt biztonsági hiányosságok kapcsán. Ezek általában az adott intézmény infrastruktúrájára szabott javasolt intézkedések.

- **Rendszeres frissítés:** Javasolt a hálózati eszközök – switchek, routerek, tűzfalak stb. – rendszeres, folyamatos frissítését a támadók által kihasználható sérülékenységek megszűntetése érdekében.
- **Rendszeres konfiguráció mentés:** Ajánlott a hálózati eszközök konfigurációinak rendszeres mentése annak érdekében, hogy hasonló károkozás esetén a csereeszközt minél hamarabb ismét működőképes állapotba lehessen állítani.
- **Loggyűjtés, rendszeres logelemzés:** Összetettebb rendszerek esetén javasolt loggyűjtő szolgáltatás bevezetése, és a keletkezett naplóállományok rendszeres elemzése kiértékelése, valamint a felhasznált tapasztalatok beépítése a védelmi intézkedésekbe.
- **Biztonsági szint:** A hálózat biztonsága érdekében javasolt a kritikus infrastruktúráknak az egyes tűzfalak, routerek, switchek, valamint egyéb hálózati eszközök konfigurációja esetén azok biztonsági szintjének növelése, valamint a minél szigorúbb követelményeknek való megfeleltetése, akár a gyártó ajánlásait felhasználva.
- **IDS/IPS-rendszerek alkalmazása:** Az infrastruktúra hálózatainak és eszközeinek védelme érdekében IDS/IPS-rendszerek alkalmazása ajánlott, melyek szignatúráik alapján képesek felismerni a gyakori támadások mintázatait.
- **WAF alkalmazása:** A weboldalt saját maguk hostoló intézmények részére javasolt a WAF-(Web Application Firewall) rendszer bevezetése, mely kifejezetten a weboldalak elleni támadások felismerésére készült termék. Hosting szolgáltatás esetén is javasolt WAF-szolgáltatás megrendelése.
- **Az állományok archiválása:** Zsarolóvírus-támadás esetén javasolt a fertőzött diszk archiválása, melynek oka, hogy a zsarolóvírusok egy része idővel visszafejthetővé válhat, illetve privát kulcsuk sok esetben kiszivárog. Hasonló esetben a titkosított állományok egésze visszafejthetővé válhat.
- **Központi mentés:** Az érintett, illetve az infrastruktúrában hasonló formában működő kiszolgálók azonnali bevonása központi mentőszerverbe, mely megbízható, riportálható módon gondoskodik az adatvagyon legalább napi szintű mentéséről.
- **Antivírustermék:** Korszerű, modern, az iparágban széles körben elismert antivírustermék használata kiszolgáló oldalon is, mely lehetőség szerint tartalmaz a különböző viselkedési mintát mutató kártevők felismerésére létrehozott, viselkedést detektáló algoritmust.

- **Csoportházirendek:** Javasolt a rendszereken a csoportházirend-objektumok megfelelő konfigurálása, az alkalmazások és scriptek futtatásának korlátozása a felhasználók esetén.
- **Tudatosítás:** Tudatos felhasználói magatartás erősítése, akár belső, információbiztonsági előadások/tanfolyamok által (pl. zsarolóvírusok gyakori bejutási formái e-mail-üzenetek által) szintén minden intézménynél javasolt.
- **Incidenskivizsgálás:** Fertőzésgyanú esetén ajánlott a munkaállomás/kiszolgáló elkülönítése, egyéb módosítás (pl. bootolás, felcsatolás másik számítógépre stb.) nélküli részletes vizsgálata az NKI által.
- **Sérülékenységvizsgálat:** Új rendszerek, valamint rendszermódosítások esetén érdemes sérülékenységvizsgálatot végeztetni.

8. Irodalomjegyzék

- Berzsenyi Dániel, Gyaraki Réka, Hámornik Balázs Péter, Hirsch Gábor, Kiss Attila, Marsi Tamás, Orbók Ákos, Simon Béla, Solymos Ákos, Tikos Anita, Zsíros Péter (2018): *Incidens-menedzsment.* Dialóg Campus Kiadó, Budapest
- Hadarics Kálmán (2014): *Incidens-menedzsment gyakorlat.* Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, URL: http://archiv.vtki.uni-nke.hu/uploads/media_items/incidens-menedzsment-gyakorlat_-bcp_-drp-integracio.original.pdf Letöltés ideje: 2017. április 6.
- Tihanyi Norbert, Vargha Gergely, Frész Ferenc (2014): *Biztonsági tesztelés a gyakorlatban.* Budapest: NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, URL: http://archiv.vtki.uni-nke.hu/uploads/media_items/biztonsagi-teszteles-a-gyakorlatban.original.pdf, Letöltés ideje: 2017. április 6.
- Európai Hálózat- és Információbiztonsági Ügynökség (2006): *Részletes leírás a CSIRT-Csoportok létrehozásáról*, URL: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-hungarian/at_download/fullReport Letöltés ideje: 2017. április 15.
- Cert Coordination Center (2003): Handbook for CSIRTs, URL: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf Letöltés ideje: 2017. április 10.
- Európai Hálózat- és Információbiztonsági Ügynökség (2016): Incident Handling Management tananyag, URL: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/setting-upcsirt#Incident_Handling_Management, Letöltés ideje: 2017. április 15.
- Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone (2013): Computer Security Incident Handling Guide, URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, Letöltés ideje: 2019. október 30.

III. HADDAD RICHÁRD: OKOSESZKÖZÖK A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁKBAN, VILLAMOSENERGETIKAI FÓKUSSZAL

1. Bevezetés

A technikai fejlődésnek köszönhetően a 21. századi ember életkörülményei és szokásai már kevésbé függenek attól, hogy városban lakik vagy falusi környezetben. A felgyorsult élet és a kényelmi szolgáltatások az energia felhasználását a mindennapi élet alapvető részévé tette. Ma már csak akkor vesszük észre az energia fontosságát, amikor megszűnik a szolgáltatás. Számos rendszer és műszaki megoldás segíti a mindennapjainkat. Ezek a jelenleg kialakított rendszerek néhány kivételtől eltekintve egymástól függetlenül működnek, a bennünk keletkezett adatok, bár hasonlóságot mutatnak, mégis szeparált rendszerekben kerülnek felhasználásra. Egy háztartásban rengeteg adat keletkezik, amelyek különböző sávszélességű rendszereken valamilyen adat központba továbbítódnak. Itt lehet gondolni a mérési adatokra (fogyasztási adatok), de idetartozhatnak a vagyonvédelmi rendszerek (riasztók) adatai is.

Az energiaszektort is elérte a hatalmas technológiai fejlődés. Ma már a termelés, a szállítás és a felhasználás szolgáltatásai magasabb szinten vannak. A különböző piaci szereplők más és más motivációval rendelkeznek és eltérő a beruházási hajlandóságuk is. Ezt képet árnyalja a regionális, esetleg kulturális különbség. Az emberiség egyik legfontosabb célja, hogy a jelenleg növekvő ökológiai lábnyom növekedését megállítsa és egy fenntartható jövőkép mellett folyamatosan csökkentse. Ennek egyik eleme az intelligens hálózatok kialakítása, melynek része maga a fogyasztó is, aki ezáltal tudatosabban használja fel az energiát. Az intelligens hálózatok képesek magukba integrálni a megújuló energiaforrásokból előállított energiát, ezzel is segítve az üvegházhatású emisszió csökkentést. Arról sem szabad megfeledkezni, hogy az új technológiák serkentik a gazdasági folyamatokat és új munkahelyeket teremtenek.

Az Európai Unió két fontos alapdokumentuma[230] is rögzíti alapvető jogként a személyes adatok védelmét. Az intelligens rendszerek terjedése viszont lehetőséget biztosít arra, hogy a rendszer üzemeltetői a fogyasztói szokásokat már nemcsak aggregáltan ismerik meg (pl. alállomási szinten összegezve egy terület energiafelhasználási szokásait) hanem egyénre lebontva egyedi információkhoz is hozzájuthatnak.

Az intelligens eszközök és a kommunikációs csatornákhoz történő hozzáférés egyszerűsödése okán a ’90-es években kezdet elterjedni az M2M, azaz a *Machine to Machine*. Ezen rendszerekben a gépek egymás közötti kommunikációja lehetőséget adott az információk egyszerű cseréjére és parancsok végrehajtására.

Ezen kommunikációs rendszerek szimmetrikusan üzemeltek, azaz a két „gép” közötti csatorna mindkét irányban jól használható volt. Az évezred fordulón jelent meg egy új koncepció, amely már a szerver-kliens architektúra alapján az adatfeltöltést preferálta. Az újonnan kialakult aszimmetrikus kommunikációk folyamatosan a feltöltés lehetőségét fejlesztették, a letöltés kárára.

[230] Az Európai Unió Alapjogi Chartájának 8. cikkelye és az Európai Unió működéséről szóló szerződés 16. cikkelye.

A koncepció alapja sok okoseszköz, szenzor adatainak küldése egy központi helyre (Big Data), ahonnan rendszerszintű változásokat tudunk kezdeményezni a szenzorállapotok szerint. Ezen technológiákat hívjuk IoT-nak (Dolgok Internetének), ipari környezetben IIoT, azaz Industrial (Ipari) IoT-nek.

Jelenleg a piacon számos cég fejleszt megoldásokat, eszközöket és szoftvereket, és léteznek olyan rendszerek, melyek nyitott kommunikációs felületeket biztosítanak. Két fontos gondolat ütközik az okoseszközök fejlődése során. Az egyik az adatok sokrétű felhasználásának előnye, a másik a személyes adatok védelme. A következő évek feladata ezen két gondolat közötti egyensúlyt megtalálni. A jelenleg látható egyedi fejlesztések („do it yourself") láthatóan törekednek a szabványosság és a megfelelő adatbiztonság irányába.

2. IoT/IIoT a villamosenergetikában

2.1. AZ IoT és AZ IIoT fogalma

Az IoT (Internet of Things) és az IIoT (Industrial Internet of Things) fogalmát először 1999-ben Kevin Ashton[231] írta le a *Hogyan reptessünk egy lovat, avagy az alkotás, a feltalálás és a felfedezés titkos története* című könyvében. A könyv részletesen elemezte az internet lehetőségeit és a szerző szerint közel 50 PetaByte adat generálódott tisztán ember és gép kapcsolata során. Ám a jövőbe tekintve, az internetre csatlakozó gépek és szenzorok világának terjedésével, ez a feltöltött adatmennyiség a többszöröse lesz.

Az elmúlt évtizedben az IoT és az IIoT név alatt a kisvállalatoktól a multinacionális vállalatokig számtalan fejlesztés készült, amelynek a célja szenzorok segítségével okos rendszerek kiépítése. Ma már alig létezik olyan területe a gazdaságnak, ahol ne kezdődött volna meg az okoseszközök használata. Van már okos autónk, otthonunk, telefonunk, sőt, még a mosóporunk is okos. Az IIoT-koncepció lényege az okos gyár kialakítása, amely a hatékonyság növelését és az erőforrás-gazdálkodását célozza meg.

Az IoT/IIoT olyan szenzorok összessége, hálózati együttműködése, amelyben a tradicionális dolgok felkapcsolódnak az internetre, pl. idősgondozásra szoruló emberek helyzete és állapota, házikedvencek helyzete vagy a mosógépünk állapota.

„A széles körben elfogadott definíció szerint az Internet of Things olyan fizikai tárgyak, eszközök, gépek, berendezések és más »dolgok« által alkotott hálózatok, amelyek rendelkeznek beágyazott (embedded) elektronikával, szoftverekkel, szenzorokkal, kommunikációs egységekkel és az interneten keresztül képesek egymással kommunikálni."[232]

2.2. Az IoT- és az IIoT-rendszerek elemei

Az IoT- és az IIoT-rendszerek négy fő részből állnak:

- dolgok,
- átjárók,
- hálózat,
- központi alkalmazás.

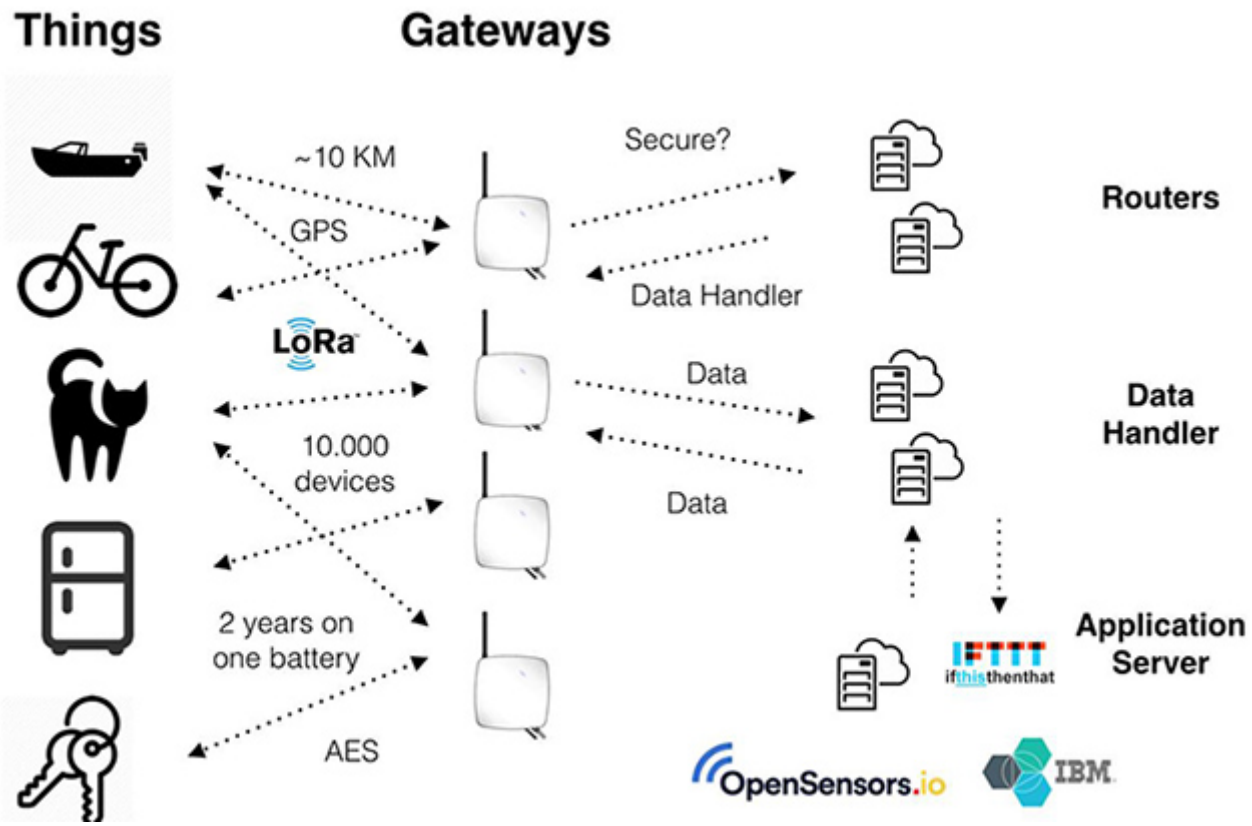
[231] Kevin Ashton angol kutató, filozófus. Ő fejlesztette ki az MIT egyetemen többek között a rádiós azonosítási technológiát (RFID), amely mára már az egyik legelterjedtebb azonosítási rendszer.

[232] Maros Dóra: *Internet of Things, azaz a Dolgok Internete.* Elektrotechnika, 2019/7–8.

A *Dolgok* (Things) alapvetően a rendszer végpontjai, amelyek lehetnek szenzorok, beavatkozók, azaz osztott intelligenciájú elektronikus eszközök. Fontos jellemzője a *Dolgoknak*, hogy egyedi azonosítóval rendelkeznek (pl. MAC address). A legtöbb esetben autonóm tápenergia (elemes) működéssel és rádiós kapcsolattal rendelkeznek.

Az *Átjárók* (Gateways) biztosítják a *Dolgok* és a *Hálózat* közötti kapcsolatot. Ezekről a *Hálózatokról* részletesen a 3.3. pontban lehet olvasni.

A *Hálózat* (Network) az az alapinfrastruktúra és fizikai környezet, amely biztosítja az adatok áramlását az adatforrás és az adatgyűjtőhely között.



1. ábra: Az IoT-hálózat felépítése
(Forrás: https://iot.ieee.org/newsletter/january-2016/building-a-crowdsourced-global-iot-network-operator.html*)*

> Az IoT/IIoT-rendszerek külső irányból legtámadhatóbb pontja a kommunikációs csatornák, amelynek zavarásával és kommunikációs protokollok biztonságának feltörésével a rendszer hozzáférhetővé válik. Egy IoT- vagy IIoT-rendszer gyakran alkalmaz különböző fizikai csatornákat, mindemellett területi kiterjedésük is nagy lehet.

A *Központi alkalmazás* (Application Server) olyan felhőalapú megoldás, amely gyűjti és kezeli a nagymennyiségű adatokat (Big Data) és megfelelő szoftverek segítségével felhasználja azt.

2.3. *Az IoT/IIoT-rendszer kialakításának kérdései*

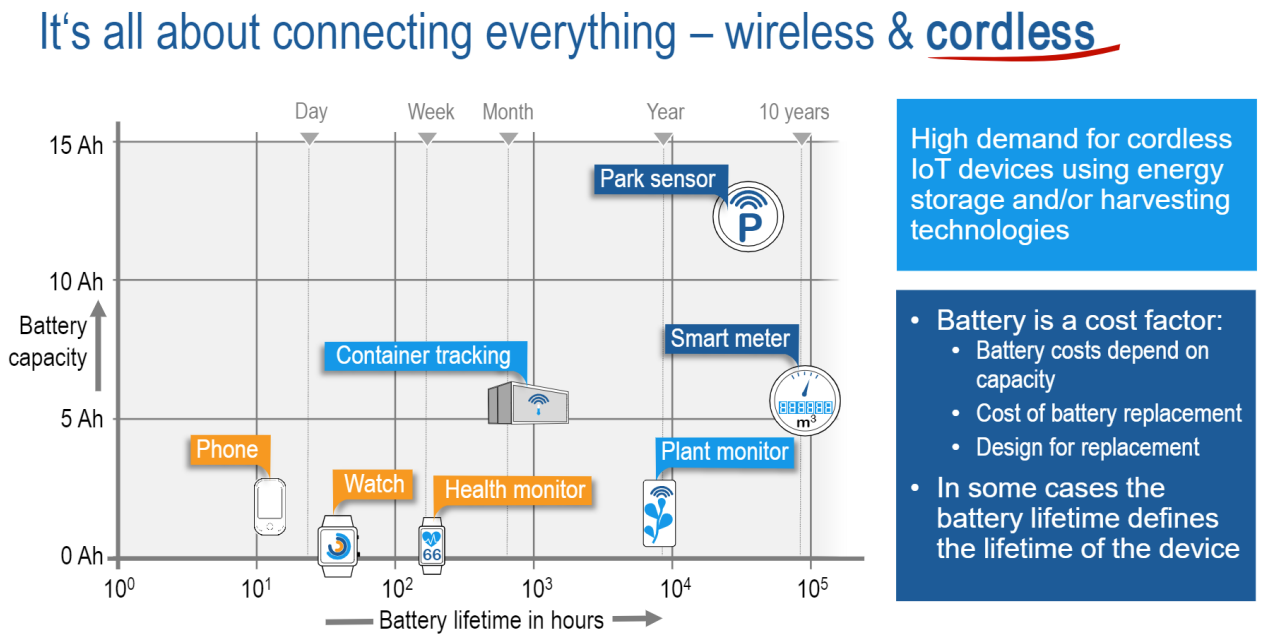
Villamosenergia hálózat esetén az IoT/IIoT-eszközök alkalmazásánál a következő alapkérdésekre kell választ adnunk:

- Milyen szenzorokra, aktorokra, beágyazott eszközökre lesz szükségünk, ezek milyen távolságra találhatóak egymástól, mekkora a hálózat tervezett mérete?
- Számíthatunk szélsőséges körülményekre (időjárás, szabotázs)?
- Környezetben vannak zavaró körülmények (rádiókommunikációs zavartatás)?
- Milyen a szenzorokhoz történő hozzáférés (karbantartás, üzemeltetés)?
- Mi az elvárt élettartam autonóm működés esetén?
- Milyen elérhető és gazdaságos technológia használható?
- Adatbiztonság, adatvédelem.

Az alapkérdések közül a megfelelő kommunikációs technológia megválasztása az egyik legkritikusabb kérdés. A rádióstechnológiák elérhetősége és beruházási költsége a legjobb, a havi díjak miatt a hátránya viszont a magasabb üzemeltetési ár.

A másik nagyon nagy kérdés az eszközök energiaellátásának lehetősége és az elvárt élettartam.

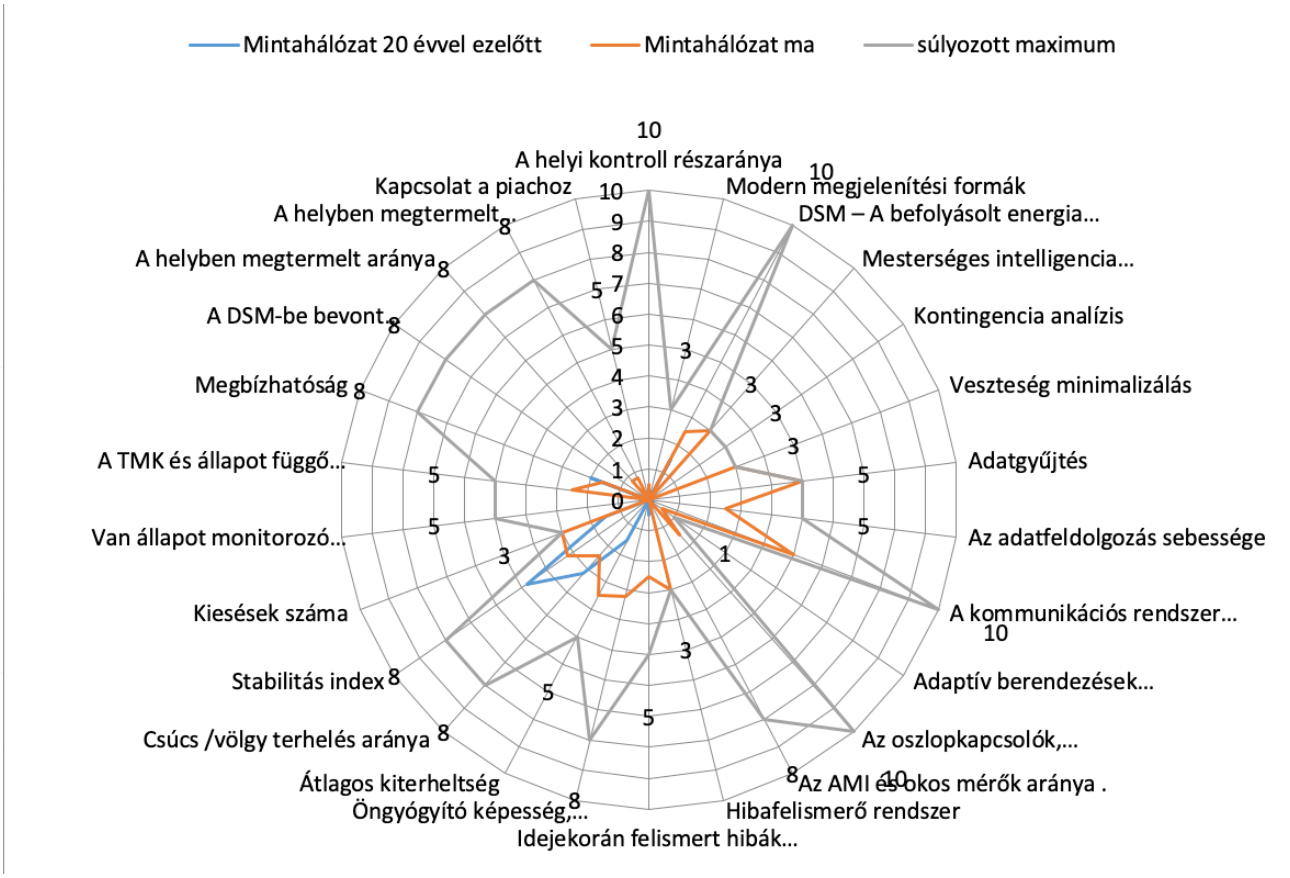
A következő *2. ábrán* összehasonlításképpen néhány eszköz elemes tápellátásának idejét látjuk. Jól látszik, hogy a mai okostelefonunkat felhasználás függvényében szinte naponta kell tölteni. A felhasznált elemkapacitás erősen függ a kommunikáció módjától, intenzitásától és időtartamától. További gondot jelent mozgó szenzorok esetében a térerősség változása. Ilyen mozgó egység tápellátása biztosan saját elemről kell, hogy történjen, hiszen a vezetékes energiaellátás korlátozza a mozgást. Maga az akkumulátor is komoly súlyt képvisel, amelynek mozgatása is energiát igényel. Ezért méretezéskor mindezek egyensúlyára figyelni kell. Speciális körülmények természetesen további szempontokat hozhatnak be. Tehenekre vagy kisállatra szerelt szenzor súlyánál tekintettel kell lenni a teherbíró képességre. Másik ilyen szélsőséges kritérium például a parkolóhelyekre bebetonozott parkolást segítő rendszer. Ebben az esetben az elemcsere a burkolat megbontásával jár, ami többszöröse egy szenzor költségének.



2. ábra: Autonóm működő eszközök energiakapacitása
(Forrás: Internet.)

Ezért 7 alapkövetelmény fogalmazódik meg egy rendszer kialakításánál, ami szenzorok együttműködését tartalmazza:

- alacsony bekerülési költség,
- távoli felügyelet, hibajavítás lehetősége,
- alacsony üzemeltetési költség,
- ha lehet, akkor multifunkciós érzékelő alkalmazása,
- miniatürizálásra törekedés a szenzoroknál,
- EMC-[233] összeférhetőség,
- magas adatbiztonság.



3. ábra: A hálózat okosságának mérése
(Forrás: Internet.)

Az „okos hálózat” fogalma nagyon nehezen definiálható, hasonlítható össze, tekinthető azonosnak más hálózatokkal. Ugyancsak nehezen mérhető, hogy egy villamosenergia-hálózat mennyire „okos”. Természetesen fontos az, hogy mérjük az okosság különböző szintjeit, amelyeket az egyes elemek már elértek.

3.1. Okos Hálózatok (Smart Grid)

A világban és itthon is megindult egy olyan irányú kutatás, amely keresi, hogy lokális struktúraváltoztatásokkal és új irányítási módszerekkel hogyan lehet a kisléptékű, új termelési lehetőségeket bekapcsolni az ellátásba (háztartási napelemes termelés), hogyan lesz a rendszer fogyasztóbarát és

[233] Az EMC – mivel az elektronikus rendszerek a környezetükkel állandó elektromágneses kölcsönhatásban vannak, így nem lehetnek elektromágneses zavarok forrásai vagy elszenvedői, ezáltal működési hiba előidézői.

hogyan lesz a fogyasztó „energiatudatos". A korszerű Informatikai Technológiák (IT) és az új energetikai eljárások a termelők és fogyasztók bonyolult rendszerének összehangolt működését valósítják meg, a termelést és ellátást biztonságosabbá, a helyi lehetőségekhez jobban illeszkedővé és a környezet szempontjából fenntarthatóbbá teszik.

A villamosenergia-termelés alapjai az utóbbi 120 évben szinte alig változott. A dinamikus igénynövekedés, a környezetvédelmi kihívások, a globalizálódó energiahálózatok az előnyök mellett problémákat is felvetnek.

Az Okos Hálózatokra persze számos definíció létezik. A National Energy Techonolgy Laboratory szerint egy modern hálózat[234] magába tud fogadni számos termelési fajtát (megújuló és nem megújulót egyaránt). A fogyasztókat energiatudatosságra sarkallja, energiamenedzsmentet alkalmaz. A hálózat rendelkezik öngyógyító képességekkel és ellenáll a külső támadásoknak. Preferálja a minőségi szolgáltatásokat és lehetőséget ad valós idejű adatok segítségével online energiakereskedelemre is. Optimalizálja az üzemeltetési költségeket az üzemidő meghosszabbítása mellett.

A KEMA holland tanácsadócég szerint[235] az okos hálózatok a következő tulajdonsággal bírnak:

- intelligens,
- jövőbe mutató, még nemigen létezik,
- a szolgáltatónak is át kell hozzá alakulnia,
- a fogyasztó aktívan részt vesz benne,
- minden termelést magára vesz, nem válogat,
- új termékek, piac,
- öngyógyító,
- kevésbé sérülékeny,
- fenntartható.

Egy másik előadás keretében[236] az alábbi értelemben használták az Okos Hálózat kifejezést:

- A digitális technológia átszövi az energiaszállítás minden részletét.
- Lehetőséget teremt az elosztott termelés integrációjára.
- Optimalizálja a hálózatot.
- A hálózat önjavító, megbízható, biztonságosabb, jobb hatásfokú lesz, miközben a fogyasztó is energiatudatossá válik.
- Mindez hozzájárul a fenntarthatósághoz, környezetvédelemhez.

Összeségében elmondható, hogy a cél a fogyasztói befolyásolás lehetőségének megteremtése, a termelésrendszer helyreállító képességének kialakítása. Fontos kérdés az energiatárolás költséghatékony kialakítása és a teljesítményelektronika széles körű alkalmazása.

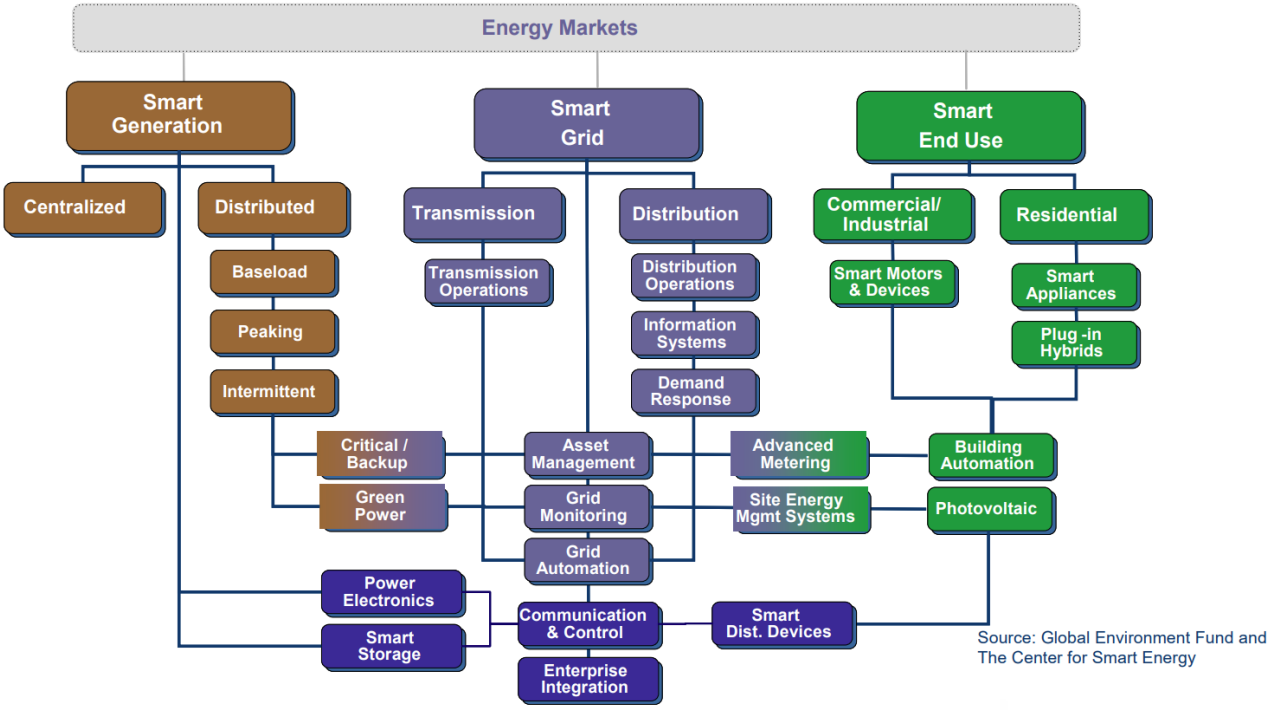
Az új innovatív megoldások és technológiák bevezetésével az energiaszektorban a kiberbiztonság (Cyber security) kockázati szintje is növekszik.

---

234 Modern Grid Initiative definíció; Modern Grid Initiative, National Energy Technology Laboratory, USA.

235 KEMA-definíció; Dr. Robert Wilhite, KEMA consulting: The Smart Grid vision for a Smarter Planet-előadás.

236 Smarter Grids for California and the Planet – KEMA's Perspective and Observations; CEC Workshop on Defining the Pathway to the California Smart Grid of 2020; Sacramento CA, August 5, 2008.



4. ábra: Okosenergia-koncepció
(Forrás: Global Environment Fund and The Center for Smart Energy.)

3.2. Okos Mérés (Smart Metering)

Az okos mérési rendszerek lehetőséget adnak arra, hogy a szolgáltatók és a hálózatüzemeltetők a végfogyasztókra lebontva képesek egyedi adatszolgáltatásra. Ennek az egyik legfontosabb előnye, hogy a fogyasztók az elfogyasztott energiával, valamint a hálózatban lévő energia költségével arányosan fizetik meg a felhasznált energiát. Mint ismeretes, a különböző napszakokban más és más energiaforrások (különböző költségen termelő egységek) érhetők el. Az okos mérési rendszerek transzparenssé tudják tenni a felhasználás és a költség mértékét. Az okos mérések ott hódítanak nagyobb teret, ahol a szabályozás legalább havonkénti leolvasást ír elő a szolgáltatók számára. Ez Magyarországon havonta 5,1 millió villamos- és 3,6 millió gáz-energiamérő leolvasását várná el a szolgáltatóktól. Az okos villamos-fogyasztásmérő élettartama min. 15 év (de elvárható a 20 vagy 25 év is). Gázmérők esetén ez az idő mindösszesen 10 év.

5. ábra: Okos mérő
(Forrás: https://www.networkedenergy.com/en/products/iec-ct-smart-meter)

Az okos mérőkre vonatkozó előírások országonként különbözhetnek. Az okos fogyasztásmérőnek legelső és legfontosabb feladata, hogy biztosítani kell a villamos energia mérését folyamatosan, rendszeres karbantartási igény nélkül, az osztálypontosságának megfelelően, a készülék hitelesítési ideje alatt. A fogyasztásmérő képes kezelni, gyűjteni az energia (kWh) és teljesítmény (Wh) adatait is. A kWh-adatok gyűjtése 3 tizedesjegy pontossággal történik.

Általános jellemzőjük, hogy kétirányú kommunikációval rendelkeznek, képesek a megmért adatokat eltárolni, kiolvasás esetén az adatokat időrendben visszaadni. A fogyasztásmérő képes a mérési adatokat önállóan, paraméterezett időközönként megküldeni a központi rendszer felé (push), illetve központi utasításra is képes rendkívüli, központi leolvasási igényre mérési adatokat továbbítani (pull). A mérő általában képes a tarifaregiszterek tárolására 30 hónapig. A mérőkből kiolvasott/leolvasott adatokat a mérési helyen min. 180 napig tárolja. Az adattárolási funkció a kommunikációs modulban vagy a smart villamosfogyasztás-mérőben valósul meg FIFO- (First in First out) rendszerű tárolással (15 perces adatintegrálási idő esetén).

A korlátozási teljesítményt vagy az áramhatárértéket külön regiszterben tárolja a készülék.

Az okos mérő többtarifás, egy- vagy háromfázisú, kétirányú (ad-vesz) elektronikus villamos fogyasztásmérő. Egyfázis esetén hatásos és meddőenergia mérésére (230V, 50Hz, Imax = 60A) alkalmas. A többtarifás, háromfázisú, kétirányú (ad-vesz) elektronikus villamos fogyasztásmérő hatásos és meddőenergia mérésére (3x230V/400V, 50Hz, Imax = 80A) is használható.

A fogyasztásmérők MID B osztályúak az MSZ EN 50470 szerint, illetve 2-es osztálypontosságúak a meddő- (az MSZ EN 62053-23 szerint) és a hatásos energia (az MSZ EN 62053-21 szerint) mérése esetén.

Terhelési görbe rögzítése esetén minimum 180 nap terhelési adatait rögzíti a fogyasztásmérő. (15 perces adatintegrálási idő esetén). Ezenfelül a fogyasztásmérő rögzítheti a különböző feszültségminőségi adatokat is, melyeknek intervallumai eltérhet az energiától: feszültségkimaradás, letörés, feszültségcsúcs, rövid idejű kimaradás. A mérőkben van lehetőség a rendszerből érkező távoli parancs hatására a fogyasztó teljesítménykorlátozására is.

A fogyasztásmérők folyadékkristályos (LCD) kijelzővel vannak felszerelve. Kijelzés: 7 karakter (abból 1 a tizedesjegy). Az alapértelmezett mértékegységek: kWh, kW, kVAr, kVArh. A kijelzőn az automata léptető az előre felprogramozott értékeket mutatja (paraméterezhető a léptetési idő 5 mp-től 15mp-ig), amely a nyomógomb segítségével megszakítható és kézzel léptethető a továbbiakban.

Egy okos mérő képes az alábbi státuszok kijelzésére is: riasztási események, kommunikáció, aktuális tarifa, leválasztó állapotának, valamint háromfázisú mérő esetén a fázisok állapotának kijelzésére. Van lehetőség a kijelző tesztelésére, amely elérhető funkció a kijelzőn megjeleníthető karakterek ellenőrzésére. A készülék regiszterében tárolt korlátozási teljesítmény vagy áramhatárérték a kijelzőn is megjeleníthető.

A naplófájl képes kb. 100 esemény tárolására, mely megvalósítása LIFO- (Last in First out) rendszerű tár szerint működik.

A naplófájl a következő eseményeket a bekövetkezést jelző időbélyeggel tárolhatja:

- teljes feszültségkimaradás,
- belső óra állítás,
- óra idővesztés,
- megszakító állapot változás,
- konfiguráció átprogramozás,
- firmware változtatás,
- szabálytalan események,
- fordított áramirány jelzése.

A fogyasztásmérő képes a fogyasztót leválasztani, illetve visszakapcsolást engedélyezni a hálózatra helyi, illetve a rendszerből érkező távoli parancs hatására. A megvalósítás beépített megszakító segítségével történik (Disconnector).

A központi rendszerből érkező előrefizetési információkat is fogadhatja. Az előrefizetési információk alapján központilag és a mérő saját maga is képes a lekapcsolásra. Képes megszakítani a fogyasztásmérő maximális áramát (Imax = 60A, ill. Imax = 80A). Hálózati hiba, zavar esetén a mérő kapcsolóműve (megszakító) a zavart megelőző állapotban marad.

A helyszíni felprogramozás és kiolvasás elvégzésére is van lehetőség egy optikai porton keresztül.

Az okos mérők helyszíni adatkapcsolatát biztosító optikai port mind hardveres, mind szoftveres védelméről gondoskodnak a szolgáltatók. Hardveres védelmet az egyedi plomba, a szoftveres védelmet többszintű jelszó használata teszi ki. Ezek kialakításakor alapvetően a szabálytalan vételezés elleni védelemet segítették. A technológiák fejlődésével a mérők egyre sebezhetőbbé válnak. A hálózatról leválasztva is 7 napig minimum működőképesek, hiszen belső tápenergia-ellátással rendelkeznek. Az elem cserélhető vagy rögzített. Cserélhető elem esetén az elem plombával védett, erre célszerűen kialakított foglalatban van elhelyezve. Az elemcsere a mérő feszültségmentesítése nélkül is végrehajtható, de a készülék naplózza az elemcsere tényét. Amennyiben a mérőben beforrasztott elemet alkalmaznak tartalék járatként, úgy annak élettartama megegyezik a mérő várható élettartamával. Az elem képes legalább hároméves összesített tartalék járat biztosítására minden funkcióhoz, amelynek tápellátást biztosít.

Az okos mérés egyik alapfunkciója a távoli kikapcsolás. Ez azt jelenti, hogy egy beépített kapcsoló (Disconnector) segítségével a szolgáltató képes a háztartást áramtalanítani távolról. Fontos biztonsági indokok miatt a visszakapcsoláshoz a felhasználó aktív közreműködése szükséges. Ez azt jelenti, hogy a szolgáltató a visszakapcsolást csak kezdeményezheti távolról, a tényleges kapcsolást a fogyasztónak kell elvégeznie. A távoli kikapcsolás lehetőséget ad előrefizetős mérési rendszer kialakítására is. Az előre megvásárolt energiamennyiség elfogyasztása után az Energiaszolgáltató lekapcsolja fogyasztót, és az új energiacsomag megvásárlása után a felhasználást engedélyezheti. Mindezt távolról megteheti, nem szükséges a fogyasztó zavartatása.

Léteznek többszolgáltatós rendszerek (Multiutility), ahol a villamos energia mérése mellett egy rendszerben leolvasásra kerül a gáz-, a víz- vagy a távhőmérő is. Itt egy infrastruktúra kiépítésével több rendszer működik együtt.

6. ábra: Okos gázmérők
(Forrás: https://www.fiorentini.com/hu/hu/product/components/gas-smart-meters)

Magyarországon kialakított többszolgáltatós rendszereknél a villamosfogyasztás-mérő gyűjti be az adatokat rövid hatótávolságú rádiós rendszer (wireless M-BUS protokoll) segítségével, majd az összegyűjtött adatokat továbbítja a központi adatgyűjtő rendszer felé.

Természetesen ez kiterjeszthető további szenzorok bevonásával, ezzel is javítva az alapinfrastruktúra megtérülését.

Néhány terület, amely kapcsolódhat az okos mérési rendszerhez:

- vagyonvédelem,
- okosotthon,
- egészségügyi felügyelet,
- kisállat-felügyelet,
- egyéb infokommunikációs szolgáltatás,
- SMART GRID-alapú vezérlés,
- elektromosautó töltésvezérlése,
- városi közlekedés támogatása (dugó figyelés),
- hírek, időjárás stb.

Néhány okos mérő technikai követelménye:

- Működési hőmérséklet: – 25 … + 70 °C.
- Páratartalom: ≤ 95%.
- Tárolási és szállítási hőmérséklet tartomány: – 40…+ 70 °C.
- Feszültségköri teljesítményfelvétel: ≤ 1W; 2,5VA (fázisonként kommunikáció nélkül).
- Áramköri teljesítményfelvétel: ≤ 1VA (fázisonként kommunikáció nélkül).
- Önfogyasztás a fogyasztásmérőre a kommunikáció során: ≤ 10W.
- Hálózati frekvencia: 50Hz (±5%).
- Lökőfeszültség-állóság (ki- és bemenetekre egyaránt): min. 6kV.
- Kettős szigetelésű készülékház elvárás (védelmi osztály II.).

A fogyasztásmérőház, a kapocstest és a kapocsfedél megfelelő védettséget nyújt tűzállósági szempontból. Az egyes alkatrészek túlterheltsége okozta melegedés nem okoz tüzet. A fogyasztásmérő megfelel a MSZ EN 60695-2-13:2001 szabvány követelményeinek, illetve lángállósági szempontból az UL-94 szabvány szerinti V0 előírásoknak.

Por és víz elleni védettségi foka IP51 az MSZ EN 60529:2001 szabvány szerint.

Az okos mérési rendszernek eleme még a fogyasztási adatok kijelzésére szolgáló otthoni kijelző (in-Home display). Ezek a kijelzők általában vezeték nélküli kapcsolatban vannak a fogyasztásmérővel és valahol a lakásban egy frekventált helyre kerülnek.

7. ábra: in-Home Display
(Forrás: https://www.bristol-energy.co.uk/smart-meters)

Az otthoni kijelzőkkel szemben támasztott követelmények a következők:

- Aktuális pillanatnyi teljesítmény megjelenítése Wattban kifejezve.
- Fogyasztás kijelzése: kWh.
- Az aktuális költség az adott időszakban.
- Szén-dioxid-kibocsátás kijelzése grammban.
- A fenti adatok átlagának, minimum- és maximumértékének, kijelzése különféle időintervallumokra vonatkoztatva.
- Előrejelzés megjelenítése az aktuális fogyasztási profilt feltételezve.
- Szabad szövegesüzenet-küldés lehetősége (pl. várható hálózatkimaradásról).

Fő feladata a fogyasztó tájékoztatása, a tudatos energiafelhasználás segítése.

Az okos mérési rendszer penetrációja az Európai Unióban a következőképpen alakult. A következő táblázat bemutatja, hogy a különböző tagállamok milyen mértékben és milyen intenzitással vezetik be az okos mérést.

EU-tagállam	Várható bevezetési arány 2020-ig	Bevezetés megkezdése	Bevezetés várható vége	Piac formája	Stratégia	Megvalósításért felelős/ tulajdonos	Adatgazda	Finanszírozás
Ausztria	Széles körű (80% vagy több okos mérő)	2012	2019	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Belgium	Nem széles körű bevezetés (< 80%)	-------	-------	Szabályozott	-------	Energiaszolgáltató	Energiaszolgáltató	-------
Bulgária	Nincs erre vonatkozó adat	-------	-------	-------	-------	-------	-------	-------
Horvátország	Nincs még adat	-------	-------	-------	-------	-------	-------	-------
Ciprus	Nincs erre vonatkozó adat	-------	-------	Szabályozott	-------	Energiaszolgáltató	Energiaszolgáltató	-------
Csehország	Nem széles körű bevezetés (< 80%)	2020	2026	Szabályozott	-------	Energiaszolgáltató	Adatközpont	-------
Dánia	Széles körű (80% vagy több okos mérő)	2014	2020	Szabályozott	Kötelező	Energiaszolgáltató	Adatközpont	Hálózati tarifák
Észtország	Széles körű (80% vagy több okos mérő)	2013	2017	Szabályozott	Kötelező	Energiaszolgáltató	Adatközpont	Hálózati tarifák
Finnország	Széles körű (80% vagy több okos mérő)	2009	2013	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Franciaország	Széles körű (80% vagy több okos mérő)	2014	2020	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	-------
Németország	Szelektív bevezetés	2014	-------	Versenypiaci	-------	Szolgáltató	Szolgáltató	-------
Görögország	Széles körű (80% vagy több okos mérő)	2015	2018	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	-------
Magyarország	Nem széles körű bevezetés (< 80%)	-------	-------	-------	-------	-------	-------	-------

EU-tagállam	Várható bevezetési arány 2020-ig	Bevezetés megkezdése	Bevezetés várható vége	Piac formája	Stratégia	Megvalósításért felelős/ tulajdonos	Adatgazda	Finanszírozás
Írország	Széles körű (80% vagy több okos mérő)	2014	2019	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Olaszország	Széles körű (80% vagy több okos mérő)	2001	2011	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák/ Energiaszolgáltatói erőforrások
Lettország	Szelektív bevezetés	2015	2017	Szabályozott	-------	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Litvánia	Nem széles körű bevezetés (<80%)	2014	2020	Szabályozott	-------	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Luxemburg	Széles körű (80% vagy több okos mérő)	2015	2018	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Málta	Széles körű (80% vagy több okos mérő)	2009	2014	Szabályozott	Önkéntes	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Hollandia	Széles körű (80% vagy több okos mérő)	2012	2020	Szabályozott	Kötelező/ kilépési opcióval	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Lengyelország	Széles körű (80% vagy több okos mérő)	2012	2022	Szabályozott	Kötelező	Energiaszolgáltató	Adatközpont	Hálózati tarifák
Portugália	Nem széles körű bevezetés (< 80%)	2014	2022	Szabályozott	-------	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák/ Energiaszolgáltató
Románia	Széles körű (80% vagy több okos mérő)	2013	2022	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák
Szlovákia	Szelektív bevezetés	2013	2020	Szabályozott	-------	Energiaszolgáltató	Energiaszolgáltató/ Adatközpont	Hálózati tarifák
Szlovénia	Nincs erre vonatkozó adat	-------	-------	-------	-------	-------	Energiaszolgáltató	-------
Spanyolország	Széles körű (80% vagy több okos mérő)	2011	2018	Szabályozott	Kötelező	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák/mérő bérbeadása
Svédország	Széles körű (80% vagy több okos mérő)	2003	2009	Szabályozott	Önkéntes	Energiaszolgáltató	Energiaszolgáltató	Hálózati tarifák/Energiaszolgáltató
Egyesült Királyság	Széles körű (80% vagy több okos mérő)	2012	2020	Versenypiaci	Kötelező	Szolgáltató	Adatközpont	Szolgáltatók

1. táblázat: Az EU-tagállamok okos mérés bevezetésének összefoglalása
Forrás: Saját szerkesztés.

A különböző országok okos mérési rendszerei természetesen különböző szolgáltatásokat biztosítanak. A napi egyszeri leolvasás mellett a fogyasztó tájékoztatást kaphat a környezetében élők átlagfogyasztásáról és ehhez viszonyíthatja saját fogyasztását, esetleg szolgáltatójától tippeket is kaphat fogyasztásának csökkentéséhez. Az adatok ilyenkor a felhasználó számára a szolgáltató által biztosított weboldalról érkeznek. Természetesen az okostelefonok elterjedésével a szolgáltatók egyedi alkalmazásokkal is segítik a fogyasztót a tájékoztatásban.

A napi egyszeri elolvasásnál sűrűbb, kis késleltetéssel kialakított rendszereknél a mérő és a szolgáltatói központ között az adatcsere „szinte" folyamatos. Ez az adatkommunikációs módszer egy részletesebb fogyasztáselemzést tesz lehetővé és célzott tanácsadással így az energiahatékonyság intenzitása növelhető.

Vannak olyan megoldások, ahol a rendszer automatikusan beavatkozik a felhasználónál (Demand Response) a fogyasztásba, és például a hálózatterheltség függvényében csoportosít át fogyasztásokat. Leggyakrabban a beavatkozás egy tarifarendszer szerint történik, de mindenhol a végcél egy dinamikus tarifarendszer üzemeltetése. A tarifa dinamitkáját a hálózat terheltsége adja.

Léteznek okos berendezések (Smart Appliencies), amelyek működésükben önállóan követik a hálózat terheltségét, ezekről részletesebben a következő fejezetben olvashatunk.

Az okos mérők egyik fontos tulajdonsága a távoli szoftverfrissítés támogatása. Egyrészről ennek komoly jelentősége van a mérők esetleges hibáinak tömeges javításában, de ugyanakkor komoly veszélyforrás külső informatikai támadás esetén.

3.3. OkosOtthon (Smart Home)

Az új kivitelezésű lakóparkokban és családi házakban elterjedőben van a lakásautomatizálás (Smart Home), melynek lényege, hogy a Felhasználó készülékei (Smart Appliencies) valamilyen hálózati kapcsolat révén kommunikálnak egy központi vezérlő/szabályozó egységgel. Ennek eredményeként a felhasználói készülékek működése valamilyen szintű „intelligenciával" vannak felruházva. Ezen intelligencia célja általában a következők valamelyikének (vagy mind a négynek) megvalósítása:

- Fogyasztói kényelem (komfort) növelése (távvezérlés, programozás).
- Fogyasztói energiamegtakarítás (pl. a szabályzási célérték módosítása).
- Fogyasztói költségcsökkentés (pl. energiavételezés alacsonyabb tarifájú időszakban).
- Fogyasztói biztonság növelése (pl. otthonlét szimulálása).

Egy okosotthon elemei és működésük nem különböznek más okos rendszerekétől. Az okosotthon lelke egy központi vezérlőegység, melyhez minden szenzor elküldi adatait és minden aktor innen kapja a vezérlő utasításokat. Az eszközök vezeték nélküli M-BUS-t vagy más szabványos kommunikációs rendszert használnak. Ilyen lehet a 2,4 GHz-es WiFi-csatorna is. Bár ilyenkor a protokoll mindig valamilyen saját gyártói protokoll, mivel a WiFit itt mint kommunikációs felületet definiáljuk.

Az okosotthon almérési rendszert is üzemeltet. Itt nemcsak villamosenergia-mérések történnek, hanem hőmérséklet-, hőmennyiség-, vízfogyasztásmérés is a rendszer része. Az órás villamosenergia-mérés mellett a pillanatnyi teljesítményt is képes elküldeni a mérő a központi vezérlőegységnek. A vezérlőegység ilyenkor saját adatbázisában gyűjti az adatokat.

8. ábra: Központi vezérlőegység
(Forrás: Internet.)

Az adatokat és a szenzorok állapotát vagy dedikált kijelzőn, vagy a felhasználó saját számítógépén láthatja. Az okostelefonok segítségével egyedi applikációkon keresztül a felhasználók akár távolról is nyomon követhetik a lakás paramétereit. Az applikáció szolgáltatásainak függvényében lehet díjmentes vagy magasabb szolgáltatási szint esetén fizetős szolgáltatás. A fejlettebb applikációk személyre szabható és egyedi adatokat is közvetíthet.

Ezekhez tartoznak az energia fogyasztási és teljesítmény adatok grafikus megjelenítése. Igény szerint az adatok megbontása választható időszakokra (napi, havi, éves ciklus). A tudatos energiafelhasználás egyik fontos eszköze az összehasonlítás. Az okosotthon szoftvere képes energia-, illetve költségalapon az összehasonlításra. A központi vezérlő segítségével a hőtárolós fogyasztók (pl. bojler, hőtárolós kályha), illetve más átmenetrendezhető fogyasztásokat is lehet távolról kapcsolni.

A kommunikációtól elvárható a megfelelő biztonság, ezért ilyen rendszereknél legalább 128 bites AES-kódolást alkalmaznak.

9. ábra: Beavatkozó eszközök
(Forrás: Internet.)

4. Háztartási villamosenergia-rendszerek és informatikai rendszereik

A háztartási villamosenergia-rendszerek informatikai kérdéseit alapvetően a felhasznált fizikai közeg jellege és távolsága szerint fogjuk vizsgálni.

A fizikai közeg szempontjából megkülönböztetünk vezetékes és vezetéknélküli megoldásra épülő rendszereket. Érdemes ezt tovább bontani a Hálózaton belüli kapcsolatok távolsága szerint. Így beszélhetünk nagy és rövid hatótávolságú alkalmazásokról. Harmadik szempont a felhasznált kommunikációs irány szerinti megkülönböztetés, hiszen a rendszerek között találhatunk egy irányba és két irányba kommunikáló rendszereket is.

Ennek a három ismérvnek a mentén kiválasztható a felhasználásra optimalizált kommunikációs megoldás.

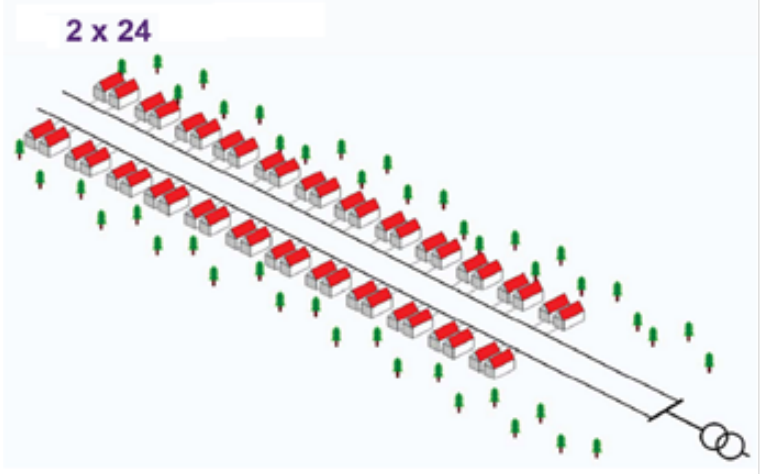
4.1. Vezetékes informatikai rendszerek

Vezetékes rendszer alatt olyan kommunikációs hálózati rendszert értünk, ahol a szenzorok egymással, illetve az átjárókkal, valamint a központi alkalmazással valamilyen fizikai szilárd vezetőn cserélnek adatot. Ez lehet:

- kommunikációs kábel (csavart érpárok),
- erőátviteli kábel (villamoshálózat maga),
- optikai kábel.

4.1.1. Rövid hatótávolságú vezetékes kétirányú kommunikációs rendszer

Olyan helyeken, ahol a szenzorok fizikai távolsága nem nagy (bérházak, lakótelepek fogyasztói) elérhetővé válik egy olyan megoldás, ahol vezetéken keresztül hatékonyan kialakítható a kommunikációs rendszer.



10. ábra: Rövid hatótávolságú vezetékes rendszer
(Forrás: Internet.)

A rövid hatótávolságú vezetékes megoldások egyik elterjedt formája az okosotthonokban használatos EIB/KNX-alapú szabvány szerinti rendszerek. Stabil, megbízható kommunikációt tesz lehetővé, de nagy hátránya, hogy nem elég rugalmas és utólagos kiépítése nagyon költséges.

Az erőátviteli kábelen történő kommunikáció PLC- (Power Line Communication) alapú megoldás lényege, hogy a kommunikációs közeg egyben a villamos hálózat maga. Így külön nem szükséges

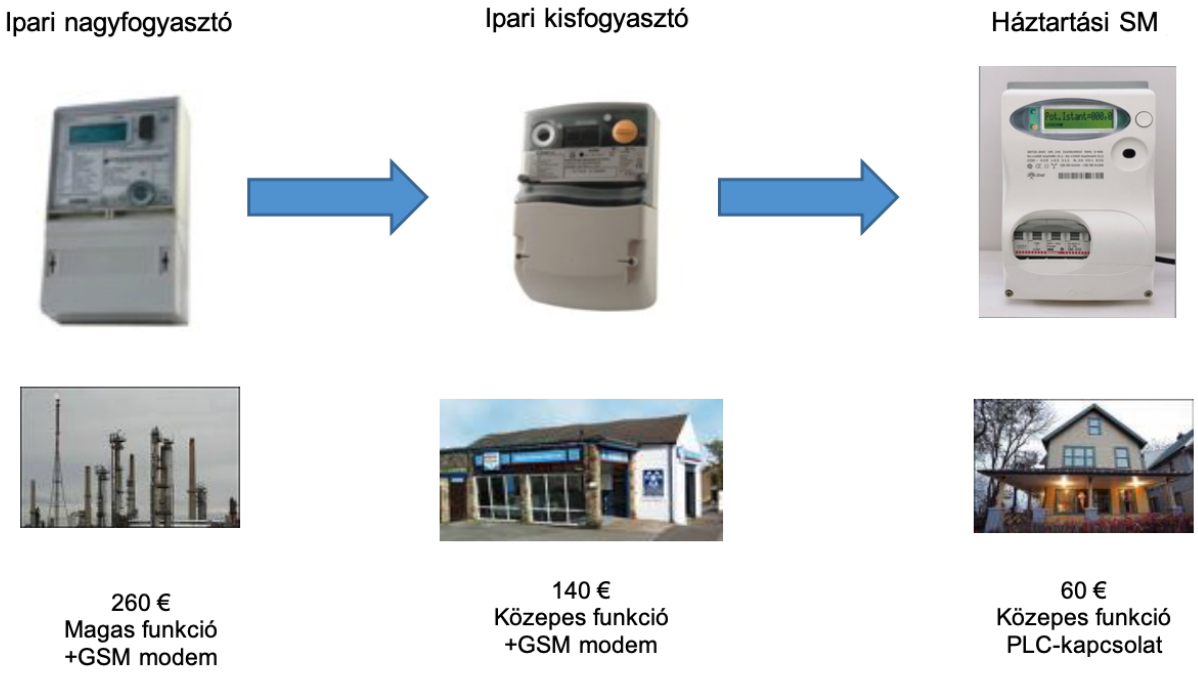
kommunikációs kábeleket kiépíteni. A hálózati jelre ültetett 50-90 kHz sávszélességű (S-FSK-moduláció CENELEC A-band) jellel nagyságrendileg 1200-2400 baudos átviteli sebességet érhetünk el.

A BPL (Broadband Powerline communication) ennek a fejlettebb és nagy sávszélességű változata. A mérők mindig egy koncentrátor vagy egy kuplung segítségével kommunikálnak, egy biztonságos csatornán, aminek több hitelesítő szintje is lehet.

Az adatküldés folyamatában az összes mérő a hálózatban képes megismételni ugyanazt az üzenetet, ezzel növelve a kommunikációs rendszer megbízhatóságát.

A jelenleg telepített PLC-alapú mérők fejlődésének útja visszanyúlik a ’90-es évekre, amikor még a nagy ipari fogyasztókat szerelték fel több tarifás kombinált mérőkkel és GSM-alapú leolvasással.

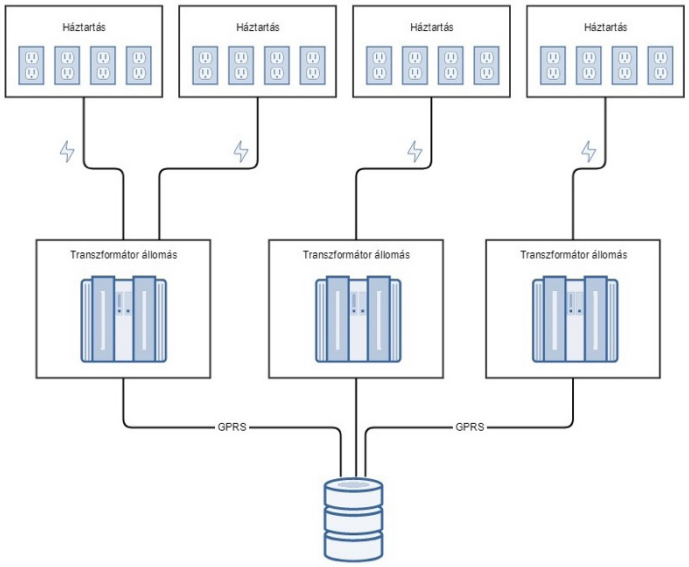
Az ipari mérők magas funkcionalitással és 1000 eurós árral rendelkeztek. 2000 után megindult a kis- és közepes fogyasztók mérési rendszerének fejlesztése és korszerűsítése, amelyre a merőgyártók alapjaiban hasonló, kisebb funkcionalitással bíró, így olcsóbb készülékkel léptek a piacra. A háztartási mérők tekintetében, már csak a tömeges gyártás és az elektronikai komponensek árcsökkenése tette lehetővé a PLC-s mérők megfizethetőségét.



11. ábra: Távleolvasható fogyasztásmérők evolúciója
(Forrás: Internet.)

A G3 PLC kommunikációs technológia megjelenésével egy gyorsabb és biztonságosabb adattovábbítás jött létre, akár nagyobb távolságokra is. Így már nagyobb mennyiségű adatokat is továbbítani lehetett. A G3 PLC kommunikációja már nem volt olyan érzékeny a hálózati zavarjelekre, és a korábbi generációs PLC-kel ellentétben, nagy „zajban” is képes megbízhatóan működni. A G3-as mérők nem csak a kommunikáció minőségén javultak, de IT-biztonsági szempontok szerint is lekörözik elődjeiket. Az új PLC-s technológia már tartalmazta a mérőnkénti egyedi titkosítást kulcsok segítségével. Ez egy aszimmetrikus titkosítási rendszer.

A fejlesztők arra is gondoltak, hogy a telepítést támogassák egy egyszeri előre definiált titkosító kulccsal, amely az első bejelentkezést követően módosult a mérő egyedi kulcsára.



12. ábra: PLC-alapú rendszerek felépítése
(Forrás: Internet.)

A háztartásokban felszerelt okos mérők egy helyi hálózatot kialakítva kommunikálnak. Az adataikat egy adatkoncentrátornak, ami a saját transzformátorállomásukban van elhelyezve, valamelyik PLC-protokoll segítségével juttatják el az adatokat. A helyi csomópontok, transzformátorállomások pedig mobil kommunikáció (GSM/GPRS/NB IoT) segítségével töltik fel az adatokat a rendszer központi adatbázisába, a mérési központba.

A háztartások felől érkező adatok a transzformátorállomásokon elhelyezett Gateway, adattovábbító eszközökön keresztül haladva egy viszonylag kis sávszéleségű csatornán kerülnek továbbításra a központ felé. Mivel manapság a kommunikációs költségek elég magasak, ráadásul az internetre kapcsolódó berendezések száma rohamosan nő, ezért sokszor az adattovábbító egyben egy intelligens berendezés is saját adattárolással. Így már optimalizált információ kerülhet a központi feldolgozás felé. A fogyasztók adatai viszont a transzformátorállomásokon is megtalálhatók, ez komoly biztonsági kockázat.

4.1.2. Nagy hatótávolságú vezetékes egyirányú kommunikációs rendszerek

Az energiaszolgáltatók célja a villamosenergia-felhasználás állandó szinten tartása a rendelkezésre álló erőművek egyenletes működtetésével, mert ennek a legkisebb a költsége is. Az energia felhasználása viszont erősen függ a lakosság életritmusától és az évszakok, valamint az időjárás változásától. Ennek megfelelően a napi fogyasztásban egy vagy több „terhelési csúcs”, valamint éjszakai „terhelési völgy” alakul ki.

Mivel manapság az energia tárolása Magyarországon egyelőre gazdaságosan nem lehetséges, az éjszakai többlet nem használható fel a nappali csúcsidőszakban, ezért a megtermelt mennyiséget a fogyasztáshoz kell igazítani. Ez azt jelenti, hogy az erőművek egy részét a völgyidőszakban vissza kell szabályozni vagy lekapcsolni a hálózatról. Ezért a szolgáltatóknak kezdetektől fogva érdeke volt a fogyasztói magatartás befolyásolása. Korábban kapcsolóórákat alkalmaztak, azonban ezek nem követték az időjárás változásait, illetve a rendszer teljesítőképességét. Ezt a rendszert ezért „passzív

vezérlési módszernek" nevezték. A rendszer fogyasztó általi befolyásolása jelentős volt, ami tarifális veszteségeket okozott a társaságoknak.

Így épült ki a hangfrekvenciás központi vezérlési, szabályozási rendszer. Hazánkban a központi terhelésvezérlés projekt 1970-ben indult. Az ELMŰ 10 évre rá indított fejlesztést majd a 90-es évekre be is fejeződtek és elmondható, hogy teljes körűvé vált a hangfrekvenciás központi vezérlés Budapesten és környékén 216,66 Hz-en, míg vidéken 183,33 Hz-en.

Napjainkban egyre fontosabb a természeti erőforrások optimális kihasználása, illetve az energiapiaci liberalizáció. A piaci szereplők szétválása megnehezítette a villamosenergia-felhasználás szabályozását és ezzel egy időben a felhasználók igényeinek gazdaságos és biztonságos kielégítését. A váltakozó áramú villamos energia nagy mennyiségben, gazdaságosan nem tárolható, ezért az erőművekben a fogyasztók pillanatnyi igényeinek megfelelő, valamint a hálózati veszteségeket fedező villamos energiát kell előállítani.

A teljesítménygazdálkodás egyik eszköze az engedélyesek kezében van azzal, hogy az ipari fogyasztókkal olyan szerződést köt, amelyben pontosan meg van adva a vételezett villamos energia mennyisége és a várható terhelési görbe a felhasználó részéről. Másik eszköz, hogy ha az engedélyes a nagyobb teljesítményű fogyasztókat saját maga kapcsolja, így a hálózat terheltségét növelheti, illetve csökkentheti igénye szerint.

A villamosenergia-felhasználás függ a mindennapi élettől, a hétköznapok, ünnepnapok változásától, az időjárástól, a televíziós műsoroktól, valamint a munkaritmustól. Ennek megfelelően a nap különböző időszakaiban más-más villamosenergia-igényt figyelhetünk meg. Az időpillanatokban vett minták alapján könnyen felrajzolható adott időszakra a napi terhelési görbe. A terhelési görbe alakulását sok tényező befolyásolja, ilyenek például a fogyasztók jellege, ipari és háztartási fogyasztók aránya és még sok más tényező. A napi terhelési görbén jellegzetesen két „púp" figyelhető meg. Ezek a délelőtti, valamint az esti csúcs. Az engedélyesek érdeke, hogy a terhelési görbét lehetőség szerint minél jobban kisimítsák, azaz a terhelési görbén jelentkező völgyeket feltöltsék, illetve a csúcsokat levágják.

Rugalmas központi vezérléssel könnyen megoldható a terhelés csúcsidőszakokban és völgyekben történő stabilizálása, biztosítva a termelt és a fogyasztott energia egyensúlyát. A hangfrekvenciás központi vezérlési rendszer technikailag olyan távparancsadó rendszer, amelynek átviteli útja maga az ipari frekvenciájú feszültség alatt levő energiaelosztó hálózat. Gazdaságilag olyan eszköz, amely alkalmas a villamosenergia-rendszer optimalizálására, ideértve a termelési, az átviteli, az elosztási és a fogyasztói optimum elérését. A kibocsátott jelsorozat frekvenciája speciális tört frekvencia, amely eltér a felharmonikus frekvenciáktól, pl. középfeszültségű csatolás esetén 183,33 Hz.

A hangfrekvenciás központi vezérlésről általánosságban elmondható, hogy felépítését tekintve egy egyszerű, egyirányú kommunikációs csatorna, amely adóból, átviteli útból és vevőből áll. Az adóberendezés feladata az adóközpontból érkező parancsok kódolása és a hálózatra ültetése. Az átviteli út maga a villamosenergia-hálózat vezetékrendszere. A fogyasztónál elhelyezett vevőkészülék kiszűri a hálózatból a parancsokat és a megfelelő kapcsolást végrehajtja.

Az adóberendezés több részből áll. Egy központi egységből, telekommunikációs csatornából, helyi vezérlőből és magából a hangfrekvenciás adóból, valamint illesztő szűrőből és csatolásból.

A kapcsolási parancsot tartalmazó impulzustáviratot a központi egységből a jelátviteli úton, amely általában egyszerű telekommunikációra használt vezeték, eljuttatjuk az adó ún. „jelfogadó" egységéhez, ahol a megfelelő berendezés előállítja a hangfrekvenciás jelet. Ezt a jelet a csatoló berendezéssel az 50 Hz-es elosztóhálózatra szuperponálják. Ha a vevőben felfogott jel (szűrő és amplitúdó diszkriminátor segítségével) dekódolás után megegyezik a központi vezérlőegység által generált impulzustávirattal, úgy a fogyasztónál a megfelelő kapcsolási parancs végrehajtódik.

Az adóberendezés feladata a kódtávirat aktív impulzusainak időtartama alatt olyan nagyságú és teljesítményű hangfrekvenciás feszültség létrehozása, amely a veszteségek fedezése után is elégséges a vevők működtetéséhez. A mai adók statikus, félvezetőkkel megvalósított főáramkörök és integrált áramkörű vezérlőáramkörök.

A főáramkör a teljesítményét a 0,4 kV-os 50 Hz-es hálózatból nyeri, így az adó lényegében egy frekvenciaváltó, amely az 50 Hz-es feszültségből néhány száz kVA teljesítményű hangfrekvenciás feszültséget állít elő.

A csatolás egyik lehetséges megoldása a soros csatolás. Ebben az esetben minden középfeszültségű kivezetésben telepíteni kell HKV-adóberendezést. Két fajtája van: csatolás áramváltóval, illetve transzformátorral. Előnye a nagy terhelhetőség, hátránya, hogy érzékeny a hálózat üzemének zavaraira.

A vezérlési információt a hangfrekvenciás jel feszültsége hordozza, amit az adóberendezés impulzusok sorozata formájában állít elő. Ez az impulzustávirat a hálózaton az 50 Hz-es feszültséggel együtt terjed, egészen a hangfrekvenciás vevőkig, ahol szűrő segítségével választjuk le a hálózatról, majd a kapott táviratot a vevő összehasonlítja a memóriájában tárolt programmal és egyezőség esetén kapcsol be vagy ki. Egy távirat átviteli ideje 40-60 másodperc.

Lehetőség van az adók párhuzamos csatolására is. Ezt a megoldást az ELMŰ 120 kV-on alkalmazta. Előnye, hogy kevesebb adóberendezéssel lehet több állomásban biztosítani a jelszintet. A hangfrekvenciás jelet (216,66 Hz) szigetelt transzformátor, csatoló induktivitás és csatolókondenzátor segítségével ülteti a hálózatra.

A jelenlegi HKV-rendszer a feladatát megfelelő üzembiztonsággal ellátja. A vevők kb. egyharmadának életkora meghaladja a 25 évet, de éves szinten a meghibásodott vevők aránya még mindig csak 1-2% között van. Tömeges cseréjükkel várhatóan 5 éven belül számolhatunk. Jelenleg éves szinten több mint tízezer vevőt vásárolnak a társaságok meglévő vevők cseréjére, új bekapcsolásra. Általában elmondható, hogy az adó- és vezérlőberendezések a várható élettartamuk utolsó harmadába léptek, a csatolók pedig élettartamuk felénél járnak. A szükséges karbantartási, üzemeltetési ráfordítások ellenére az üzembiztonság, üzemfolytonosság fenntartása érdekében középtávon várhatóan meg kell kezdeni az adók rekonstrukcióját.

A ma ismert tömegvezérlési funkciók, amelyek általánosságban a következő vezérlési helyeken alkalmazzák:

- hőtárolós fűtő készülékek vezérlése,
- forróvíz-tároló készülékek vezérlése,
- háztartási kiserőművek szabályozása (Németország),
- csúcskizárás és templomfűtés,
- tarifakapcsolás kisfogyasztói,
- tarifakapcsolás alapdíjas és lakossági fogyasztók esetén
- közvilágítás-vezérlés egész éjjel,
- közvilágítás-vezérlés féléjszaka,
- díszvilágítás,
- tűzijáték-elsötétítés,
- geotarifa.

További lehetőségek a jelenleg ismert funkciókon túl, amelyek bevonhatók a tömegvezérlésbe:

- teljesítménygazdálkodás,
- terheléskorlátozás,
- klímavezérlés,
- e-mobility, villanyautók töltésvezérlése,
- szirénavezérlés, katasztrófavédelem.

Az Okos Hálózat kialakításában a központi vezérlés jelentős szerepet játszhat. Egyrészről egy meglevő rendszer, így beruházási költséget nem jelent. Fenntartási és szolgáltatási költségben elhanyagolható. Az Okos Hálózat- és Okos Mérés-fejlesztésekben kevés figyelmet kap a központi vezérlés. Ez azzal magyarázható, hogy ahol nincs meg a központi vezérlés infrastruktúrája, ott már nem látják

célszerűnek a kiépítést. Abban bíznak, hogy az okos mérési rendszer részeként a fogyasztók a kétirányú hírkapcsolatokkal – vezetékre telepített (PLC-s) és a vezetéknélküli (pl. ZigBee) – uralható lesz.

A különböző gyártók kétfajta, szabványosított egyirányú adatátviteli protokollt használnak a 200 Bd-os hosszúhullámú kommunikációs csatornán. Az egyik a DIN 43861-401 Typ A, vagy népszerűbb nevén Versacom, a másik a DIN 43861-402 Typ B, vagy népszerűbb nevén Semagyr Top. Mindkettő a HKV-rendszerekben alkalmazott protokollokból jött létre.

A Semagyr Top a Landys&Gyr gyártói protokolljából nőtte ki magát DIN-szabvánnyá. Alapjai még a bájt szervezésű világ előtt, az analóg áramkörökön megvalósított pulzus alapú HKV-kommunikációra készültek, aminek jellemzőit az RKV-ra (Rádiós KörVezérlés) átfogalmazott szabvány is megtartotta, azaz az információs egységek nem byte-határra esnek, hanem eshet a fele az egyik, másik fele a másik bájtba. Ezzel együtt is egy nagyon jól használható, sok lehetőséget és rugalmasságot adó protokoll. Címzési rendszere elsődlegesen a vevőkészülékeket, azok csoportjait célozza. Adatátviteli parancsai pedig nem közvetlenül a relék ki-, bekapcsolását kezdeményezik, hanem kisebb programok, algoritmusok futtatását, amelyek tartalmazhatják a fizikai relék kapcsolását is, de nem szükségszerűen.

A Versacom több gyártó által közösen megformált, szintén elsődlegesen HKV-rendszerekre fogalmazott szabvány. A Semagyr Tophoz viszonyítva egyszerűbb, könnyebben megérthető, de kevesebb lehetőséget és rugalmasságot adó rendszer. Címzési megoldásának központjában nem a készülékek, hanem a relék és relécsoportok állnak. Adatátviteli parancsai zömében az egyes relék ki-, bekapcsolásaira vonatkoznak.

Az EON németországi és magyarországi cégei a Semagyr Top-protokollt használják, amely jelenleg semmilyen kódolást nem tartalmaz.

4.2. Vezeték nélküli informatikai rendszerek

A rövid hatótávolságú (short range, pár tízméter) technológiák esetében a legismertebb jelenleg a bluetooth, illetve az RFID és az NFC. Ilyen technológiákat tipikusan kis fogyasztású, kis átviteli sebességet igénylő alkalmazásoknál (max. néhány kbit/s) és területileg is korlátozott lehetőségek mellett használhatjuk. A bluetooth elterjedését segíti a különböző felhasználástámogatás. A bluetooth-t a mindennapokban az egyszerűsége miatt használjuk, mint telefonos kihangosító, okosóra vagy egyszerű adatátvitelként két telefon között.

A már kicsit nagyobb hatótávolságra (pár száz méterre) és nagyobb sávszélességű igényre egy még népszerűbb kommunikációs megoldás terjedt el, a WiFi, ami az IEEE 802.11 szabvány szerinti működő rendszer. Felhasználásuk igen széles körben elterjedt, az egyszerű otthonoktól, a nagy irodaházas rendszerekig, de szinte mindenki keresi az okos készülékével. Ma már népszerű helyek, közösségi terek elképzelhetetlenek WiFi-csatlakozás nélkül. A szálláshelyek (szállodák, panziók) alapszolgáltatásai között megtalálható. Jelenleg két frekvenciasávban működnek ezek a rendszerek, a 2,4 és az 5 GHz (ezek úgynevezett szabadfelhasználású [ISM] sávok, amelyeket bármilyen más eszköz is, nem csak WiFi-eszközök használhatnak). Ennek a két sávnak nagy előnye, hogy a levegőben jól terjed, így nem csak beltéren, de kültéren is jól használható.

Ha az IoT/IIoT-rendszerünket az ISM-sávra tervezzük, szembe kell nézni azzal a problémával, hogy ezen a frekvencián más rendszerek (riasztók, kamerarendszerek) is működnek. Bár a szabvány korlátozza ebben a tartományban is a rádiós jelek teljesítményét, előfordulhat, hogy az eszközeink nem tudnak kommunikálni. Ezért a tervezés során együttélhetőségi vizsgálatokat célszerű lefolytatni.

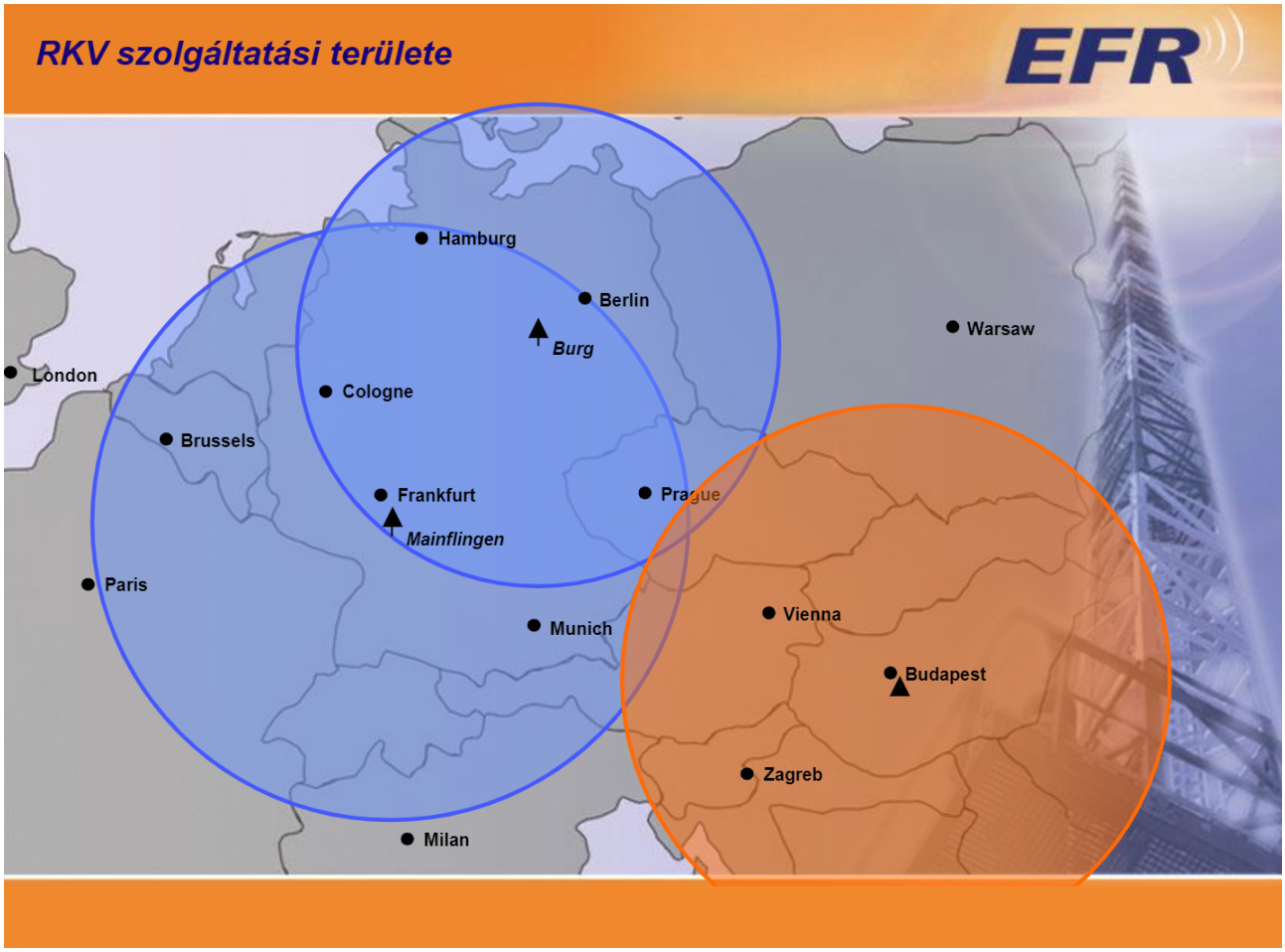
4.2.1. Nagy hatótávolságú vezeték nélküli egyirányú kommunikációs rendszerek (RKV, Rádiófrekvenciás Központi Vezérlés)

A HKV-rendszerek mellett a rádiós központi vezérlés (RKV) megjelenésével a rendszerek felhasználási lehetőségei jelentősen javultak. Egyrészről a táviratok hossza akár néhány másodpercre rövidíthetők, működik egyedi címzés, a realtime óra 1 msec pontosságú. Az RKV szóba jöhet – mivel a működtető irányban teljeskörű – az összes kapcsolási utasítás kiadásában, a kapcsoló berendezések távműködtetésében is.

Részletes vizsgálatot jelenthetne majd az IoT/IIoT területén is az RKV beintegrálása. Egyrészről költséghatékonyságot jelent az RKV beintegrálása, másrészről az Okos Mérés lényeges funkcióinak – tarifaváltás, terhelésvezérlés és a realtime óra – megbízhatóságát növelné. A mérők távkiolvasásának megbízhatósága többszörös próbálkozással jelentősen emelhető, míg a tarifaváltás, fogyasztásvezérlés késlekedést nem visel el. Az okos mérők kommunikációs egysége alacsony költséggel kiegészíthetővé válna egy ún. RKV-chippel (2-3 eurós költség).

A rádiófrekvenciás központi vezérlés szintén tömegvezérlési feladatok ellátására készült. Korábban az RKV-szolgáltatást kizárólagos joggal az EFR CEE Kft. cég végezte Magyarországon a lakihegyi adóberendezés segítségével, amit az Antenna Hungária vett át.

Az adó terepviszonyoktól, adóteljesítménytől függően akár 1000 km távolságra is eljuttathatja a vezérlőinformációt 200 Baud sebességgel. Így a teljes Kárpát-medencén túl Csehországban is fogható a vezérlőjel.



13. ábra: Rádiós körvezérlés lefedettsége Európában
(Forrás: http://www.mee.hu/files/images/5/EFR_general_HU_25_Juni_09.pdf.)

Az RKV a HKV-hez hasonlóan egyirányú kommunikációt tesz lehetővé, és hasonló feladatok ellátására alkalmazható, úgy, hogy egy központi helyről nagyszámú végpontra tudja eljuttatni a vezérlőinformációt hosszúhullámú rádiójel segítségével. Előnye, hogy a felhasználónál nem igényel adóberendezést, csatolókat, így csökken a hálózatveszteség. Egy távirat kiadásának ideje töredéke a HKV-táviratnak.

Az RKV-állomás egyszerű PC, standard Windows operációs rendszerrel és szerverrel működik. Feladata a táviratok létrehozása és változtatása. A központi egység kommunikál a felhasználói állomásokkal. A rádiófrekvenciás jelek továbbítására azokat a felületi hullámokat használják, amelyek követik a föld görbületét.

Az RKV-rendszernek számos előnye van:

- szinte korlátlan külön címezhetőség valósítható meg,
- gyorsabb táviratküldés,
- a rendszer alapvetően a vevők önálló, belső program szerinti működésére épít,
- nem kell adóra beruházni,
- központi órajel szinkronizálása folyamatosan,
- nincs adóüzemeltetési költség,
- jelentős mértékben csökken a rendszer üzemeltetéséből származó hálózati veszteség,
- földrajzilag független.

Tényleges előnyt a következőkben lehet megfogalmazni:

- nincs szükség saját tulajdonú adóberendezésekre,
- nincs szükség párhuzamos csatolás esetén külön mezők üzemeltetésére,
- alállomási berendezések egyszerűsödnek, kevesebb hibaforrás (elmaradnak a csatolók, csatoláskapcsolók, adóberendezések, vezérlő konzolok stb.),
- üzemeltetés egyszerűsödik,
- csökken a hálózati veszteség.

4.2.2. Nagy hatótávolságú rádiós kétirányú kommunikáció

A közepes vagy nagyobb sávszélességű rendszerigények esetén a GSM-hálózatok adhatnak megoldást. A GSM-rendszernek az evolúciós fejlődése során folyamatosan változott az adatátviteli sebessége, bővültek szolgáltatásai. Ezt a megoldást olyan helyre célszerű telepíteni, ahol nincs más elérés. A GSM/GPRS-hálózat segítségével egyszerűen kapcsolhatjuk a rendszerbe a végpontjainkat.

A jelenleg elérhető rádiós szolgáltatások választéka nagy. Figyelembe kell venni a rendszer lefedettségigényét, az igényelt sávszélességet, esetleges elemes működést. Az IoT/IIoT-eszközök tipikusan két szolgáltatási csoportot vesznek igénybe:

- GSM 2G (GPRS – esetleg 2,5G EDGE),
- Narrowband (NB) IoT.

14. ábra: Mérő egy GSM/GPRS-modemmel RS-232-n keresztül
(Forrás: Internet.)

GSM 2G esetén gyakran használják az okos mérőket egy megfelelő kommunikációs port segítségével.

A port lehetőséget ad távprogramozásra és kiolvasásra egy GSM/GPRS- (EDGE-) modemen keresztül.

A modem ilyenkor a mérőtől kap táplálást, így könnyen telepíthető és konfigurálható.

A modem védett az elektromágneses zavarokkal szemben (EMC) és a kezelő felületén (GSM-modem esetén a SIM-kártyatartót) leplombálható az IEC/EN 60950 szabványnak megfelelően.

GSM 2G- és 2,5G-modemmel szembeni elvárások:

A GSM-modul minimum 10-es osztályú GPRS-technológiát kell használjon, 300 bps-től 57 600 bps-ig terjedő sebességgel, külső vagy belső antennás kapcsolattal.

Az adatokat a kialakított védett csatornán (VPN) keresztül juttatják el a központi rendszer szervereire.

A homogenitást megtartva minden ilyen mérőt, ami egy GSM/GPRS-modemhez csatlakozik, egy virtuális adat koncentrátorként kezelnek a mérési központban.

A fejlettebb generációs megoldások (3G–4G és nemsokára, remélhetőleg, széles körben elérhető az 5G is) alkalmazása sokkal költségesebb. Fontos megjegyezni, hogy a mobilszolgáltatók a 3G és 3,5G rendszerek kikapcsolását tervezi, így hosszú távon ezen technológiák nem lesznek elérhetőek. A magasabb generáció magával hozza a magasabb szintű szolgáltatási szinteket (Quality of Service, QoS), mivel ezek esetében a rádiós tornyok telepítése sűrűbb. Összehasonlítva a WiFi-rendszerekkel a biztonság, a sebesség és a költség viszonylatában, elmondható, hogy egy magasabb biztonsági szinttel (SIM-kártyás egyedi azonosítással és Layer 2 védelmi szintekkel), sávszélességben megfelelő, bár költségesebb megoldásról beszélünk.

A piaci igény abba az irányba mutatott, hogy az IoT/IIoT-rendszerek terjedéséhez szükség van olyan Hálózatra, amely egyesíti a GSM szolgáltatásaihoz hasonló, de a WiFi előnyeit is magában ötvöző, megoldást. A GSM-lefedettség, bár megfelelő mértékű, de a havi költségét az IoT-rendszerek nem bírják el. Erre a problémára született válasz a LPWAN- (Low Power, Wide Area Network) technológiák, amelyek egy másik ISM-sávban a 868 MHz-es frekvencián működnek. A világban számos rendszer került kifejlesztésre, hogy ebben a szabadadon felhasználható sávban, ahol sok eszköz működik (távirányítók, hangrendszerek stb.), zaj alatt működjenek. Két rendszer ért el nagy eredményt: a LoRa és a Sigfox. A LoRa- és a Sigfox-rendszer közötti különbség, hogy míg a LoRa egy szabadon felhasználható technológia, addig a Sigfox egy francia cég által licencelt megoldás. Mindkét rendszerre jellemző, hogy kicsi a zajérzékenysége, elemes működést támogat és nagy kiterjedésű rendszerekben is használható.

Magyarországon telepített infrastruktúraként már üzemel a Long Range WAN (LoRaWAN), amit az Antenna Hungária üzemeltett, emellett elérhető a Sigfox-rendszer is, amit az Omnicell Hungary kínál.

Az újonnan megjelenő igényekre a mobilszolgáltatóknak is lépniük kellett. Hiszen az IoT/IIoT-üzlet robbanás előtt áll. A mobilszolgáltatók saját frekvenciatartományukban kerestek megoldást. A rádiófrekvenciák felhasználásával foglalkozó világszervezet, a Nemzetközi Távközlési Unió (ITU), felismerte ennek a kérdésnek a fontosságát, és olyan frekvenciakiosztást alakított ki, ami lehetőséget biztosít a mobil szolgáltatóknak olyan szolgáltatás kialakítására, ami versenyképes az IoT területein.

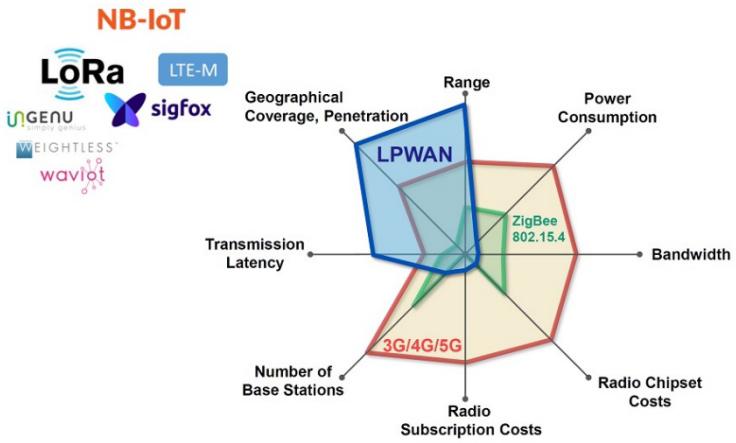
Ezt az új keskenysávos részt nevezik NarrowBand IoT-nek. Ez a megoldás támogatja az elemes, kis energiafelhasználású modulok alkalmazását. Ma már több hazai mobilszolgáltató is kínál NB IoT-megoldást.

A 16. ábrán összehasonlításra került a három vezeték nélküli technológia:

- rövid hatótávolságú (ZigBee),
- LPWAN (LoRa, Sigfox),
- GSM-szolgáltatós megoldás (NB IoT).

Az értékelési szempontok:

- hatótávolság (Range),
- energiafogyasztás elemes működés esetén (Power Consumption),
- sávszélesség (Bandwidth),
- rádiós modul bekerülési költség (Radio Chipset Costs),
- hálózathasználati költség (Radio Subscriptiopn Costs),
- rádió bázisállomások száma (Number of Base Station),
- üzenetküldés hossza (Transmission Latency),
- földrajzi lefedettség (Geographical Coverage, Penetration).



15. ábra: Vezeték nélküli kommunikációs megoldások összehasonlítása (Forrás: Internet.)

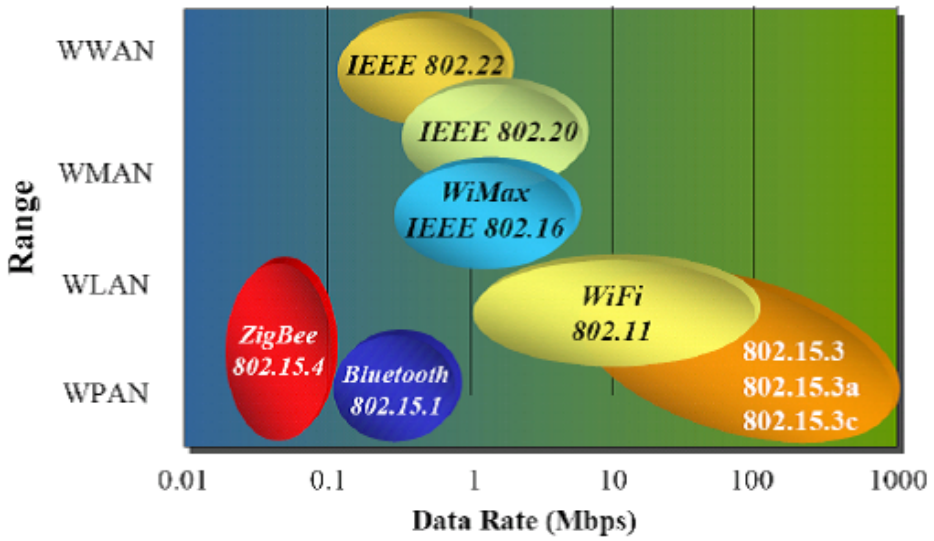
Ezen értékelési szempontok alapján, az LPWAN-technológiák a legalkalmasabbak az IoT/IIoT felhasználására, mivel alacsony a rádiósmodul bekerülési és üzemeltetési költsége, magas lefedettség érhető el alacsony számú rádióállomás telepítésével. Mindezen felül kicsi az energia működési igénye, ezért elemes megoldással hosszú ideig használható. Egy paraméterében gyenge, ez pedig a sávszélesség, de ez IoT/IIoT-rendszernél nem elvárás.

4.3. Rövid hatótávolságú vezeték nélküli rendszerek

Nemzetközi téren látható, hogy a ZigBee-protokoll legutóbbi változatai egyre jobban terjednek, ezért részletesen megvizsgáljuk a működését.

2010-ben egy ZigBee-konferencián, a következő nyitómondat szerepelt egy felvezető előadásban: „ZigBee THE open standard for Wireless Sensor Networks", azaz, a „ZigBee a nyitott szabvány a vezeték nélküli szenzorhálózatokban"[237].

A piac különböző szereplőitől természetesen olvashatunk különböző véleményeket. Vannak, akik az egész vezeték nélküli technológiát nem tartják alkalmasnak sem háztartási (IoT), sem ipari környezetben (IIoT) történő nagyszámú végpont megbízható adatátvitelére, és akik alkalmasnak is találják, azok is különböző technológiára esküsznek. A szabványalkotók természetesen folyamatosan próbálják követni a piaci igényekből származó innovatív megoldások által generált fejlesztéseket. Ez a változás folyamatos, újabb és újabb fejlesztések jelennek meg.



16. ábra: Vezeték nélküli kommunikációs szabványok
(Forrás: Internet.)

4.3.1. Az IEEE 802.15.4 szabvány

Az IEEE 802.15.4 szabványt 2003 óta kifejezetten az alacsony átviteli sebességű rövid hatótávolságú vezeték nélküli technológiákra fejlesztik. Ezt a technológiát LR-WPAN-nak nevezi (Low-Rate Wireless Personal Area Network). Ebbe tartozik a ZigBee is, amelyen keresztül bemutatásra kerül a rendszer architektúrája. A megoldást PAN (Personal Area Network) létrehozására szokták alkalmazni, ami azt jelenti, hogy az eszközök az egyén körül hoznak létre hálózatot.

[237] ZigBee Developers Conference – 2010. április 27, München – Keynote, Bob Heile)

17. ábra: Okosotthon PAN-technológiával
(Forrás: Internet.)

Ezen IEEE 802.15.4-hálózatok egyik legfontosabb tulajdonsága az önkonfigurálás és az öngyógyító képesség. Ez azt jelenti, hogy a benne működő egységek a hálózatot önszervezéssel úgy hozzák létre, ahogy a kommunikációs lehetőségek adják. Ennek a lehetőségeknek a megváltozása esetén, képesek újrakonfigurálással öngyógyító szolgáltatásokat biztosítani. Ehhez a szövevényes (Mesh) hálózati topológiát használják.

Felhasználási területek:

Energiahatékonyság és -menedzsment, amelyben a fogyasztót támogatja azzal, hogy energiafogyasztásról több információt szolgáltat, támogatja az energiafelhasználás felügyeletét, több lehetőséget és szolgáltatást nyújt a felhasználónak az energiaforrások hatékonyabb felhasználására és ökológiai lábnyomunk csökkentésére. A másik nagy terület az Okosotthon, ahol a kényelem és hatékony szolgáltatás biztosítása kifejezetten az otthoni felhasználók számára a világítás, hűtés-fűtés, biztonságtechnika és szórakoztató elektronika felügyelete, integrációja és távirányíthatósága révén az egész lakáson belül. Idetartozik még az egészségügyi állapot- és a kisállat-felügyelet is.

Ipari alkalmazások területén az épület- és gyártásautomatizálás vagy kereskedelmi szolgáltatást támogató megoldások segítik a felhasználókat. Az épületek esetén az energetikai (világítás, légkezelés) és a biztonságtechnikai rendszerek integrációját biztosítja. Kereskedelmi szolgáltatás például nagy bevásárló központok árucikk-követése, bevásárlókocsik követése vagy árucikk-azonosítása.

Ezen rendszerek Európában és Amerikában eltérő sávokban, de mindkét helyen ISM-tartományban működnek. Míg Európában a 868 MHz, addig Amerikában a 915 MHz került definiálásra. A 900 MHz körüli sáv mellett alkalmazzák a 2,4 GHz-es tartományban is. A sávokon belül természetesen több csatornát is használ a ZigBee-rendszer. Az európai rendszerben 868 MHz-en egy csatorna, az amerikai 915 MHz-es sávban 10, míg a 2,4 GHZ-en 16 csatorna áll a kommunikációs berendezések számára.

Ebből adódott, hogy a fejlesztők a stabilabb működés érdekében a legtöbbcsatornás sávot preferálták, ráadásul a 2,4 GHz az egyik legelterjedtebb ISM-sáv frekvenciája a világon.

Viszont lassan látszik a 900 MHz körüli technológiák terjedésének és jelentőségüknek növekedése. Ez annak tudható be, hogy sokkal jobbak a terjedési paraméterei beltéren (falak és födémek között), mint a 2,4 GHz-es technológiának, ráadásul ilyen kis teljesítények mellett. A WiFi-technológiához képest itt a tizedakkora a megengedett rádiós teljesítmény, ami nem elegendő beltéren a sok térelválasztó fal vagy kültéren nagyobb távolság esetén.

A technológia jellemzői röviden:

Adatátviteli sebességek:
- 250 kbit/s (2.4 GHz),
- 40 kbit/s (915 MHz),
- 20 kbit/s (868 MHz).

Hálózati topológia:
- csillag,
- egyenrangú.

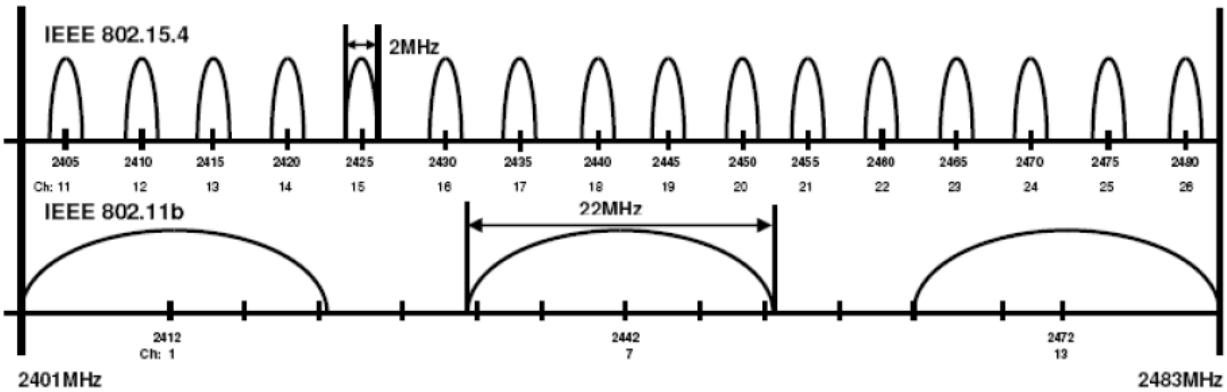
Hálózati cím:
- 64 bites egyedi,
- 16 bites logikai.

Ezenfelül garantált kommunikációs időszelet (GTS – guaranteed time slot) és CSMA/CA-csatorna-hozzáférés (Carrier sense multiple access with collision avoidance). A kommunikáció nyugtázott csomagküldéssel működik. Alacsony fogyasztás az elemes működést támogatja, illetve az energia detektálása a kommunikációs csatorna kiválasztásakor. A rendszer figyeli a kapcsolatminőség-indikátort. (LQI – Link quality indicator).

Csatornahasználat:
- 1 csatorna (868 MHZ),
- 10 csatorna (915 MHz),
- 16 csatorna (2.4 GHz).

4.3.2. Csatornák, kommunikáció

A ZigBee-szabvány (IEEE 802.15.4) szórt spektrumú rádióhullámokkal kommunikál a 2,4 GHz-es sávban 16 különböző csatornán. A frekvencia sávot 2405 MHz-től 2480 MHz-ig használja, a csatornák 5 MHz távolságra helyezkednek el egymástól és 2 MHz sávszélességgel bírnak.



18. ábra: A ZigBee (IEEE 802.15.4) és a WiFi (IEEE 802.11b) elhelyezkedése az ISM-sávban (Forrás: Internet.)

Az adatküldés alapja a „hallgass bele, majd beszélj” (CSMA/CA – Carrier sense multiple access with collision avoidance), ami sok technológiában elterjedt, többek között ezt használja a WiFi-technológia is. A lényege, hogy az adatküldést megelőzően a kommunikációs berendezés belehallgat

a csatornába, és ha úgy érzékeli, hogy éppen semelyik másik eszköz nem használja a csatornát, akkor megkezdi az adást. Persze, nem szabad elfelejteni, hogy kis adatmennyiségre készült a szabvány. Ezt, ha betartjuk, akkor ilyen működés mellett a rendszer robusztusan tud működni.

Az IEEE 802.15.4-hálózatban alapvetően kétféle eszközt használunk:
- teljes funkcionalitású eszköz (FFD – Full-function device),
- csökkentett funkcionalitású eszköz (RFD – Reduced-function device).

Egy FFD háromféle szerepet tölthet be a hálózatban:
- hálózati koordinátor,
- koordinátor,
- végpont.

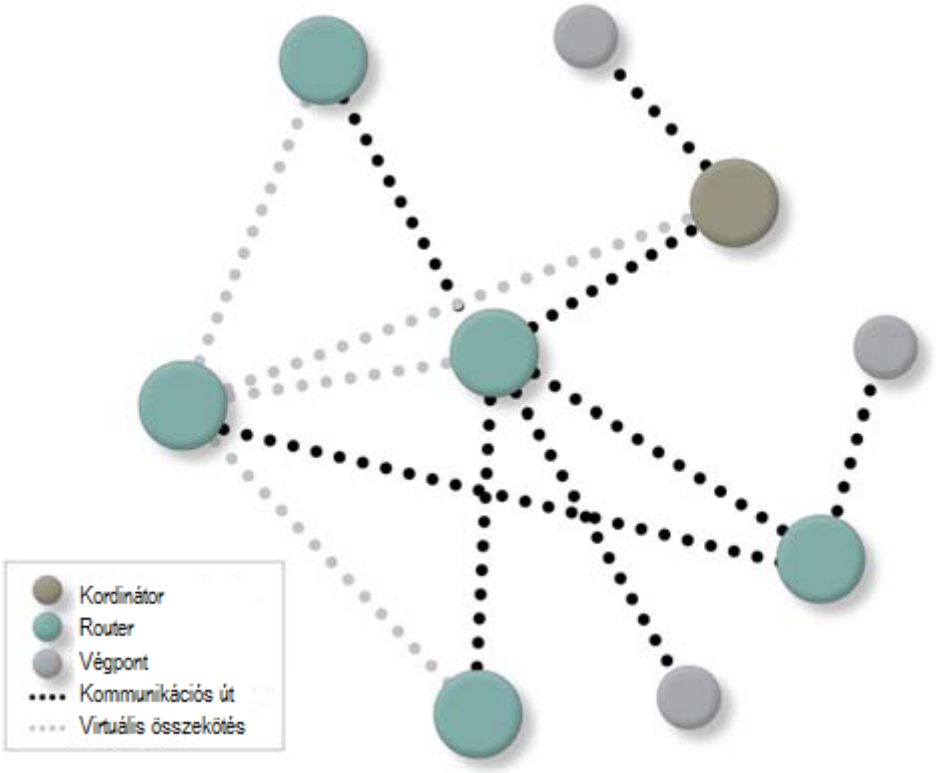
Az FFD-k kommunikálhatnak egy másik FFD-vel vagy RFD-vel, viszont egy RFD csak FFD-vel kommunikálhat. Ennek az oka, hogy a csökkentett funkciójú eszközök (RFD) végponti szerepet töltenek be a rendszerben, elemes működésűek (kis energiafogyasztás) és egyszerűségre optimalizáltak (hálózat szervezési feladatokat nem képesek ellátni).

Egy ZigBee- és minden PAN-hálózat minimálisan kell, hogy tartalmazzon egy Hálózati koordinátort és legalább egy végpontot. A média-hozzáférést vezérlő réteg (Medium Access Control layer, MAC) az eszközök és a hozzájuk kapcsolódó másik rendszerelemek közötti megbízható kapcsolatáért felelős. Segít a csatorna kihasználtságának növelésében úgy, hogy az egyszerre történő kommunikációs zavarokat csökkentse. Ennek a MAC-rétegnek a feladata továbbá, hogy az eszközök által küldött csomagokhoz a kereteket összeállítsa, illetve a kapott csomagokat felbontsa.

A másik réteg a fizikai réteg (Physical layer, PHY), amely biztosítja a kommunikációhoz a közvetítő közeget. IEEE 802.15.4 esetén ez maga a rádióskommunikációs rész. A fizikai réteg két alréteget is tartalmaz:

Alacsony frekvenciás sávok:
- Európában 868MHz,
- Amerikában 915MHz.

Magas frekvenciás sávok:
- 2,4 GHz (egész világon).
- Egy ZigBee-hálózat az eszköztípusokat figyelembe véve a következő elemekből állhat:
- koordinátorok,
- útválasztók (routerek),
- végponti eszközök.



19. ábra: Egy tipikus MESH-hálózat
(Forrás: Internet.)

A koordinátor fő feladata a Hálózat által használt csatorna kiválasztása és a hálózat kialakítása, majd működtetése. A koordinátor a hálózatra vonatkozó információkat is tárolja, emellett a hálózat biztonsági központja is egyben hiszen a hálózati kulcsok tárolása is a feladata.

Az útválasztó (router) berendezések alapvető feladata a hálózat lefedettségének megnövelése, dinamikus és tartalék útvonalak biztosítása a hálózaton közlekedő információk számára. Az útválasztók képesek csatlakozni koordinátorokhoz és másik útválasztókhoz is. Fontos feladatuk, hogy képesek kiszolgálni egyéb eszközöket is, mint más útválasztók vagy végponti eszközök.

A végponti eszközöknek (End devices) azokat a berendezéseket hívjuk, amelyek csomagokat képesek küldeni és fogadni, de egyéb forgalomirányítási szerepük nincs. Közvetlenül csatlakozhatnak koordinátorokhoz vagy útválasztóhoz. Másik végponti eszközöket nem szolgálnak ki.

Ezt a működést hívják mesh (szövevényes) hálózati topológiának. A MESH-topológiát gyakran nevezik egyenrangú hálózatnak is (peer-to-peer), mivel egymással kapcsolatban álló útválasztók és végponti eszközök szövevényét adja. Mindegyik útválasztó célszerűen legalább két útvonallal csatlakozik a szomszédjaihoz és ezeken képes továbbítani az adatait.

Ahogy az 20. ábrán is látszik, egy MESH-hálózat egy koordinátort, több útválasztót és végponti eszközt tartalmazhat.

A MESH-topológia a többugrásos (multi-hop) kommunikációt támogatja, amelyben a csomag csomópontról csomópontra utazik, megkeresve az optimális költségű utat, amíg a célját el nem éri. A kommunikációs költségszámítás az eszközök feladata és a hálózatban elfoglalt helytől függ. A rendszer törekszik a kommunikációs utak rövidítésére. Egyben ez a megoldás lehetővé teszi, hogy amennyiben egy eszköz meghibásodik, vagy egyéb okból kiesik a hálózatból, akkor a hálózat képes egy másik útvonalra terelni a forgalmat a működő eszközökön keresztül, így növelve a megbízhatóságot.

A MESH-hálózat előnyei:

- Ez a topológia robosztus és nagy megbízhatóságú. Bármely útválasztó kiesése esetén alternatív útvonalakon folytatódik az adatforgalmazás.
- Köztes eszközök (útválasztók) telepítésével a hálózat mérete jelentősen megnövelhető, ezzel nagymértékben skálázhatóvá válik.
- Gyenge térerő és leárnyékolt helyen lévő eszközök is bekapcsolhatóak a hálózatba további útválasztók telepítésével.

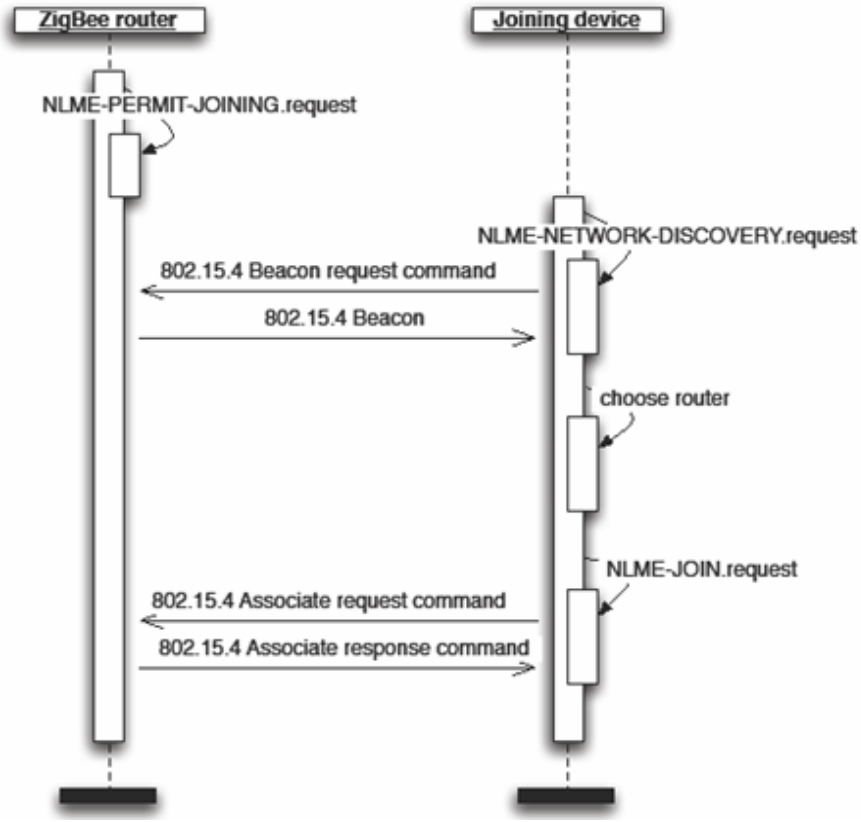
A hálózati csomópontok (útválasztók, végponti eszközök) kétféle módon csatlakozhatnak a hálózathoz. Az egyik a MAC association, a másik a NWK rejoin.

A MAC association csatlakozási módra alapértelmezésben minden ZigBee-eszköz képes, lévén, hogy ez kötelező jelleggel implementálva van a MAC-rétegben.

Ebben az esetben a ZigBee útválasztó vagy koordinátor, amelyik engedélyezni kívánja további eszközök csatlakozását, ki kell adnia az NLME-PERMIT-JONING.request parancsot. Ez utasítja a hálózati réteget, hogy a csatlakozás engedélyezett.

A csatlakozó eszköz, miután felderítette a hálózatot, amelyhez csatlakozni kíván, valamint azt, hogy melyik útválasztó vagy koordinátor eszköz engedi a csatlakozást, kiad egy NLME-JOIN. request parancsot. A parancs paramétereiben számos jelző (flag) található, ezek közül a rejoin flaget törölni kell. Ez a parancs eljut az útválasztó vagy koordinátor eszközhöz, amely egy válaszüzenettel (response) válaszol. A válaszban a szülő elküldi a csatlakozó eszköz hálózati címét, amelyet kiosztott a számára. Ez a fajta csatlakozási mód nem biztonságos, mert a csomagok kódolás nélkül utaznak a fizikai rétegen.

A folyamatot az alábbi ábra szemlélteti:



20. ábra: Csatlakozás MAC association segítségével
(Forrás: Daintree Networks Getting Started with ZigBee, www.daintree.net)

A ZigBee természeténél fogva képes az alábbi alkalmazásprofilokat egymással együtt élve működtetni. Ez a tulajdonsága az egyik nagy előnye.

21. ábra: A különböző alkalmazásprofilok
(Forrás: Daintree Networks Getting Started with ZigBee, www.daintree.net)

4.3.3. A ZigBee fejlesztésének motivációi

A ZigBee fejlesztése során a következő igényeket helyezték fókuszba:

- alacsony bekerülési és üzemeltetési költségek,
- biztonság (adatbiztonság),
- megbízható és önszervező, öngyógyító hálózat,
- flexibilitás és bővíthetőség,
- alacsony fogyasztás (elemes működés),
- könnyű és olcsó telepítési költségek,
- szabad frekvenciasáv használata világszerte,
- automatikus, intelligens hálózati konfiguráció és üzenettovábbítási mechanizmus.

Jelenleg a ZigBee az egyetlen, szabványosított technológia, amely a felügyeleti és vezérlő hálózatok ilyen igényeit kielégíti.

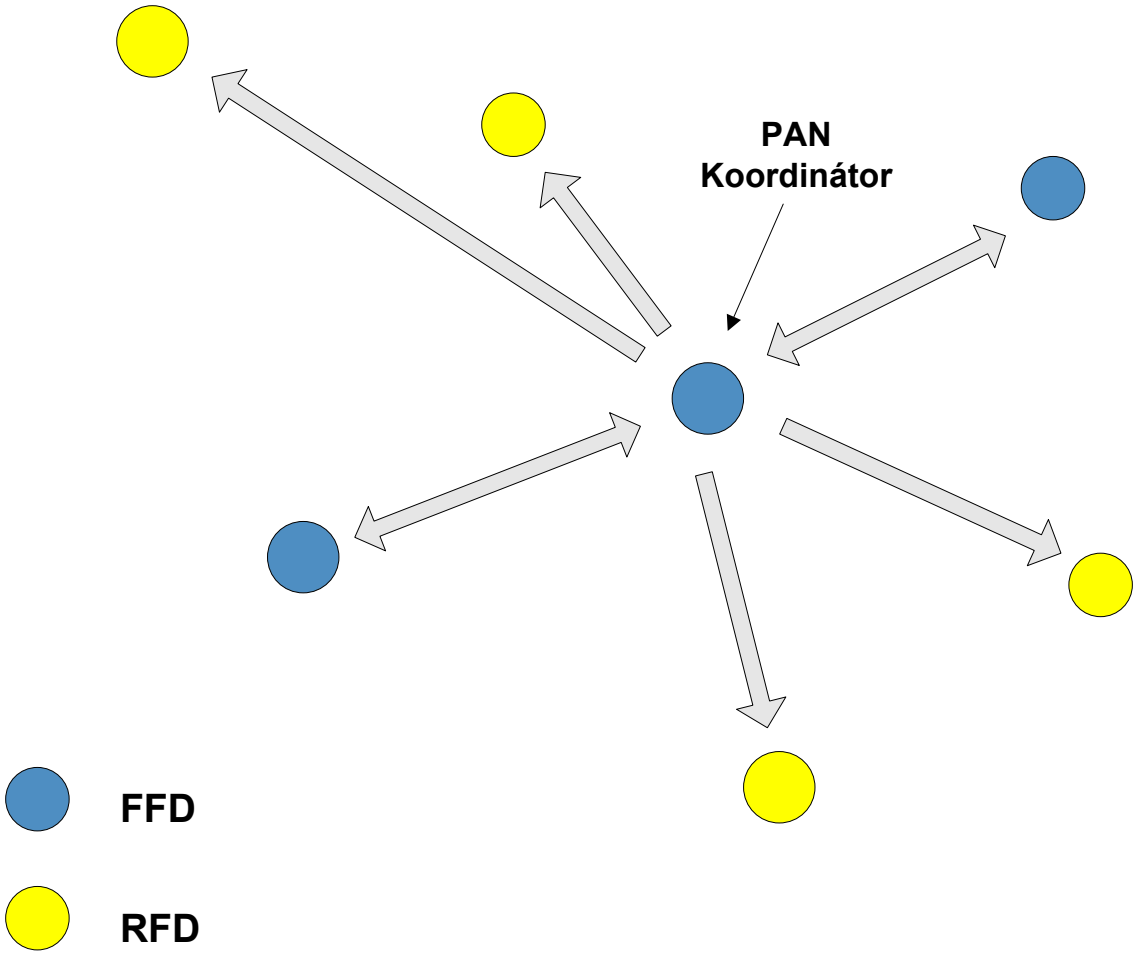
Alapvetően egy WPAN (Wireless Personal Area Network) kétféle topológia szerint szerveződhet.

- csillag topológia,
- egyenrangú hálózat.

A két típus közül egyszerűbb a csillag topológia, ami a központi koordinátor köré szerveződő végpontokból áll. Az eszközök mindegyike rendelkezik egy gyárilag beépített 64 bites fizikai címmel (hosszú cím). A hálózat kialakítása során a koordinátor feladata, hogy a bejelentkező végpontoknak logikai címeket (rövid cím) osszon ki, amelyek 16 bit hosszúak. A berendezések ezen címek bármelyikével képesek kommunikálni egymással a hálózaton.

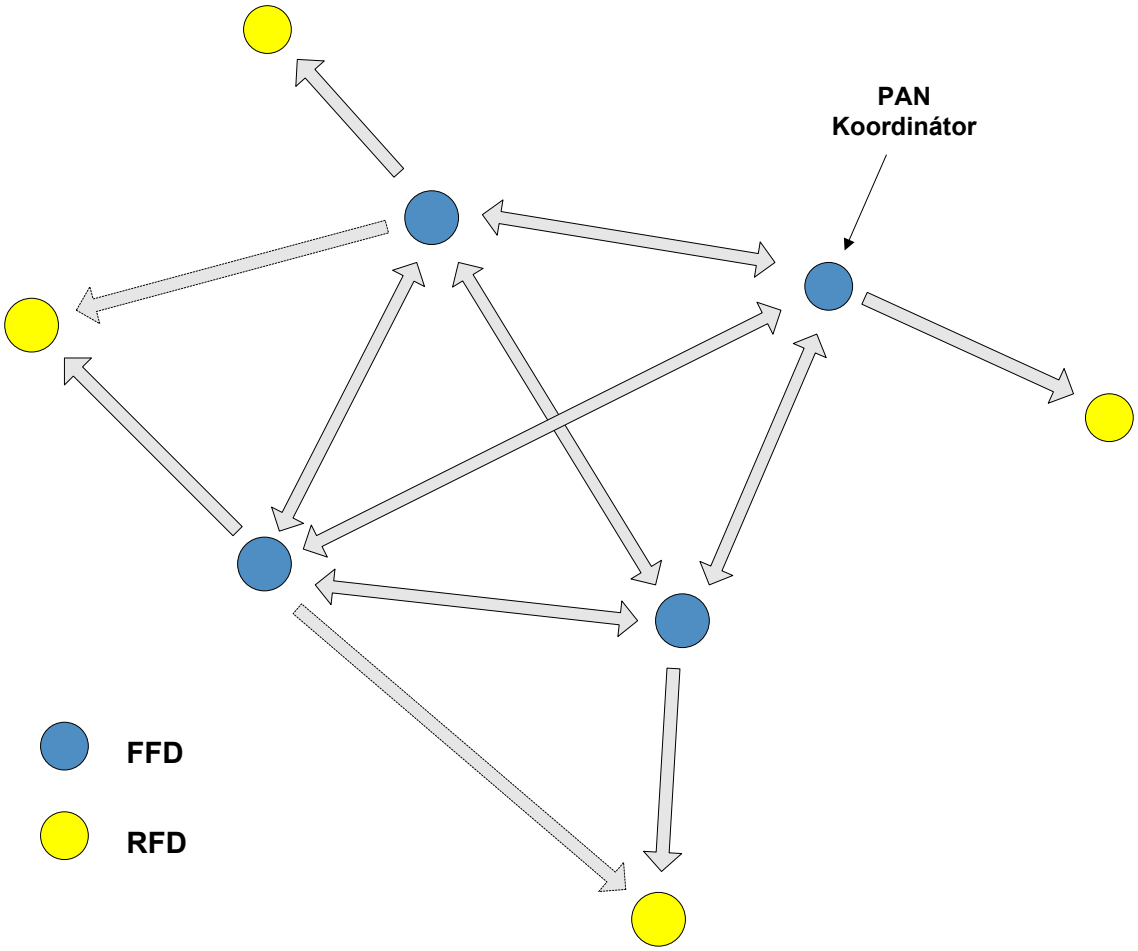
A hálózat folyamatos működése érdekében a koordinátornak állandóan működnie kell, ezért biztosítani kell a folyamatos tápellátását. Többszolgáltatós okos mérési rendszerekben általában a villamosfogyasztás-mérő tölti be ezt a szerepet.

A végpontoknál megengedett az elemes táplálás, ilyenkor viszont az idő nagy részében alvó üzemmódban van az eszköz, hogy kímélje az elemet. Ez az eszköztípus főleg idősfelügyleti, egészségügyi, okoseszközökben használatos, jellemzően kevés hálózati végponttal. Többszolgáltatós rendszerben a gáz-, víz- és távhőmérő berendezésnél alkalmazzák ezt a típust.



22. ábra: IEEE 802.15.4 csillag topológia

A másik hálózati topológia az egyenrangú hálózat. Hasonlóan a csillag topológiához, a hálózatoknak ebben az esetben is rendelkezniük kell egy WPAN koordinátorral, amely folyamatosan üzemel. Ez a topológia sokkal összetettebb hálózatok kialakítását teszi lehetővé, mint például fa (cluster tree) vagy szövevényes (MESH) hálózat. Ez a típusú szerveződés ad hoc jellegű, önszervező és öngyógyító képességekkel rendelkezhet. Ez azt jelenti, hogy egy útvonalon lévő eszköz meghibásodása esetén egy másik képes átvenni a szerepét automatikusan. Ugyancsak lehetőség van a csomagok többféle útvonalon történő célba juttatására, bár ezek a hálózati funkciók ebben a szabványban nincsenek definiálva, ez már a felsőbb applikációk feladata (pl. ZigBee).



23. ábra: IEEE 802.15.4 Egyenrangú hálózat (Peer-To-Peer)

A hálózat kialakítása során a koordinátor választ egy véletlenszerű vagy előre definiált ún. WPAN-ID-t (vezetéknélküli hálózati azonosítót), aminek segítségével a csatlakozó eszközöket egy logikai hálózatba szervezi.

Így lehetséges, hogy több, akár egymás hatókörén belül működő hálózat is képes legyen működni, akár úgy is, hogy az végponti eszközök a másik, független hálózatban lévőkkel is kommunikálhatnak. Ezt a működési módot Inter-PAN-kommunikációnak nevezzük.

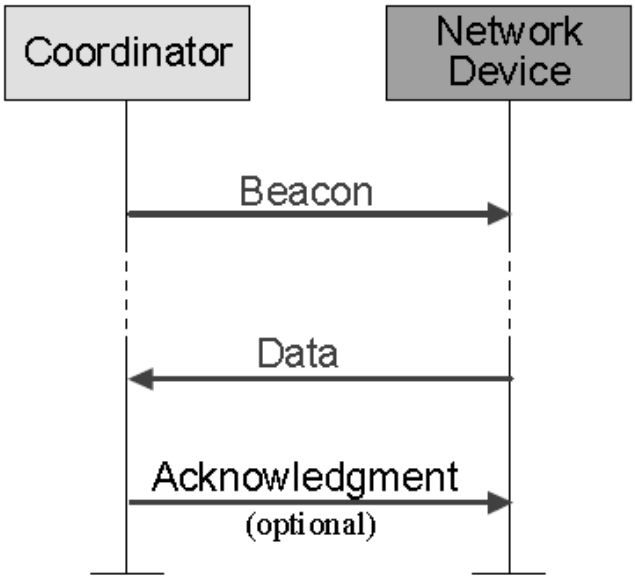
A működés szempontjából fontos még megemlíteni, hogy a hálózatot vezérlő koordinátor, a hálózat logikai kialakítása előtt megvizsgálja a rendelkezésre álló csatornákat és kiválasztja azokat, amelyekben a legkisebb a zaj. Ezeket a csatornákat használja a működés során. Ezt a folyamatot energiadetektálásnak (ED – energy detection) hívjuk. Ennek során az eszközök képesek feltérképezni a nagyon sok zavarral szennyezett csatornákat az adott helyszínen és ennek megfelelően választanak egyet a saját hálózatuk kialakítására. A 2007-ben megjelent ZigBee Pro szabvány már azt is lehetővé tette, hogy akár menet közben is frekvenciát váltson a teljes hálózat, ezzel is növelve a rendszer megbízhatóságát.

4.3.4. ZigBee hálózati hozzáférés

Az eszközök közötti kommunikáció időzítése kétféle módon történhet:

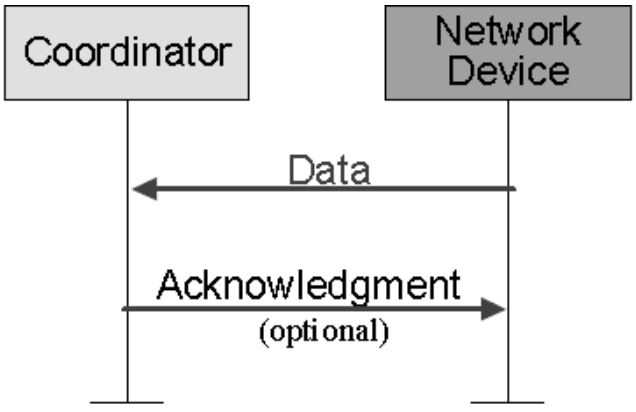
- szinkronizált,
- nem szinkronizált.

Szinkron mód esetén a 24. ábra szerint a koordinátor úgynevezett Beacon-jeleket küld időközönként. Ezek a speciális üzenetek tartalmazzák a hálózat paramétereit, valamint ezzel szinkronizálják a többi eszköz csomagküldését.



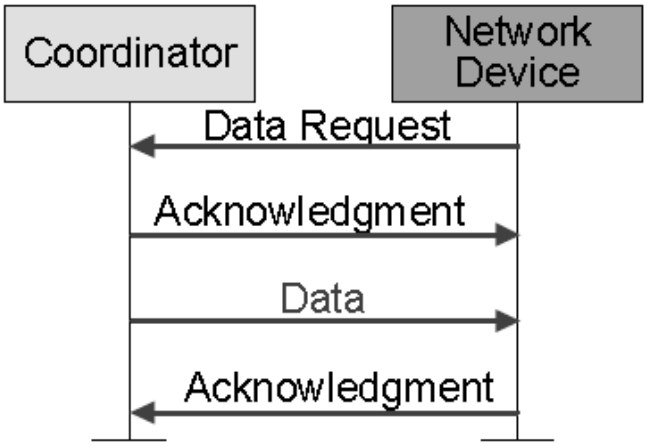
24. ábra: Az adatküldés Beacon szinkronizált hálózatban
(Forrás: IEEE 802.15.4 Std. 2003 Beaconed network.)

Nem szinkronizált módban az eszközök bármikor, aszinkron módon küldhetnek információt a hálózatra. A cél az, hogy a végpontok nagyon pici energiafelhasználás mellet, tudjanak működni és bármikor tudjanak kommunikálni. Így nem kell várni szabad csatornára, ezzel is az elem élettartamát növelhetjük. A ZigBee-protokoll nem szinkronizált hálózat szerint működik.



25. ábra: Az adatküldés nem Beacon szinkronizált hálózatban
(Forrás: IEEE 802.15.4 Std. 2003 Non-Beaconed network.)

Persze, felmerül egy kézenfekvő probléma, hogy hogyan tud a koordinátor üzenetet küldeni egy végpontnak, amikor az éppen energiatakarékos üzemmód miatt alvó állapotban van. A szabvány alkotói erre válaszként egy olyan mechanizmust terveztek, amely úgy működik, hogy az eszköz a „felébredése” után megkérdezi a hálózat szervezőjét, hogy van-e adat, amit még nem kapott meg, és ezután vár (Data Request). Ha van neki szóló adat, akkor a hálózatszervező jelzi ezt az adatkérésre adott nyugtájában. Ebből fogja tudni a végpont, hogy még nem szabad kikapcsolnia, hanem tovább figyeli a kommunikációs vonalat.



26. ábra: Az adatkérés a szülő felé
(Forrás: IEEE 802.15.4 Std. 2003.)

Rádiófrekvenciás kommunikációs hálózatok kapcsán mindig felmerül a hatótávolság, lefedettség és zavartatás kérdése. Műszakilag pontos, kiszámítható választ nagyon nehéz adni arra kérdésre, hogy egy adott területen milyen paramétereket célszerű alkalmazni.

Gyakorlati módszer ennek megoldására az empirikus módon történő megközelítés, valamint a mérési eredmények alapján történő válaszadás. A szakirodalomban megjelent tanulmányok és publikált tesztek alapján kijelenthető, hogy a 2,4 GHz-es sávban, a megengedett teljesítményviszonyokat feltételezve, épületen belül néhányszor 10 m a hatótávolság, szabadban, közvetlen rálátás mellett, akár néhány száz vagy akár ezer méter is lehet. Az épület szerkezete, anyaga, kialakítása jelentősen befolyásolhatja a terjedési viszonyokat.

5. Rövidítésjegyzék

AES (Advanced Encryption Standard) – Fejlett kódolási szabvány

AMM (Automatic Meter Management) – Mérési rendszer

AMR (Automatic Meter Reading) – Mérő távleolvasás

COSEM Companion Specification for Energy Metering

DC (Data Concentrator) – Adatkoncentrátor

DLMS (Device Language Message Specification) – Definiált nyelvezetű eszköz üzenet

EMC – Elektromágneses összeférhetőség

EN (European Norm) – Európai Szabvány

FTP (File Transport Protocol) – Fájlküldési protokoll

GSM/GPRS (Global System for Mobile communication/General Packet Radio System) – Rádiós Mobil Kommunikációs Rendszer / Általános Csomagkapcsolt Rádiós Rendszer

HKV – Hangfrekvenciás Körvezérlő Vevő

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secured

IEC – International Electrotechnical Commission

IP – Internet Protocol

LAN (Local Area Network) – Helyi hálózat

Load Management – Terhelésvezérlés

Load Profile – Terhelési görbe

M-BUS – Mérők közötti kommunikációs adatbusz rendszer

OBIS (Object Identification System) – Végpont / Mérésiérték Azonosító Rendszer

Optical link – Optikai kapcsolat

Plug & Play technology – Gyorsan és egyszerűen összeállítható technológia

PLC (Power Line Carrier) – Erőátviteli vezetéken történő adatátvitel

RKV – Rádiós Körvezérlő Vevő

S-FSK (Sinusoidal-Frequency Shift Keying) – Frekvencia modulált eljárás

SMART METER – Okos mérő

SMART METERING – Okos mérési rendszer

SQL (Structured Query Language) – Nagy adatok tárolására és keresésére kialakított nyelvezet

URL (Universal Resource Locator) – Univerzális forráshely

VET – Villamosenergia-ellátási Törvény

VHR – Végrehajtási rendelet

VPN (Virtual Private Network) – Virtuális magánhálózat

M2M – Mashine To Mashine

PAN – Personal Area Network

XML (eXtensible Mark-up Language) – Egységes Jelölő Nyelv, amely szabványos adatcserét tesz lehetővé

6. Irodalomjegyzék

- International Conference on Electricity Distribution, CIRED Working Group on Smart Grid: Smart Grid on the Distribution Level, CIRED's point of view; Final report, 2013. 03. 18.
- U.S. Department of Energy, prepared for the U.S. Department of Energy by Litos Strategic Communication under contract No. DE-AC26-04NT41817, Subtask 560.01.04, "The Smart Grid: An Introduction," 2009.
- International Energy Agency (IEA), OECD: "Technology Roadmap Electric and plug-in hybrid electric vehicles"; Paris, France, 2009.
- „HKV-RKV és az intelligens fogyasztásmérés" BME VET; Elektrotechnika, 2011/01.
- http://www.efr.de/en/efr-system/
- Szabó Ervin: Megújuló energiatermelő rendszerek elosztó hálózatra való visszatáplálásának szabályozása és eszközei. Elektrotechnika 2013/11 (14–16. o.)
- Dr. Varjú György: Meggondolások a Központi Okoshálózati Operátor (KOO) működési modellhez. (MEE OHM Munkacsoport szervezésű konzultáció Budapest, 2013. június 4 Hunguest Hotel Griff Budapest.)

IV. PONGRÁCZ PÉTER: KIBERTÁMADÁSOK VILLAMOS-ENERGETIKAI KÖRNYEZETBEN

1. Bevezetés

A XX. század során kialakult modern ipari társadalmakban az ipari irányító rendszerek (Industrial Control Systems, ICS) nélkülözhetetlen szerepre tettek szert, majd a XXI. század elejére szétválaszthatatlanul összefonódtak az információs technológiai berendezésekkel. Mára a legtöbb ICS-rendszer és -berendezés ugyanolyan vagy legalábbis nagyon hasonló komponensekből épül fel, mint a más szektorok (pénzügy, államigazgatás, szolgáltatói szektorok) IT-rendszerei. Ezek nélkül a rendszerek nélkül ma már elképzelhetetlen a közműszolgáltatások, a gyártósorok vagy éppen a közlekedés és szállítmányozás zavartalan működésének biztosítása.

Ezzel párhuzamosan a dolgok internete (Internet of Things, IoT), vagy hétköznapi megnevezéssel: okoseszközök, robbanásszerű elterjedése a XXI. században a mindennapok láthatatlan szereplőivé tette a különböző (szigorúan véve nem ipari) irányító rendszereket. Ilyenek sok más mellett például az orvostechnikai automatizálási eszközök (IP-hálózatokon kommunikáló inzulinpumpák, szívritmus-szabályozók stb.), a modern autók (elég csak a jövő, de valamilyen szinten akár már a jelen önvezető autóira gondolni) vagy akár a polgári repülőgépekben és hatalmas teherszállító hajókon használt folyamatvezérlő rendszerek. Az egyszerűség kedvéért a továbbiakban az ICS rövidítést fogjuk használni minden vezérlőrendszerre.

A villamosenergia-iparban használt vezérlőrendszerek esetén jellemzően két nagy rendszer-, illetve eszközcsoportról szoktunk beszélni. Az egyik az EMS/SCADA-[238] (Energy Management Systems/Supervisory Control and Data Acquisition) és DCS- (Distributed Control Systems) rendszerek, a másik csoport pedig az alállomási automatizálási rendszerek és berendezések csoportja (digitális védelmek, áramváltók stb.). Az ezeket a rendszerek fejlesztő, üzemeltető és a fizikai folyamatok irányítására használó mérnököket nevezik általánosan OT- (Operations Technology) mérnököknek. Ők azok a mérnökök, akik az ICS-rendszerek által irányított folyamatokkal kapcsolatban a lehető legmélyebb szakmai ismeretekkel rendelkeznek. A villamosenergia-szektorban ők jellemzően erősáramú villamosmérnökök.

2. Eltérések az IT és az OT világai között

Az OT világa a nagyvállalati IT-nél jelentősen (több évtizeddel) hosszabb múltra tekint vissza. Már az 1960-as évek óta üzemelnek számítógépes folyamatvezérlő rendszerek, ebben a szerepben a ma ismert IT-komponensek valamikor a ’90-es években jelentek meg, majd igen gyorsan nyertek teret úgy a hardverek, mint a szoftverek terén, és ez alól a népszerű és széles körben alkalmazott IT-protokollok (HTTP, FTP, SSH, TCP/IP stb.) sem maradtak ki.

Annak ellenére, hogy az IT- és az OT-világ közötti különbségek folyamatosan tűnnek el, van néhány olyan jellegzetesség, ami napjainkban is jelentős. Egyrészt az OT-rendszereket jellemzően

[238] A dokumentumban előforduló szakkifejezések részletesebb magyarázatát a https://icscybersec.blog.hu oldalon lehet megtalálni: https://icscybersec.blog.hu/2015/12/12/ics_rendszerekkel_kapcsolatban_ismetlodo_kifejezesek

több évtizedes tervezési elvek mentén fejlesztik. Az ezekhez a rendszerekhez tartozó üzemeltetési gyakorlatok hosszú évtizedek alatt alakultak ki, bizonyultak helyesnek és üzembiztosnak, éppen ezért a folyamatirányítási területeken dolgozó mérnökök, ha tehetik, kerülik a rendszereken végzett módosításokat (mottójuk általában valami ilyesmi: *„Ha működik, ne nyúlj hozzá!”*). Másrészt az OT világában egy rendszer vagy berendezés beállításaiban végrehajtott változtatás nem marad meg a bitek és bájtok szintjén, hanem a felügyelt és vezérelt folyamatokon keresztül megjelenhet a fizikai világban is. Éppen ezért az IT és információbiztonság világában ismert biztonsági szempontok (bizalmasság, sértetlenség, rendelkezésre állás) mellett két további, az előzőeknél sokkal fontosabb szempont is megjelenik. Az első a *safety* (mivel az angol szó tükörfordítása a biztonság lenne, ami azonban nem adja vissza az eredeti angol kifejezés minden értelmét, ezért ebben a dokumentumban az angol változatot fogjuk használni), ami a fizikai folyamatok emberek életének és/vagy testi épségének védelmére vonatkozik. A másik a megbízhatóság (*reliability*), ami alatt a folyamatvezérlő rendszerek működésének megbízhatóságát kell érteni, különösen a rendszerben működő szenzoroktól érkező adatok, illetve a vezérlőrendszerek működésének megbízhatóságára vonatkozóan.

Fontos szempont továbbá, hogy az ICS-rendszerek által vezérelt folyamatok zavartalansága minden közösség számára elsődleges fontossággal bír. Elég csak arra gondolni, hogy egy atomerőmű bármilyen kicsi üzemzavara azonnal hírértékkel bír, hogy egy áramkimaradás mekkora fennakadásokat okozhat akár csak egy kistelepülésen vagy hogy egy gyárban a termelésirányító rendszer néhány órás leállása mekkora veszteséget jelenthet a vállalat számára.

További jelentős különbség, hogy az ICS-rendszerek életciklusa nagyságrendekkel hosszabb, mint amit egy IT-rendszertől megszokhattunk. Egy-egy vállalati IT-rendszer néhány év után már legalább komolyabb verziófrissítésen kell, hogy átessen, de a felhasználói eszközök háromévenkénti, a szerverek 4-6 évenkénti cseréje sem számít rendkívülinek egy-egy nagyvállalati IT-részlegnél. Ezzel szemben az ICS-rendszerek esetében gyakran évtizedekre terveznek egy-egy rendszert, a villamosenergia-iparban az alállomásokon használt automatizálási eszközök életciklusa jelenleg például 15-20 évtől akár 40 évig is terjedhet.

Arról nem is beszélve, hogy az ICS-rendszerek és -berendezések jellemzően több nagyságrenddel drágábbak, mint az IT-rendszerek: egy SCADA-rendszer ára könnyedén lehet milliárdos tétel, de egy RTU vagy egy transzformátor árából is fel lehetne építeni egy közepes magyar vállalat teljes IT-rendszerét. Emiatt aztán ritka az olyan ICS-rendszer, amiből a produktív és tartalék rendszer (illetve tartalék berendezések) mellett rendelkezésre állna teszt- és/vagy fejlesztői rendszer is, így viszont nem mindig van lehetőség a változások tesztrendszerben történő alkalmazására és a változtatások hatásainak alapos tesztelésére.

A fentiek miatt nem meglepő, ha az OT-mérnökök csak nagyon súlyos indokok alapján kezdenek hozzá az általuk üzemeltetett rendszereken módosítások végrehajtásához.

3. Ismert sebezhetőségek a villamosenergetikai környezet informatikai rendszereiben

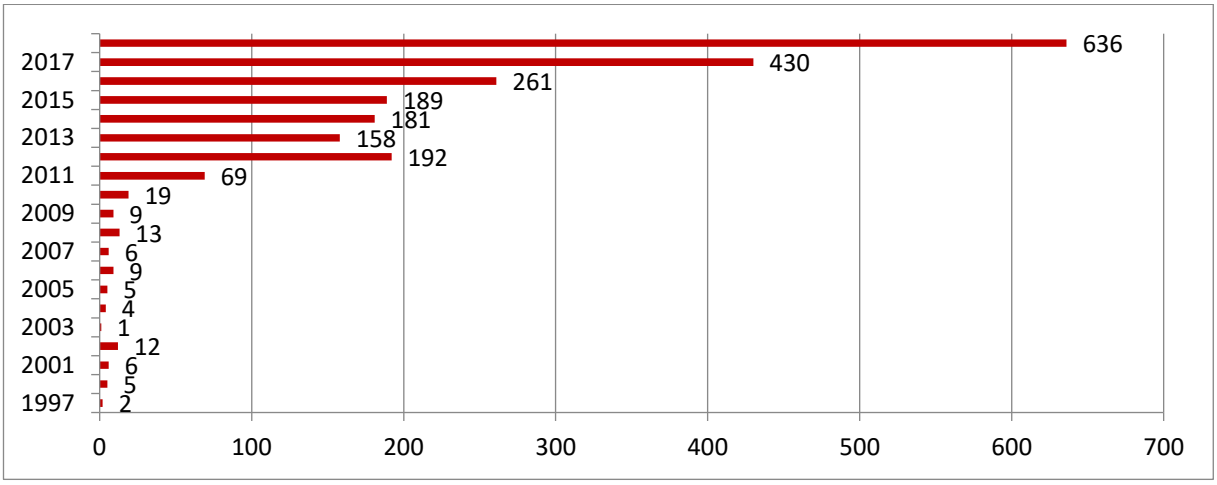
Egészen 2007-ig az ICS-rendszerek kiberbiztonsági sérülékenységei és fenyegetettsége alig néhány embert foglalkoztatott. Ebben az évben végezték az USA Idaho National Labs intézetében az első, mérföldkőnek számító Aurora-teszteket, ezek során a résztvevőknek sikerült bebizonyítani, hogy fizikai hozzáférés nélkül, kizárólag a tesztelt generátorok IT-komponenseinek sérülékenységeit kihasználva, távolról tönkre lehet tenni egy ICS-berendezést[239].

[239] Bővebb információ az INL Aurora-tesztjéről:
https://www.youtube.com/watch?v=9pkDmvF8C2A – rövid összefoglaló az Aurora-tesztről.
https://www.youtube.com/watch?v=LM8kLaJ2NDU – videófelvétel a teszt során leégő generátorról.

A villamosenergetikai informatikai rendszerek sebezhetőségei (ahogyan általában az ICS-rendszerek sebezhetőségei is) több összetevőből állnak. Az egyik az ICS-rendszerek már említett, az IT-rendszerek esetén megszokottnál nagyságrendekkel hosszabb életciklusa. A gyakorlatban ez sokszor azt eredményezi, hogy bár a gyártó már régen felhagyott pl. egy operációs rendszer verziójának támogatásával, az OT világában még számos ICS-rendszer vagy ICS-berendezés üzemeltetéséhez használják azt. Ennek oka gyakran az, hogy az adott ICS-berendezés konfigurálásához használt szoftver nem fut pl. Windows XP-nél újabb verzión. Egy másik kiváló példa, hogy egyes termelésirányító rendszerek mind a mai napig Windows NT 4.0 operációs rendszert futtató vezérlőrendszerek irányításával működnek. Itt fontos megemlíteni, hogy igen gyakori az a tévhit, hogy az ICS-rendszereket, -berendezéseket nem lehet elérni az adott szervezet vállalati IT-hálózatából, de egy felkészült auditor általában néhány jól irányzott kérdés után már képes megtalálni azokat a pontokat, ahol bizony a vállalati IT- és OT-hálózatok között létezik hálózati kapcsolat, amin keresztül aztán adott esetben egy támadó is hozzáférhet az ICS-rendszerek hálózatához.

A másik sebezhetőséget az egyre nagyobb arányban használt IT-komponensek hétköznapi sérülékenységei jelentik. A különböző ICS-gyártók egyre nagyobb arányban használják a kommersz IT-megoldásokat hardverek, szoftverek és protokollok terén egyaránt, közben pedig makacsul tartják magukat azok a több évtizedes hiedelmek, hogy az ICS-rendszerek annyira bonyolultak és egyediek, hogy azokhoz csak a megfelelően képzett OT-mérnökök érthetnek. Mivel azonban a modern ICS-rendszerek már mind nagyobb számban épülnek Microsoft Windows operációs rendszerekre vagy különböző Linux-disztribúciókra, az azokban felfedezett és nyilvánosságra hozott (ha előbb nem is, de a sérülékenységre kiadott gyártói javítás után már mindenképp) sérülékenységi információkat az érintett ICS-rendszerek esetén is ki lehet használni. Különösen igaz ez az ICS-rendszerekre azért, mert még ha egy adott sérülékenységre a gyártó elérhetővé is tette egy sérülékenység javítását, az üzemeltető különböző megfontolások miatt gyakran nem telepíti a hibát javító verziót. Az ICS-rendszerek esetén bizony sokkal gyakrabban lehet találkozni olyan esetekkel, hogy egy adott rendszer vagy berendezés támogatását a gyártó már megszüntette, de az ügyfelek még hosszú éveken át használják, hiszen funkcionálisan a rendszer hibátlan és a már említett tévhitek miatt úgy gondolják, hogy csak azok az OT-mérnökök férnek hozzá ezekhez az eszközökhöz, akiknek ez a feladatuk, mások pedig úgysem fogják érteni a működésüket. Ugyanezen okok miatt, illetve a tesztrendszerek már említett hiánya és az ICS-rendszerektől elvárt, kiemelten magas rendelkezésre állási szint miatt sokkal nagyobb az ismert sérülékenységekkel futó ICS-rendszerek száma, mint az egyébként sem alacsony, ismert sérülékenységekkel rendelkező vállalati IT-rendszerek száma.

Éppen emiatt aggasztó az a tény, hogy 2010 (a Stuxnet megjelenése) óta évről évre ugrásszerűen nő az ICS-rendszerekkel kapcsolatban publikált szoftveres (és ritkább esetben, mint például a Meltdown/Spectre-sérülékenység esetén, hardveres) sérülékenységek száma.



1. ábra: Évenként publikált ICS sérülékenységek száma 1997–2018
(Forrás: Kaspersky Lab és saját gyűjtemény.)

Az ICS-rendszerek magukban hordoznak még egy sebezhetőséget, ami szintén a sok évtizedes múltjukra, illetve a másfél-két évtizedes életciklusukra vezethető vissza, ez pedig a már nem biztonságosnak tekintett protokollok használata. Az ICS-rendszerek és berendezések esetén mind a mai napig megszokott jelenségnek számít, ha egy eszköz nem titkosított protokollokat használ a hálózati kommunikáció során. Telnet, FTP/TFTP, RSH, rexec, HTTP – csak néhány, az ICS-rendszerek esetén mindmáig széles körben használt, az IT világában már régen elavultnak és biztonsági kockázatnak tartott protokollok közül. A régi és nem biztonságosnak tekintett IT-protokollok mellett az ICS-specifikus protokollok (Modbus, Modbus/TCP, DNP3, ICCP, BacNET, PROFINET, Ethernet/IP – ebben az esetben az IP az Industrial Protocol rövidítése – stb.[240]) többségével kapcsolatban szintén számos biztonsági probléma ismert. Ennek egyik fő oka megint csak az a tény, hogy ezeket a protokollokat évtizedekkel ezelőtt, a vállalati IP-hálózatok kialakulása és ICS-hálózatokkal történő összekapcsolása előtt tervezték, emiatt pedig nem csak a titkosítás hiányzik belőlük, de olyan alapvető biztonsági funkciók is, mint például a hálózati kommunikáció hitelesítéshez (authentikációhoz) kötése. Például egy Modbus/TCP-hálózaton az eredeti protokollspecifikáció szerint bármilyen, a hálózaton megjelenő szereplőnek joga van vezérlési utasításokat kiadni, a hálózaton található többi eszköz pedig ezt bármilyen ellenőrzés nélkül végre is fogja hajtani, mert az eredeti tervezőknek a fejében meg sem fordult olyan gondolat, hogy támadók juthatnak be ezekre a hálózatokra és ezt a tervezési hiányosságot a saját céljaikra tudják majd kihasználni.

A Stuxnet nyilvánosságra kerülése óta eltelt 9 év alatt számos fejlesztés kezdődött annak érdekében, hogy ezeket a protokoll szintű biztonsági hibákat fel lehessen számolni, azonban az ICS-rendszerek életciklusa és statikussága mellett még egy problémával szembe kell nézni, ez pedig az, hogy az ICS-berendezések egy része egyszerűen annyira az adott célra lett tervezve és méretezve, hogy nem rendelkeznek a titkosításhoz szükséges teljesítménytartalékokkal. Ez az oka annak is, hogy a Meltdown/Spectre CPU-sérülékenységek az ICS-rendszerekre még az IT-rendszereknél is komolyabb fenyegetést jelentenek, mert ezekre a rendszerekre sok esetben nem lehet telepíteni a megfelelő javításokat és felvállalni a jelentős teljesítményvesztést.

Az ICS-rendszerek sebezhetőségeinek listája még legalább egy tételt tartalmaz, ez pedig az emberi tényező, ami azonban többféle formában is fenyegetésként jelenhet meg az ICS-rendszerek számára. Az IT/információbiztonság világából már ismert humán kockázatok az ICS-világát sem kerülik el, az ICS-rendszerek felhasználóinak és üzemeltetőinek a biztonságtudatossági szintje semmivel sem rosszabb vagy éppen jobb, mint azt az átlagos IT-felhasználók vagy -üzemeltetők esetén már megszokhattuk. Az ICS-rendszerekkel kapcsolatban itt is van egy sajátosság, mégpedig az IT-, illetve az IT-biztonsági és az OT-szakterületek közötti ellentétek, amik az egyes szakterületeken dolgozók nagyon eltérő szakmai szocializációjából és eltérő prioritásaiból adódnak. Az IT- és IT-biztonsági területeken dolgozó mérnököket már másfél-két évtizede arra oktatják, hogy az adott szoftverek újabb kiadásait (a megfelelő tesztelések után) minél előbb telepíteni kell, ezzel javítva biztonsági és/vagy funkcionális hibákat. Az ICS-rendszerek üzemeltetőit, ahogy azt korábban már érintettük, ezzel szemben az első munkanapjuktól arra tanítják, hogy a folyamatvezérlő rendszer zavartalan működésénél csak egyetlen fontosabb szempont létezik, a rendszereikkel kapcsolatba kerülő emberek élete és testi épsége (*safety*). Ezeken kívül bármi mást alá lehet és alá kell rendelni a rendszer rendelkezésre állásának és zavartalan működésének, ha pedig emiatt néhány biztonsági javítás telepítése késedelmet szenved vagy éppen teljesen el is marad, az nem számít komoly problémának. Ezek a hozzáállásbeli különbségek igen gyakran vezetnek szakmai nézeteltérésekhez, ahol szinte minden esetben nehéz igazságot tenni, hiszen a saját nézőpontjából mindkét szakterületnek igaza van. Tovább súlyosbítja a problémát, hogy a másik szakterület kihívásai és prioritásai a legtöbb esetben mind az IT/IT-biztonsági, mind az OT-mérnökök számára ismeretlenek, ami nehezíti a párbeszéd kialakítását is.

[240] Az ICS protokollokról részletesebben egy három részes sorozatban lehet olvasni:
1 https://icscybersec.blog.hu/2015/12/16/ics_protokollok_1_resz
2 https://icscybersec.blog.hu/2015/12/19/ics_protokollok_2_resz
3 https://icscybersec.blog.hu/2015/12/23/ics_protokollok_3_resz

4. IT- és OT-védelem kibertámadások ellen

Ahogy korábban már érintettük, az ICS-eszközök és -rendszerek (általában az OT) nagyon sokáig egyáltalán nem foglalkozott kiberbiztonsági kérdésekkel. A Stuxnet 2010-ben történő felfedezése után ez részben megváltozott, azonban az ICS-eszközök életciklusa miatt az új eszközökbe tervezett és fejlesztett biztonsági funkciók elterjedése nagyon lassú – 9 évvel a Stuxnet nyilvánosságra kerülése után a legtöbb ICS-berendezés még mindig mindenfajta aktív biztonsági funkció nélkül üzemel. Ennek egyik legfőbb oka (túl azon, hogy még mindig sok olyan ICS-eszköz üzemel, amiket több mint 10 évvel ezelőtt helyeztek üzembe, amikor még szinte senkiben nem merült fel a kiberbiztonság kérdése), hogy az ICS-gyártók túlnyomó többsége, még ha fejleszt is biztonsági funkciót a berendezéseibe, mind a mai napig hajlamos ezeket a biztonsági funkciókat alapértelmezetten letiltott/leállított konfigurációval átadni. Ezen az állapoton azonban a már ismertetett OT-szakterületi hozzáállás miatt később már szinte lehetetlen változtatni, tehát az ICS-rendszerek biztonsági funkcióit az esetek többségében nem használják. Ez viszont azt is jelenti, hogy jelenleg az ICS-rendszerek kiberbiztonsági védelmének javításával megbízott szakembereknek, az adminisztratív kontrollokon túl, szinte kizárólag csak IT-biztonsági eszközök állnak rendelkezésükre.

Sok helyen tanítják, hogy az IT-biztonság már a tervezésnél elkezdődik és nincs ez másképp az ICS-biztonság esetében sem. Az ICS-rendszerek és -hálózatok biztonságával kapcsolatban gyakran találkozhatunk a Purdue-modell említésével. Az eredeti Purdue-modellt az 1990-es évek elején készítették el a Purdue Egyetemen[241], majd Luciana Obregon ezt dolgozta át 2015-ben Secure Architecture for Industrial Control Systems néven.[242] Terjedelmi korlátok miatt a következő bekezdésekben a Purdue-modell nagyon vázlatos áttekintésére nyílik csak mód, aki a modellt részletesebben szeretné megismerni, megteheti a megadott hivatkozásokon.

A Purdue-modell az üzleti és folyamatirányítási rendszerek hálózatait 4, a Secure Architecture for Industrial Control Systems pedig 5 (+ 1 a safety-berendezések számára) zónára osztja és szigorúan szabályozza az egyes zónákból indított, más zónákba irányuló hálózati forgalmakat. Az egyik legfontosabb elve, hogy egy adott hálózatban működő berendezések csak a közvetlenül felettük vagy alattuk elhelyezkedő zónákban üzemelő eszközökkel kommunikálhatnak – így nem fordulhat elő, hogy egy, a vállalati IT-hálózatban működő és internet-hozzáféréssel rendelkező, a támadók által kompromittált számítógép közvetlenül kommunikáljon a folyamatok vezérléséért felelős RTU-kkal vagy PLC-kkel.

A Purdue-modell (és a Purdue-modell alatt mostantól az egyszerűség kedvéért a *Secure Architecture for Industrial Control Systems*t is értjük) szerint az első zóna a vállalati zóna, és ez két szintből (5. és 4.) áll. Az 5. szinten üzemelnek többek között azok a rendszerek, amelyek a vállalat internetes megjelenését vagy a VPN-szolgáltatását biztosítják. A 4. szinten a vállalat belső életét összefogó webes alkalmazások, levelezőrendszerek, a könyvelési és egyéb nyilvántartási rendszerek találhatóak.

A következő biztonsági zóna az ICS DMZ, ahol jellemzően olyan szolgáltatások találhatóak, amik az ICS-rendszerekhez történő hozzáférések szabályozását végzik és ebben a zónában üzemelnek az infrastruktúra-üzemeltetéshez, illetve IT-biztonsági szempontból szükséges szerverek, mint például a végpontvédelmi megoldások szerverei vagy a patchmenedzsmenthez használt szerverek.

A harmadik zóna az ipari biztonsági zóna, ahol 4 további szint található. A 3. szinten az ipari vezérlőrendszerek azon komponensei üzemelnek, amik a rendszerek működésének a hátterét adják, például tartományvezérlők, történeti adatbázisok stb. A 2. szinten üzemelnek jellemzően a SCADA- és DCS-rendszerek, ezek a rendszerek fogják össze, esetenként nagy távolságból, időnként akár több ezer km-ről, a logikailag az 1. szinten elhelyezkedő ICS-eszközök működését és felügyeletét. Az 1. szinten található eszközök jellemzően azok a berendezések, amik összeköttetést képeznek a digitális és a fizikai folyamatok világa között, sok más eszköz mellett ezen a szinten leggyakrabban PLC-k, RTU-k jelennek meg. Az utolsó, 0. szinten már azok a fizikai folyamatokban közvetlenül érintett esz-

241 https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

242 https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327

közök találhatóak, amik fizikailag is beavatkoznak a folyamatokba, illetve adatokat gyűjtenek azokról és a környezetükből. Ilyenek a szenzorok, motorok, áramváltók, összeszerelő robotok, szivattyúk és pumpák és nagyon sok egyéb berendezés.

Az egyes biztonsági zónák és szintek közötti forgalmakra, ahogy már említettük, szigorú szabályok vonatkoznak, ezek betartatását különböző hálózatbiztonsági eszközökkel szokták elérni. A különböző tűzfalak és IDS/IPS-eszközök között egyaránt megtalálhatóak a vállalati IT-ben ismert és széles körben elterjedt gyártók megoldásai, ugyanakkor az ICS világa rendelkezik egyedi megoldásokkal is. Ez az egyediség igaz a hálózatbiztonsági eszközök fizikai kiépítésére is, ahol az eszközöket felkészítik az átlagos adatközpontinál sokkal zordabb környezeti körülmények közötti működésre is. Mivel az ICS-rendszerek egyes komponensei gyakran az adatközpontokban megszokottnál sokkal magasabb vagy alacsonyabb hőmérsékleten, jelentősen nagyobb porban, adott esetben viharos időjárásnak kitett helyeken vagy éppen egy olajfúró tornyon, tengervíz közelében is megbízhatóan kell működniük, ezért számos gyártó készít ún. ruggedized-eszközöket, amiket ilyen mostoha körülmények között történő működésre szánnak. A hálózatbiztonsági eszközök természetesen önmagukban, hálózati eszközök nélkül nem sokat érnek, így a hálózati eszközökből ugyanígy készülnek ruggedized kivitelű modellek.

Ezek a tűzfalak belső működésükben nem térnek el jelentősen az adatközponti tűzfalaknál megszokottaktól, azonban az IDS/IPS-eszközöknél van egy jelentős különbség. Az ICS-hálózatokban működő IDS/IPS-eszközök nagyon ritkán működnek IPS-módban, a rendszerek megbízható és kiemelkedően magas rendelkezésre állása miatt jellemzően csak IDS-módban szokták használni őket.

A hagyományos, IT-biztonságban használt végpontvédelmi megoldások ICS-környezetekben történő felhasználására is igaz az, amit már említettünk: ezeket az eszközöket a(z ipari) folyamatirányítási rendszerek világában egy kicsit máshogy kell használni, mint amit a nagyvállalati IT-biztonságban megtanultunk, megszoktunk. A végpontvédelmi megoldások használata során több különbség is van, az első rögtön az ICS-rendszerek megbízhatóságát és rendelkezésre állását érinti. Figyelembe véve, hogy az ICS-rendszereket teljesítmény szempontjából nagyon gyakran pont akkorára méretezik, amekkora teljesítményre az adott folyamatvezérlési funkcióknak szükségük van, sok eszközre nem lehet végpontvédelmi megoldást telepíteni, mert egyszerűen nincs benne az a teljesítménytartalék, amire egy további kliensszoftvernek szüksége lenne. De még ha van is ilyen tartalék az adott eszközben és az üzemeltetési szempontok figyelembevételével fel lehet telepíteni a végpontvédelmi szoftvert, az esetek döntő többségében a szoftver működését jelentősen korlátozni szokták, például az antivírus-komponens nem blokkolhatja a binárisok futását és semmilyen körülmények között nem karanténozhat vagy törölhet semmit az adott rendszerről. A legtöbb, amit tehet, hogy jelzi, hogy gyanús vagy kártékony kódot talált és a döntést az emberre kell bíznia.

Ezzel el is érkeztünk a következő védelmi eszközhöz, ami az aktív kiberbiztonsági intézkedések tárháza, az ICS-világban is ismert angol kifejezést használva az Active Cyber Defense Cycle, röviden ACDC. Rögtön az elején érdemes eloszlatni egy tévhitet: az aktív kiberbiztonság nem egyenlő a támadók ellen indított kibertámadásokkal! Az aktív kiberbiztonság négy nagyobb tevékenységből áll, melyek a következők:

- fenyegetéselemzés és információgyűjtés (threat intelligence consumption);
- eszközleltár és hálózatbiztonsági monitoring;
- incidenskezelés;
- fenyegetés- és környezetkezelés (threat and enviroment manipulation).

A következő fejezetekben azt vizsgáljuk meg, mi is tartozik a fenti tevékenységek körébe.

4.1. Fenyegetéselemzés és információgyűjtés

Az Active Cyber Defense Cycle első tevékenységének lényege, hogy a lehető legjobban ismerjük a lehetséges támadók céljait, valamint eszközeit, módszereit és eljárásait (ismét az angol kifejezés – Tools, Techniques and Procedures, más források szerint Tactics, Techniques and Procedures – rövidítését használva: TTP). Ha jól végiggondoljuk, beláthatjuk, hogy egészen máshogy kell védekezni egy olyan támadó ellen, aki a szervezetünk bizalmas adatait akarja megszerezni (gondoljunk itt pl. az Anonymous neve mögé bújó hacktivistákra), mint egy olyan kiberbűnöző ellen, aki az eszközeink számítási kapacitását kihasználva akar kriptovalutát bányászni. Ezektől is jelentősen eltérhetnek egy olyan támadói csoport módszerei, akik az ICS-rendszereink által vezérelt fizikai folyamatokat akarják megzavarni.

Az információgyűjtés és fenyegetéselemzés tevékenységéhez dolgozták ki az információgyűjtés életciklus-modelljét. Mint oly sok minden, eredendően ez a modell is az amerikai fegyveres erőkig vezethető vissza, az USA vezérkari főnökeinek egyesített bizottsága által 2013-ban kiadott Joint Publication 2.0[243] alapján a Tripwire nevű IT-biztonsági cég készített egy bevezető anyagot az IT-biztonsági információgyűjtés témájában[244].

Az információgyűjtés életciklusában az első lépés a célok minél alaposabb meghatározása és a saját terveink kidolgozása. Ahogy korábban már érintettük, ha az ICS-rendszereinket fenyegető lehetséges támadásokról akarunk információt gyűjteni, akkor a legújabb banki hozzáféréseket kereső malware-ről szóló elemzések és adatok nem lesznek hasznosak. Helyesen kell meghatározni, hogy milyen adatokra van szükségünk, reális célokat kell kitűzni magunk elé és ezeket lehetőleg egyszerű formában kell elmagyarázni azoknak az embereknek, akik ezeket az információkat fogják keresni.

Az életciklus második lépése, az információk keresése történhet publikusan (pl. nagy IT-biztonsági gyártó és -szolgáltató cégek publikációi) vagy korlátozottan elérhető (pl. iparági CERT-ek) forrásokban, illetve a saját szervezetünk határvédelmi és végpontvédelmi megoldásainak vagy bármilyen más rendszerünk, eszközünk logjainak segítségével vagy akár egy jól felépített és felparaméterezett SIEM-rendszer felhasználásával.

A harmadik lépés az összegyűjtött adatok feldolgozása és a hasznos információk kinyerése. Ez az a lépés, amikor a korábban összegyűjtött nyers adatokból kinyerjük azokat az információkat, amiket már érdemes elemezni. Erre azért van szükség, mert mint minden IT-rendszerben, úgy az ICS-rendszerekben is biztonsági elemzői szempontból nagyon sok esemény történik, ami normálisnak számít, éppen ezért az esetek többségében nem számít érdekesnek. Azonban ezeket is érdemes lehet összegyűjteni és például trendanalízis vizsgálatnak alávetni, mert – ahogy korábban már említettük, az ICS-rendszerek nagymértékű statikussága miatt – ilyen elemzések során könnyen észre lehet venni bármilyen változást (pl. megváltozik az adott időszakban kiadott Modbus write-utasítások száma), ami pedig már jele lehet egy nem engedélyezett változtatásnak, amit adott esetben egy illegális hozzáférésen keresztül hajtottak végre.

Az információgyűjtés és fenyegetéselemzés során ritka, hogy a harmadik lépés során már meg lehessen állapítani, hogy egy incidens (akár rosszindulatú, akár jó szándékú beavatkozás nyomán kialakuló incidens) nyomait fedeznénk fel. Erre általában az elemzés és jelentés készítés lépés során kerül sor. Az elemzés során a különböző forrásokból származó adatok együttes vizsgálatát értjük, amiben nagyon jelentős szerep jut a tapasztalt elemzőknek. A fenyegetettségelemzési jelentés az elemzési folyamat terméke, ami számos formát ölthet (lehet prezentáció, szöveges dokumentum, grafikonok stb.).

Az információgyűjtési életciklus utolsó lépése az elemzésről készített riport megosztása a további érintettekkel. Ez a lépés gyakran ütközik nehézségekbe, mert a legtöbb ilyen riport elkerülhetetlenül tartalmaz olyan információkat, amiket az adott szervezet bizalmasan akar kezelni (adott esetben még

[243] https://fas.org/irp/doddir/dod/jp2_0.pdf
[244] https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/

a szervezeten belül sem mindenkinek akarnak hozzáférést adni ezekhez). Ez azonban meglehetősen gyorsan képes rontani az egyébként jó minőségű elemzés értékét. Ezt a helyzetet a szervezetek saját jó hírének megőrzésére való törekvésén túl erősítik a különböző nemzeti jogszabályok, amik gyakran igen szigorúan szabályozzák, hogy ilyen információkat kivel és milyen módon lehet megosztani. Sajnos, ezek a szabályok többnyire nincsenek tekintettel a modern kiberbiztonság és az ICS-kiberbiztonság szükségleteire, így szándékaik ellenére is a támadók dolgát könnyítik meg ahelyett, hogy a létfontosságú rendszerek védelmében dolgozókat segítenék.

Ha a fenti lépéseket mind hatékonyabban vagyunk képesek végrehajtani, már van esélyünk idejében felismerni, hogy milyen fenyegetésekkel kell szembenéznie az általunk védett ICS-rendszernek. Ez azonban még csak az egyenleg egyik fele; a lehető legalaposabban ismernünk kell a saját rendszereinket is.

4.2. Eszközleltár és hálózatbiztonsági monitoring

Nagyon nehéz megvédeni olyan dolgokat, amiket nem ismerünk vagy éppen nem is tudunk a létezésükről. Éppen ezért az ACDC egyik legfontosabb eleme az, hogy tisztában legyünk azzal, mi és hogyan működik a megvédeni kívánt ICS-rendszerben. Ehhez egy olyan, átfogó nyilvántartást kell készíteni, amiben a hardver- és szoftverleltár mellett megtalálhatóak az egyes rendszerek belső és külső irányú, legitim kommunikációinak adatai is. Ez ugyan első pillantásra komoly kihívásnak tűnhet, de az ICS-környezetekben van néhány olyan sajátosság, ami segíthet célt érni. Az első, hogy az ICS-rendszerek – ahogy már említettük – nagyságrendekkel statikusabbak, mint a vállalati IT-rendszerek, sokkal ritkábbak, ellenben (jó esetben) jobban dokumentáltak és szigorúbban ellenőrzöttek a változások. Ez pedig azt is jelenti, hogy egy alaposan felmért és dokumentált helyzet esetén a nyilvántartások napra kész állapotban tartása jóval kevesebb idő és energia ráfordítását igényli, mint egy napi szinten változó vállalati IT-rendszer esetén. A másik ilyen tényező az az ICS-biztonsági szakértők között széles körben, konszenzusként terjedő ajánlás, hogy ICS-rendszereket és -környezeteket ne csatlakoztassunk publikus hálózatokra (elsősorban az internetre), illetve az ICS-rendszerekhez és -berendezésekhez hozzáféréssel rendelkező eszközöknek se legyen internet-hozzáférése. Ezt az egy ajánlást szabállyá emelve és betartva máris jelentősen csökkenthetőek az ICS-rendszerek kockázatai.

A hálózatbiztonsági monitoring az elsődleges eszköz az IT- és ICS-biztonsági incidensek minél előbb történő észlelésére. IT-biztonsági iparági források szerint 2018-ban átlagosan még mindig kb. 200 napig tudtak a támadók anélkül tevékenykedni a megtámadott és valamilyen szinten kompromittált hálózatokban, hogy az adott hálózat biztonságáért felelős szervezet ezt észlelte volna. Az elmúlt közel egy évtized ICS-biztonsági incidenseinek utólagos elemzései azt mutatják, hogy ez az idő ICS-rendszerek elleni támadások esetén nem rövidebb, többnyire még hosszabb is lehet.

A hálózatbiztonsági monitoring egy soha véget nem érő folyamat, aminek az első lépése az ismert eszközök és hálózati forgalmak alapján gyanúsnak vagy éppen csak furcsának, szokatlannak tűnő események adatainak összegyűjtése. Ebben lesz hasznos a fenyegetéselemzés és információgyűjtés során szerzett információhalmaz, ami segíthet felfedezni azokat az apró jeleket, amik mentén fel lehet ismerni egy folyamatban lévő támadási kísérletet vagy incidenst. Ezek az adatok a szerverek, munkaállomások és a különböző automatizálási eszközök logjain kívül lehetnek az adott eseményhez tartozó teljes hálózati forgalom adatai (pl. egy tcpdump-kimenet .pcap fájlban), metaadatok, hálózati forgalmak session/flow adatai, történeti adatok (pl. egy SCADA-rendszer történeti adatbázisából származó adatok) statisztikák és a különböző (időnként nem is feltétlenül IT/ICS-biztonsági eszközökből, rendszerekből származó) riasztások. Az így látókörünkbe került események elemzése a következő lépés, aminek során egyetlen kérdésre kell választ adni: elég információnk van-e, hogy az adott eseményt incidensnek tekintsük? Ha a válasz igen, akkor el kell indítani az incidenskezelési folyamatokat, ha pedig nemleges a válasz, akkor vagy fals pozitív volt az eredeti találat és foglal-

kozhatunk a következővel, vagy további információkat kell keresni a rendszereink által szolgáltatott adatforrások között.

Talán észre lehet venni, hogy a hálózatbiztonsági monitoring kapcsán a korábbiaknál jóval kevesebb szó esik az ICS-rendszerekről és -berendezésekről. Ennek oka az, hogy az ICS-rendszerekből és -berendezésekből származó eseményeket és naplóbejegyzéseket és egyéb jeleket, riasztásokat célszerű nem a vállalati IT-biztonsági ellenőrzésektől elkülönítetten, hanem azokkal együtt, egymást kiegészítő módon vizsgálni és elemezni. Ahogy korábban már beszéltünk róla, ahogy a vállalati IT- és ICS-rendszerek és -hálózatok egyre szorosabb integráció mellett működnek, úgy a hálózatbiztonsági monitoring tevékenység esetén is egyre inkább oda kell figyelni mindkét környezetre és a rendszerek közötti összefüggéseket új kontextusban is vizsgálni kell.

4.3. Incidenskezelés

Ahogy az eddig tárgyalt témák, úgy az ICS-biztonsági incidensek kezelése is több ponton eltér az IT/információbiztonság esetén bevett gyakorlatoktól, azonban az alapok és sok eszköz ugyanaz.

Az ICS-rendszerek incidenskezelésében ugyanazokat a kérdések kell feltenni, mint általában az IT-rendszerek vizsgálata során: Ki mit tett, annak milyen hatásai vannak? Hol voltak a rendszerek, amikor kompromittálták őket és mikor következett be az esemény, ami az incidenshez vezetett? Milyen módon ért el sikereket a támadó?

Részletesen most nem fogunk kitérni az IT-rendszerek incidenskezelésének minden részletére, ezekről kiváló forrásanyagok érhetőek el.[245]

A különbségek sorában az első, amivel az IT-rendszerek incidenskezelése közben jellemzően nem kell foglalkozni, az a szabályozások kérdése. A legtöbb ICS-rendszert üzemeltető szervezetnek számos, egy-egy szűkebb iparágra szabott jogszabályi és/vagy egyéb szabályozási követelménynek kell megfelelnie. Ezek jelentősen befolyásolhatják, hogy az incidenskezelés során mit és milyen körülmények között tehetnek.

Még ennél is fontosabb, hogy a folyamatirányító rendszerek esetén az incidenskezelés során is elsődleges fontosságú a biztonságos (*safe*) és megbízható vezérlés biztosítása a fizikai folyamatok megfelelő irányítása érdekében. Ahogy arról korábban már volt szó, ez a két szempont az ICS-rendszereket működtető szervezetek számára minden más szempontot felülír. Csak ezután következhet az incidenskezeléshez szükséges adatok összegyűjtése, de kizárólag olyan módon, hogy az adatgyűjtés nem lehet hatással a biztonságos (*safe*) és megbízható ICS-rendszerműködésre.

Az összegyűjtött adatok elemzése az ICS-rendszerek esetén megint egy eltérő céllal történik. Az IT-biztonsági incidensek esetén az elemzés elsődleges célja, hogy meg lehessen állapítani az incidens kiterjedését és ez alapot nyújtson az incidens káros hatásainak behatárolásában és felszámolásában. Az ICS-rendszerek esetén az incidensről gyűjtött adatok elemzése során az elsődleges feladat annak meghatározása, hogy az incidens volt-e, van-e és lehet-e hatással a folyamatok vezérlésére és az incidens felszámolásának fontossága és időzítése annak ismeretében kerül majd meghatározásra, hogy a folyamatvezérlést ez miben és mennyire érinti. Némileg furcsa lehet a gondolat, hogy egy kiemelten fontosnak tekintett ICS-rendszerben felfedezett malware-t, amennyiben az az elemzések alapján várhatóan semmilyen komoly fenyegetést nem jelent az folyamatvezérlő rendszer vagy berendezés üzemszerű működésére, illetve az ezek által felügyelt folyamatok zavartalanságára, hosszabb-rövidebb ideig is az eszközön lehet hagyni az eltávolítása előtt. Ennek az oka ilyen esetekben jellemzően nem a malware viselkedésének vizsgálata, hanem az ICS-rendszer által vezérlet folyamatok zavartalanságának biztosítása. A malware karanténba helyezése vagy törlése ICS-környezetekben gyakran

[245] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
https://www.enisa.europa.eu/publications/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems
https://www.first.org/resources/papers/conference2004/t1_01.pdf

csak akkor történik meg, amikor az adott ICS-rendszer vagy -berendezés előre tervezett karbantartása során erre lehetőség nyílik.

Felmerülhet a kérdés, hogy hogyan célszerű felépíteni egy ICS-környezetekre tervezett incidenskezelési csapatot és folyamatokat, ha ennyi ponton különbözhet az incidenskezelés ICS-rendszerek esetén? A válasz alapja (ahogy az már korábban is szóba került) az igények minél pontosabb felmérése. Konkrétumokat nagyon nehéz mondani, hiszen ahogy az ICS-rendszereket használó szervezetek, úgy az ICS-incidenskezelési folyamatok és csapatok felépítése is nagyban különbözhet az egyes szervezetek és rendszerek által támasztott igények alapján. Ennek a leginkább hatékony módja, ha az adott szervezet menedzsmentjének és a fizikai folyamatok irányításáért felelős mérnököknek (akik felhasználói, illetve üzemeltetői az ICS-rendszereknek) felteszünk néhány egyszerűnek tűnő kérdést, például: *„Mi történne, ha az adott szivattyútelep, alállomás vagy gyártósor teljesen leállna?”* Fel kell mérni továbbá a függőségeket, mert egy adott rendszer leállása hatással lehet egy másik, logikailag az elsőtől teljesen független(nek látszó) rendszerre is.

Az ICS-incidenskezelésbe bevont csapat esetén az első kérdés, amit fel kell tenni, hogy saját alkalmazottakból álló csapatot vagy külső incidenskezelési támogatókat akarunk alkalmazni? Mindkét változatnak megvannak a maga előnyei és hátrányai. A belső incidenskezelő csapat megfelelő képzések és belső kommunikáció esetén minden valószínűség szerint sokkal mélyebb és alaposabb ismeretekkel fog rendelkezni az adott ICS-rendszerek és -berendezések működésével, céljával és feltételezhető gyenge pontjaival kapcsolatban, mint egy külsős támogató csapat. Hosszabb távon azonban a belsős csapat szakmai és (valljuk be őszintén, a jelenlegi, 2019-es munkaerőpiaci helyzet alapján) anyagi motivációjának fenntartása egy igen komoly kihívás lehet még egy nagy szervezet számára is. Ezzel szemben egy külső incidenskezelő csapat esetén a szervezet számára sokkal tervezhetőbb az incidenskezelési szakértő bevonásának költsége, azonban (lévén olyan személyekről beszélünk, akik mindenképp kevesebb ismerettel fognak rendelkezni a szervezetről, a rendszerekről – ideértve az ICS-rendszereket is) a munkavégzésük során végig a szervezet belső munkatársainak szakértelmére kell majd támaszkodniuk. Amennyiben a gyakorlatok során a külső és belső szakértők nem szereznek megfelelő gyakorlatot az együttműködésben, és ami még fontosabb, az egyértelmű kommunikációban, ez jelentősen ronthatja a hatékonyságot egy nagy mértékben időkritikus tevékenység során.

Mekkora legyen az incidenskezelésre kijelölt csapat mérete? Mindenképp szükség van egy operatív csoportvezetőre, aki az incidenskezelésben részt vevő csapat munkáját szervezi és az általuk feltárt részleteket közli az incidenskezelést vezető személlyel (aki jellemzően már a menedzsment tagja, ő fogja tájékoztatni a teljes menedzsmentet és szükség esetén a sajtót, illetve az ügyfeleket). Ideális esetben a szervezetnél van egy főállású incidenskezelő, akinek az elsődleges feladata az incidensek bekövetkezésére történő felkészülés, eljárások, szabályok kidolgozása, azok rendszeres tesztelése és – szükség esetén – hangolása.

Az operatív incidenskezelő csoport létszáma 3-4 fő esetén már megfelelő lehet, esetükben arra kell ügyelni, hogy minden érintett szakterületet és kompetenciát le tudjunk fedni. Figyelembe kell venni azt is, hogy a 3-4 embernek minden körülmények között (szabadságolások, betegségek, felmondások miatti időszakos létszámcsökkenés stb.) rendelkezésre kell állnia. Ráadásul a legtöbb kiberbiztonsági incidens nem néhány óra alatt felszámolható esemény és bár ilyenkor egy váltás akár 12-16 órás műszakokat is képes és hajlandó végigdolgozni, mindenképp célszerű legalább két váltásban gondolkodni. A fáradt incidenskezelők sokkal könnyebben siklanak el nehezen észrevehető, de fontos részletek fölött, így mindenképp hasznos megfelelő pihenőidőt biztosítani az operatív incidenskezelésben résztvevő kollégák számára – még akkor is (és ezt célszerű adott esetben utasításba is adni), ha ők maguk úgy érzik, nincs szükségük pihenésre!

Milyen képességekkel rendelkezzenek az incidenskezelésben résztvevő csoport tagjai? Egyrészt legyenek tapasztalt és gyakorlott szakemberek a saját szakterületükön, legalább egy-egy folyamatirányítási mérnök, OT-mérnök és *computer forensics* szakértő mindenképp legyen a csoport tagja.

Emellett nem árt, ha rendelkezésre áll néhány további szakember IT- és OT-területről, akiktől szükség esetén azonnal pontos válaszokat lehet kapni a feltett kérdésekre.

Emberi képességek terén fontos, hogy türelmes emberek dolgozzanak az incidens felszámolásán, akik képesek ellenőrzőlista alapján dolgozni. Vannak olyan kiváló szakemberek, akik, bár saját szakmájukat olyan magas szinten űzik, hogy azt már művészetnek is nevezhetnénk, de talán éppen ezért képtelenek az incidenskezelésnél szükséges fegyelmezett munkavégzésre és folyamatosan elkalandoznának egy-egy nyomot követve – ők erre a feladatra nem lesznek alkalmasak. További nagyon fontos képesség, hogy az incidenskezelésben operatív szinten részt vevő embereink legyenek képesek segítséget kérni, ha úgy érzik, erre van szükség. Az incidenskezelés minden esetben csapatmunka, az egyéni ambíciók nem segítik, csak hátráltatják az egyetlen célt, az incidens mielőbbi felszámolását és a normál, üzembiztos folyamatok helyreállítását. Az incidenskezelés több szempontból is egy nagyon stresszes feladat, emiatt az incidenskezelő csoport tagjainak jól kell tudniuk teljesíteni nagy nyomás alatt. Elég csak arra gondolni, hogy a menedzsment irányából folyamatosan érkezni fognak a kérdések azzal kapcsolatban, hogy mekkora a baj, mikorra lehet helyreállítani a normális állapotokat. Az incidenskezelési vezető, másrészt az operatív csoportvezető feladata, hogy minden zavaró körülményt távol tartsanak az incidenskezelés operatív részét végző csapattól, hogy nekik csak a saját feladataikra kelljen koncentrálni. Ez még csak a stresszfaktorok egyik fele, nyilván az incidenskezelési csoport tagjai is pontosan tudják, mekkora a tét és milyen sok függ attól, hogy ők milyen gyorsan és alaposan dolgoznak, azonban figyelembe kell venni, hogy az incidenskezelés napokig, de akár hetekig, hónapokig is tarthat – erre volt példa a 2015-ös, nyugat-ukrajnai áramszolgáltatók elleni és a 2019. tavaszi, Norsk Hydro elleni ransomware-támadás is. Végül, de nem utolsósorban, az incidenskezelésben résztvevőknek kiemelkedően jó kommunikációs képességekkel kell rendelkezniük.

Az incidenskezelés hatékony gyakorlásához elengedhetetlen, hogy azonnal rendelkezésre álljon minden olyan felszerelési tárgy, amire az incidenskezelési csoportnak szüksége lehet. A felszerelések listája szervezetenként különbözhet, most csak egy nagyon általános felsorolás következik:

- digitális forensics eszközök (olyan szoftverek, amikkel össze lehet gyűjteni egy számítógép merevlemezén vagy memóriájában tárolt adatokat);
- olyan hálózati eszköz, ami képes az adott környezetben előforduló legnagyobb sávszélességet is kezelni;
- hálózati kábelek és átalakítók (USB-soros port átalakítók stb.);
- Több, nagy kapacitású (akár több TB-os) USB, HDD/SSD az egyes számítógépekről és a hálózatból gyűjtött adatok tárolására;
- számos kisebb kapacitású (8–256 GB) USB-adathordozó;
- néhány darab írható CD/DVD (arra az esetre, ha egy adott ICS-környezetben az USB-portok használata tiltva van);
- a feladatra felkészített, tiszta laptopok az engedélyezett/bevizsgált scriptekkel és szoftverekkel az első elemzések elvégzéséhez;
- nagy felbontású fényképek készítésére alkalmas fényképezőgép (szükség esetén erre ma már a mobiltelefonok is megfelelőek lehetnek, azonban minden eszköznél érdemes ügyelni arra, hogy az incidenskezelés során készített képeket szabad-e az adott szervezet szabályai szerint felhős tárhelyre szinkronizálni!);
- antisztatikus műanyag zacskók, öntapadós címkék és jegyzetfüzetek;
- ellenőrzőlista a korábban kidolgozott és tesztelt eljárásokkal és a fontosabb személyek elérhetőségeivel;
- személyi biztonsági eszközök (pl. munkavédelmi sisak);
- az informatikai hálózattól független kommunikációs eszközök (pl. CB-rádiók).

Természetesen ez a lista korántsem teljes, de kiindulási alapnak bárhol jó lehet, ami aztán a (jó esetben csak tesztek során szerzett) tapasztalatok alapján módosítható.

4.4. Fenyegetés és környezet kezelése

Az Active Cyber Defense Cycle utolsó nagy témaköre a fenyegetések és környezet kezelése. Ahogy az incidenskezelésről szóló fejezetben is szóba került, egy éles ICS-környezetben bekövetkező kiberbiztonsági incidens esetén arra nincs mód, hogy hosszan tartó vizsgálatokkal részletekbe menően megismerjük az incidens során talált malware-ek, illetve a felfedezett támadók tevékenységének minden részletét, ezt az ICS-rendszerek legfontosabb biztonsági szempontjai, a safety és a rendelkezésre állás nem teszik lehetővé. Éppen ezért fontos, hogy az incidens elhárítása és a legfontosabb tanulságok levonása, majd a szükséges intézkedések megtétele után egy megfelelően szeparált laborban tudjuk tovább vizsgálni az incidens során felfedezett malware-eket és a támadók egyéb eszközeit és módszereit.

Az ICS-környezetekben felfedezett malware-ek döntő többségét nem célzottan ICS-rendszerekre tervezték és hozták létre, az esetek nagyobbik részében egy általános, IT-rendszerek elleni támadásra felkészített malware talál utat az ICS-rendszerekbe is (ilyenek voltak pl. 2017-ben a WannaCry- és a NotPetya-malware-ek is, amik számos ipari rendszert is használhatatlanná tettek, de mindmáig nincs bizonyíték arra, hogy ezeket a támadásokat célzottan az áldozatul esett ipari szereplők ellen indították volna).

A támadók által használt malware-ek és egyéb eszközök elemzése, különösen célzott támadások esetén nagyon összetett és komoly elméleti és gyakorlati tapasztalatokat igénylő feladat, amit célszerűbb és hatékonyabb lehet erre specializálódott szakértőkre, külső szolgáltatókra bízni. Ha ilyen szolgáltató bevonása mellett dönt a vállalat, hasznos lehet – amennyiben ezt kölcsönösen szükségesnek és hasznosnak találják – egy rövid képzés keretében megismertetni a külső szakértőket a malware által megfertőzött rendszer vagy rendszerek működési alapelveivel és a vezérelt folyamatokkal kapcsolatos alapismeretekkel.

Ha semmiképpen nincs mód külső szakértőket bevonni és muszáj belső erőforrásokkal elvégezni az elemzést, első lépésként ki kell alakítani a malware elemzéséhez használt (labor)környezetet. Ezek az esetek többségében virtuális gépek, hiszen ez a leginkább költséghatékony módja a malware-gyanús kódok tesztelésének, de célszerű néhány natív számítógépet különböző, az éles környezethez hasonló szoftverekkel telepített tesztgépként kéznél tartani, mert a kifinomultabb malware-ek napjainkban már képesek figyelni bizonyos, a virtuális környezetekre jellemző tulajdonságot és amennyiben egy vagy több ilyet találnak, megszakíthatják a futásukat, hogy el tudják kerülni a sandboxban történő felfedezésüket.

A tesztkörnyezet kialakítása után érdemes részletesen dokumentálni minden, az incidenssel kapcsolatban összegyűjtött bizonyítékot (sok egyéb mellett adathalász e-maileket, érdekesebb hálózati forgalmakról készített .pcap fájlokat, memóriaképfájlokat stb.). Ezután az első vizsgálatok során azt kell megállapítani, hogy a talált malware-minták ismert malware-családhoz tartoznak-e. Ez ismét egy olyan pont, ahol a legjobb megoldás egy erre szakosodott külső szakértő bevonása. Ha erre nincs lehetőség, akkor az adott szervezet által használt antivírus-megoldással, illetve, ha rendelkezésre áll, saját antivírusfarmmal lehet zárt hálózatokban vizsgálatokat folytatni. Az interneten elérhető sandbox-szolgáltatásokat (pl. VirusTotal) csak akkor érdemes bevonni a vizsgálatokba, ha már legalább egy kereskedelmi forgalomban kapható AV-termék felismerni vélte a vizsgált mintát. Amennyiben minden rendelkezésre álló antivírustermék ártalmatlannak találta az adott mintát és akár csak a leghalványabb gyanú is felmerülhet egy célzott támadással kapcsolatban, érdemes nem feltölteni a malware-gyanús mintát az internetes sandbox szolgáltatásokba. A legtöbb célzott támadásra képes csoport ugyanis ma már felkészül arra, hogy figyelje, mikor kerül fel az általa fejlesztett malware egy példánya ezekbe a szolgáltatásokba és elveszítjük a velük szemben szerzett előnyünket, ha ilyen módon tudatjuk velük, hogy felfedeztük a támadásukat (amivel lehetőséget adunk nekik, hogy új módszerekkel ismét próbálkozzanak és nekünk ismét fel kelljen fedeznünk, hogy ezúttal milyen módon és hol törtek be megint a rendszereinkbe). Ha az automatizált malware-elemző megoldások és a különböző IoC-k (Indicatior of Compromise, a már ismert malware-ek és egyéb támadói eszközök

adatai) nem hoznak eredményt, az elemzést kézi módszerekkel lehet folytatni, a különböző dinamikus és statikus elemzési módszerekkel. Ahogy ebből a fejezetből is látható, a malware-elemzés egy igen összetett és komoly szakmai ismereteket és tapasztalatot igénylő tevékenység, ezért érdemesebb inkább ezen a téren megfelelő tapasztalatokkal rendelkező külső szakértőkre bízni, ha erre lehetősége van az adott szervezetnek.

5. Kiberbiztonsági műszaki megfelelőségi követelmények villamosenergia-környezetben

5.1. Jogszabályi követelmények

5.1.1. EU NIS

Az Európai Unió Hálózat- és Információbiztonsági Irányelve (Network and Information Security Directive, NIS, EU 2016/1148) az Európai Bizottság által az EU kiberbiztonsági stratégiája alapján készülő átfogó kiberbiztonsági jogszabályok első eleme. Irányelvként minden EU-tagországnak egyedileg kell beillesztenie a benne foglaltakat a nemzeti jogrendbe. Az NIS-direktíva célja, hogy az EU teljes területén fejlessze a kiberbiztonság szintjét.

Az EU NIS-direktíva három részből áll:

- nemzeti képességek (pl. nemzeti CERT/CSIRT létrehozása és üzemeltetése);
- határokon átnyúló együttműködések (pl. EU-szintű incidenskezelési operatív hálózat, stratégiai együttműködési csoport stb.);
- nemzeti kritikus infrastruktúrák (energiaszektor, közlekedés és szállítmányozás, víziközmű hálózat, egészségügy és pénzügyi szektor, valamint a nemzeti kritikus digitális szolgáltatók – az egyes országok internetes forgalom kicserélő központjai, DNS szolgáltatás stb.).

5.1.2. Magyar jogszabályi helyzet

Magyarországon a villamosenergia-szektorban a jogszabályi követelmények helyzete jelenleg (2019 augusztusában) nem egészen tiszta. Az EU NIS egyértelműen a direktíva hatálya alá tartozóként jelöli meg az villamosenergia-szektort, ebbe meglehetősen nehéz nem beleérteni az ország villamosenergia-ellátásáért felelős szervezeteket (a nagyobb erőműveket, az átviteli rendszerirányítót és az áramszolgáltatókat). A magyar országgyűlés azonban az EU NIS-direktívában megfogalmazott elvárásokat a 2012. évi CLXVI. törvénybe (a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvénybe) illesztette be. A 2012. évi CLXVI. törvény hatálya alá tartozó szervezetekre automatikusan hatályos a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról és a kapcsolódó, 41/2015. BM rendelet. Az érdekes helyzetet az eredményezi, hogy számos villamosenergia-ipari szereplő nem tartozik a 2012. évi CLXVI. törvény hatálya alá, ezáltal pedig sem az információbiztonsági törvény, sem a kapcsolódó BM rendeletben foglalt követelményeknek nem kötelező megfelelniük, ami azzal jár, hogy ezek a szervezetek jellemzően nem törvényi kötelezettségük, hanem saját józan belátásuk alapján fejlesztik az IT- és ICS-rendszereik kiberbiztonsági védelmét.

5.1.3. Szabványok

Az ICS-rendszereket használó szervezetek különböző okokból (jogszabályi megfelelési kényszer vagy saját jól felfogott érdekük miatt) számos kiberbiztonsági szabványt vezettek be, ezek azonban (ritka kivételektől eltekintve) többnyire inkább az általános információ-/IT-biztonsági kontrollokra koncentrálnak (a leggyakoribb az ISO 27000-es szabványcsaládból az ISO 27001/27002/27005). Amióta a magyar jogszabályok megkövetelik, hogy a szervezetek által kibocsátott számlákat előzetesen auditálja egy, az állam által erre akkreditált ellenőr (jelen sorok írása idején ilyen akkreditációval a Hunguard Kft. rendelkezik), azóta nagyjából minden ICS-rendszert alkalmazó magyar közép- és nagyvállalat évente át kell, hogy essen egy újabb auditon, amelynek alapja jelenleg az NIST (az amerikai nemzeti technológiai és szabványügyi testület) SP 800-53-as kiadványában összefoglalt biztonsági kontroll-gyűjtemény. Az alábbiakban az ezeken túlmutató, kifejezetten az ipari automatizálási és folyamatvezérlési feladatokra használt rendszerek sajátosságait is ismerő szabványok közül fogunk röviden áttekinteni néhányat.

5.1.4. ISA/IEC 62443

Az ISA/IEC 62443 szabványcsalád az ISA99 (az International Society of Automation, a Nemzetközi Automatizálási Társaság biztonsági kérdéseivel foglalkozó szervezete) által kidolgozott és az IEC (International Electrotechnical Commission, a Nemzetközi Elektrotechnikai Tanács) által elfogadott biztonsági szabványokat tartalmazza. Jelenleg az ISA/IEC 62443 családba két szabvány tartozik, a 62443-4-1, ami az ipari automatizálási és vezérlési rendszerek (Industrial Automation and Control Systems, IACS) biztonságos fejlesztési életciklusát írja le és a 62443-4-2, amiben az IACS-rendszerek műszaki biztonsági követelményeit foglalják össze.

Az ISA/IEC 62443 a szabványokon túl egy 4 részből álló kiberbiztonsági tanfolyamsorozatot is tartalmaz, minden tanfolyamhoz egy-egy vizsgával, a vizsgát sikeresen teljesítők pedig egy nemzetközileg elismert minősítést szerezhetnek. A négy tanfolyam az alábbi témakörök köré épül:

1. ISA/IEC 62443 Cybersecurity Fundamentals (alapok),
2. ISA/IEC 62443 Cybersecurity Risk Assessment (kockázatelemzés),
3. ISA/IEC 62443 Cybersecurity Design (tervezés),
4. ISA/IEC 62443 Cybersecurity Maintenance (karbantartás).

5.1.5. ISO 27019

Az ISO 27000-es szabványcsaládban az ISO 27019-es szabvány (a legfrissebb verzióját 2017-ben adták ki) foglalja össze az energetikai szektorban működő közművek információbiztonsági kontrolljait. Maga az ISO 27019 a 27002-es szabványt veszi alapul és ezt egészíti ki olyan ajánlásokkal, amiket kifejezetten a villamosenergia-, gáz- és olajipari szektorokban használt ICS-rendszerek sajátosságait is figyelembe véve dolgoztak ki. A szabvány külön figyelmet szentel a központi és elosztott vezérlő és monitoringrendszerekre, a különböző digitális/analóg interfész berendezésekre (RTU-k, PLC-k stb.) és mindazokra a támogató informatikai és kommunikációs rendszerekre, amelyek nélkül ma már az ICS-rendszerek megbízható működése elképzelhetetlen. Egyetlen terület van, amit az ISO 27019 nem fed le, ez a nukleáris létesítményekben alkalmazott rendszerek, ezt a területet az IEC 62645-ben kezelik.

5.1.6. NIST Special Publication 800-82 Revision 2

Az NIST SP 800-82-t az ICS-rendszerek biztonsági útmutatójaként hozták létre 2011-ben, azóta két nagyobb felülvizsgálaton esett át, legutóbb 2015 elején. A 800-82 jelenleg a 800-53 Revision 4 kiadásához igazítva ad útmutatást az ICS-rendszerek (ideértve a SCADA- és DCS-rendszereket, RTU-kat, PLC-ket és egyéb, a Purdue-modell alapján összefoglalóan Level 1 és Level 0 eszközökként hivatkozott ICS-berendezéseket) biztonságával kapcsolatban, egyben szem előtt tartva az érintett berendezések egyedi teljesítmény, megbízhatósági és biztonsági (safety) szempontjait is.

A második felülvizsgálat a korábbiak mellett frissítéseket tartalmaz az ICS-fenyegetések és sérülékenységek témájában, a kockázatelemzéshez és a biztonságos rendszertervezéshez is tanácsokat ad és harmonizálja a 800-82 viszonyát más ICS-biztonsági szabványokkal.

6. Konkrét kibertámadások és azok tanulságai

6.1. Korai kibertámadások ICS-rendszerek ellen

A 2010-es évek végére az ICS-rendszerek és általában a létfontosságú rendszerek elleni kibertámadások száma jelentősen megnőtt. 2010 nyara, a Stuxnet nyilvánosságra kerülése előtt az ICS-rendszerek elleni kibertámadásokról csak egy nagyon szűk szakmai közösségen belül folyt az eszmecsere, ez azonban a Stuxnet megjelenése után szinte azonnal komolyan vett témává vált. Az ezt megelőző ICS-biztonsági incidensek esetén mindmáig vita van arról, hogy ezeknél a támadásoknál a kiberbiztonsági komponens része volt-e az incidens bekövetkeztének.

Az első ilyen incidens az 1982-es transzszibériai gázvezeték felrobbanása. Számos forrás tényként kezeli, hogy a Szovjetunió, mivel a gázvezeték vezérléséhez használható ICS-rendszer COCOM-listás termék volt (vagyis olyan termék, amit az egykori keleti blokk országainak tilos volt eladni), ezért a KGB erre szakosodott főigazgatósága ellopta a szükséges szoftvereket, amiben azonban egyes nyugati titkosszolgálatok egy trójait helyeztek el. A trójai végül 1982 júniusában robbanást idézett elő a gázvezetékben.[246]

Bruce Schneier, ismert IT-biztonsági kutató állítása szerint a 2003-as nagy amerikai áramszünetet, ami az USA északkeleti és Kanada délkeleti államaiban okozott jelentős károkat, közvetetten a Blaster néven ismert számítógépes féreg okozta. Az üzemzavar utáni vizsgálatok ugyan azt állapították meg, hogy az érintett területek villamosenergia-ellátásáért felelős ICS/SCADA-rendszerek nem Windows operációs rendszert futtattak, így azokra a Blaster közvetlenül nem jelentett veszélyt, de Bruce Schneier szerint az ezeket a rendszereket monitorozó rendszerek Windows-alapúak voltak és azok egy részét érintette a Blaster-féreg támadása. A monitoringrendszerek átmeneti üzemképtelensége pedig ahhoz vezetett, hogy a rendszer felügyeletét ellátó mérnökök nem vették észre a kezdeti, kisméretű üzemzavart, ami aztán egy jelentősen nagyobb üzemzavarrá tudott nőni.[247]

6.2. Stuxnet

A Stuxnet máig ható mérföldkőnek számít az ICS-biztonság területén, ezért mindenképp érdemes összefoglalni, hogy pontosan mi is történt az iráni urándúsítási projekt körül a 2000-es évek végén.

Az utólagos elemzések szerint a Stuxnet USB-adathordozó(ko)n jutott be az iráni urándúsítási folyamat központjának számító natanzi létesítményben üzemelő Windows-os számítógépekre, majd ott két, tajvani hardvergyártó/-fejlesztő cég kódaláíró tanúsítványát felhasználva, több, korábban

[246] Reed, Thomas C. (2007): *At the Abyss: An Insider's History of the Cold War.* Random House Publishing Group.
[247] Schneier, Bruce (2018): *Click here to kill Everybody.* W. W. Norton & Company, ,94.

ismeretlen (0-day) sérülékenységet kihasználva rendszerszintű jogosultságot szereztek. Ezt a jogosultsági szintet kihasználva az urándúsító centrifugák vezérléséért felelős PLC-k és a Windows-t futtató mérnöki munkaállomások közötti Siemens WinCC egyik DLL-jét cserélték le a támadók a saját változatukra. A WinCC és a PLC-k között Man-in-the-Middle helyzetbe kerülve a támadók képesek voltak egy 21 másodperces, normál működési mintát rögzíteni, majd visszajátszani a mérnöki munkahely előtt ülő felhasználók számára, akik így nem lehettek tisztában azzal, hogy a képernyőkön látható értékek nincsenek összhangban a centrifugák valós fordulatszámával. Miután az urándúsítási folyamatot felügyelő mérnökök megtévesztése készen állt, a támadók elkezdték az általuk rögzített 21 másodperces felvételt végtelen ciklusban ismételni, közben pedig a Step7-illesztőprogramon keresztül megfordították az egymás után sorba kötött centrifugák forgási irányát, ezzel máris használhatatlanná téve az urándúsítási folyamatban kulcsfontosságú urán-hexafluorid gázt. Ezután pedig elkezdték fel (86400 fordulat/perc sebességig) és le (120 fordulat/percre) szabályozni a centrifugák fordulatszámát, amivel nem csak a különböző uránizotópok keveredtek össze, de az egymás után sokszor történő felgyorsítás és lelassítás végül a centrifugák mechanikai sérüléseihez is vezettek. Egyes források szerint a Stuxnet működése akár 1000 centrifuga meghibásodását is okozhatta, bár vannak olyan elemzések, amelyek szerint nem a centrifugák fizikai megsemmisítése volt a támadók célja. A támadók egyébként annyira jó munkát végeztek a Stuxnet lopakodó képességeinek fejlesztésekor, hogy (megint csak az incidensről készített elemzések szerint) közel 6 évig tudott működni a malware anélkül, hogy bárki észrevette volna.

A Stuxnetről számos elemzés készült, az ICS-biztonsági szakmán belül többé-kevésbé konszenzus van azzal kapcsolatban, hogy az egyik legjobb Ralph Langner munkája, ami *„To Kill a Centrifuge”* címmel jelent meg.[248]

6.3. Havex/Dragonfly

2013. február és június között támadók célzott adathalász támadások keretében malware-fertőzött PDF-dokumentumokat küldtek e-mailben különböző, energiaszektorban dolgozó felsővezetőknek. Az általános adathalász támadásokkal ellentétben ezek az e-mailek nagyon jól kidolgozottak és személyre szabottak voltak, így a sikeres támadások aránya is jóval nagyobb volt, mint az átlagos adathalász próbálkozások esetén.

Ezután, illetve részben ezzel párhuzamosan, a támadás második fázisaként a támadók több, az energiaszektorban működő szervezet weboldalát kompromittálták és ún. watering hole-támadásokat (az ilyen típusú támadásokról a *Számítógépalapú Social Engineering-technikák bemutatása* című fejezetben még bővebben lesz szó) indítottak újabb célpontok ellen. Ennek a fázisnak a célja egy Remote Access Tool (RAT) telepítése volt, hogy hátsó ajtót nyissanak a célba vett rendszereken.

A harmadik fázisban a támadók három ICS/SCADA-gyártó vállalat (német, svájci és belga cégek) rendszereit kompromittálták és módosították a weboldalaikat, ezzel elérve, hogy az ügyfelek az adott cég ICS/SCADA-szoftverei helyett a Havex malware-rel fertőzött változatot töltsék le és telepítsék. A fertőzött fájlok 10 nap és 6 hét közötti időtartamig voltak elérhetőek a gyártók weboldalain, mielőtt felfedezték és eltávolították volna őket.

A Havex/Dragonfly-támadásokat utólag több nagy IT-biztonsági cég is részletesen elemezte (emiatt is van az esetnek egynél több neve, az F-Secure Havexként[249], a Symantec Dragonfly-ként[250] hivatkozik nagyjából ugyanarra a támadói csoportra és támadásokra). Az elemzések alapján arra a következtetésre jutottak, hogy a támadás célja a megcélzott szervezetek hálózatainak és ICS-, valamint

248 https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
249 https://www.f-secure.com/weblog/archives/00002718.html
250 https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

IT-rendszereinek felderítése volt, ehhez az OPC (Open Platform Communication) ipari protokollt használták, ami egy ipari telekommunikációs szabvány protokoll.

A Havex/Dragonfly-támadásokról (mint a legtöbb kibertámadásról általában) nem sikerült minden kétséget kizáróan megállapítani, hogy kik is állhattak mögötte, bár a támadásokat elemző szakértők többnyire az orosz állami hátterű APT-csoportok egyikét tartják felelősnek. Évekkel később történt incidensek után olyan feltételezések is megjelentek, hogy a Havex/Dragonfly-támadások valóban felderítési célú műveletek voltak, amikor felmérték a későbbi, immár a fizikai világra is hatást gyakorló támadások lehetséges célpontjait. Az első ilyen támadásokra nem is kellett nagyon sokat várni.

6.4. Kibertámadás ukrán áramszolgáltatók ellen

2015. december 23-án, helyi idő szerint délután fél négy körül a nyugat-ukrajnai régióban működő Kyivoblenergo áramszolgáltatónál ügyeletes villamosmérnökök azt tapasztalták, hogy bár senki sem ér az elosztóhálózat alállomási távkezelését biztosító számítógépek beviteli eszközeihez, a kurzor mozogni kezd és sorban megpróbálja kikapcsolni az egyes alállomásokat.[251] A támadók összesen 7 darab 110kV-os és 23 darab 35 kV-os alállomáson idéztek elő üzemzavart, ami összesen mintegy 225 000 fogyasztót hagyott villamos áram nélkül a tél közepén.

Az üzemzavar és az áramkimaradások előidézése után a támadók törölték az üzemirányításhoz használt ICS/SCADA-rendszerek számítógépeinek merevlemezeit, különös gondot fordítva arra, hogy néhány, kulcsfontosságú binárist ne csak egyszerűen töröljenek, hanem felül is írjanak, így téve még nehezebbé a helyreállítást. Ezzel párhuzamosan az alállomásokon használt RTU-k egy jelentős hányadán illegális firmware-frissítéseket hajtottak végre, ami után az érintett RTU-k végleg üzemképtelenné váltak (a korábbi, megfelelően működő firmware helyreállítása is lehetetlenné vált), végül DoS-támadást indítottak az ügyfélszolgálati telefonvonalak és a hibabejelentésre használható weboldalak ellen.

Csak néhány órával később derült ki, hogy nem egy, hanem összesen négy nyugat-ukrajnai regionális áramszolgáltatót ért támadás, ezek közül háromnál a fent leírtakhoz hasonlóan idéztek elő üzemzavart, majd tették tönkre az alállomási automatizálás és távkezelés eszközeit.

Az ukrán áramszolgáltatók annak köszönhetően tudták néhány óra alatt helyreállítani az áramszolgáltatást, hogy az érintett áramszolgáltatók és alállomások esetében az automatizáltság foka még nem volt nagyon magas, ezért rendelkezésre álltak azok az elektrikus szakemberek, akiket az érintett alállomásokra vezényelve kézi vezérlésre tudták állítani az alállomásokat és így december 23-án késő estére a legtöbb érintett területen sikerült helyreállítani az áramszolgáltatást. A támadásoknak azonban hosszabb távú hatásai is voltak, a tönkretett RTU-k egy részét még 2016 áprilisában sem tudták kicserélni.

Az ukrán kormány hivatalosan is az orosz titkosszolgálatokat vádolta a támadásokkal, egyértelmű bizonyítékokkal azonban nem rendelkeztek. Már december 23-án ukrán és amerikai állami szervek, valamint IT- és ICS-biztonsági magáncégek szakértői indultak az incidensek helyszíneire. Az általuk rögzített nyomok és az azok alapján készült elemzések szerint a támadók 9 hónappal korábban, 2015. márciusban makróvírussal fertőzött Microsoft Office-dokumentumokat küldtek a célba vett áramszolgáltatók dolgozóinak. A makrók futtatása annak ellenére sikeres volt, hogy az érintett áramszolgáltatók a megfelelő házirenddel tiltották a makrók futtatását, azonban a támadók social engineering-technikákkal rávették a célba vett felhasználókat, hogy engedélyezzék a makrók futtatását. Az így elinduló makró volt az ún. dropper, ami egy előre megadott IP-címen elérhető szerverről letöltötte a BlackEnergy nevű malware-t, ami hátsó ajtókat nyitott a megfertőzött számítógépeken, így biztosítva hosszabb távon hozzáférést a támadók számára és lehetőséget az adott szervezet IT- és ICS-

[251] Az alábbi linken egy YouTube-ra feltöltött videón az látható, ahogy a támadók éppen próbálják lekapcsolni az egyik alállomás eszközeit: https://www.youtube.com/watch?v=8ThgK1WXUgk

hálózataiban a további célpontok keresésére. Ezután legitim felhasználói azonosítókat és jelszavakat kerestek (és találtak is), amelyek birtokában újabb rendszerek felett szereztek irányítást és egyre több adatot loptak ki az áramszolgáltatók rendszereiből, amik később hasznosnak bizonyulhattak az üzemzavar előidézése során.

A 2015. decemberi ukrán áramszolgáltatók ellen végrehajtott támadásokról a SANS Institute munkatársai, Robert M. Lee, Michael J. Assante és Tim Conway, az amerikai E-ISAC-kel közösen egy nagyon alapos elemzést készítettek, amiben nem csak a támadások részleteit mutatták be, hanem vázolták egy várható jövőbeli támadásnál használt eszközök tárházát és tanácsokat is megfogalmaztak az ilyen támadások elhárítására.[252]

6.5. Industroyer/CrashOverride

Szinte pontosan egy évvel később, 2016. december 17-én ismét kibertámadás érte az ukrán villamosenergia-rendszert, ezúttal az Ukrenergo, az ukrán villamosenergia-ipari rendszerirányító Kijev melletti alállomásán (egy 330 kV-os alállomáson) idéztek elő üzemzavart a támadók. Bár a 2016-os támadás az alállomások számában (2015-ben több mint 50 áramszolgáltatói alállomás volt érintett a 2016-os egyetlen alállomással szemben) nem ért fel az egy évvel korábbi incidenssel, de a támadás hatására kieső teljesítmény mégis nagyobb volt (2015-ben 135 MW, 2016-ban 200 MW).

A másik jelentős különbséget a támadáshoz használt moduláris malware jelentette. Az első elemzést a malware-ről az ESET szlovák IT-biztonsági cég készítette, ők nevezték el a malware-t Industroyernek. A CrashOverride nevet a Dragos, egy amerikai ICS-biztonságra specializálódott cég adta a malware-nek, az ő elemzésük szerint a támadás mögött egy általuk ELECTRUM névvel azonosított támadói csoport áll.

A 2015-ös incidensnél a támadók a malware-eket a kezdeti számítógép-kompromittálásokhoz és a megfertőzött gépek törléséhez használták fel, magát az üzemzavart a támadók manuálisan idézték elő. Ezzel szemben a 2016-os támadás során bevetett moduláris malware nagymértékben automatizált volt, a támadóknak sokkal kevésbé kellett manuális műveletekre hagyatkozni. A moduláris felépítés miatt a malware-t kisebb módosításokkal fel lehet használni gyakorlatilag bármilyen ICS-rendszer elleni támadásnál. A 2016-os ukrán incidens idejéről származó minta a 101-es (IEC 60870-5-101), 104-es (IEC 60870-5-104), IEC 61850-es és OPC DA (OLE for Process Control Data Access) protokollokat ismerte. A támadásról és a malware-ről több, kifejezetten színvonalas elemzés látott napvilágot.[253]

Az Industroyer/CrashOverride malware a negyedik, kifejezetten ICS-rendszerek ellen tervezett malware (az első a Stuxnet, a második a BlackEnergy, a harmadik a Havex) és egyben az első, amit kifejezetten a villamosenergia-rendszer elleni támadásra hoztak létre. Veszélyességét a modularitása és a nagyfokú autonóm működése mutatja (a Stuxnet után ez volt a második olyan, ICS-rendszereket célzó malware, ami emberi beavatkozás nélkül volt képes megzavarni az ICS-rendszerekkel vezérelt fizikai folyamatokat).

2017 során többen (köztük Marina Krotofil, egy ukrán származású, Amerikában élő ICS-biztonsági szakértő) is megfogalmaztak olyan véleményeket, amelyek szerint az ukrán villamosenergia-rendszert egyes támadók (és itt ismét az orosz, állami/titkosszolgálati hátterű csoportokat említették) mintegy tesztkörnyezetként használják, hogy itt próbálják ki az ipari (elsősorban közüzemi) célpontok elleni támadásokhoz használható eszközeiket és technikáikat.

---

252 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

253 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/wp-content/uploads/CrashOverride-01.pdf

6.6. Támadások az USA villamosenergia-rendszere ellen

2016 végéig hivatalos források szerint az USA villamosenergia-rendszere ellen még nem hajtottak végre sikeres kibertámadást, ennek ellenére az ICS-biztonsági szakmának elég erős és nyíltan vállalt meggyőződése volt már akkor is, hogy ez nem fedte a valóságot. Ahogy korábban már említettük, bár kézzel fogható bizonyítékok nem álltak és állnak rendelkezésre, de a 2003-as amerikai áramszünet kiváltó okaként több biztonsági kutató a Blaster-féregtámadásra vezeti vissza. Ugyanígy kibertámadásként tartják számon a 2004-es, amerikai közmű cég elleni rootkit-támadást is, aminek következtében az érintett közműcég ICS/SCADA-rendszerét két hétre kellett leállítani. A Havex- és a BlackEnergy-támadásoknak az európai célpontok mellett voltak amerikai áldozatai is és egyes szakértők (többek között Joe Weiss, az ICS-biztonsági téma egyik legnagyobb veteránja) szerint ennek keretében a támadók 2014-ben sikeresen juttattak be malware-eket az amerikai villamosenergia-rendszer számítógépeibe. Ezt a DHS az ICS-CERT *Monitor* nevű kiadványának 2015. júniusi számában el is ismerte. Ebben a kiadványban ismét hangsúlyozták, hogy jelentős kockázatokat vállalnak azok a szervezetek, amelyek ICS/SCADA-rendszereket és -berendezéseket tesznek elérhetővé az internetről, dacára annak, hogy az ICS-CERT már évekkel korábban arra figyelmeztetett, hogy az ilyen kialakításokat mindenképpen kerülni kell és ahol korábban történt meg az ICS-eszközök/rendszerek internetre csatlakoztatása, ott ezeket minél gyorsabban meg kell szüntetni.

2018. júliusban az amerikai Belbiztonsági Minisztérium (Department of Homeland Security, DHS) egy publikus webes előadás-sorozatot tartott az USA kritikus infrastruktúrája elleni orosz kibertámadásokról[254]. Ebben az egyik újdonság az volt, hogy a támadók a különböző célba vett kritikus infrastruktúrákat gyakran azok beszállítóin (nem csak fejlesztő, hanem gyakran szolgáltatást biztosító vállalatokon) keresztül, a beszállító rendszereit és gyakran termékeit kompromittálva támadták. Érdemes megfigyelni a hasonlóságot a Havexnél már bemutatott módszerrel, amikor európai ICS-gyártók letölthető binárisait cserélték le malware-rel fertőzött változatokra, így támadva a kiszemelt szervezeteket.

7. Számítógép-alapú Social Engineering-technikák bemutatása

7.1. Általában a Social Engineering-kockázatokról

A social engineering-támadások, vagyis azok a támadások, amik a digitális eszközt használó embert veszik célba és csapják be, hogy a támadók céljainak megfelelő tevékenységekre (malware-fertőzött e-mail-csatolmány megnyitása, hamis weboldalon személyes adatok megadása stb.), az ICS-rendszerek esetén is ugyanúgy működnek és ugyanolyan hatásosak, mint bármilyen más IT-rendszer ellen indított támadás esetében. Ez nem is lehet meglepő, hiszen az ICS-rendszerekkel dolgozó mérnökök (fejlesztők, üzemeltetők, folyamatirányítási szakterületeken dolgozó mérnökök és technikusok) általában semmivel sem teljesítenek jobban vagy rosszabbul a biztonságtudatosság terén, mint bármelyik másik fejlesztő, üzemeltető vagy felhasználó. Ami miatt a social engineering-támadások az ICS-világában az IT-nél jóval veszélyesebbek, az az, hogy az ICS-rendszerek elleni támadások sokkal nagyobb hányadban célzott támadások, amikor a támadó alaposan felkészül a célba vett szervezet és emberek hátteréből, körülményeiből. Egy ilyen jól előkészített social engineering-támadást pedig sokkal nehezebb kivédeni, mint egy láthatóan rossz magyarsággal (vagy éppen egy online fordítóval magyarra fordított és csapnivaló minőségben) megírt e-mailben pénzt kérő „nigériai herceg” próbálkozását.

[254] Az előadás prezentációja a US-CERT weboldalán érhető el: https://www.us-cert.gov/sites/default/files/c3vp/Russian_Activity_Webinar_Slides.pdf

Az ICS-rendszerek ellen támadást tervező csoportok mögött (ahogy arról már volt szó) gyakran egyes nemzetállamok katonai/titkosszolgálati szervezetei is állhatnak, ezeknek a csoportoknak pedig olyan képességeik és lehetőségeik is vannak, amiket felhasználva akár egy, az adott szervezet számára ismert és megbízható másik szervezet (beszállító, felügyeleti szerv stb.) rendszereit, például webes szolgáltatásait is képesek kompromittálni. Ez az ún. watering hole-támadás (az elnevezés a természetből vett példára utal, amikor a támadók nem üldözik az áldozatukat, hanem mint az oroszlán a szavannán, az itatónál várja az elejteni próbált gazellát), amikor a támadók egy legitim (vagy annak látszó) weboldalon helyezik el azt a kártékony kódot, amivel utána hátsó ajtót tudnak nyitni a weboldalt letöltő számítógépen. Ezután már csak egy jól megformázott hamis e-mailt kell beküldeni a célba vett személyeknek, ami az előkészített weboldalra vezeti a gyanútlan áldozatot és már rendelkezésre is áll egy hátsó bejárat az adott szervezet hálózatába. Az ilyen kifinomult watering hole-támadások ellen nagyon nehéz védekezni, mert a bejövő e-mailről, ha figyelmesen készítik elő a támadók, csak a fejléc-információk alaposabb vizsgálatával lehet megállapítani, hogy nem attól a szervezettől jött, amelyik nevében küldték, a kártékony kóddal preparált weboldalt pedig valóban az igazi partner szerverei futtatják.

7.2. Jellemzők ICS-környezetekben

Az ICS-rendszerek, illetve az ezeket üzemeltető/használó szervezetek elleni social engineering-támadásokat két aktuális példán keresztül szemléltetjük. Az első a 2015-ös, ukrán áramszolgáltatók elleni BlackEnergy-támadás első fázisában használt, Microsoft Excel-makróvírus. A korábban már hivatkozott elemzések szerint a megtámadott ukrán áramszolgáltatóknál a Microsoft Office programcsomag az ajánlott biztonsági beállításokkal futott, a külső forrásból származó makrókat alapértelmezetten nem engedte futni, ezt a célba vett felhasználónak szándékosan kellett engedélyeznie. Ez látható a *2. ábrán*.

2. ábra: BlackEnergy-malware-rel fertőzött Microsoft Office-dokumentum megnyitása utáni üzenet (Forrás: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, 12. o.)

A 2. ábrán látható felirat szerint a dokumentum a Microsoft Office egy újabb verziójában készült és a makrókat engedélyezni kell, hogy a dokumentum helyesen megjelenjen.

A másik példa egy 2019. júliusi támadási hullám, amikor a támadók az amerikai energiaszektor egyes vállalatai ellen indítottak támadást célzott adathalász e-mailekkel, amikben mérnöki vizsgák eredményeiről ígértek tájékoztatást. Még ha egy, az energiaszektorban dolgozó mérnök tisztában is van azzal, hogy ő mostanában nem vizsgázott az e-mail feladójaként feltüntetett szervezetnél, a kíváncsiság erősebb lehet a biztonságtudatosságnál, és előfordulhat, hogy megnyitja a csatolt dokumentumot. Ezt a fajta emberi viselkedést pedig nem tudjuk 100 százalékosan kivédeni, hiszen a social engineering-támadások pont azt a fajta, bizalmon alapuló emberi viselkedést használják ki, ami alapja szinte minden társas viszonynak.

7.3. Supply chain-támadások veszélyei ICS-rendszerekre

A beszállítói lánc (supply chain) elleni támadások minden szervezet számára jelentős fenyegetést képviselnek. Az IT- és ICS-rendszerek bonyolultsága már régen elérte azt a szintet, hogy egy ilyen rendszereket használó szervezet külső fejlesztők nélkül nem képes megfelelni a kihívásoknak, ezért kipróbált és megbízhatóként kezelt külső szállítókra (hardverszállítókra, szoftverfejlesztőkre) bízza ezeket a feladatokat. A különböző beszállító cégek biztonsági szintje (ideértve a fizikai biztonsági intézkedéseket, az alkalmazottak háttérellenőrzését, a biztonságtudatosság kérdését és a logikai biztonsági kontrollokat egyaránt) az esetek döntő többségében nem éri el az ICS-rendszereket használó ügyfeleiknél tapasztalható szintet. Ez azonban azt is jelenti, hogy ha egy, a támadók által célba vett ipari szereplő jól teljesít a korábban tárgyalt biztonsági területeken, a támadók figyelme lehet, hogy inkább az adott szervezet beszállítói felé fog fordulni. Ha elfogadjuk, hogy az 1982-es transzszibériai gázvezeték robbanását valóban a nyugati titkosszolgálatok által a gázvezeték vezérlésére használt (és a KGB által ellopott) ICS-rendszerben elhelyezett malware okozta, akkor ezt is tekinthetjük a beszállítói lánc elleni támadások egyik első és nagyon jó példájának.

Ahogy korábban már érintettük, nem minden ICS-biztonsági incidens hátterében áll célzott támadás, amivel az ICS-rendszerek által vezérelt folyamatokat próbálják a támadók megzavarni. 2019 júliusában publikáltak részleteket arról az esetről, amikor egy David Tinley programozó, aki korábban a Siemens alvállalkozójaként dolgozott, bűnösnek vallotta magát azokkal a vádakkal kapcsolatban, hogy szándékosan hibás kódrészleteket helyezett el egyes Siemens-termékekben, amiken a szerződése szerint dolgozott. Ezeket a hibákat egy bizonyos, előre meghatározott időben aktiválta az általa írt rutin, amivel azt igyekezett biztosítani, hogy a fejlesztési projekt után is szükség legyen a munkájára az érintett szoftvereknél. Tinley 14 éven át dolgozott a Siemens alvállalkozójaként és bár a hírekben nem részletezték, milyen szoftvereken dolgozott, figyelembe véve, hogy a Siemens a világ egyik legnagyobb ICS-gyártója, akár az is előfordulhat, hogy az érintett szoftverek között vannak ipari környezetben használt programok is. Ez a példa is kiválóan mutatja, hogy mennyire fontos a beszállítói láncban érintett szervezetek ellenőrzése és a megfelelő biztonsági kontrollok megkövetelése.

8. Villamosenergia-irányító rendszerek kibertámadásának hálózati és informatikai következményei, teendői

A villamosenergia-rendszer irányításáért felelős szervezetek (ideértve az erőműveket, átviteli rendszerirányítókat és áramszolgáltatókat egyaránt), hasonlóan a legtöbb, más ipari szektorban tevékenykedő szervezethez hasonlóan legnagyobb részben az IT-biztonsági trendek mögött lemaradva, követő viselkedést tanúsítanak, tehát csak a már elterjedt, kipróbált és bizonyítottan jó és stabil megoldásokat alkalmazva fejlesztik az ICS-rendszereik kiberbiztonsági védelmének szintjét. Többségük számára a Stuxnet nyilvánosságra kerülése volt az a motiváló esemény, aminek nyomán 2010-ben vagy

néhány évvel utána továbbléptek az akkor elfogadottnak számító tűzfal és antivírus megoldás-pároson és elkezdtek további hálózat- és host-szintű biztonsági megoldásokat telepíteni és használni. Ahogy az újabb és újabb, ICS-rendszereket célzó támadásokról mind több részletet lehetett megtudni, úgy kezdett fejlődni az ICS-kiberbiztonság világa mind a gyártói/szállítói, mind a felhasználói oldalon. A gyártók között megjelentek a kifejezetten ICS-kiberbiztonságra szakosodott cégek (ilyen cégek sok más mellett pl. a Nozomi Networks, a Dragos LLC, az Indegy, a Claroty vagy az Applied Risk) és elindultak az első, kifejezetten ICS-kiberbiztonságra kidolgozott tanfolyamok (ilyeneket kínálnak többek között az Idaho National Labs az USA-ban, az ENCS Hollandiában, a SANS Institute és az ISA világszerte). Felhasználói oldalon az ipari szereplők változó felkészültségi szinten állnak jelenleg, aminek az egyik fő oka a szabályozói oldalon meglévő hiányosságok. Magyarországon furcsa módon azok a kormányzati erőfeszítések, amelyek például a pénzügyi szektor esetében már több mint egy évtizede meglehetősen szigorú jogszabályi követelményeket támasztanak a bankokkal, biztosítókkal szemben, nagyjából érintetlenül hagyták nem csak az ország gazdasági teljesítménye szempontjából kiemelten fontos termelővállalatok, hanem a közüzemi szolgáltatók által használt ipari automatizálási rendszereket is. Hovatovább, a számlázásnál használt rendszerek jelenleg évről évre alaposabb ellenőrzésen esnek át, mint az ország működése szempontjából talán leginkább nélkülözhetetlen, jelentős részben IT-komponensekből felépülő rendszerek.

Mit kellene tenni ebben a helyzetben?

1. A magyar államnak a szakma bevonásával jogszabályt kéne készítenie a nemzetgazdaság számára kiemelten fontos szektorok kiberbiztonsági szabályozásáról. Ebben (a 2013. évi L. törvényben és a kapcsolódó 41/2015. BM rendeletben az állami és önkormányzati szervek információbiztonsági szabályozásához kapcsolódóan meghatározotthoz hasonló részletességgel és az ICS-rendszereket használó szervezetek sajátosságait szem előtt tartva) követelményeket kéne megfogalmazni az ipari szektorokban működő szervezetek információbiztonságával kapcsolatban. Ennek nyomán pedig a következő feladatokat kell elvégezniük az érintett szervezeteknek.
2. Teljes körű hardver-, szoftver- és hálózati kapcsolat leltár felépítése és folyamatos karbantartása (ahogy arról az „*Eszközleltár és hálózatbiztonsági monitoring*” fejezetben már volt szó).
3. Évenkénti kockázatelemzés. A kockázatelemzésnél célszerű megfontolni, hogy a vagyonelemeken alapuló kockázatelemzés helyett egy folyamatalapú megközelítés pontosabb eredményt hozhat-e? Különösen igaz lehet ez egy közüzemi szolgáltató számára, hiszen egy termelővállalat (pl. egy autógyár vagy egy gyógyszergyár) esetében a gyártási technológiák vagy a know-how, mint adatvagyon, képezhet ugyanakkora vagy nagyobb értéket, mint maguk az ICS-rendszerekkel vezérelt gyártási folyamatok, de egy közüzemi szolgáltatónál nem lehet nagyobb érték azoknál a folyamatoknál, amikkel biztosítják az ügyfeleik zavartalan ellátását. Ez a kockázatelemzés azután alapul szolgálhat minden további intézkedéshez, hiszen tiszta képet adhat a biztonsági intézkedések prioritásaihoz: melyik rendszer, folyamat vagy adatvagyonelem esetében melyik biztonsági szempont az elsődleges, melyik biztosítására kell nagyobb erőforrásokat csoportosítani?
4. A kockázatelemzés alapján lehet kidolgozni a végponti és hálózati szintű biztonság műszaki kontrolljait, amik meghatározhatják (más szempontok figyelembevételével együtt), hogy melyik gyártó milyen megoldását érdemes beszerezni és használni.
5. Ugyanígy, a kockázatelemzés eredményei alapján lehet a továbbiakban döntést hozni arról, hogy milyen információ/IT- és ICS-biztonsági kompetenciák fejlesztésére kell erőforrásokat fordítania az adott szervezetnek, illetve mik azok a szaktudások, amiket házon belül kell felépíteni/megtartani és melyek azok, amiket ki lehet (vagy éppen kell) szervezni és szolgáltatásként beszerezni.
6. Az eszközökkel és megfelelő szakmai tudással rendelkező csapat összeállítása közben el kell kezdeni kidolgozni azok a szabályokat és eljárásokat, amik keretet adnak a szervezet kiberbiztonsági működésének, ideértve az általános információ- és IT-biztonsági szabályokat és az ICS-specifikus szabályzatokat is, a normál időszakok eljárásrendjeit és az incidenskezelési,

üzletmenet-folytonossági és katasztrófaelhárítási szabályokat. Nagyon fontos kiemelni, hogy az ipari szervezetek üzletmenet-folytonossági terveinek ki kell térniük azokra az esetekre is, amikor a folyamatok irányítására használt ICS-rendszerek egy része vagy egésze használhatatlanná válik és vissza kell térni a folyamatok manuális irányítására. Erre a vészhelyzeti megoldásra az elmúlt években több példát is láthattunk, a 2015-ös ukrán áramszolgáltatók elleni támadások során a manuális vezérlés volt az egyik olyan intézkedés, ami miatt alig néhány óra alatt képesek voltak az érintett áramszolgáltatók helyreállítani a szolgáltatást az ügyfeleiknél. Egy másik példa a 2019 tavaszán történt, a Norsk Hydro nevű alumíniumgyártó vállalat elleni ransomware-támadás, amelynek következtében a cég nemcsak a vállalati, hanem a termelésirányító rendszereinek egy részét is elvesztette, ők is a manuális feladatvégzéshez tértek vissza[255].

7. Rendszeres külső auditokkal kell megbizonyosodni arról, hogy az érintett szervezetek minden előírt adminisztratív és műszaki biztonsági kontrollal és szükséges eljárással rendelkeznek, amik birtokában képesek lehetnek megelőzni vagy észlelni és elhárítani az olyan kibertámadásokat, amik a szervezet adatvagyonát vagy létfontosságú fizikai folyamatainak vezérléséhez használt ICS-rendszereit fenyegetik.

Részben a fentiek nyomán az USA törvényhozása 2019 nyarán fogadott el egy olyan javaslatot, aminek nyomán az erre kijelölt szövetségi szervezetek az USA villamosenergia-rendszerének esetében a digitális technológiákról az analóg vezérlésre történő visszaállás lehetőségeit fogják kutatni[256].

[255] https://icscybersec.blog.hu/2019/04/21/norsk-hydro-toulouse

[256] https://www.king.senate.gov/imo/media/doc/01-17-19%20Securing%20Energy%20Infrastructure.pdf

JOGSZABÁLYTÁR

1. Magyar jogszabályok

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
  https://net.jogtar.hu/jogszabaly?docid=a0100108.tv
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1500222.tv
- 2003. évi C. törvény az elektronikus hírközlésről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV
- 2009. évi CLV. törvény a minősített adat védelméről
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131
- 2021. évi XCI. törvény a nemzeti adatvagyonról
  https://net.jogtar.hu/jogszabaly?docid=a2100091.tv
- 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
  https://net.jogtar.hu/jogszabaly?docid=A1100128.TV
- 2011. évi CXII. törvény információs önrendelkezési jogról és az információszabadságról
  https://net.jogtar.hu/jogszabaly?docid=a1100112.tv
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1600451.kor
- 84/2012. (IV. 21.) Korm. rendelet az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.kor
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158
- 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól. *Hatályon kívül helyezte: 2015. évi CCXXII. törvény 121. § (1) b).*
  https://net.jogtar.hu/jogszabaly?docid=A1300220.TV&txtreferer=A0400140.TV
- 65/2013 (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
  https://net.jogtar.hu/jogszabaly?docid=a1300065.kor
- 360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. *Hatályon kívül helyezte: 374/2020. (VII. 30.) Korm. rendelet 22. §.*
  https://net.jogtar.hu/jogszabaly?docid=a1300360.kor
- 512/2013. (XII. 29) Korm. rendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról
  https://net.jogtar.hu/jogszabaly?docid=a1300512.kor
- 540/2013. (XII. 30) Korm. rendelet a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=A1300540.KOR

- 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=a1300541.kor
- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR
- 157/2016. (VI. 13.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet módosításáról. *Hatályon kívül helyezve: 2010. évi CXXX. törvény 12. § alapján.*
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600157.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- 2016. évi CL. törvény az általános közigazgatási rendtartásról
  https://net.jogtar.hu/jogszabaly?docid=A1600150.TV
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=A1500246.KOR
- 330/2015. (XI. 10.) Korm. rendelet a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=a1500330.kor
- 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=a1500359.kor
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről. *Hatályon kívül helyezte a 44/2017. (XII. 29.) BM rendelet.*
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm
- 249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=A1700249.KOR
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről
  https://net.jogtar.hu/jogszabaly?docid=A1800270.KOR
- 271/2018. (XII. 20. Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1800271.kor
- 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=212067.363096

2. Európai uniós jogi aktusok

- Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv
https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32008L0114&from=EN
- A fogyasztói jogviták alternatív rendezéséről, valamint a 2006/2004/EK rendelet és a 2009/22/EK irányelv módosításáról szóló, 2013. május 21-i 2013/11/EU európai parlamenti és tanácsi irányelv
https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0011&from=EN
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=HU
- Számítástechnikai bűnözésről szóló Egyezmény (2001)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa405
- Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10) az Európai Hálózat és Információbiztonsági Ügynökség létrehozásáról
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML
- Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013R0526&from=HU
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU
- Az Európai Parlament és a Tanács rendelet tervezete az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról
https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52017PC0477R%2801%29
- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU
- Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU
- Az Európai Parlament és a Tanács 2013. augusztus 12-i 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról
https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33193&from=EN
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- Közös Közlemény az Európai Parlamentnek és A Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése vonatkozásában
http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

- Az ENSZ Közgyűlés a 2003. december 8-i 58/32-es számú határozata https://undocs.org/A/RES/58/32
- Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé” című dokumentumról (2011/2284(INI)) https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012IP0237&qid=1521197299768&from=HU
- A Tanács következtetései a kiberdiplomáciáról (2015) http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf
- A Bizottság 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.HUN&toc=OJ:L:2017:239:TOC
- A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (2017): http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf

3. Külföldi jogi aktusok

- Az EBESZ Állandó Tanácsának PC.DEC/1039 számú döntése: https://www.osce.org/pc/90169?download=true
- Az EBESZ bizalomépítő intézkedései: PC.DEC/1106 https://www.osce.org/pc/109168

FOGALOMTÁR

- **Adat:** Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. [1]
- **Adatbiztonság:** Az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében. [2]
- **Adathalászat:** Más néven phishing, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. [3]
- **Adatfeldolgozás:** Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől). [2]
- **Adatfeldolgozó:** Az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi. [2]
- **Adathordozó:** Minden olyan anyagi eszköz, mely alkalmas adatok megőrzésére, tárolására. Az Európai Parlament és a Tanács 2002/65/EK irányelve szerint, amely már tartós adathordozóként nevesít: „olyan eszköz, amely lehetővé teszi a fogyasztó számára a személyesen neki címzett adatoknak a jövőben is hozzáférhető módon és az adat céljának megfelelő ideig történő tárolását, valamint a tárolt adatok változatlan formában történő megjelenítését”. Így adathordozó a pendrive, a DVD, CD, SD-kártya, amely alkalmas kisebb vagy nagyobb mennyiségű adat tárolására. [4]
- **Adatkezelés:** Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése. [2]
- **Adatkezelő:** Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja vagy az általa megbízott adatfeldolgozóval végrehajtatja. [2]
- **Adatvédelem:** A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások. [5]
- **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot, nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens. [2]

- **Adattal rendelkezés:** A birtokban tartás, az adat alapján további adat készítése, az adat másolása, sokszorosítása, a betekintés engedélyezése, a feldolgozás és felhasználás, a minősítés (biztonsági osztályba sorolás) felülvizsgálata, a minősítés (biztonsági osztályba sorolás) felülbírálata, a nyilvánosságra hozatal, titoktartási kötelezettség alóli felmentés, megismerési engedély kiadása. [5]
- **Adatokat érintő beavatkozás:** Információs rendszerekben található digitális adatok törlése, károsítása, rongálása, megváltoztatása, eltávolítása vagy hozzáférhetetlenné tétele. A fogalom emellett magában foglalja az adatlopást, valamint a pénzeszközök, a gazdasági erőforrások, illetve a szellemi tulajdon eltulajdonítását is. [6]
- **Adatkifürkészés:** digitális adatok információs rendszeren belüli, odairányuló vagy onnan kiinduló nem nyilvános továbbításának – így például az információs rendszerből kibocsátott, ilyen digitális adatokat hordozó elektromágneses jeleknek – a kifürkészése műszaki eszközökkel. [6]
- **Advanced persistent threat (APT):** Magas szintű, tartós vagy más néven (és az anyagban is használt) célzott támadás olyan titkos és folyamatos számítógépes hackerfolyamatok sorozatát jelenti, amelyeket gyakran meghatározott személy, személyek vagy szervezet ellen követnek el. Az APT általában magánszervezetek, államok vagy mindkettő ellen irányul, és üzleti vagy politikai motívumok vezérlik az elkövetőket, a cél általában információszerzés, de előfordult már olyan támadás is, melynek célja a szabotázs volt. [7]
- **Aktív kiberbiztonság (Active Cyber Defence Cycle** – ACDC): Aktív kiberbiztonsági intézkedések gyűjtőfogalma. Az aktív kiberbiztonság négy nagyobb tevékenységből áll, ezek a fenyegetéselemzés és információgyűjtés (threat intelligence consumption); az eszközleltár és hálózatbiztonsági monitoring; az incidenskezelés; a fenyegetés és környezet kezelése (threat and enviroment manipulation). [8]
- **Alapvető szolgáltatást nyújtó szereplő:** Alapvető szolgáltatást nyújtó szereplő Magyarországon azon intézmény lehet, amely kijelölt nemzeti létfontosságú rendszerelem üzemeltetője, a NIS-irányelv II. mellékletében felsorolt ágazatok és alágazatok valamelyikébe sorolható szolgáltatást nyújt, szolgáltatása elektronikus információs rendszerektől függ, valamint a szolgáltatását érintő biztonsági esemény jelentős zavart okozna az általa nyújtott szolgáltatás biztosításában. Alapvető szolgáltatásoknak tekinthetők a társadalom vagy gazdaság szempontjából fontos szerepet betöltő magán- és állami vállalkozások, például vízellátás, villamosáram-szolgáltatás stb. [9]
- **Android:** Linux-kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobileszközökre (okostelefon, táblagép) tervezve. [10]
- **Authentikáció:** Az authentikáció az a folyamat, amelynek során ellenőrizzük a felhasználó identitását és azt, hogy hozzáférhet-e a rendszerhez. A felhasználók azonosításakor az alábbi négy lehetőség közül választhatunk: tudás (valami, amit csak a felhasználó tud), tulajdon vagy birtok (valami, ami csak a felhasználónál van), tulajdonság (a felhasználóra jellemző egyedi biológiai tulajdonság). [11]
- **Automatizált informatikai biztonsági vizsgálat:** Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre. [12]
- **Backdoor (hátsó ajtó) program:** A felhasználók számára általában nem látható elem, amelyet a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nem csak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként. [13]

- **Bejelentésköteles szolgálgatásokat nyújtó szereplő:** Magyarországon bejelentésköteles szolgáltatásoknak nevezzük azon szolgáltatásokat, melyek a NIS-irányelv szerinti digitális szolgáltatók körébe tartoznak. Továbbá azon nem mikro- és kisvállalkozásokat, melyek online piacteret, online keresőprogramot, valamint felhőalapú számítástechnikai szolgáltatást nyújtanak. [9]
- **Betörés detektáló eszköz:** Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e vagy sem. Fajtái a mintaalapú betörés detektáló eszközök (signatura-based IDS) és a viselkedést vizsgáló betörés detektáló eszközök (behavior-based IDS). Intrusion Detecting Systems (rövidítve: IDS). [14]
- **Big Data:** A cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és ügyfelek számára. [15]
- **Biometrikus azonosítás:** Olyan eszközök és eljárások összessége, amely a személyek mérhető testi tulajdonságait használják fel valamilyen technika segítségével azonosításra vagy a személyazonosság megállapítására. Az azonosítás szempontjából a legalkalmasabb adatok, illetve eljárások: a DNS-minta, ujjnyomatok, retinaképek, hangelemzés, íriszdiagnosztika, a tenyér vénamintáinak azonosítása, gépelési mintaalapú azonosítás. [16]
- **Bizalmasság elve:** Az elektronikus információs rendszer azon tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról. [1]
- **Biztonság:** A biztonságot olyan állapotnak tekinthetjük, amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak a veszéllyel szembeni eredményes védekezés feltételei. [5]
- **Biztonsági esemény:** Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. [5]
- **Biztonsági esemény kezelése:** Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység. [5]
- **Biztonsági osztály:** Az elektronikus információs rendszer védelmének elvárt erőssége. [5]
- **Biztonsági osztályba sorolás:** A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása. [5]
- **Biztonsági szint:** A szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonsági szintbe sorolás:** A szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonságtudatosság:** A felhasználó azon magatartása, amikor betartja az információbiztonsági szabályokat, megérti az információbiztonságban betöltött szerepét és figyel az őt esetlegesen érintő fenyegetésekre. [17]
- **Célzott támadások** (Targeted Attacks): Célzott támadásoknak nevezzük az olyan fenyegetéseket, melyeket a támadók kifejezetten egy adott célpont (személy vagy szervezet) ellen használnak. Egy számítógépes vírushoz képest a fenyegetés "megalkotója" ebben az esetben nem arra törekszik, hogy a kártékony kód minél jobban elterjedjen, hanem arra, hogy a kiszemelt célpont eszközére, eszközeire bejusson. [14]

- **CIA:** Az elektronikus információs rendszer védelmének alapvető céljának, a bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) védelmi hármasának jelölése. [5]
- **Cloud computing:** („számítástechnikai felhő", „felhőalapú informatika"): A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhőalapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhőalapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (például: Gmail) vagy az online tárhelyek (például: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhőalapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhőalapú szolgáltatástól szabadulni. [2]
- **Digitális szolgáltatás:** Az (EU) 2015/1535 európai parlamenti és tanácsi irányelv (1) 1. cikke (1) bekezdésének b) pontja szerinti, a III. mellékletben felsorolt típusok valamelyikének megfelelő szolgáltatás. [18]
- **Digitális szolgáltató:** Minden olyan jogi személy, amely digitális szolgáltatást nyújt. [18]
- **Domain Name System (DNS):** A tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott tartománynevekhez (doménekhez) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le", „oldja fel", melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton. [19]
- **DNS-szerver:** A DNS-kiszolgáló egy olyan szolgáltató oldali szerver, amely az internetes címek fordításáért felelős. Ezen szerver segítségével tudunk az interneten keresztül weboldalakon böngészni, e-maileket küldeni és fogadni. [19]
- **EC3:** Az Europol Európai Kiberbűnözés Elleni Központja, amelynek fő feladata a szervezett bűnözés ellehetetlenítése, elsősorban a tagállamok nyomozóhatóságainak nyújtott, operatív támogatása által. [18]
- **Egyetlen kapcsolattartó pont (SPOC):** A kapcsolattartó pont fő feladata az Európai Unión belüli nagy hatású kiberincidensek hazai koordinálása, valamint az incidensekkel kapcsolatos jelentések fogadása, küldése az EU-s tagállamok SPOC-ai számára. [9]
- **Elektronikus információbiztonság:** Távközlési és informatikai, valamint egyéb elektronikus rendszerekben és a támogató infrastruktúrákban alkalmazott rendszabályok összessége, amelyek védelmet nyújtanak az elektronikusan előállított, feldolgozott, tárolt, továbbított és megjelenített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkentése ellen. [3]
- **Elektronikus információs rendszer:**
  a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
  b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

Egy elektronikus információs rendszernek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében az adatok, információk kezelésére használt eszközök – így különösen környezeti infrastruktúra, hardver, hálózat és adathordozók –, eljárások – így különösen szabályozás, szoftver és kapcsolódó folyamatok –, valamint az ezeket kezelő személyek együttesét. [1]

- **Elektronikus információs rendszer biztonsága:** Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [5]
- **Elosztott szolgáltatás megtagadásos támadás:** Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **ENISA (Európai Uniós Kiberbiztonsági Ügynökség):** Az EU elsőszámú kiberbiztonsággal foglalkozó intézménye, a kiberbiztonsággal kapcsolatos tanácsadásért felelős ügynökség, amely információs és tudásközpontként működik. [18]
- **EPCIP (European Programme for Critical Infrastructure Protection):** A kritikus infrastruktúrák védelmére irányuló európai program, amelynek célkitűzése, hogy javítsa a létfontosságú infrastruktúrák védelmét az Európai Unióban. [18]
- **Ethernet:** A DEC, Intel és Xerox cégek által kidolgozott alapsávú LAN-ra vonatkozó specifikáció. Az Ethernet-hálózatok az ütközések feloldására a CSMA/CD-t használják. Számos kábeltípuson (csavart érpár, optika stb.) működik legalább 10 Mbps sebességgel. [22]
- **Europol:** Európai Rendőrségi Hivatal, amelynek fő feladata segítséget nyújtani az EU-s tagállamok bűnüldöző hatóságainak a terrorizmus elleni fellépésben, illetve a súlyos nemzetközi bűncselekmények felderítésében. [18]
- **Eseménykezelő Szakterület (Event Detection Team):** Intézmények közti megállapodás keretében a biztonság növelése érdekében folyamatosan monitorozza a hálózati forgalom különböző szegmenseit. A szakterület által végzett feladat preventív és detektív jellegű, hiszen alapvetően passzív adatforgalom ellenőrzésről és annak elemzéséről van szó. A szisztematikusan összegyűjtött támadási kísérletek rendszerezett adatai alapján azonosíthatjuk a támadók által felhasznált internetes erőforrások címeit, másrészt – különböző elemző algoritmusok segítségével – felfedezhetjük a behatolási módszerek alkalmazási trendjeinek aktuális alakulását, valamint következtetéseket vonhatunk le az internetre épülő szolgáltatások hátterét nyújtó szoftverkörnyezet esetleges gyenge pontjairól, illetve sebezhetőségeiről. [20]
- **Fenyegetés:** Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemeinek védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát. [5]
- **Folytonos védelem:** Az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [1]
- **Fluxus:** A fluxus a felületet metsző mágneses erővonalak mennyisége. [21]
- **Gateway:** Átjáró, konverter eszköz különböző protokollon kommunikáló eszközök között. [22]

- **GDPR:** A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, más néven általános adatvédelmi rendelet (General Data Protection Regulation). A GDPR közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó. Ennél fogva minden tagállamban ez a rendelet lesz a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekintetében, attól eltérni csak akkor lehet, ha azt maga a GDPR megengedi. A rendeletet 2018. május 25-től kell alkalmazni.
- **Hacker:** Az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő személy. A tömegkommunikációban helytelenül minden számítógépes bűnözőre használják. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. [5]
- **Hacktivizmus:** Olyan cselekedet, amelyben a támadók számítógép hálózatokba hatolnak be és az ott megszerzett adatokat közzéteszik, hogy így hívják fel a figyelmet az általuk képviselt célokra. Fogalmilag, bár nem azonos, mégis számos közös pontja van a kiberterrorizmussal. Mindkettőre jellemző, elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadások, amelyek célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Hatásuk, bár elenyésző, ugyanis nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport. [23]
- **Hálózat:** Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége. [5]
- **Hálózati és információs rendszer:** elektronikus hírközlő hálózat vagy minden olyan eszköz, vagy egymással összekapcsolt eszközök csoportja, amelyek digitális adatokat dolgoznak fel, valamint a tárolt, kezelt, visszakeresett vagy továbbított digitális adatok. [6]
- **Hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia:** Olyan stratégiai dokumentum, amelyben legalább a NIS-irányelv szerinti hálózati és információs rendszerek biztonságára vonatkozóan nemzeti szinten stratégiai célkitűzéseket és prioritásokat állapítanak meg a tagállamok. [9]
- **Hardver:** Az információs rendszerek (talán) legegyértelműbb eleme, mely magában foglal minden olyan eszközt vagy részelemet, mely az információ feldolgozásában, továbbításában, tárolásában részt vesz. Az okoseszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, melyek ideiglenesen vagy állandó módon csatlakoztathatók az eszközhöz. [24]
- **Hitelesség:** Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [5]
- **Honeypot (csapdarendszer):** Elsődleges célja az, hogy – valós működést szimulálva – elhitessék a támadókkal, hogy éles szolgáltatást nyújtó rendszert sikerült elérniük. Mindeközben azonban a jól felépített csapdarendszerek a támadó valamennyi tevékenységét letapogatják, módszeresen összegyűjtik, rögzítik és naplózzák. Tekintettel arra, hogy a csapdarendszer valójában nem működtet „igazi" szolgáltatást, a rajta észlelt valamennyi tevékenység jogtalannak minősíthető, azaz potenciális támadásként fogható fel. A csapdarendszerek tehát lényegében arra szolgálnak, hogy a támadók saját magukat leplezzék le egy olyan álcázott környezetben, ahol minden tevékenységük nyomot hagy. [20]
- **IKT-folyamat:** Valamely IKT-termék vagy IKT-szolgáltatás tervezése, fejlesztése, rendelkezésre bocsátása, illetve nyújtása vagy karbantartása céljából végzett tevékenységek összessége. [18]
- **IKT-szolgáltatás:** Olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információhálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll. [18]

- **IKT-termék:** Valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja. [18]
- **Illetéktelen személy:** Valamely tevékenység végzésére nem jogosult személy. Az informatikai biztonság esetében tipikusan az objektumba, az informatikai rendszerbe történő belépésre, adatkezelésre nem jogosult személy. [5]
- **Információ:** Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti. [1]
- **Információbiztonság:** Olyan tevékenység vagy állapot, amely középpontjában: a bizalmasság, a sértetlenség és rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (például: alfabetikus, numerikus, grafikus, képi forma) és milyen adathordozón jelenik meg. [25]
- **Informatikai biztonság:** Egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ez azt jelenti, hogy egy, az összes fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelmi rendszer. [5]
- **Informatikai biztonságpolitika:** A biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására. [5]
- **Informatikai biztonsági stratégia:** Az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere. [5]
- **Infrastruktúra:** Ember alkotta rendszerek és eljárások hálózata, amelyek szinergikusan együttműködve arra törekszenek, hogy folyamatosan alapvető termékeket és szolgáltatásokat állítsanak elő és terjesszenek. [18]
- **Internet of Things (IoT):** A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra és azok internetszerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, „mérni" és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek. [26]
- **Ipari irányító rendszerek (Industrial Control Systems):** Ezek nélkül a rendszerek nélkül ma már elképzelhetetlen a közműszolgáltatások, a gyártósorok vagy éppen a közlekedés és szállítmányozás zavartalan működésének biztosítása. Mára a legtöbb ICS-rendszer és -berendezés ugyanolyan vagy legalábbis nagyon hasonló komponensekből épül fel, mint a más szektorok (pénzügy, államigazgatás, szolgáltatói szektorok) IT-rendszerei. [8]
- **iOS:** Az Apple Inc. mobil operációs rendszere, amelyet iPhone, iPod touch és iPad készülékekre fejlesztenek.
- **Katonai Nemzetbiztonsági Szolgálat Kibervédelmi Központja:** A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelését végző szerv.
- **Kémprogramok** (**Spyware**)**:** A rendszerbe jutva a háttérből figyelik a rendszerben lezajló eseményeket, melyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [13]
- **Kiberbiztonság:** A kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez. [1]

- **Kiberfenyegetés:** Bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat. [18]
- **Kibervédelem:** A kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertérképességek megőrzését. [1]
- **Kiberbűnözés:** Célja az informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, amelyek rendkívül adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ezen a területen meglevő lehetőségeket**.**
- **Kiberhadviselés:** Az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még inkább a konvencionális hadviselés támogatására. [27]
- **Kiberkémkedés:** Az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzés. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület. [28]
- **Kihívás:** Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége, amelyek eredői hátrányosan befolyásolják a belső és külső stabilitást és kihatással lehetnek egy adott régió hatalmi viszonyaira. [29]
- **Kockázat:** A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ezáltal okozott kár nagyságának a függvénye. Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek megvalósulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. [5]
- **Korai Figyelmeztető Rendszer (Early Warning System – EWS):** Az EWS az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának az ún. szenzorokkal történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményt. [20]
- **Közigazgatás:** Azon szervezetek összessége, amelyek közhatalmat gyakorolva, az állam vagy az önkormányzat nevében közfeladatokat látnak el és jogszabályokat hajtanak végre. A helyi közügyekben az önkormányzati igazgatás, az országos jelentőségű ügyekben a központi közigazgatás jár el.
- **Központi alkalmazás (Application Server):** Olyan felhőalapú megoldás, amely gyűjti és kezeli a nagymennyiségű adatokat (Big Data) és megfelelő szoftverek segítségével felhasználja azokat. [30]
- **Kritikus információk:** Azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük, hatékony tervezéséhez és végrehajtásához. [20]
- **Kritikus infrastruktúra:** Azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, a közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére. [14]
- **Kritikus sérülékenység:** Kritikusnak tekinthető az a sérülékenység, amely a bizalmasságot, sértetlenséget vagy rendelkezésre állást nagymértékben sérti, illetőleg a sérülékenység távolról, könnyedén vagy hitelesítés nélkül kihasználható, tehát valós és komoly veszélyt jelent a rendszerre és az abban tárolt adatokra. [14]
- **Létfontosságú rendszerelem:** az Lrtv. 1. mellékletében meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi

feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. [31]

- **Mágneses tér:** A töltések rendezett mozgása, azaz az áram révén az áramjárta vezető körül elektromágneses erőtér jön létre. Az egy irányba, egyenletesen mozgó töltések áramlásának (azaz az egyenáramnak) a hatására állandó, míg a váltakozó irányba, változó sebességgel mozgó töltések áramlásának (azaz a váltakozó áramnak) a hatására változó mágneses tér keletkezik. Ugyanakkor a folyamat visszafelé is működik, azaz a mágneses erőtér változása erőt fejt ki a vezetőben lévő töltött részecskékre, mely erő elmozdítja e részecskéket, ezzel áramot hoz létre. [21]
- **Malware:** Az angol *malicious software* (kártékony szoftver, káros szoftver, rosszindulatú szoftver) összevonásából kialakított mozaikszó. Rosszindulatú szoftvernek tekinthetők azok a szoftverek, amelyek célja nem az információs rendszer működésének biztosítása és fenntartása, hanem bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek végzése. Ezen rosszindulatú szoftverek segítségével a támadó könnyedén zavart okozhat a célszemély számára, például túlterhelheti, működésében akadályozhatja, valamint akár működésképtelenné teheti a felhasználó bármely infokommunikációs eszközét. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program. [13]
- **Minősített adat:** A minősített adat (korábbi elnevezése: államtitok vagy szolgálati titok) olyan minősítéssel védhető közérdek körébe tartozó információ, amelyről megfelelő eljárásban megállapította a minősítésre jogszabályban felhatalmazott személy, hogy az adat érvényességi időn belüli nyilvánosságra hozatala, illetéktelen személy részére hozzáférhetővé tétele veszélyezteti Magyarország biztonságát. „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása, nyilvánosságra hozatala bűncselekmény. [5]
- **Mozgási indukció:** A mágneses mező és valamely vezető anyag egymáshoz képesti, a mágneses erővonalakat metsző elmozdulásakor mozgási indukcióról beszélünk. A mozgási indukció a feszültség létrehozásának mozgással történő módja, a villamos energia előállításának, a generátorok működésének az alapja. [21]
- **NAIH:** Nemzeti Adatvédelmi és Információszabadság Hatóság: az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.
- **NEIH:** Nemzeti Elektronikus Információbiztonsági Hatóság, amely az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. A hatóság egyik legfontosabb feladatként elbírálja az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását, valamint ellenőrzi az elektronikus információs rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését. A rendelkezésre álló információk alapján kockázatelemzést végez és az éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést. Ezen túlmenően a hatóság elrendeli az ellenőrzés során feltárt vagy más módon tudomására jutott biztonsági rések elhárítását és ellenőrzi a helyreállító intézkedés eredményességét. [14]
- **Nemzeti Kiberbiztonsági Koordinációs Tanács:** Az e-közigazgatásért felelős miniszter (jelenleg a belügyminiszter) által vezetett Nemzeti Kiberbiztonsági Koordinációs Tanács a

Kormány javaslattevő, véleményező szerveként gondoskodik az Ibtv. hatálya alá tartozó szervezetek információbiztonsági tevékenységeinek összehangolásáról. [14]

- **Nemzeti Kibervédelmi Intézet:** A kiberfenyegetések okozta kihívásokra reagálva, a kiberbiztonság növelése, az egységes és hatékony, párhuzamosságokkal kevésbé tagolt kibervédelmi struktúra megteremtése érdekében jött létre a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI). Az NKI legfőbb feladata és célja, hogy Magyarország egy összehangolt, szervezett tevékenység keretében legyen képes a modern kor egyik legnagyobb kihívásának, a kiberbiztonság megteremtésének és erősítésének az élharcosa és a kibervédelem letéteményese lenni, a globális és a hazai kibertérből érkező fenyegetéseket hatékonyan kezelni, azok megelőzésére szakszerű segítséget nyújtani. [14]
- **Nyugalmi indukció:** El nem mozduló, de változó mágneses mező és el nem mozduló vezető között megvalósuló indukció esetén nyugalmi indukcióról beszélünk. Ebben az esetben az el nem mozduló, de időben változó áram által létrehozott elektromágneses erőtér változó mágneses erővonalai – azaz az időben változó fluxus – révén jön létre az indukció. [21]
- **Okos mérés (Smart metering):** Az okos mérési rendszerek lehetőséget adnak arra, hogy a szolgáltatók és a hálózatüzemeltetők a végfogyasztókra lebontva képesek egyedi adatszolgáltatásra. [30]
- **Okosotthon (Smart Home):** A felhasználó otthoni készülékei (Smart Appliencies) valamilyen hálózati kapcsolat révén kommunikálnak egy központi vezérlő/szabályozó egységgel. Ennek eredményeként a felhasználói készülékek működése valamilyen szintű „intelligenciával" van felruházva. [30]
- **Online piactér:** Olyan digitális szolgáltatás, amely a 2013/11/EU Európai Parlamenti és Tanácsi irányelv (18) 4. cikke (1) bekezdésének a) és b) pontjában meghatározott fogyasztók és/vagy kereskedők számára lehetővé teszi, hogy az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi vagy szolgáltatási szerződéseket kössenek. [9]
- **Ransomware (zsarolószoftver):** Célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsarolóprogramok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó egy zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejében visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, akkor a zsaroló kiterjeszti a fizetésre rendelkezésre álló időt vagy törli az adatokat a felhasználó infokommunikációs eszközéről. [32]
- **Rendelkezésre állás elve:** Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak. [5]
- **Scareware (pánikprogram):** Álvírusirtók és egyéb más hamis biztonsági termékek csoportja, összefoglaló nevükön scareware-ek. Ahogyan az elnevezésük is utal rá, ezek a kártevők valamilyen vírusirtó programnak, esetleg biztonsági frissítésnek vagy más biztonsági terméknek álcázzák magukat. Általános jellemzőjük, hogy ingyenesek (legalábbis kezdetben, míg meg akarják győzni a felhasználót a „teljes verzió" megvásárlásáról), és semmilyen, vagy legalábbis minimális, víruseltávolító képességgel sem rendelkeznek – viszont annál több kártékony programot töltenek le a számítógépre. [17]
- **Sértetlenség elve:** Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [5]
- **Sérülékenység:** Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [5]

- **Sérülékenységvizsgálat:** Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása. [5]
- **Social engineering (pszichológiai befolyásolás):** Az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését vagy éppen egy kártékony program terjedését és működését. [17]
- **Súlyos biztonsági esemény:** Olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek. [14]
- **Számítógépes eseménykezelő központ (CERT/CSIRT):** Az Európai Hálózat- és Információ-biztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)]. [33]
- **Számítógépes féreg:** Egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak, illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. [5]
- **Személyes adat:** Az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. [34]
- **Szolgáltatásmegtagadásos támadás:** Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokolltulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógéprendszer vagy akár a számítógéphálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **Stuxnet:** A kártevő még 2010 nyarán bukott le Iránban, Busehr (Bushehr) város erőművének egyik számítógépén. Akkor mintegy százezer számítógépet sikerült megfertőznie. Csak az országban legalább 45 ezer felügyeleti számítógép és szerver hordozta a vírust. Az már a felfedezés utáni első elemzések során kiderült, hogy a Stuxnetet ipari folyamatirányító rendszerek ellen fejlesztették ki. A Stuxnet végső célja ipari vezérlőrendszerek automatikus folyamatainak újraprogramozása volt. [35]
- **TCP/IP:** A TCP/IP betűszó az angol Transmission Control Protocol/Internet Protocol (átviteli vezérlő protokoll/internetprotokoll) rövidítése, mely az internetet felépítő protokollstruktúrát takarja. Nevét két legfontosabb protokolljáról kapta, a TCP-ről és az IP-ről. [22]
- **Teljes körű védelem:** Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [5]
- **Trójai program:** Egy olyan malware program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tar-

talmaz rosszindulatú programkódot, azonban a többségük tartalmazza az úgynevezett *hátsó kapu* telepítését, ami a fertőzés után biztosítja a hozzáférést a céleszközhöz. Ezek a programok látszólag vagy akár valójában is hasznos funkciókat látnak, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak könyvtárakat vagy akár adatállományokat törölnek. [13]

- **Tűzfal:** Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is. [36]
- **Üzletmenet-folytonosság tervezés:** Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. (Ang.: Business Continuity Planning, rövidítve: BCP). [5]
- **Válságkommunikáció:** Tulajdonképpen nem más, mint a hatóságok, a szervezetek, a média és az érdekelt személyek, illetve csoportok közötti információcsere, amely a válságesemény előtt, alatt és után történik. Az információáramlás három dolog körül összpontosul: a tényleges válság, a válság kezelésének folyamata, a válság (különféle közvéleménycsoportokban és különböző szintű nyilvánosságokban kialakuló) képe. [37]
- **Védelmi intézkedések:** Kockázatok csökkentésére, a védendő rendszerek biztonsági szintjének emelésére meghatározott intézkedések, amelyek lehetnek logikai, fizikai és adminisztratív jellegűek. [5]
- **Vezeték nélküli személyi hálózat (WPAN):** A vezeték nélküli személyi hálózat célja tipikusan egy adott felhasználó közvetlen környezetében, néhány méteres távolságon belül levő intelligens eszközök összekötése egy rádiós interfész segítségével. [30]
- **Villamos erőtér:** Az elektromosan töltött részecskék és testek erőhatást gyakorolnak egymásra. Az azonos töltésűek taszítják, a különböző töltésűek vonzzák egymást. A nyugalomban lévő töltések közötti erővonalak terét villamos erőtérnek nevezzük. [21]
- **Vírus:** A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve azáltal, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A vírusok a rendszerbe a felhasználó engedélye nélkül kerülnek be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD-kártya, merevlemez, MP3- és videólejátszó, mobiltelefon stb.) vagy akár hálózati kapcsolat (internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tartalmát is törölheti vagy módosíthatja, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nem csak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [13]
- **Virtuális magánhálózat (VPN):** Olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva és így a nyilvános hálózaton belül védett kommunikációt valósít meg. [5]
- **Zárt védelem:** Az összes számításba vehető fenyegetést figyelembe vevő védelem. [5]

A fogalmak forrásjegyzéke

{1} 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

{2} Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár*. Forrás: https://www.naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2018. 03. 22.)

{3} Muha L. – Krasznay Cs. (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Nemzeti Közszolgálati Egyetem, Budapest.
{4} *Az Európai Parlament és a Tanács 2002/65/EK irányelve (2002. szeptember 23.) a fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról.*
{5} Muha L. (2004): *Fogalmak és definíciók.* In. Az informatikai biztonság kézikönyve. URL: http://lmuha.hu/defins.html (utolsó letöltés: 2018.03.22.)
{6} Molnár A. (2019): *Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{7} Ságí G. (2017): *Informatikai rendszer támadási folyamata.* Műszaki Katonai Közlöny, URL: http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/015_Sagi_Gabor.pdf (utolsó letöltés: 2018. 03. 24.)
{8} Pongrácz P. (2019): Kibertámadások villamosenergetika környezetben, In *Kritikus információsinfrastruktúrák védelme*, Dialóg Campus Kiadó, Budapest.
{9} Tikos A. (2019): A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései, In *Kritikus információs infrastruktúrák védelme*, Dialóg Campus Kiadó, Budapest.
{10} Rédecsi M. – Tóth G.: (2013) Android. URL: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (utolsó letöltés: 2018.03.24.)
{11} Gyurák G. (2015): *Informatikabiztonság I.* Pécsi Tudományegyetem Műszaki és Informatikai Kar, Pécs.
{12} *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.*
{13} Haig Zs. – Kovács L. (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* URL: http://hdl.handle.net/11410/285 (utolsó letöltés: 2018. 03. 24.)
{14} Marsi T. (2018): A célzott támadások és megelőzésük sérülékenységvizsgálattal. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.
{15} *A Big Data a hivatalos statisztikában.* 2016. URL: https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (utolsó letöltés: 2018. 03. 24.)
{16} Mátrai J. (2016): *Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás*. URL: http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (utolsó letöltés: 2018. 07. 04.)
{17} Oroszi E. (2008): *Social Engineering.* Budapesti Corvinus Egyetem, Budapest.
{18} Bonnyai T. (2019): *Kritikus információs infrastruktúra védelem*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{19} Kaczur G. (2018): *Spearphishing.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{20} Marsi T. (2019): *Incidenskezelés kritikus infrastruktúrák esetén*. In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{21} Görgey P. (2019): *A villamosenergia-szektor mint kritikus infrastruktúra*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{22} Danyek M. (2019): *A villamosenergia szektor mint kritikus információs infrastruktúra,* In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{23} Emmanuel Carabott (2011): *Hacking Motivations – Hactivism*, URL: http://www.gfi.com/blog/hacking-motivations-hacktivism/ (utolsó letöltés: 2018.03. 22.)
{24} Solymos Á. (2018): *Identitás- és jogosultságkezelés, mint a célzott támadások megelőzésének technológiai eszköze.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{25} László G. (2014): *Kockázatértékelés, kockázatmenedzsment*. URL: http://vtki.uni-nke.hu/uploads/media_items/kockazatertekeles_-kockazatmenedzsment.original.pdf (utolsó letöltés: 2018. 03. 22.)

{26} Kóbor Á. (2014): *Mi az a „dolgok internete”?* URL: https://ithub.hu/blog/post/Mi_az_a_dolgok_internete/ (utolsó letöltés: 2018. 07. 03.)
{27} Cser O. (2018): *Célzott támadás a pénzügyi szektor ellen.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{28} Krasznay Cs. (2012): *A polgárok védelme egy kiberkonfliktusban,* Hadmérnök 2012/4, URL: http://hadmernok.hu/2012_4_krasznay.pdf (utolsó letöltés: 2018.03.22.)
{29} Resperger I. (2002): Kockázatok, kihívások és fenyegetések a XXI. században. ZMNE, Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest.
{30} Haddad R. (2019): *Okoseszközök a kritikus információs infrastruktúrákban*. In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{31} *A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. tv.*
{32} Yaqoob, I. – Ahmed, E. – Imran, M. (2017): *The rise of ransomware and emerging security challenges in the Internet of Things.* Computer Networks, 6 September (2017), URL: https://doi.org/10.1016/j.comnet.2017.09.003 (Utolsó letöltés: 2017.10.20.)
{33} Bodó A. – Zámbó N.: *A közreműködők kötelezettségei a célzott támadások elhárításában az Ibtv. szerint.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest
{34} Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.
{35} Sebők V. (2018): Új típusú támadások az államok és szervezetek ellen. In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{36} Gyaraki R. (2018): *Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{37} Kriskó E. (2019): *Válságkommunikáció kibertámadás esetén*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

A Nemzeti Közszolgálati Egyetem kiadványa.

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

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

Olvasószerkesztő:
Zsoldos Sándor

Tördelőszerkesztő:
Vörös Ferenc

Borítóterv:
Friebert Máté

ISBN 978-963-498-485-6 (PDF)