



Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve



Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve

ISBN 978-615-00-9827-2

Készült a SeConSys együttműködés keretében

www.seconsys.eu

Szerzők:

Angyal István (5. fejezet), Arató György (5. fejezet, 10. melléklet), Bakos Béla (11. melléklet), Baranya Zsolt (3., 5. fejezet, 1., 4., 6., 12. melléklet), Bocskó Viktor (3. fejezet, 3., 8. melléklet), Bogáncs Tamás János (Fogalmak, rövidítések), Dr. Bonnyai Tünde (5. fejezet, 8., 9. melléklet), Dr. Buttyán Levente (5., 6. fejezet, 3. melléklet), Dr. Csátár János (6., 7. fejezet, 15. melléklet), Dr. Danyek Miklós (6., 7. fejezet, 15. melléklet), Deák Veronika (5. fejezet), Görgey Péter (1., 2., 4., 5., 7. fejezet, Fogalmak, rövidítések, 1., 2., 5., 7. melléklet), Gyebnár Gergő (6. fejezet, 14. melléklet), Illés Gábor (6. fejezet), Dr. Krasznay Csaba (1., 2., 5. fejezet, Fogalmak, rövidítések, Irodalomjegyzék), Molnár Ferenc (10., 13. melléklet), Pongrácz Péter (3., 7. fejezet, 1. melléklet), Szabó-Nyakas Zsolt Csaba (5. fejezet), Szádeczky Tamás (13. melléklet), Szent-Királyi Balázs (9. melléklet), Winter Gábor (Fogalmak, rövidítések)

Munkacsoport vezetőik:

Dr. Bonnyai Tünde, majd Baranya Zsolt

Dr. Danyek Miklós

Illés Gábor

Szabó-Nyakas Csaba Zsolt

Mentorok:

Görgey Péter

Dr. Krasznay Csaba



Kiemelt szakmai támogatók:

Balasys IT Kft.

Magyar Elektrotechnikai Egyesület

Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet

Nemzeti Közszolgálati Egyetem

Szakmai támogatók:

Black Cell Kft.

BM Országos Katasztrófavédelmi Főigazgatóság

BME-VET

CCLab Kft.

CrySyS Lab

MAVIR ZRt.

MVM Zrt.

Paks II. Zrt.

Ukatemi Kft.



Előszó

A technikai fejlődés következtében az emberiség egyre inkább kiszolgáltatottabbá vált az informatikai rendszerek működésének. Kiépítettünk magunknak egy olyan infrastruktúra rendszert, amely a mindennapi életünket támogatja, komfortosabbá teszi, azonban ezek a rendszerek szinte teljes mértékben az informatikai rendszerekre támaszkodnak. A 2000-es évek elején lezajlott információtechnológiai fejlődés által azonban olyan szintre emelkedett az infokommunikáció biztosított távkezelés, illetve a kényelmi szolgáltatások színvonala és száma, hogy ma már szinte nem is található olyan kritikus infrastruktúrát működtető szervezet vagy cég, amelyik nem csatlakozik valamilyen szinten a világhálózathoz.

Mindenhez azonban villamos energiára van szükség. A villamosenergia-rendszer az elmúlt évtized óta jelentős változáson megy keresztül: összetettebb, továbbá a zöld energia terjedésével kiszámíthatatlanabb az út a villamosenergia-termeléstől a fogyasztóig. Mindez abszolút rávilágít az ellátásbiztonság kulcsfontosságú szerepére.

Az Európai Unió által elfogadott klímapolitikai és Tiszta Energia Csomagban megfogalmazott célok kizárólag tagállami szinten már nem teljesíthetőek. Ehhez összekapcsolt rendszerekre és együttműködésre van szükség.

Mindez nemcsak Magyarországon, hanem egész Európában jelentős kihívások elé állítja a villamosenergia-szolgáltatókat. A rendszerek nem csak határon belül, hanem országhatáron kívül is egyre inkább összekapcsoltabbak, sőt a határon túl nem tervezetten megtermelt zöld energia mennyisége hazánkban is megjelenik. Emiatt, illetve az ehhez kapcsolódó szabályozások hatására a villamosenergia-rendszerirányítók működése is megnehezül. Elkerülhetetlen a szorosabb együttműködés, és már megjelentek további törekvések is arra vonatkozóan, hogy a szabályozást hogyan lehet a leghatékonyabb módon alakítani és működtetni.

Ez az összekapcsoltság egyértelműen magával hozza az informatikai rendszerek fokozott egymásra utaltságát is, elsősorban az adatok hálózaton való továbbítása által. Azt sem szabad figyelmen kívül hagyni, hogy a megújuló termelő egységek és a nemzetközi szabályozás hatására jóval nagyobb mennyiségű adattal kell dolgozni, jóval nagyobb mennyiségű adat elérhető, mint akár egy évtizeddel korábban.

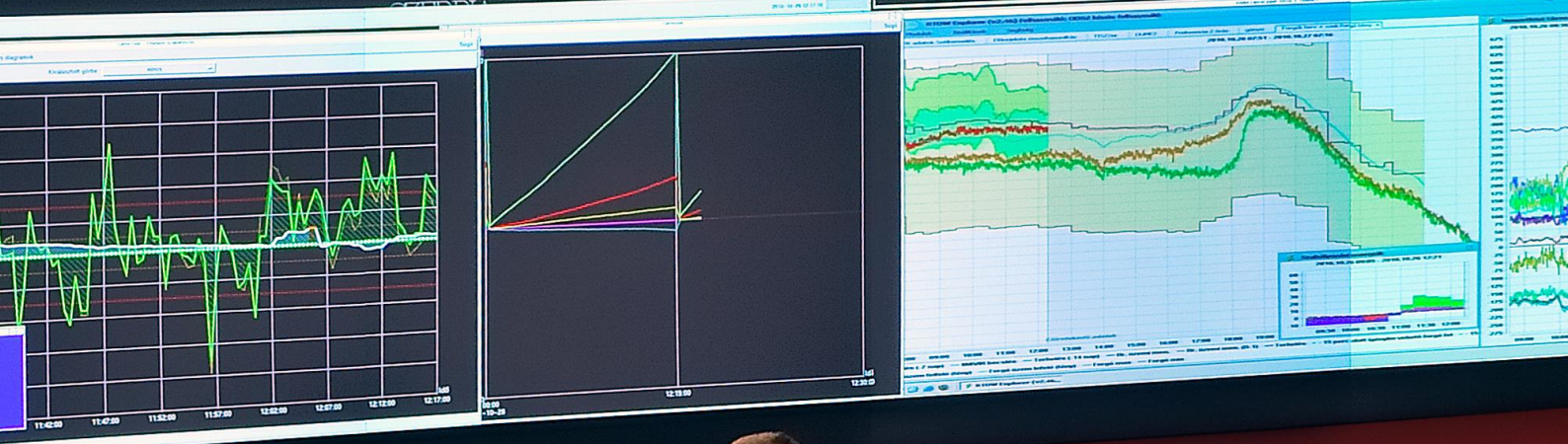
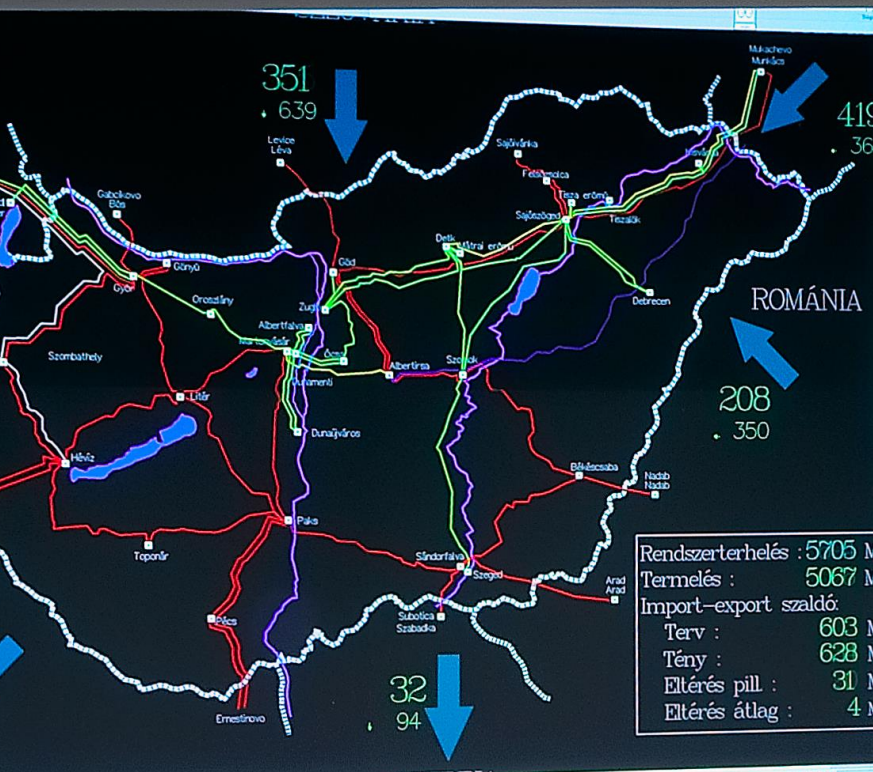
A SeConSys együttműködés keretében készült, eddigi tapasztalatokat, legjobb gyakorlatokat és megalapozott szakmai javaslatokat tartalmazó kézikönyv ezen kihívások kezelésében nyújthat segítséget üzemeltetők és szakértők számára, de a szakterületi sajátosságok iránt érdeklődőknek is hasznos olvasmány.



dr. Bencsik Balázs
Nemzeti Kibervédelmi Intézet, igazgató







Tartalom

1. Bevezető.....	12
2. A SeConSys együttműködés	13
2.1. Kezdetek és célok.....	13
2.2. Partnerek.....	14
2.3. Működési struktúra és módszer	15
3. Fenyegetések	16
3.1. Aktuális helyzet.....	16
3.2. Fenyegetettségi térkép.....	18
3.3. Támadási vektorok.....	18
3.4. Támadó profilok	21
3.5. Energetikai incidensek és azok tanulságai	23
3.6. Hibrid fenyegetések.....	25
4. A villamosenergia-rendszer és annak ICS/SCADA-i	30
4.1. A villamosenergia-ellátás alapjai.....	30
4.2. A villamosenergia-rendszer ICS/SCADA-komponensei.....	30
4.3. A jelenlegi villamosenergia-rendszer ICS/SCADA-komponenseinek kiberbiztonsági kihívásai.....	31
4.4. A paradigmaváltó villamosenergia-rendszer ICS/SCADA-i kiberbiztonsági kihívásai	32
5. A villamosenergia-rendszer ICS/SCADA-i kibervédelmének szabályozása	34
5.1. Stratégiai környezet.....	34
5.2. A SeConSys stratégiai megközelítése.....	35
5.2.1. Kiberbiztonsági kutatás-fejlesztés.....	36
5.2.2. Kiberbiztonsági oktatás, képzés.....	40
5.2.3. Kibertámadást megelőző képesség fejlesztése.....	43
5.2.4. Kibertámadást észlelő képesség fejlesztése.....	45
5.2.5. Kibertámadásra való reagáló képesség fejlesztése.....	46
5.3. Jogszabályi háttér	47
5.3.1. A létfontosságú rendszerek (kritikus infrastruktúrák) védelmével kapcsolatos törekvések időrendi áttekintése.....	47
5.3.2. Magyarországi általános szabályozás.....	48
5.3.3. Energia ágazati szabályozás.....	49



5.3.4. Információbiztonsági kötelezettségek.....	50
5.4. Nemzetközi gyakorlat.....	51
5.5. Hazai gyakorlat.....	53
5.5.1. Jelenlegi helyzet.....	53
5.5.2. A szabályozásfejlesztés lehetőségei.....	53
6. A villamosenergia-rendszer ICS/SCADA-i gyakorlati kibervédelme.....	58
6.1. Általános szempontok.....	58
6.1.1. Fenyegetés felderítés.....	59
6.1.2. Kockázatértékelés.....	60
6.1.3. Kiindulópontok, alapesetek felállítása.....	61
6.1.4. Képzés és tudatosság növelés.....	61
6.2. Ajánlások: Megelőzés.....	62
6.2.1. Sebezhetőség vizsgálat.....	62
6.2.2. Konfiguráció- és javításkezelés.....	62
6.2.3. Azonosítás és hozzáférés kezelés, ellenőrzés.....	64
6.2.4. Határvédelem.....	64
6.2.5. Behatolás megelőzés.....	67
6.2.6. Adatbiztonság.....	69
6.3. Ajánlások: észlelés.....	69
6.3.1. Helyzetismeret.....	70
6.3.2. Naplógyűjtés, kezelés és elemzés (SIEM).....	70
6.3.3. Rosszindulatú kód (malware) észlelés.....	71
6.4. Ajánlások: reagálás.....	71
6.4.1. A reagálás folyamata.....	72
6.4.2. Villamosenergia-rendszer specifikumok.....	73
6.4.3. Számítógépes kriminalisztika (Forensics).....	74
7. Rendszertechnika	78
7.1. Architektúra-modell ICS/SCADA-k tervezéséhez: a Purdue-modell.....	78
7.2. Javaslat a villamosenergia-rendszer ICS/SCADA-k kiberbiztonsági szintjeire.....	83
7.3. Villamosenergetikai ICS/SCADA-k felépítése.....	87
Energetikai, informatikai és kiberbiztonsági fogalmak, rövidítések jegyzéke ..	89
Ábrajegyzék.....	94



Mellékletek	97
1. melléklet: Incidens katalógus (2020. októberi állapot).....	99
2. melléklet: A villamosenergia-rendszer kiberbiztonsága és az OSINT	117
3. melléklet: Fenyegetettségi térkép.....	127
4. melléklet: Az Európai Unió tagállamainak nemzeti kiberbiztonsági stratégiái vizsgálatának és a magyar kiberbiztonsági stratégia elemzésének összefoglaló jelentése.....	148
5. melléklet: A 2020. évi Nemzeti Energiastratégia kiberbiztonsági vonatkozásai	154
6. melléklet: A 2020. évi Nemzeti Biztonsági Stratégia kiberbiztonsági vonatkozásai ..	156
7. melléklet: A 2020. május 1-jei elnöki rendelet és annak háttere.....	157
8. melléklet: A hatályos hazai szabályozási környezet bemutatása	162
9. melléklet: Útmutató a létfontosságú rendszerelemmé kijelölt villamosenergia alágazati szereplők jogszabályi megfeleléséhez	177
10. melléklet: Svájci modell.....	199
11. melléklet: Észak-amerikai modell.....	205
12. melléklet: Osztrák modell	212
13. melléklet: Német modell.....	215
14. melléklet: SNORT alkalmazási példák	219
15. melléklet: Villamosenergetikai ICS/SCADA-k felépítése	224
Irodalomjegyzék	237

Lezárva: 2020. október





1. Bevezető

A 2015., majd 2016. decemberi ukrajnai, tömeges fogyasztói ellátatlansággal járó kibertámadások bizonyították, hogy a nemzeti villamosenergia-rendszerek biztonságáért felelős szervezeteknek, személyeknek összetett, nagy erőforrásigényű, koordinált kibertámadásokkal is számolniuk kell. A megtörtént támadások azt is bizonyították, hogy immár a villamosenergia-rendszer ipari felügyeleti rendszerei (ICS¹) esetében sem lehet abban bízni, hogy ezek speciális jellege érdemben akadályozhatná a támadót. Sőt a történetek tükrében manapság arra is készülni kell, hogy az ICS által felügyelt villamos technológiáról is mélyebb ismereteket szerezve a támadó a technológiát érintő fizikai károkozásra (!) is képes lehet. Különösen nagy kockázatot jelenthetnek a régebbi, az aktuális kiberbiztonsági kihívásoknak megfelelni képtelen ICS/SCADA-komponensek.

Mindennek tükrében a villamosenergetikai ICS/SCADA-k kiberbiztonságát új, lényegesen magasabb szintre kell emelni. Ennek velejárója az is, hogy a kiberbiztonsági szint emelése magával hozhatja a kapcsolódó szabályozások célirányos továbbfejlesztését és a szükséges erőforrások biztosítását. E teendők szakmai megalapozására és támogatására a villamosenergetikai ICS/SCADA és a kiberbiztonság legjobb hazai cégei és szakemberei együttműködésre léptek. Célul tűzték ki egy olyan kézikönyv elkészítését, amely a villamosenergia-rendszer kiberbiztonságában érdekelt feleknek (stakeholder-eknek) szakmai ajánlások megfogalmazásával nyújthat támogatást.

A magyar villamosenergia-rendszer kiberbiztonsági rendszere továbbfejlesztése szempontjából különösen figyelemreméltó – és a hazai alkalmazhatóság szempontjából további részletesebb vizsgálatra érdemes – a német modell.

A villamosenergetikai ICS/SCADA és a kiberbiztonság legjobb hazai cégei és szakemberei a jelzett célok érdekében együttműködésre léptek. Célul tűzték ki egy olyan kézikönyv elkészítését, amely a villamosenergia-rendszer kiberbiztonságában érintett stakeholder-eknek szakmai ajánlások megfogalmazásával nyújthat támogatást.

A jelen kézikönyv hosszas műhelymunka, számos egyeztetés eredménye, így a benne foglaltak a lehető legszélesebb szakmai egyetértésen alapulnak. A kézikönyv a villamosenergia-rendszer legnagyobb teljesítményű, legnagyobb energiaáramokat kezelő – így esetlegesen sikeres kibertámadás miatti üzemzavarokkal a legnagyobb zavarokat, károkat okozó – elemeiben (erőműveiben, alállomásokban stb.) üzemelő ICS/SCADA-kra fókuszál.

¹ ICS: Industrial Control System. A hazai gyakorlatban elterjedt megnevezésre tekintettel a továbbiakban ICS/SCADA néven említjük.



A kiberbiztonsági szempontból ugyan egyre fontosabb, de villamosenergetikai szempontból kisebb jelentőségű egyéb hálózati elemek és rendszerek (pl. okos hálózat, IoT/IIoT stb.) maximum említés szinten jelennek meg, de a kézikönyvnek nem fókuszterületei.

A kézikönyv jelenlegi változata a jelen állapot tükrében szakértői szinten optimálisnak tartott ajánlásokat tartalmazza. Ugyanakkor az új fejlemények, támadások ismeretében folyamatosan tovább zajlik a történetek szakértői értékelése és a kézikönyv elektronikusán elérhető változatának szükség szerinti finomítása. A kézikönyv elektronikusán a www.seconsys.eu honlapon érhető el.

A kézikönyvben használt fontosabb energetikai, informatikai és kiberbiztonsági fogalmakat, rövidítéseket ezek jegyzéke értelmezi.

2. A SeConSys együttműködés

2.1. Kezdetek és célok

Az emberi civilizáció fejlettségének jelen fokán a közszolgáltatások – azon belül hangsúllyal a villamosenergia-ellátás – folyamatossága a társadalmak működésének, békéjének alapvető feltételévé vált. A villamosenergia-ellátás tartós és kiterjedt kiesése a kölcsönös függőségek² [1] nyomán előbb-utóbb szükségképpen egyre súlyosabb zavart okoz pl. a víz- és gázellátásban, a közlekedésben, a bankrendszerben, az egészségügyben, a telekommunikációban stb.

E függőségek alapján talán nem túlzás azt állítani, hogy a villamosenergia-rendszer a „legkritikusabb kritikus infrastruktúra”.³

A folyamatos villamosenergia-ellátás egyik garanciája a villamosenergia-rendszer ICS/SCADA-t alkotó felügyeleti, védelmi, automatika, adatátviteli rendszereinek (és ezek szünetmentes tápellátásának) zavartalan működése. E rendszerek meghatározó többsége digitális és hálózatban működik, így ezek egyre inkább támadhatók, mint a megtörtént esetek mutatják.

² Rinaldi, S.M. & Peerenboom, James & Kelly, T.K.. (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE. 21. 11 - 25. 10.1109/37.969131.

³ A magyar szabályozások „létfontosságú rendszer”, a nemzetközi szakmai terminológia „kritikus infrastruktúra” megnevezést használ, de a kettő szinonimája egymásnak.



A 2018 decemberében indult SeConSys (Security for Control Systems) együttműködés a magyar villamosenergia-rendszer kiberbiztonságának erősítése iránt elkötelezett személyek és hazai szervezetek nyitott, önkéntes, nonprofit, szakmai együttműködési formája az 1. fejezet szerinti cél elérése érdekében. A kézikönyv ehhez kíván szakmai támogatást nyújtani.

2.2. Partnerek

A hangsúlyosan szakmai, önkéntes, jogi személyiség nélküli együttműködésben a jelzett alrendszereket tervező, gyártó, létesítő, üzemeltető, valamint a kiberbiztonság területén tevékenykedő élvonalbeli hazai cégek mellett a szakmailag illetékes alábbi állami szervezetek, egyesületek, felsőoktatási intézmények (1. ábra) összességében mintegy 50 fővel vesznek részt, képviselik magukat, illetve fejezik ki egyetértésüket (2020. júliusi állapot).



1. ábra: A SeConSys együttműködés résztvevői (2020. júliusi állapot)



2.3. Működési struktúra és módszer

A SeConSys együttműködés tagjai az 1. fejezet szerinti szakmai megalapozó és támogató céllal összhangban két munkacsoportban – Szabályozási (WG-R) és Technológiai (WG-T) – tevékenykednek, illetve szükség szerint plenáris üléseket tartanak. A WG-kben együtt dolgoznak a villamos és kiberbiztonsági szakemberek, mint ahogy a WG-k munkáját is két-két vezető koordinálja. A SeConSys-szintű koordinációt két mentor – egyikük a Magyar Elektrotechnikai Egyesület (MEE), másikuk a Nemzeti Közzolgálati Egyetem (NKE) részéről – és a WG-vezetők rendszeres egyeztetései biztosítják. A WG-k önállóan, a maguk által meghatározott munkaterv szerint tevékenykednek. A működés alapvető kereteit – közte a témához elkerülhetetlen bizalmasságot – a valamennyi résztvevő által elfogadott Működési rend és Titoktartási nyilatkozat jelöli ki. A munkaanyagok a munkacsoportokban megvitatásra, szükség szerint átdolgozásra kerülnek, majd munkacsoport-szinten véleménynyilvánítással fogadják el az érintettek.

A SeConSys működési struktúrája és módszere biztosítja az eddig jórészt elkülönülten tevékenykedő szakemberek összefogásából, a szakterületi sajátosságok kölcsönös megismeréséből fakadó szinergiák hasznosulását és közös anyagok – mint pl. a jelen kézikönyv – létrejöttét.



3. Fenyegetések

3.1. Aktuális helyzet

A világ villamosenergia-rendszereiben alapvető változások zajlanak. Az energiamixben folyamatosan nő a megújuló alapú villamosenergia-termelés aránya; a hagyományos (többnyire nukleáris vagy fosszilis, kisebb részben nagy gátrendszerekre épülő víz-) erőművek továbbélése mellett gyorsan terjednek az elosztott – akár háztartási méretű – villamosenergia termelési megoldások. Ezek, valamint a villamosenergia-tárolás és a különféle okos technológiák (okos mérés, okos hálózat, mikro okos hálózat) terjedése miatt változik a villamosenergia-hálózati fizika; csökken az eddig jól tervezhető mennyiségű és irányú energiaáramok tervezhetősége.

A műszaki változások nem csak a villamosenergia-termelés, tárolás és felhasználás területén okoznak már-már paradigmaváltásnak is nevezhető változásokat, hanem az ezeket a tevékenységeket támogató informatikai és ipari felügyeleti rendszerek (ICS/SCADA-k) területén is. Az elmúlt nagyjából két évtizedben megdőlt az a régóta élő alapvetés, hogy a villamosenergia-rendszerben használt digitális megoldások – szemben más területek, pl. a pénzügyi szektor által használt rendszerekkel – egyediségük, robusztusságuk és zártságuk miatt nem lehetnek kibertámadások áldozatai. Az elmúlt évtizedekben történt, villamosenergia-ipari cégeket ért kiberbiztonsági incidensek (1. melléklet) azt mutatják, hogy a villamosenergia-ellátás biztonságáért felelős szervezetek és az általuk használt ICS/SCADA rendszerek és berendezések semmivel sem ellenállóbbak, mint más szektorok által használt IT rendszerek, legfeljebb eddig kevés támadás érte őket és a támadók ritkán voltak motiváltak egy komolyabb üzemzavar előidézésében.

Napjainkban a legtöbb ICS/SCADA rendszer és berendezés ugyanolyan hardver és szoftverelemekből épül fel, mint bármelyik nagyvállalati IT rendszer és már érkeznek az első olyan felhős megoldások is, amiket kifejezetten ipari rendszerekhez gyártanak. Azonban a nagyvállalati IT rendszerek többségével ellentétben az ICS/SCADA-komponensek 15-20 évre tervezetten kerülnek üzembe helyezésre, ami azt jelenti, hogy nagyon sok olyan ICS/SCADA működik, amely esetében a gyártó idővel már semmilyen támogatást nem nyújt a rendszeréhez, így a szoftveres sérülékenységek sem kerülnek javításra. Ez nem csak az üzembiztonsági kockázatokat növeli, hanem egy támadónak is könnyebbé teszi a dolgát, amikor az adott ICS/SCADA-t próbálja kompromittálni. Ráadásul a még támogatott rendszerek esetén sem mindig könnyű és egyszerű a gyártó által biztosított javítások alkalmazása. Ezt részben az IT és ICS/SCADA rendszerek üzemeltetési filozófiáiban meglévő különbségek okozzák.



Az IT és ICS/SCADA rendszerek közötti mind szorosabb kapcsolat nem csak műszaki téren jelentkezik, ugyanez a folyamat megfigyelhető a rendszerekkel dolgozó mérnökök munkavégzésében is. Míg a korábbi évtizedekben az ICS/SCADA rendszereket és berendezéseket telepítő, üzemeltető villamosmérnökök és a nagyvállalati IT rendszerekért felelős informatikus mérnökök között elvétve volt csak kapcsolat (akkor is inkább csak IT rendszerüzemeltető és felhasználó közötti kapcsolat), addig napjainkban egyre gyakrabban, egyes helyeken már napi szinten kell az IT és OT szakterületek mérnökeinek együttműködni azért, hogy a feladataikat az elvárt határidőre és magas színvonalon legyenek képesek ellátni. Ez az együttműködési kényszer, az egymásra utaltság kezelése pedig gyakran nagyobb kihívást jelent, mint a műszaki problémák megoldása.

Fentieket akkor is figyelembe kell venni, amikor az átalakulóban lévő villamosenergia-rendszer kiberbiztonsági szabályozói környezetét vizsgáljuk. Jelenleg nincs olyan, kifejezetten a villamosenergia-rendszerben működő szervezetekre vonatkozó, átfogó kiberbiztonsági minimum szintet meghatározó követelményrendszer, aminek megfelelően biztosítani lehetne a magyar villamosenergia-rendszer üzembiztonságához nélkülözhetetlen IT és ICS/SCADA rendszerek legalapvetőbb logikai biztonsági követelményszintjét.

Az előzőekben leírt, egyre gyorsabban változó (főként termelési oldalon diverzifikálódó) villamosenergia-rendszert figyelembe véve a SeConSys keretében már megfogalmazódott olyan gondolat is, hogy nem is feltétlenül egyetlen kiberbiztonsági követelményrendszert kéne érvényesíteni a teljes villamosenergia-rendszerre. Ha ezt a kérdést onnan vizsgáljuk, hogy ugyanannak a biztonsági szintnek kell-e érvényesülnie egy háztáji kiserőmű vagy egy hagyományos (fosszilis tüzelésű), több száz MW beépített teljesítményű alaperőmű esetében, egyértelmű a válasz: nem. Ezenél valóban indokolt lehet az eltérő minimum biztonsági szint meghatározása és megkövetelése.

Villamosenergetikai szakértőkkel egyeztetetten a villamosenergia-rendszer kiberbiztonságát részletesen a 7.2. pont szerinti négy – két kötelező és két ajánlott – védelmi szintbe célszerű szervezni. Az egyes szintek konkrét kiberbiztonsági követelményeire vonatkozó javaslatokat a SeConSys a folytatódó munka keretében dolgozza ki.



A villamosenergia-rendszer változásai léptékük és összetettségük alapján összességében paradigmaváltásként jellemezhetők és szinte kivétel nélkül növelik a villamosenergia-rendszer infokommunikációs technológiáknak – ezzel együtt a kiber fenyegetettségnek – való kitettségét. A következő időszak egyik – ha nem a – legfontosabb feladata a villamosenergia-szektorban ezeknek a kockázatoknak és kitettségnek csökkentése lesz.



3.2. Fenyegetettség térkép

Jelen fejezet a villamosenergia alágazatot, annak rendszereire és rendszerlemeire vonatkozó fenyegetettségeket a kapcsolódó támadási vektorok és az egyes támadó profilok alapján mutatja be, konkrét támadási módszerekre nem tér ki. A fejezet nem tárgyalja azon, környezeti (természeti csapások), illetve társadalmi (háború stb.) eredetű tényezőket, amelyek nem értékelhetők specifikus, kiberbiztonsági fenyegetettségként.

3.3. Támadási vektorok

A villamosenergia alágazat rendszereinek és rendszerlemeinek sérülékenységei komoly kockázatot jelentenek. Az alábbiakban több olyan támadási vektor kerül felsorolásra, amelyekkel a kockázatelemzés során számolni kell.

Sérülékenységeket kihasználó támadások: a sikeres támadások mindig valamilyen – fizikai, logikai, szervezeti, humán – sérülékenység kihasználására épülnek. A sérülékenységek a rendszer minden szintjén, illetve az üzemeltető működésében is előfordulhatnak. A *fizikai* sérülékenységek a rendszerek (köztük a primer berendezések) fizikai védelmi megoldásaiban található hibák (egyszerűen hozzáférhető hálózati eszközök és csatlakozók, árnyékolás hiánya stb.), amelyek a fizikai szabotázs és behatolás különböző formáit teszik lehetővé. A *logikai* sérülékenységek az IT és ICS /SCADA rendszerekben található hibák, amelyek tervezési és implementációs szinten, a rendszert alkotó hardver- és szoftverkomponensekben, kommunikációs protollokban egyaránt előfordulhatnak. A *szervezet működési- és munkafolyamataiban* található sérülékenységek olyan eljárás hibák, amelyek kihasználása elősegítheti a fizikai és logikai támadások kivitelezését (pl. jogosultsági szintek indokolatlan engedélyezése, túlzott alvállalkozói függés stb.). A *humán erőforrás sérülékenysége* (pl. a biztonságtudatosság hiánya) ugyancsak megkönnyítheti a rendszer elleni fizikai és logikai támadásokat. A sérülékenységek létezésével folyamatosan számolni kell, a rendszerek és szervezetek felépítése egyre komplexebb, ami növeli a hibalehetőséget. A sérülékenységek folyamatos jelenléte annak is köszönhető, hogy a rendszereket emberek tervezik és implementálják, általában szoros határidők és limitált költségvetés mellett. Valamennyi sérülékenység azonosítása és kijávítása lehetetlen, de folyamatosan törekedni kell az azonosításukra, az ismert sérülékenységekkel kapcsolatos kockázatok felmérésére, arányos csökkentésükre. A sérülékenységek két fő osztályra, publikusan ismert és zero-day sérülékenységekre⁴ bonthatók. A publikusan ismert sérülékenységekkel kapcsolatos információk a támadók számára is elérhetők.

⁴ zero-day sérülékenység: még nem javított és nem publikált sérülékenység



Ha a javítás a gyártó érdekkörébe tartozik, az üzemeltető a javításig ki van téve a sérülékenység kihasználásából eredő veszélynek, ipari létesítmények esetében ugyanakkor azzal is számolni kell, hogy az üzemeltető szándékosan nem javít egy hibát, mivel a javítás olyan változtatást jelentene a rendszerben, amelyet alapos tesztelés, hatáselemzés, adott esetben egy felügyelő szervezet formális jóváhagyása nélkül nem hajthat végre. A nagyobb technikai tudással rendelkező támadók folyamatosan keresik a még nem ismert zero-day sérülékenységeket, melyek (elsősorban célzott támadások során) nagy valószínűséggel sikeresen és többnyire észrevétlenül használhatók ki.

A fizikai behatolás, mint támadási vektor nem elsődlegesen kiberbiztonsági kérdés, ugyanakkor előfordul, hogy a fizikai és a logikai biztonság összemosódik. Ilyen, amikor a támadó fizikailag fér hozzá egy rendszerhez, ami erősebb, komolyabb következményekkel járó logikai támadást tesz lehetővé. Ha a rendszerelem nem kifejezetten bontásálló (tamper resistant⁵), akkor a hozzáférés a tárolt adatok kiolvasásához, az eszközön futó programok módosításához vezethet. Emellett e fizikai védelmi rendszerek programozható rendszereket is tartalmazhatnak, melyek kompromittálásával a védett objektumba történő fizikai behatolás is végrehajtható.

Hálózati behatolás: a rendszerek ritkán működnek izolált környezetben, jellemzően hálózatok részei, akár az internet felől is elérhetők. Hálózati behatolásról akkor beszélünk, amikor a támadó ezen kapcsolatokat kihasználva, távolról kompromittálja a rendszert (pl. kívülről elérhető hálózati szolgáltatásban felfedett hiba kihasználásával átveszi egy belső komponens feletti irányítást, vagy a távoli hozzáférés lehetőségét kihasználva, hitelesítő információkat megszerezve, legitim felhasználó vagy szolgáltatás nevében távolról belép). A hálózati behatolások elleni megelőzési és észlelési módszerek kombinációjával lehet védekezni. Létfontosságú vagy magas fokú üzembiztonságot igénylő rendszerek – mint a villamosenergia-ipari létesítmények – esetében azonban nagyobb hangsúlyt kell fektetni a megelőzésre, mert a szolgáltatások legcsekélyebb mértékű kiesése sem tolerálható. A megelőzés és észlelés együttes érvényesítését szolgálja a hálózat szegmentálására épülő mélységi védelem (defense in depth) elvének érvényesítése.

Kártékony programok használata: a támadó több szinten alkalmazhat kártékony kódokat; első behatolás alkalmával általában a rendszerben eleve meglévő, a távoli hozzáférés lehetőségét biztosító funkciókat aktiváló kódot, majd ennek segítségével újabb és komplexebb modulokat (privilegium növelés, perzisztencia⁶ biztosítása, védelmi funkciók kikapcsolása stb. érdekében) juttat a rendszerbe. E programokat korábban *vírus*, *féreg*, és *trójai* kategóriákba sorolták, de a kódok ma már nehezen kategorizálhatók. A modern kódok moduláris felépítésűek, távolról vezérelhetők, elemeik önállóan futtathatók, már futó folyamatokba vagy az operációs

⁵ tamper resistant: jogosulatlan fizikai hozzáférés ellen védett eszköz

⁶ perzisztencia: tartós fennmaradás, túlélés



rendszerbe is beépülhetnek. A távoli vezérléshez szükséges kommunikáció általában rejtjelezett és fedő forgalomba ágyazott, melyet a tűzfalak átengednek. A kódnak önálló terjedést megvalósító funkciói is lehetnek, de jellemzően használt disztribúciós módszerek az e-mail, a drive-by-download⁷ vagy watering hole⁸, esetleg fertőzött adathordozó is. A kód által megvalósított funkciók és a kód minősége a támadó technikai tudásától és anyagi erőforrásaitól függ. Kártékony programokkal PLC-eket⁹ és RTU-kat¹⁰ is meg lehet fertőzni. Kártékony funkció nemcsak utólag, hanem a tervezés, fejlesztés fázisában is bekerülhet a rendszerbe.

Kriptográfiai sérülékenységek kihasználása: az adatok átvitel vagy tárolás során történő védelmének eszközei a – felhasználók és szolgáltatások hitelesítésére, adatátvitel lehallgatás és módosítás elleni védelmére használt – kriptográfiai algoritmusok és protokollok. A kriptográfia, mint a védelem láncszeme, hatással van a teljes rendszer biztonságára. Jelenleg viszonylag kevés kriptográfiai sérülékenység és támadás ismert, egyszerűbb az algoritmust futtató számítógép, beágyazott eszköz kompromittálása, mint az algoritmus feltörése, ugyanakkor mélyebb tudással rendelkező támadók esetében a lehetőséget nem lehet kizárni.

Protokoll és API¹¹ hibák kihasználása: a protokollokban és az API-kban található sérülékenységek tervezési szintű hibák, melyek javítása nehezebb, mint az implementációs hibáké, módosításuk a rendszerben mélyebb szintű változtatásokat igényel. Az elterjedt protokollokban talált hibák javítása új verziókat eredményezett, az ezekre való áttérés azonban sokszor gyakorlati problémákba ütközött, egyes esetekben nem valósulhatott meg. A rendszerek így egy protokoll több verzióját is támogatják, ami további támadási lehetőségekhez vezetett. A protokollok elleni támadásoknak több fajtája létezik. Cél lehet egy résztvevő megszemélyesítése; a kulcs megszerzése; régebbi, már kompromittált kulcs elfogadtatása; a védett üzenetek feltörése, módosítása, visszajátszása; hamis üzenetek előállítás. A protokollokhoz hasonlóan biztonsági API-kkal is számos környezetben találkozhatunk, esetükben a támadó olyan, előre nem látott módon hívja meg a függvényeket, hogy végül kompromittálja a rendszert.

Social engineering¹², phishing, OSINT¹³: a technikai jellegű támadások mellett a humán felhasználók ellen irányuló támadások is hatékonyak. Sokan a felhasználókra úgy tekintenek, mint az rendszerek biztonságának leggyengébb láncszemeire.

⁷ drive-by-download: letöltés általi támadás

⁸ watering hole: gyakran látogatott weboldalak támadása

⁹ PLC: Programmable Logic Controller (programozható logikai vezérlő)

¹⁰ RTU: Remote Terminal Unit (telemechanikai alközpont)

¹¹ API: Application Programming Interface (alkalmazásprogramozási interfész/felület)

¹² social engineering: a pszichológiai befolyásolás, félrevezetés és megtévesztés módszere

¹³ OSINT: Open Source Intelligence (nyílt forrású információszerzés)



Ez a tekintetben igaz, hogy hiába alkalmazunk technikailag erős biztonsági megoldásokat, ha a felhasználók nem felkészültek ezek megfelelő használatára. Phishing támadások során a támadó a felhasználók számára hamis információt tartalmazó e-mail-t küld vagy weboldalt jelenít meg, rávéve őket valamilyen kompromittáláshoz vezető lépésre. E támadások hatékonyságát a támadók úgy növelik, hogy minden elérhető forrást felhasználnak a rendszerrel és a felhasználókkal kapcsolatos információk gyűjtésére. Az elégtelen biztonságtudatosság miatt szabadon elérhető információkat OSINT keretében gyűjtve és feldolgozva a támadó további értékes információk birtokába juthat. Lásd bővebben a 2. mellékletben.

Belső támadó, beszállító felől érkező támadás: a belső támadók valamilyen legitim hozzáféréssel és a külső támadóknál több információval rendelkeznek, amit rosszindulatúan használnak fel. Nemcsak magát a rendszert ismerhetik jól, hanem annak gyengeségeit, a szervezet biztonsági eljárásrendjét is. A leggyakrabban előforduló támadások az információlopás, illetéktelen felhasználás és rosszindulatú programok alkalmazása. A belső fenyegetettség körébe tartoznak a beszállítói lánc felől érkező támadások is (a fejlesztés, illetve üzemeltetés/karbantartás során szándékosan elhelyezett hibák, kiskapuk), melyek ugyanakkor nem feltétlenül a beszállító tudtával történnek, külső támadó a beszállítók rendszerét kompromittálva, jogosultságaikkal is végrehajthat támadó műveleteket.

3.4. Támadó profilok

A rendszereket fenyegető támadások forrása sokféle lehet, ezért a villamosenergia alágazat létesítményeit fenyegető egyes támadókat *motiváció, az információszerzési képesség mélysége, a technikai tudás szintje*, valamint a rendelkezésre álló *erőforrások mennyisége* alapján, az alábbiak szerint érdemes osztályozni:

Script kiddie¹⁴: korlátozott tudással, információszerzési lehetőséggel és erőforrásokkal rendelkező külső támadó. Motivációja elsődlegesen az önkifejezés. Jellemzően mások által kifejlesztett módszereket és eszközöket használ, célpontját nem előre megtervezett stratégia mentén választja, többnyire az lényeges számára, hogy a célpont könnyen kompromittálható legyen. A script kiddie-k által felhasználható, publikusan elérhető információk és eszközök mennyisége folyamatosan növekszik. Egy-egy régebbi eszköz vagy technika a technológia fejlődésével elavulhat, ennek üteme azonban az ipari létesítmények tekintetében lassabb (a hosszú életciklus modell miatt sokszor régi technológiák használtak), ezért hosszabb távon technikai képességeinek folyamatos növekedésével kell számolni. Alacsony kockázatot jelent, mert motivációja nem kifejezetten ezekre a rendszerekre irányítja figyelmét.

¹⁴ Script kiddie: komoly szaktudással nem rendelkező kezdő hacker



Elégedetlen munkatárs/beszállító: motivációja személyes jellegű. Veszélyesebb, mint a script kiddie, mert célpontja egy konkrét szervezet, motivációja általában átgondolt stratégia követésére ösztönözi, több információval rendelkezik vagy képes megszerezni, hozzáférési jogosultságokkal rendelkezhet, illetve személyes kapcsolatban állhat a többi felhasználóval. Technikai tudásának mélysége változó, ipari környezetben ismerheti a kontrollált fizikai folyamatok jellemzőit, tudhatja milyen beállítások vezethetnek súlyos következményekhez, ismerheti az eszközök korlátait. Anyagi erőforrásai általában korlátozottak. Jelentős kárt okozó támadások végrehajtására is képes lehet, ezért jelentős kockázatot jelent. A kockázatot mérsékeli, hogy általában egyedül tevékenykedik és többnyire a közvetlenül megszerezhető információknak és saját technikai tudásának megfelelő támadást hajt végre.

Hacktivista csoportok: jellemzően akciószerűen, nem hosszútávú stratégia mentén működő laza szerveződések. Motivációjuk valamilyen társadalmi vagy politikai ideológia védelme, ez határozza meg a támadás célpontját és célját. Alapvetően külső támadók, általában kevés belső információval rendelkeznek. Anyagi erőforrásaik limitáltak, információszerző képességük korlátozott, jellemzően technikai eszközökkel, a támadás kivitelezése közben próbálnak több információt gyűjteni, hozzáféréseket szerezni. Technikai tudásukat tagjaik tudása határozza meg, így az széles skálán mozog; jellemzően van néhány magas képzettségű tag, ám a csoport nagy része amatőr. Kapcsolatban állhatnak kiberbűnözői csoportokkal. A csoportok korlátozott információszerző képessége és tudása valószínűleg nem elegendő kritikus következményekkel járó támadások végrehajtásához, valószínűbb, hogy politikai vagy társadalmi üzeneteiket weboldalak lebénításával, módosításával próbálják elérni, ugyanakkor az ilyen kis komplexitású támadásoknak is lehetnek súlyos mellékhatásai.

Terrorszervezetek: tendenciózus, hogy terrorista szervezetek eszköztárukat információs támadó eszközökkel bővítik, ezek ugyanakkor egyelőre inkább a hagyományos módszerek kiegészítésére szolgálnak. E szervezetekre a determináltság és sokszor az irracionalitás jellemző, motivációjuk általában politikai vagy vallási ideológiára épül, stratégiai céljaik átgondoltak, elsősorban média jelenlétre és a lakosság megfélemlítésére törekшенek. Célpontjaikat tudatosan választják. Anyagi erőforrásaik számottevők is lehetnek, így jelentős mennyiségű információt szerezhetnek. Sok esetben modern eszközrendszerrel rendelkeznek és fejlesztik tudásukat. Bűnszervezetekkel kooperálhatnak, jelentős kockázatot, komoly fenyegetést jelentő támadók. A villamosenergiái-ipari létesítmények ellátási láncban betöltött szerepük miatt közvetlen célpontjaik lehetnek.



Kiberbűnözők: motivációjuk a haszonszerzés, amelynek érdekében, átgondolt stratégiai célok mentén, nagyszabású, térben és időben kiterjedt támadó kampányokat hajtanak végre. A támadások célja többnyire személyes adatok, jogosultságok gyűjtése, hozzáférések ellehetetlenítése zsarolási céllal, illetve az irányítás átvétele és a kompromittált számítógépek botnet-be¹⁵ szervezése. Az információk és a botnet által biztosított támadói potenciál közvetlenül felhasználható, de akár értékesíthető is. A sikeres szervezetek számottevő információszerző képességgel, jelentős anyagi erőforrásokkal és tudással rendelkezhetnek. A villamosenergia-ipar létesítményei tekintetében a csoportok kétféleképpen jelenthetnek kockázatot: támadó eszközeiket el- vagy bérbe adhatják más csoportoknak, de közvetlenül is támadást indíthatnak a létesítmények, illetve az ellátási lánc ellen. Veszélyes támadók, motivációjuk ugyanakkor a villamosenergia-ipar létesítményei elleni támadásra jelenleg limitált, egyelőre egyszerűbben is képesek hasznot termelni.

Idegen állam által támogatott csoport: motivációját, stratégia céljait és célpontjait a támogató állam politikai céljai határozzák meg, jellemző a kémkedés, a szabotázs, illetve katonai akciók támogatása. Erősen motivált, világos stratégiai célokkal rendelkezik, és tudatosan választ célpontot. Szervezett és erőforrásokban gazdag, emellett hagyományos hírszerzői módszerekre és tevékenységekre is támaszkodhat. Ez lehetővé teszi információszerző képességének mélyítését, komplex, térben és időben nagy kiterjedésű támadások végrehajtását. Technikai tudása mélyebb, anyagi erőforrásai komplex kutatási és képzési programok végrehajtását is biztosítják. Jellemzője a kifinomult és fejlett, nem ritkán mások által még teljesen ismeretlen támadási módszerek és eszközök alkalmazása. Jelentős kockázatot hordozhat.

A részletes fenyegetettségi térképet a 3. melléklet tartalmazza.

3.5. Energetikai incidensek és azok tanulságai

Az egyes országok, régiók villamosenergia-rendszereiben már az 1990-es és 2000-es években széles körben elterjedtek a részben kereskedelmi forgalomban kapható (COTS¹⁶), hagyományos IT komponensekből is épített ICS/SCADA-k. Ezek a megoldások tették lehetővé és megfizethetővé az egyes villamosenergia-ipari szereplők számára a villamosenergia-rendszer egyre nagyobb mértékű helyi, majd távkezelését. Ebben az időben egy nagyon kis létszámú szakmai közösségen kívül szó szerint senki nem foglalkozott az ICS/SCADA-k kiberbiztonsági kérdéseivel. Nem volt ez másképp a villamosenergia-rendszerekben használt ICS/SCADA-k esetében sem. Ha valaki a 2000-es évek közepére más, üzleti területeken

¹⁵ Botnet: internetre kötött vezérelt eszközök

¹⁶ COTS: Commercial off-the-shelf (kereskedelmi forgalomban kapható, ún. „dobozos” szoftverek és hardverek)



tevékenykedő szervezetek (pl. pénzintézetek) esetében törvényi kötelezettségként megjelenő információ- és IT biztonsági elvárás rendszerek alkalmazását akár csak feltételesen szóba hozta, az azonnal heves ellenállásba ütközött (jellemzően az ICS/SCADA-kat üzemeltető – a szinte kizárólag villamosmérnöki háttérrel rendelkező – mérnökök irányából). Az érvek az ICS/SCADA biztonság témájával foglalkozók számára általában jól ismertek (az alábbiak csak példaként szolgálnak):

- Az ICS/SCADA-k tulajdonképpen nem IT rendszerek, ezért nem is kell őket úgy kezelni, mint egy bármilyen más szervezet IT rendszereit;
- Az ICS/SCADA-k nincsenek összekapcsolva más rendszerekkel, ezért az IT hálózatok irányából nem érhetőek el, így nincs is értelme hálózatbiztonsági kérdésekről beszélni;
- Az ICS/SCADA-k működése egyedi és specifikus, csak az érti őket, akinek értenie kell és hozzáféréssel kell rendelkeznie ezekhez a rendszerekhez, ezért még ha egy támadó be is tudna jutni az egyébként fizikailag szeparált hálózatban működő ICS/SCADA-komponensek valamelyikébe, nem lenne képes észrevétlenül üzemzavarhoz vezető változtatásokat végrehajtani.

Ehhez képest a villamosenergia-rendszerben bekövetkezett első üzemzavart a Blaster néven ismertté vált számítógépes féreg 2003-as elszabadulása okozhatta.

A 2006-os, Idaho National Labs által végzett kísérlet igazolta az addig hipotézisként létező gondolatot, hogy kizárólag kiberbiztonsági incidensből is származhat fizikai károkozás (pl. leégő transzformátor).¹⁷

Az ICS/SCADA elleni első bizonyított támadás a Stuxnet néven elhíresült malware-hez köthető. Az utólagos elemzések szerint a Stuxnet különböző verziói több, mint fél évtizeden át működtek észrevétlenül. A támadók fő célja az iráni nukleáris program és az urándúsítási folyamat megzavarása, tönkretétele volt. Amikor 2010 nyarán a világ tudomást szerzett a Stuxnet-ről, már több száz urándúsításhoz használt centrifugát tett teljesen használhatatlanná, ezzel az elemzők szerint legalább 2 évvel vetette vissza az iráni atomprogramot.

A következő súlyos, ICS/SCADA-t érintő kiberbiztonsági incidens 2013-ban történt, amikor ismeretlen támadók egy kifinomult adathalász támadás-sorozatot indítottak, főként villamosenergia-szektorban tevékenykedő cégek ellen és kompromittálták több szervezet weboldalát kiszolgáló infrastruktúrát, ezeken keresztül további támadásokat indítva más szervezetek ellen. Ezzel párhuzamosan több európai ICS/SCADA-gyártó rendszereit is kompromittálták és egy, a Havex malware-rel fertőzött változatra cserélték az érintett gyártók weboldalaikról letölthető telepítő fájlokat.

¹⁷ <https://www.youtube.com/watch?v=LM8kLaJ2NDU>



2015. december 23-án délután kibertámadás ért hat ukrán szervezetet. A támadók három – közte kritikus infrastruktúraként működő – társasághoz bár behatoltak, a támadás nem járt egyéb következményekkel. Ugyanakkor három regionális áramszolgáltató (Prykarpattya-, Kyiv- és Chernivtsioblenergo) rendszerei esetében a támadás jelentős fogyasztói ellátatlanságokat okozott. Az elérhető adatok szerint az üzemirányítók összességében legalább 57 db 110 kV-os és 35 kV-os alállomás esetében veszítették el a távfelügyelet lehetőségét. A 15:30 és 16:10 közötti időszakban a három üzemirányítóközpont HMI-jeiről¹⁸ – kezelői beavatkozás nélkül – megszakító kikapcsolási parancsok kerültek kiadásra. Az ukrán hivatalos szervek és később az események elemzését végző szakértők által egyaránt orosz titkosszolgálatokhoz kapcsolható APT¹⁹ csoportként azonosított támadók közel 225.000 fogyasztót érintő üzemzavart okoztak. Mivel a call-centerek is elérhetetlenné váltak, így a fogyasztók sem tudtak kapcsolatba lépni a szolgáltatókkal. A villamosenergia-szolgáltatás – mintegy 3-6 órányi időtartamú és mintegy 130 MW-nyi teljesítményt érintő fogyasztói ellátatlanságot követően – csak az alállomásokra kiküldött üzemeltető személyzet helyszíni, kézi kapcsolásaival volt visszaállítható. Az áramszolgáltatás helyi idő szerint 18:56-ra állt helyre.

Egy évvel később, 2016. december 17-én kibertámadás érte az ukrán villamosenergia-hálózati rendszerirányítóját. Az Ukrenergo Kijev melletti alállomásán történt incidens több szempontból is jóval súlyosabb volt, mint az egy évvel korábbi, nagyobb rendszerteljesítményt érintett, sokkal fejlettebb volt (a különböző biztonsági elemzők által Industroyer/CrashOverride néven emlegetett malware a Stuxnet után a második olyan ismert, ICS/SCADA-specifikus malware, ami képes volt emberi közreműködés nélkül, autonóm módon megzavarni fizikai folyamatok vezérlését) és jelentősen nagyobb károk okozása volt a célja.

A fentieken túl a SeConSys tagjai által készített, kifejezetten villamosenergia-iparban tevékenykedő szervezetek elleni kibertámadások részleteit összefoglaló incidens katalógusban (1. melléklet) jelenleg 21 incidensről találhatóak információk, beleértve több atomerőmű elleni kibertámadást is.

3.6. Hibrid fenyegetések

Valamennyi kritikus infrastruktúra üzemelésének és üzemeltetésének az alapja, hogy villamosenergia ellátottságuk folyamatosan biztosított. Napjaink társadalmi és technológiai

¹⁸ HMI: Human Machine Interfész (ember-gép kapcsolati felület)

¹⁹ APT: Advanced Persistent Threat (Olyan kifinomult és összetett támadási formákat alkalmazó támadókra, gyakran támadói csoportokra használt kifejezés, akik hosszú ideig képesek észrevétlenül tevékenykedni a megtámadott szervezet IT és esetenként ICS/SCADA rendszereiben. Az APT csoportok gyakran rendelkeznek nemzetállami (titkosszolgálati) háttérrel.)



érettsége okán természetesnek hat, hogy – rövidebb áramszünetek ellenére – a villamos energia korlátlan mennyiségben és időben a rendelkezésünkre áll.

Ez mindaddig így is van, amíg egy olyan összehangolt hatás nem éri a villamosenergia szektor szereplőit, amely a rendszerelemek kiesését, ezáltal az általuk nyújtott szolgáltatás folyamatosságát rövidebb-hosszabb időre megszakítja. A hibrid fenyegetések²⁰ vagy támadások több összetevőből épülnek fel. Ilyenek pl. a politikai vagy egyéb támadásokkal kombinált kibertámadások is, amely támadásokat a jellegükből adódó komplexitás miatt neveznek hibridnek. Fontos megjegyezni, hogy valamely természeti katasztrófa, esetleg világjárvány is alkalmas arra, hogy az egyik összetevőjévé váljon egy ilyen hibrid fenyegetésnek, amely végső célja a támadott nemzet polgáraiban bizalmatlanság keltése az ország vezetése irányába, ezáltal káosz okozása, és a befolyás növelése a támadó szempontjából. [2]

A villamosenergia alágazati szereplők azért kerülhetnek a hibrid fenyegetések középpontjába, mert minden más kritikus infrastruktúra ágazat működéséhez is nélkülözhetetlenek, de egyben a kölcsönös függések is bonyolítják a helyzetet²¹. A folyamatos áramszolgáltatás kiesése esetén valamennyi további ágazat és alágazat szereplőjének folyamatos, elvárt szintű működése válik bizonytalanná. A hibrid fenyegetések alapvető célkitűzése a villamosenergia elérhetetlenné tétele, amely által rombolják a társadalom államigazgatás iránti bizalmát, gyengítve ezzel az ellenálló képesség²² mértékét.

A támadási faktorok számbavétele során – az előző fejezetben már említett ukrainai 2015. évi BlackEnergy támadás teljes kronológiájára alapozva – szükséges elkülönítenünk az eltérő támadási tényezőket. A fentiekben említett támadássorozat elemeinek rendkívül széles skálája mutatkozott meg: megtalálhatók voltak a fizikai támadások („Krími Blokáda” – távvezetékoszlopok lerombolása), illetve humán és logikai faktorok sérülékenységeinek, valamint a meglévő eljárásrendek hiányosságainak kiaknázása is. Az ukrainai támadások egyik tanulsága a lélektani hatások tudatos alkalmazása (a 2015. évi támadás során a call-center támadásával, 2016-ban pedig a kezelőszemélyzet hibára kényszerítési kísérletével).

²⁰ Hibrid fenyegetések: A hibrid fenyegetéseknek nincs általánosan elfogadott meghatározása. A NATO walesi csúcstalálkozójának zárónyilatkozata (2014. szeptember) szerint a hibrid fenyegetés széles körű nyílt és fedett katonai, félkatonai és nem katonai eszközök és eljárások alkalmazása egy szorosan integrált műveleti terv mentén. Forrás: Kiss, Á. P. (2019). A hibrid hadviselés természetrajza. Honvédségi Szemle, 2019/4. 17-37.

²¹ Rinaldi, S.M. & Peerenboom, James & Kelly, T.K.. (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE. 21. 11 - 25. 10.1109/37.969131.

²² Angol terminológiával: resilience



Éppen ezért a hibrid fenyegetésekre való felkészülés során fontos a komplex, átfogó megközelítés alkalmazása, amelyre jó alapul szolgálhat egy részletes kockázatelemzés kidolgozása, valamennyi kockázati tényező beemelésével, nagymértékben építve a már megtörtént támadások tanulságaira.

Érdemes megjegyezni, hogy a MAVIR Zrt., mint TSO által üzemeltetett átviteli hálózat összeköttetésben van más nemzetek rendszereivel. Az ENTSO-E²³ által összefogott kontinentális hálózat csökkenti egy esetleges dominó hatás következményeit.



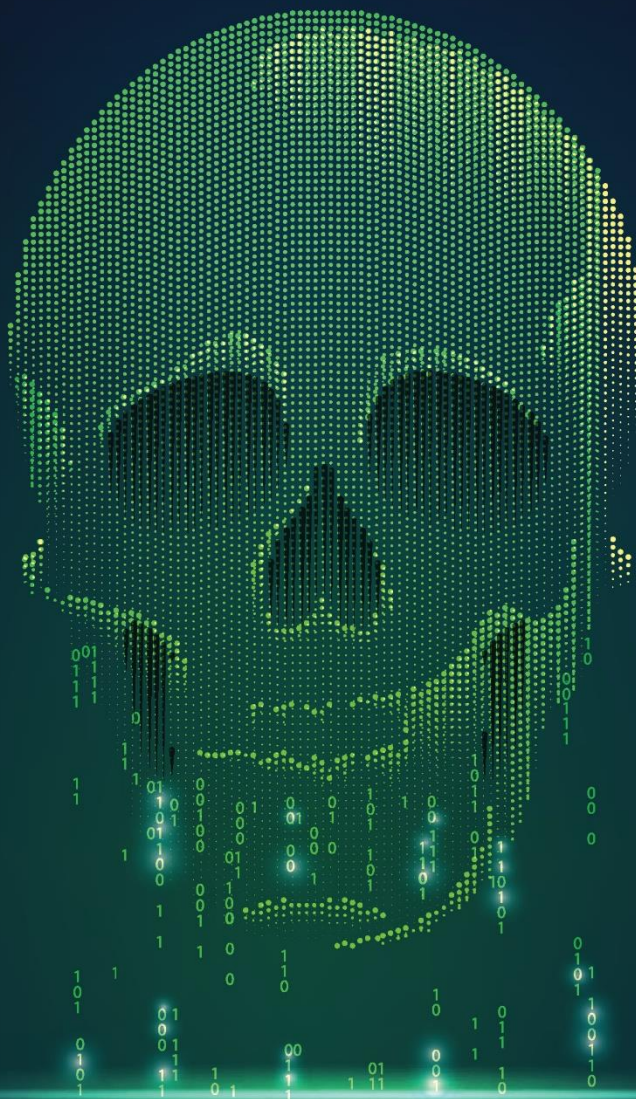
A villamosenergia alágazat üzemeltetőinek minden olyan rendkívüli helyzetben különösen érdemes számolniuk kibertámadás növekvő kockázatával, amely az eddigi mintázatoktól eltérő, azaz hibrid fenyegetést valószínűsít. Ilyen esetben kulcsfontosságú a kritikus infrastruktúra – hangsúlyos villamosenergia alágazat – üzemeltetők közötti rendszeres, kölcsönös és érdemi információmegosztás.



²³ ENTSO-E: European Network of Transmission System Operators for Electricity (Európai Villamosenergia-átviteli Rendszerirányítók Szervezete)







4. A villamosenergia-rendszer és annak ICS/SCADA-i

4.1. A villamosenergia-ellátás alapjai

A folyamatos villamosenergia-ellátás egy egyensúlyi feladvány. Alapja, hogy a mindenkori villamosenergia-termelésének és -fogyasztásnak minden időpillanatban egyensúlyban kell lennie. A termelési, átviteli és elosztási folyamatokat, az azokat megvalósító, százezermilliárd forintos nagyságrendű energetikai infrastruktúrát magas szinten és folyamatosan irányítani kell, mind üzemi, mind üzemzavari helyzetben fenn kell tartani az üzemét, meg kell védeni az esetleges romboló hatású zavaroktól stb. Ezeket a funkciókat a villamosenergia-rendszer ICS/SCADA-i, azok komponens alrendszerei hivatottak biztosítani.

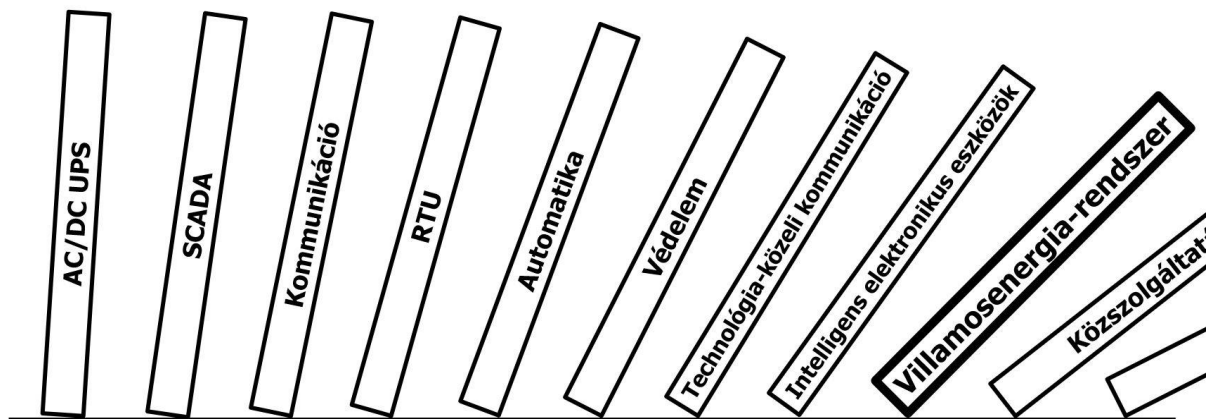
4.2. A villamosenergia-rendszer ICS/SCADA-komponensei

A villamosenergia-rendszer technológia berendezéseivel a jelző, mérő és működtető funkciókat ellátó intelligens elektronikus eszközök (IED²⁴) vannak közvetlen kapcsolatban. Ezek között, valamint a felsőbb szintekkel a technológia-közel kommunikáció biztosít kapcsolatot. A villamos berendezésekben, rendszerekben és hálózatokban fellépő rendellenességek elhárítása a védelmek, míg az ezek nyomán szükséges üzemi beavatkozások gyors és autonóm végrehajtása az automatikák feladata. Mindezen ICS/SCADA-komponensek információit az RTU-k kezelik, részben a felügyelt villamos technológiáról gyűjtött információknak a felsőbb szintre, részben az onnan érkező működtető parancsoknak az alsóbb szintre továbbításával. Az RTU-k által technológiai szinten gyűjtött adatok kommunikációs rendszeren keresztül jutnak a technológiai adatokat magas szinten gyűjtő, tároló, feldolgozó, megjelenítő SCADA rendszerekbe.

A felsorolt ICS/SCADA-komponensek kivétel nélkül digitális és hálózati rendszerek. Ezek kizárólag akkor képesek ellátni a folyamatos villamosenergia-ellátás szempontjából kulcsfontosságú feladataikat, ha maguk is folyamatosan kapnak villamosenergiát. Az ezt biztosítani hivatott szünetmentes tápellátó berendezések maguk is magas szinten digitalizáltak és távmenedzseltek. Minderre tekintettel a SeConSys megközelítésében a sorolt ICS/SCADA-komponensek szünetmentes energiaellátását biztosító berendezések maguk is ICS/SCADA-komponensek.

²⁴ IED: Intelligent Electronic Device (intelligens elektronikus eszköz)





2. ábra: A villamosenergia-rendszer ICS/SCADA-komponensei

A villamosenergia-ellátás fenntarthatósága szempontjából a sorolt ICS/SCADA-komponensek hierarchiát alkotnak és rendeltetésszerű működésükben is függenek egymástól.

4.3. A jelenlegi villamosenergia-rendszer ICS/SCADA-komponenseinek kiberbiztonsági kihívásai

A villamosenergia-rendszer ICS/SCADA-komponenseinek az átlagos élettartama 15-20 év. Ebből következően többségük csak erősen korlátozottan alkalmas az utóbbi évek új kiberbiztonsági kihívásainak kezelésére. Már tervezési szinten alapvető szemléletváltás szükséges. Az eddig velük szemben támasztott alapvető szempont a megbízhatóság és gyorsaság volt, amelyet a rendelkezésre álló processzor és memóriakapacitások maximális kihasználásával értek el. E megközelítésben általában nem áll rendelkezésre bennük olyan performancia-tartalék, amely lehetővé tenné a mai kihívásoknak megfelelő szintű kibervédelmüket megvalósítani hivatott alkalmazások pótlólagos telepítését.

A villamosenergia-rendszer ICS/SCADA-komponensei csak szigorú tesztelési, üzembehelyezési procedúrák nyomán léphetnek üzembe. Ha valamely azonosított sérülékenység nyomán a gyártó ki is ad javítást (patch-et), akkor annak érvényesítése a nehézkezesen végrehajtható újbóli villamostechnológiai tesztelések miatt általában csak lassan, nehézkesen, vagy egyáltalán nem történik meg. Jelenleg sem valós szándék, sem valós kényszer nincs a villamosenergia-rendszer ICS/SCADA-komponensek átfogó és fenntartható patch-elési rendszerének kidolgozására és működtetésére. Márpedig ennek tartós hiánya az ICS/SCADA-komponensek akár 10 évet is meghaladó élettartamára előre vetítheti azok ismert, de kijavíthatlan sérülékenységeit, ennek összes kockázatával együtt.



Fokozott figyelmet kíván az ICS/SCADA-komponensek tekintetében is terjedő távmenedzselési lehetőségek által jelentett kockázat. Az elvileg a komponensek beszállítói felé is megadható hozzáférési jogosultság elégtelen menedzselése a beszállító esetleg elégtelen biztonsági gyakorlatával párosulva illetéktelen hozzáférésre adhat esélyt.

4.4. A paradigmaváltó villamosenergia-rendszer ICS/SCADA-i kiberbiztonsági kihívásai

A villamosenergia-rendszert érintő alapvető változás az elosztott – akár háztartási méretű – termelő és tároló technológiák megjelenése. A korábbi koncentrált, nagyerőművi szén-, olaj-, atom-bázisú energiatermelés mellett egyre nagyobb arányban épülnek ki megújuló (nap-, szél- stb.) energia alapú termelő kapacitások. Ezek évszak-, napszak-, időjárásfüggése új egyensúlyi kihívásokat támaszt a rendszerirányító felé, amit a nagykapacitású és gazdaságos villamosenergia-tárolók megjelenése idővel csökkenthet. A kisebb teljesítményű elosztott kapacitásokat virtuális erőművek (szabályozó központok) foglalhatják nagyobb, piacon is értékesíthető virtuális „erőművi blokkokba”. A megújuló alapú, elosztott energiatermelő kapacitások további közös jellemzője, hogy a nagyerőművi energiatermelő forgógépes blokkokkal szemben statikus módon, forgó tömeg nélkül állítják elő a villamosenergiát. A nagyerőművek arányának csökkenésével a villamosenergia-rendszer frekvenciáját stabilizálni hivatott forgó tömeg (inercia) arányának csökkenése megváltoztatja a rendszer fizikáját, csökkenti annak stabilitását. Ez a manapság intenzív kutatás és fejlesztés alatt álló, jelentős teljesítményelektronikai és digitális szabályozástechnikai alapokon nyugvó ún. szintetikus inerciával lesz kezelhető. További jelentős hatást fog kiváltani a smart gridek²⁵ tömegessé válása, annak fejlettebb változataként a microgrid-ek elterjedése, az IoT/IIoT eszközök térhódítása, az e-mobility felfutása. E fejlemények révén egyes ICS/SCADA-komponensek terjedelme idővel egészen a fogyasztókig fog nyúlni.

A villamosenergia-rendszerben intenzíven zajló változások mennyiségükben, de főleg minőségükben paradigmaváltásként értékelhetők. A változások közös jellemzője a kiterjedt ICT-vonzat, ezzel a kibertámadásokkal szembeni minden eddiginél nagyobb kitettség.

²⁵ smart grid: okos hálózat (energiatermelés és -fogyasztás decentralizált menedzselése digitális eszközökkel a stabil, fenntartható, hatékony és megbízható működés érdekében)



5. A villamosenergia-rendszer ICS/SCADA-i kibervédelmének szabályozása

5.1. Stratégiai környezet

Egy nemzet kiberbiztonsági alapjait a nemzeti biztonságpolitika és azon belül a kiberbiztonsági stratégia kell, hogy jelentse.

A Magyarországon jelenleg hatályos kiberbiztonsági stratégia a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat (a továbbiakban NKS). Ezt egészíti ki a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat (a továbbiakban NIS stratégia).

Az NKS és a NIS stratégia nem kezeli megfelelően a kritikus infrastruktúrák, és azon belül a villamosenergia alágazat kiberbiztonsági kérdéseit, nincs konkrét feladat, határidő és felelős meghatározva a stratégiákban. Az EU tagállamok kiberbiztonsági stratégiáinak jó gyakorlatai megfontolásra méltók a magyar villamosenergia alágazati szereplők kiberbiztonságának megteremtése érdekében.

A 4. melléklet szerinti összefoglaló (a továbbiakban: stratégia összefoglaló) számos jó gyakorlatot mutat be. Ilyen például pl. a szektor specifikus stratégia megalkotása (amely figyelembe veszi a speciális irányító rendszerek kiberbiztonsági sajátosságait), amely PPP keretein belül valósul meg, vagy a supervisor team általi felügyeleti tevékenység, amely az osztrák modellben kerül bővebben kifejtésre, és a stratégiában meghatározott feladatok megvalósulását hivatott ellenőrizni, illetve a stratégia meghatározott időtávra történő meghatározása is. Ezen felül a stratégia összefoglaló körképet ad arra vonatkozóan, hogy a többi EU tagállam miként valósítja/valósította meg a kiberbiztonsági stratégia megalkotását.

Új fejleményként 2020 év elején megjelent a Nemzeti Energiastratégia, amely tartalmazza a villamosenergia alágazati szereplők kibervédelmével kapcsolatos helyzetképet, illetve intézkedései javaslatokat.

A kiberbiztonsággal kapcsolatos megállapításait az 5. melléklet tartalmazza.

Magas szintű stratégiai fejlemény a 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

A kiberbiztonsággal kapcsolatos megállapításait a 6. melléklet tartalmazza.



Végül globális szinten lehet stratégiai hatása annak, hogy Donald J. Trump elnök az Egyesült Államok villamosenergia-rendszerét fenyegető veszélyek miatt 2020. május 1-jén elnöki rendelettel országos vészhelyzetet hirdetett ki. Az Egyesült Államokon messze túlmutató elnöki rendeletet és annak hátterét a 7. melléklet mutatja be.

« Megfelelő kiberbiztonsági stratégia nélkül esélytelen hatékony kibervédelem kialakítása. A stratégiának tartalmaznia kell a feladatokat (határidőkkel és felelősökkel, valamint a visszaellenőrzés rendszerével). Kiberbiztonsági stratégia nélkül az érintett szervezetek előtt nincsenek világosan megfogalmazott célok és feladatok. Ezek nélkül pedig nem létezik komplex és hatékony kibervédelmi rendszer sem. »

5.2. A SeConSys stratégiai megközelítése

A SeConSys együttműködés álláspontja szerint a magyar villamosenergia-rendszer ICS/SCADA-i kiberbiztonságának célszerűen öt pilléren kell nyugodnia:

I. Kiberbiztonsági kutatás-fejlesztés

Célja, hogy a nemzetközi legjobb gyakorlatok megismerésén túl, azokat a magyar villamosenergia-rendszer ICS/SCADA sajátosságait is figyelembe véve és alkotó módon továbbfejlesztve álljanak rendelkezésre komplex – a kiberbiztonsági és villamosenergetikai szempontokat, ismereteket egységben, összefüggéseiben tartalmazó – szakmai anyagok és megoldások. A hazai tervező, gyártó, létesítő, üzemeltető társaságok, valamint szakterületi államigazgatási szervezetek legyenek képesek a szükséges és egyben elégséges szintű kiberbiztonságnak megfelelő sokirányú – és az előbbiek szerinti komplex szemléletű – fejlesztésekre (beleértve a mindenkor célirányos szabályozási és finanszírozási környezetre vonatkozó elemzések végzését, döntéselőkészítő javaslatok kidolgozását), majd az elért eredmények folyamatos szinten tartására.



II. Kiberbiztonsági oktatás, képzés

Célja:

- a. fiatal villamosenergetikai és kiberbiztonsági szakemberek oktatása,
- b. végzett, szakterületen tevékenykedő szakemberek (tovább)képzése,
- c. szakterületi döntéselőkészítők és -hozók, jogalkotók, társasági közép- és felsővezetők számára naprakész ismeretek rendszeres átadása a villamosenergia-rendszer ICS/SCADA energetikai és kiberbiztonsági sajátosságairól és mindenkori aktuális kihívásairól.

III. Kibertámadást megelőző képesség fejlesztése:

Célja a villamosenergia-rendszer ICS/SCADA-t érő mindenkori kiberfenyegetések elleni komplex kiberbiztonsági rendszer minden oldali jellemzőinek, elemeinek meghatározása, kiépítése és működtetése az aktuális új kihívások szerinti folyamatos javító, fejlesztő tevékenység végzése mellett.

IV. Kibertámadást észlelő képesség fejlesztése:

Célja a komplex megelőző intézkedések ellenére bekövetkező villamosenergetikai incidensek felderítésére, kezelésére hivatott komplex kiberbiztonsági rendszer jellemzőinek, elemeinek meghatározása, kiépítése és működtetése.

V. Kibertámadásra történő reagáló képesség fejlesztése

Célja a bekövetkezett incidensek mindenre kiterjedő felderítése, elemzése, javító intézkedésekre vonatkozó javaslatok kidolgozása, a felelősség megállapítása és a szükséges komplex képességfejlesztések végrehajtása.

Az egyes stratégiai pillérek kifejtését a következő pontok tartalmazzák.

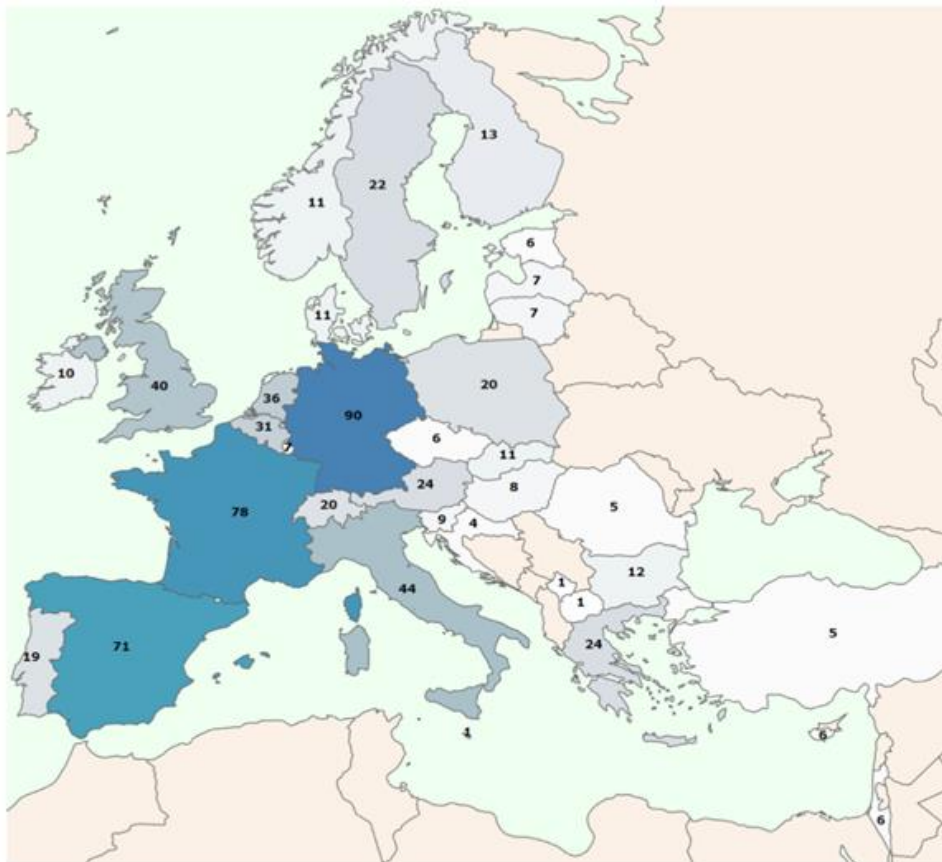
5.2.1. Kiberbiztonsági kutatás-fejlesztés

Ha eddig nem éreztük volna, hogy függünk az információs rendszerektől, a negyedik ipari forradalom változásai egészen biztosan mindenki számára tudatosítani fogják, hogy informatika nélkül nincs modern társadalom. Ha tehát ezek az információs rendszerek nem úgy működnek, ahogy kellene, az jelentős gazdasági-társadalmi hatásokkal járhat, biztonságuk megteremtése ezért alapvető érdek. Az elmúlt évek kibertámadásainak köszönhetően egyre több ország nemzeti biztonsági és kiberbiztonsági stratégiája foglalkozik a kibertéri fenyegetésekkel kiemelt nemzetbiztonsági problémaként.



A kockázatok enyhítése céljából folyamatosan dolgozzák ki azokat a szabályozókat, amelyek kötelezik az okos infrastruktúrák építőit és üzemeltetőit bizonyos informatikai védelmi intézkedések megtételére.

Mindezen kihívások következeképpen megkövetelik az innovatív kiberbiztonsági megoldások létrejöttét. 2018-ban az Európai Unió, készülve a kiberbiztonsági szabályozásainak bevezetésére és a 2021-től induló költségvetés megtervezésére, felmérte a kutatás-fejlesztéssel foglalkozó azon intézmények számát az Európai Unió tagállamaiban, amelyek kimondottan kiberbiztonsággal foglalkoznak. Azt lehetett látni a válaszadásból, hogy míg pl. Németországban, Franciaországban vagy éppen Spanyolországban meglehetősen sok olyan intézmény van, ahol kiberbiztonsági kutatás-fejlesztés-innovációval foglalkoznak, Kelet-Közép-Európában, így Magyarországon is ezen intézmények száma alacsony, ahogy a 3. ábrán is megjelenik. Ez azt is jelenti, hogy a globális versenyben, ahol hatalmas országokkal és tudástőkével kell versenyeznie az európai iparnak, nem igazán van meg az az alap, amire fel lehet építeni a saját információbiztonsági piacot, illetve tudásbázist.



3. ábra: Európai kiberbiztonsági kutatóközpontok [3]

Ez azért lenne fontos, mert a negyedik ipari forradalom robbanásával Európa egyre inkább ki lesz Európa téve azoknak a gyártóknak, amelyek nem európaiak. A hardvereszközöket jellemzően Kínában gyártják, a szoftverek jellemzően amerikai forrásból érkeznek. Éppen ezért az egyes államok által indított kibertámadások előtt gyakorlatilag védtelenül állnak az európai államok és vállalkozások, tekintettel arra, hogy az európai kibervédelem jelenleg nem, vagy nagyon kis számban tud olyan saját gyártású eszközöket használni, amelyek felhasználhatók a külső, akár kiberbűnözéssel összefüggő, akár állami finanszírozással megvalósuló támadásokkal szemben.

Az Európai Bizottság tervei alapján a következő kutatási érában három pillérre épül a kutatás-fejlesztés-innováció támogatása, ebből az első pillér a kiváló tudományról, a második pillér a globális kihívásokról és az európai ipar versenyképességéről, míg a harmadik pillér az innovatív Európáról fog szólni. Ezt ábrázolja a 4. ábra. A második pillérben „A társadalmat szolgáló polgári biztonság” nevű klaszterben a kiberbiztonság nevesítve szerepel, ez pedig meglehetősen pozitív jövőképet fest azoknak a kutatás-fejlesztés-innovációval foglalkozó intézményeknek és szakembereknek, akik szeretnék az európai kiberbiztonsági ipart megteremteni. Az Európai Bizottság tervei alapján a 2021-27 közötti szakaszban 100 milliárd euró nagyságrendű összeg áll majd rendelkezésre a kutatás-fejlesztés-innovációra, ezen belül a Globális kihívások és az európai ipar versenyképessége pillér 52,7 milliárd euróra számíthat. Tovább bontva, A társadalmat szolgáló polgári biztonság klaszterben szerepel a kiberbiztonság, amely a jelenlegi tudásunk szerint körülbelül 2 milliárd euróval fog részesülni ebből a hatalmas összegből.²⁶

²⁶ Európai Bizottság 2018





4. ábra: EU-finanszírozás a kutatás és az innováció területén (2021–2027) [4]

Magyarország természetesen aktívan követi az Európai Unió innovációs törekvéseit, és bár a következő időszakra vonatkozó tervek még nem ismertek, a kiberbiztonság biztosan része lesz a magyar kutatás-fejlesztés-innovációs stratégiának. Ezt támasztja alá, hogy a 2020-ban érvényes stratégiai dokumentumok is kivétel nélkül foglalkoznak ezzel a szakterülettel. A 1414/2013. (VII. 4.) Korm. határozat a Nemzeti Kutatás-fejlesztési és Innovációs Stratégia (2013–2020) elfogadásáról már kiemeli, hogy az egyik cél az adaptív innovációs megoldások – elsősorban informatikai és kommunikációs technológiákra alapozott – terjedésének gyorsítása. A részleteket a 1640/2014. (XI. 14.) Korm. határozat a Nemzeti Intelligens Szakosodási Stratégia (S3) elfogadásáról és a Kutatási Infrastruktúrák Európai Stratégiai Fóruma Útitervében szereplő kutatási infrastruktúra nagyprojektekben való magyar részvételről mentén kiadott Nemzeti Intelligens Szakosodási Stratégia (S3) – 2014-2020 segít megérteni. Ebben az IKT terület céljait az alábbiak szerint fogalmazza meg: „Az infokommunikációs technológiák széleskörűen fogják át és segítik elő az alágazati prioritásokat, úgy is, mint az egészségiparban a bioinformatika, vagy a diagnosztikai képalkotás, a járműiparban az intelligens közlekedési rendszerek, az energetikában a „smart city”. Az alágazati prioritásokhoz nem, vagy nem egyértelműen, vagy akár több alágazathoz is sorolható IKT megoldások alatt olyan technológiák érthetőek (példálózó jelleggel, nem kizárólagosan), mint: (...) információbiztonság, biztonságtechnika.” A kiberbiztonság, mint fejlesztési terület emiatt az összes releváns kormányzati stratégiában visszaköszön, így a 2020-ban elfogadott Mesterséges Intelligencia Stratégia is kitér erre a szempontra.



5.2.2. Kiberbiztonsági oktatás, képzés

A kibertámadások jelentős gazdasági, politikai, nemzetbiztonsági, de a társadalomra is kiterjedő káros következményt idézhetnek elő. Az elmúlt évek tapasztalatai alapján elmondható, hogy egyes kritikus infrastruktúrák kiemelt célpontjai a kibertámadásoknak, így különösen nagy hangsúlyt kell fektetni a lehetséges támadási alternatívák megismerésére és alkalmazhatóságára a hatékony védelem kialakítása érdekében. A különféle infrastruktúrák védettségének teszteléséhez szükség van a védelmi képesség képzési lehetőségeinek meghatározására, a kockázatok és sebezhetőségek feltárása érdekében. A létfontosságú rendszereknél dolgozó személyek nap, mint nap részt vesznek a döntéshozatalban, amiket döntően befolyásolnak a kibervédelemmel kapcsolatos stratégiai kérdések. Ahhoz, hogy az infrastruktúrák tesztelése és ellenőrzése, valamint az esetleges támadások elhárítása és megelőzése hatékonyan, illetve eredményesen megvalósulhasson, továbbá a döntéshozatalban megfelelő lépések kerüljenek végrehajtásra, elengedhetetlen a szakértők bevonása.



Különösen igaz ez a kritikus információs infrastruktúrák területén, ahol az üzemeltetésért felelős OT szakértők (jellemzően villamosmérnökök), az IT rendszerekért felelős informatikusok és a védelmi igazgatásban érdekelt, jellemzően rendvédelmi szakemberek nagyon eltérő szemléletmóddal rendelkeznek, amely az esetek többségében inkább akadály, mint előmozdítója a sikeres kibervédelemnek.

Különösen hiányzik az olyan szervezett képzés, amely kimondottan a SCADA/ICS rendszerek biztonsági kérdéseivel foglalkozna, fókuszálva akár a villamosenergia-rendszerek területére.



A kiberbiztonsággal, információbiztonsággal foglalkozó szakemberek hiánya és az érintett szervezetek vezetőinek kiberbiztonsági tudatosságával kapcsolatos kihívások indokoltá teszik ezen terület képzési programjának kidolgozását a kritikus információs infrastruktúra (KII) védelmének fejlesztése érdekében. A jelenlegi hazai helyzet alapján számos olyan, a kibertámadási és védelmi képesség kialakítását szolgáló képzés létezik, amelyek vagy csak informatikai tudást adnak át, vagy csak jogi ismeretek elsajátítását célozzák meg. Azonban a KII területen dolgozók számára olyan képzés, amely ezen két terület megfelelő részét együttesen fedné le, jelenleg hazánkban nem elérhető.



Mindezek miatt szükséges olyan képzési programok megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a nem informatikai végzettségű személyek kibervédelmi képességének kialakítására, a műszaki képzésekben a szakirányú tudás megszerzésére és a műszaki végzettséggel rendelkező, létfontosságú információs rendszerek területén dolgozó személyek szakirányú továbbképzésére.

A bolognai folyamat részeként átalakult felsőoktatási képzési rendszer az alábbi fázisokból épül fel: *alapképzésből és mesterképzésből*, illetve az alap vagy mesterképzés után is elvégezhető *szakirányú továbbképzésből*. A jelenlegi hazai kiberbiztonsági képzéseket ezen három csoport alapján mutatjuk be a következőkben.

5.2.2.1. Alapképzési szakok

Az alapképzés általában 3-4 éves időtartamot felölelő képzési forma, amelyen tudományterülettől függően BA (Bachelor of Arts), illetve BSc (Bachelor of Science) fokozat szerezhető. Ezen képzés során tulajdonképpen széleskörű alapszintű ismeretek elsajátítása a cél, amely a munkaerőpiacon hasznosítható szakmai ismereteket és megfelelő elméleti alapot nyújt az adott szakterületen a tanulmányok mesterképzésben történő folytatásához.

Kiberbiztonsághoz kapcsolódó hazai alapképzések:

- a) Nemzeti Közszerálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány (NKE KNY)²⁷
- b) Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció (ÓE BM)²⁸

5.2.2.2. Mesterképzési szakok

A mesterképzés, amelyen MA (Master of Arts), illetve MSc (Master of Sciences) fokozat és szakképzettség szerezhető. Mesterképzésre az jelentkezhets, aki legalább egy alapképzési diplomával vagy a korábbi képzési rendszer szerinti főiskolai/egyetemi diplomával rendelkezik, de a felvétel pontos követelményeit és feltételeit a felsőoktatási intézmények maguk határozzák meg. A mesterképzés általában 2-4 féléves időtartamot ölel fel. Összességében megállapítható, hogy a mesterképzés során szakterület specifikus és mélyebb elméleti és gyakorlati ismeretek átadása a cél, amely elvégzését követően lehetőség van kilépni a

²⁷ Felvi.hu szakeleírások: Nemzeti Közszerálati Egyetem - Bűnügyi alapképzési szak - Kiber nyomozó szakirány, https://www.felvi.hu/felveteli/egyetemek_foiskolak/IntezmenyiOldalak/meghirdetes.php?meg_id=20905&elj=20a.

²⁸ Felvi.hu szakeleírások: Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció, https://www.felvi.hu/felveteli/szakok_kepzesek/szakeirasok/Szakeirasok/index.php/szak/36/szakeiras.



munkaerőpiacra, illetve jelentkezni lehet a képzési rendszer harmadik lépcsőfokát jelentő doktori képzésre, amely a tudományos fokozat megszerzésére készít fel.²⁹

Kiberbiztonsághoz kapcsolódó hazai mesterképzések:

- a) Nemzeti Közszerolálati Egyetem – Kiberbiztonsági mesterképzés (NKE KB)³⁰
- b) Nemzeti Közszerolálati Egyetem – Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány (NKE VIKR)³¹
- c) Budapesti Műszaki és Gazdaságtudományi Egyetem – Mérnök-informatikus mesterképzés, IT biztonság mellékspecializáció

5.2.2.3. Szakirányú továbbképzések

Fontos megemlíteni a szakirányú továbbképzés szintjét is, amely a már korábban megszerzett alap- és mesterfokozatra, főiskolai vagy egyetemi szintű végzettségre épülő oklevet adó, 2-4 félév időtartamú képzési forma. A mesterképzéstől eltérő képzési forma, amely speciális feladatok ellátására ad felkészítést, valamint lehetővé teszi a korábban szerzett ismeretek meghatározott irányú elmélyítését. Azonban az elvégzését követően megszerzett oklevél nem emeli a korábbi végzettség szintjét.³²

Kiberbiztonsághoz kapcsolódó hazai szakirányú képzések:

- a) Nemzeti Közszerolálati Egyetem – Elektronikus infokommunikációs vezető szakirányú továbbképzés (NKE EIB)³³
- b) Eötvös Loránd Tudományegyetem – Adatbiztonsági és adatvédelmi szakjogász/szakember szakirányú továbbképzés (ELTE ASZ)³⁴
- c) Óbudai Egyetem – Kiberbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE KSZ)³⁵

²⁹ 2011. évi CCIV törvény a nemzeti felsőoktatásról.

³⁰ Felvi.hu szakleírások: Nemzeti Közszerolálati Egyetem – Kiberbiztonsági mesterképzés, https://www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/Szakleirasok/index.php/szak/20554/szakleiras.

³¹ Nemzeti Közszerolálati Egyetem: Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány szakleírás, tematika, <https://hhk.uni-nke.hu/oktatas/mesterkepzes/vedelmi-vezetestechnikai-rendszertervezo>.

³² 87/2015. (IV. 9.) Korm. rendelet a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról.

³³ Nemzeti Közszerolálati Egyetem: Elektronikus infokommunikációs vezető szakleírás, <https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok>.

³⁴ ELTE: Adatbiztonsági és adatvédelmi szakjogász szakleírás, <https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406>.

³⁵ Óbudai Egyetem: Kiberbiztonsági szakmérnök/szakember képzés tartalma, http://bmi.nik.uni-obuda.hu/kiber_kovetelmeny.



- d) Óbudai Egyetem – Információbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE ISZ)³⁶
- e) Gábor Dénes Főiskola – Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés (GDF AIM)³⁷

Meg kell jegyezni, hogy a Nemzeti Közszerológati Egyetem Elektronikus információbiztonsági vezető szakirányú továbbképzéséhez kapcsolódóan évről évre készülnek olyan e-learning formában elérhető éves továbbképzések, amelyek az információbiztonsági szakemberek mellett a közreműködő informatikusoknak és a szervezetek vezetőinek is szólnak. Mindez az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet alapján kötelező állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó szervezetek dolgozói, így a létfontosságú (villamosenergetikai) rendszerek vezetői és informatikusai számára is.

Összességében megállapítható, hogy a jelenlegi felsőoktatási képzési rendszer minden szintjén elérhető kiberbiztonsággal, információbiztonsággal foglalkozó képzés. Fontos kiemelni, hogy a jelenlegi képzési rendszer fázisaiban átadott ismeretek mennyisége és mélysége eltérő, jelentősen befolyásolja azt a képzési forma struktúrája, követelményei, időtartama, valamint a képzés során elsajátítandó készségek, képességek, ismeretek halmaza.

A kiberbiztonság azonban egy gyorsan változó, folyamatosan fejlődő és bővülő terület, amely egyre újabb és újabb kihívásokat, illetve fenyegetéseket tartogathat számunkra. A közszolgáltat és a létfontosságú rendszerek hatékony és eredményes működéséhez elengedhetetlen a kibertér használata, azonban számos előnye mellett a hátrányaival és az esetleges kockázatokkal is számolnunk kell. Szükséges tehát egy olyan, eddig még nem létező képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgáltatban és a KII³⁸ területen dolgozó személyek kibervédelmi képességének kialakítására.

5.2.3. Kibertámadást megelőző képesség fejlesztése

A legjobb kibertámadás a sikertelen kibertámadás. Ennek előfeltétele a célpont által kiépített koherens kibervédelmi rendszer és annak keretei között végzett komplex és folyamatos kibervédelmi tevékenység.

³⁶ Óbudai Egyetem: Információbiztonsági szakmérnök/szakember képzés tartalma, <http://www.bgk.uni-obuda.hu/hu/kepzesek/tovabbkepzesek/informaciobiztonsagi-szakmernokszakember>.

³⁷ Gábor Dénes Főiskola: Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés tartalma, <http://gdf.hu/szakiranyu-tovabbkepzesek/adatvedelmi-es-informaciobiztonsagi-menedzser/>.

³⁸ KII: kritikus információs infrastruktúra



Az 5.2. pont szerinti stratégiai pillérek közül a kiberbiztonsági kutatás-fejlesztés (5.2.1. pont), valamint oktatás, képzés (5.2.2. pont) a támadás megakadályozásának szükséges, de nem elégséges feltételei. Egy kibertámadás megelőzése ezeken túlmenő komplex és permanens intézkedések rendszerét teszi szükségessé.

Stratégiai cél a naprakész és hatékony kiberbiztonsági tevékenységek és technológiák rendszerének kiépítése, működtetése és folyamatos fejlesztése. Ennek keretében folyamatosan visszacsatolni és elemezni kell az észlelés és a reagálás során képződő információkat, majd szükség szerinti kutatás-fejlesztés, vagy más alkalmas módszer (pl. beszerzés) révén gondoskodni kell a megelőző képesség aktuális fenyegetéseknek megfelelő, azokat kezelni képes folyamatos fejlesztéséről.

A megelőzés a lehető legtágabb körben értelmezendő. Kulcsmozzanata az emberi oldal folyamatos fejlesztése, azon belül az érzékenyítés, a biztonságtudatosság valamennyi stakeholdert érintő erősítése. Célul kell kitűzni azon mindinkább tarthatatlan nézet megváltoztatását, hogy a kiberbiztonság csak egy kiberbiztonsági specialistákból álló szűk szakértői kör feladata. Egy esetlegesen sikeres kibertámadás lehetséges roppant anyagi – de főleg reputációs – kárával a megelőzési szakaszban valamennyi érintettnek (stakeholdernek) szembesülnie kell és a hatás-, illetve feladatkörébe tartozó intézkedések megtételével kell reagálnia azokra. Pl.:

- az állami szervek illetékeseinek a mindenkori aktuális kihívásokhoz rugalmasan alkalmazkodó és megfelelő szabályozási környezet biztosításával,
- a társasági felsővezetőknek a gazdasági mellett a biztonsági szemlélet meghonosításával és fejlesztésével, az ehhez szükséges képzési rendszer működtetésével, a kibervédelmi rendszer működtetéséhez szükséges források biztosításával, a rendszeres, célzottan kiberbiztonsági ellenőrzésekkel, a vészhelyzeti tervek elkészítésével, az abban foglalt rendszeres gyakoroltatásával, a válságkommunikációs tervek előkészítésével stb.

További stratégiai léptékű teendő az ICS/SCADA-k kiberbiztonságát érintő eltérő IT és OT oldali nézetek, gyakorlatok és szakemberek mielőbbi közelítése. Téves az az IT megközelítés, hogy az ICS/SCADA maga is csak egyfajta IT, azaz kiberbiztonsági vonatkozásai sem specifikusak. Az IT-ben megszokott bizonyos eljárások OT környezetben vagy nem kivitelezhetők (pl. pentest működő technológiai rendszeren), vagy aránytalan mértékű következményekkel járnak (pl. testbed aránytalan költsége). Ugyanakkor téves az az OT megközelítés is, amely szerint az IT kiberbiztonsági megoldásainak jelentős hányada ne lenne alkalmazható, avagy adaptálható ICS/SCADA környezetbe. Incidensekkel bizonyítottan tarthatatlan az a korábbi OT álláspont, hogy speciális kialakításuk, protokolljuk stb. önmagában is megvédi az OT rendszereket.



Az eddigi „IT vs. OT” megközelítés helyébe a két terület szakemberei közötti olyan együttműködésnek kell lépnie, amelyben egyfelől az IT-oldali jó gyakorlatok, másfelől a konkrét technológiára vonatkozó specifikus mérnöki ismeretek együttes bázisán közösen hoznak létre az adott technológiai környezetben megvalósítható, fenntartható és hatékony védelmi stratégiát.³⁹ [5] A SeConSys együttműködés egyik missziója az eltérő IT és OT megközelítések közötti híd kiépítése.

Külön kiemelendő a megelőző képesség fejlesztésének forrásigénye. Indokolt a stakeholderek szembesítése megtörtént kibertámadások akár közvetlen, akár közvetett (pl. reputációs) kárértékeivel.⁴⁰ Az elvégzendő kockázatértékelés egyik elemeként ezek tükrében is értékelhető a megelőzési tevékenységre fordítandó források biztosításának indokoltsága.

A villamosenergetikai ICS/SCADA rendszerek sajátosságait, valamint a megtörtént kibertámadásokat a SeConSys keretei között elemezve ugyancsak stratégiai jelentőségű annak felismerése, hogy a villamosenergetikai és a kiberbiztonsági oldal szakértőinek már a megelőzés szakaszában is szorosan együtt kell működniük. Csak komplex szakmai megközelítés ad esélyt arra, hogy pl. már az ICS-komponensek tervezési szakaszában is beépüljenek azokba olyan kapacitástartalékok, amelyek az alapfunkcióik mellett a kibervédelmi funkciók implementálását is lehetővé teszik úgy, hogy ezek ne okozzanak performancia csökkenést az alapfunkcióik tekintetében.

5.2.4. Kibertámadást észlelő képesség fejlesztése

A támadás-védekezés logikájából adódóan a támadó többnyire lépéselőnyben van. Ebből következően adódhat olyan helyzet, amikor a legmagasabb szintű megelőző intézkedések ellenére is a támadás kisebb-nagyobb eredménnyel járhat.

Stratégiai cél a megelőzést szolgáló komplex intézkedések ellenére bekövetkező kibertámadások – avagy azok előkészítésével kapcsolatos támadói tevékenységek – lehető legkorábbi szakaszban való észlelése és azonosítása, az ellenlépések megalapozása.

A minél előbbi felismeréshez az szükséges, hogy az üzemeltető személyzet mindig pontosan tisztában legyen a rendszer állapotával, ugyanis operatív és effektív intézkedéseket csak ezek birtokában lehet hozni.

Az észlelt támadásokból leszűrhető információk folyamatosan hasznosítandók mind a képzésben (pl. az aktuális támadási technikákhoz illeszkedő humán kompetenciák létrehozásában, fejlesztésében), mind a kutatás-fejlesztésben (pl. az új támadási

³⁹ J. Slowik. „The False Choice of IT Vs. OT.” Dragos. <https://www.dragos.com/blog/industry-news/the-false-choice-of-it-vs-ot/> (Letöltve: 2020. augusztus 26.)

⁴⁰ PI. ICS/OT snapshot 2019 (Black Cell Magyarország Kft.)



technológiáknak megfelelő támadási mintázatok felismerését támogató megoldások kidolgozásában), de főleg a megelőző képesség fejlesztésében.

A kritikus infrastruktúrákat – így különösen a villamosenergia-rendszert – érintő incidensek kezelésében, a (köz)szolgáltatások zavarának minimalizálásában különös jelentősége van felkészült és gyakorlott, 365x24 rendszerben rendelkezésre álló szakszemélyzetű eseménykezelő szolgálati hely(ek) (SOC⁴¹) működtetésének. A saját körben vagy másokkal összevont SOC működtetése komplex elemzésen nyugvó döntési kérdés. Előbbi mellett szól a fókuszáltság és kisebb leterheltség (ezáltal incidens esetén hatékonyabb működés), míg utóbbi esetben a SOC gazdaságosabb fenntartása mellett a nagyobb rendszeráttekintés több információt és ezáltal megalapozottabb döntési, intézkedési lehetőséget biztosít.

5.2.5. Kibertámadásra való reagáló képesség fejlesztése

Stratégiai cél a gondos megelőző előkészületek ellenére bekövetkező kibertámadás előkészített, rendszeresen aktualizált és gyakorlattal tesztelt vészhelyzet-kezelési és helyreállítási tervek alapján történő hatékony kezelése, az incidens történéseinek átfogó – az eredményes elemzést, majd javító tevékenységeket megalapozó – dokumentálása.

Mivel a villamosenergia-rendszert érintően már megtörtént támadások elemzése tükrében a támadóknak egyre inkább a technológiai berendezést érintő károkozás is célja, így a reagálásban – pl. az incidensek kivizsgálásában – is különös jelentősége van a villamosenergetikai és a kiberbiztonsági oldal szakértői szoros együttműködésének. Ezzel összhangban a forensics⁴² tevékenységben mindkét szakterület szakértőinek részt kell venniük.

Az incidensek kivizsgálásának tanulságait vissza kell csatolni és be kell építeni a képzésbe, a kutatás-fejlesztésbe, a megelőzésbe és az észlelésbe. A minőségirányítási rendszerekhez hasonlóan a kiberbiztonsági rendszer működtetésében is érvényesítendő a PDCA-ciklus⁴³ [6] szerinti folyamatos fejlesztés. Jelentős, minőségileg új elemet hozó incidens nyomán a kutatás-fejlesztést – szükség esetén a képzést is – magában foglaló bővebb PDCA ciklus indítandó, míg egyéb esetekben elégséges lehet a megelőzést, az észlelést és a reagálást magában foglaló szűkebb PDCA ciklus.

Kiemelt fontosságú az incidensek vizsgálati eredményeinek intézményes keretek közötti, a szükséges bizalmasság megtartása melletti, kölcsönösségi alapon álló megosztása mind hazai, mint nemzetközi keretek között.

⁴¹ SOC: Security Operations Center

⁴² forensics: informatikai eszközön vagy rendszerben bekövetkezett események hiteles rekonstruálása

⁴³ Turcsányi K., Minőségelmélet és -módszertan. Budapest: Nemzeti Közszolgálati Egyetem, 2014. 234. oldal



A komplex szakmai megközelítés jegyében az információmegosztás köre is bővítendő, azaz a szorosan vett kiberbiztonsági vonatkozások mellett a (villamos) technológiaiak is megosztandók.

5.3. Jogsabályi háttér

5.3.1. A létfontosságú rendszerek (kritikus infrastruktúrák) védelmével kapcsolatos törekvések időrendi áttekintése

- Legfőbb kiváltó okok:
 - 2001. szeptember 11.: terrortámadás az USA-ban;
 - 2004. március: terrortámadás Madridban a közlekedési infrastruktúra ellen;
 - 2005. július: terrortámadás Londonban a metró ellen.
- EU szintű intézkedések:
 - átfogó program azon létesítmények és rendszerek védelme érdekében, amelyek a gördülékeny életvitelt garantálják;
 - 2004. European Programme for Critical Infrastructure Protection⁴⁴;
 - 2005. Zöld könyv ennek végrehajtásáról, lehetőségeiről, tagállamok véleményének kikérése érdekében⁴⁵;
 - 2008. CIP irányelv (114/2008/EK irányelv)⁴⁶.
- CIP irányelv implementációja tagállami szinten (kötelező elemek):
 - energia és közlekedés ágazatok prioritásként történő kezelése;
 - sebezhetőségi pontok meghatározásának kötelezettsége;
 - azonosítás és kijelölés folyamatának meghatározása;
 - horizontális kritériumok tagállami átvétele és értelmezése;
 - ágazati kritériumok tagállami szintű megfogalmazása;
 - üzemeltetői biztonsági terv készítési kötelezettség meghatározása;
 - biztonsági összekötő személy alkalmazásának kötelezettsége;
 - felülvizsgálat, rugalmasság, kiegészítő jelleg (meglévő szabályozásokat nem kell felülrírni, hanem harmonizálni szükséges azokkal).

⁴⁴ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF>

⁴⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=en>

⁴⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>



5.3.2. *Magyarországi általános szabályozás*

Mindezek végrehajtása keretében lépett hatályba 2013 márciusában a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.) és annak végrehajtási rendelete (65/2013. (III. 8.) kormányrendelet, a továbbiakban: Lrtv. vhr.). A törvény melléklete sorolja fel azokat az érintett ágazatokat, amelyekben hatósági eljárás keretében azonosítani és kijelölni szükséges a – hazánkban vagy az európai uniós értelmezésben – létfontosságúnak minősülő rendszereket/rendszerelemeket/létesítményeket. Jelen hatály⁴⁷ szerint 10 ágazat van: energia, közlekedés, agrárgazdaság, egészségügy, társadalombiztosítás, pénzügy, víz, infokommunikációs technológiák, honvédelem, közbiztonság-védelem.

A definíciók háttér tekintetében a következő fogalmak irányadóak:

- *létfontosságú rendszerelem:* az Lrtv. 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 egészségüghöz, 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,
- *európai létfontosságú rendszerelem:* a törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra.

A potenciális nemzeti létfontosságú infrastruktúrák azonosítása keretében történik az infrastruktúrák kockázatbecslés alapú vizsgálata, amelynek elsődleges célja, hogy az egyes ágazatokra – ágazati kormányrendeletekben – meghatározott kritériumok alapján, az üzemeltetők által működtetett infrastruktúrák értékelésre és rangsorolásra kerüljenek és megállapítást nyerjen, hogy működésük tekintetében teljesül-e valamely ágazati kritérium. Összességében tehát az ágazati kormányrendeletek határozzák meg, hogy melyik üzemeltetők kötelezettek azonosítás lefolytatására, annak keretében azonosítási jelentés készítésére, amely:

- a vizsgált rendszerelemre vonatkozó kockázatelemzést és annak eredményét,
- a kijelölésre irányuló javaslatot (vagy a kijelölés indokolatlanságát),
- a teljességére vonatkozó üzemeltetői nyilatkozatot, valamint
- az azonosítási vizsgálat kezdő- és zárónapját tartalmazza.

⁴⁷ 2020. július 1.



A benyújtás az ágazati kijelölő hatóság (szintén ágazati kormányrendeletben rögzítve) részére történik. A benyújtást követően az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (Ákr.) szerinti közigazgatási hatósági eljárás indul az adott infrastruktúra nemzeti kritikus infrastruktúrává történő kijelölésének megállapítására, amelyben a felelős hatóságok az adott rendszerelem tekintetében azt vizsgálják, hogy teljesülnek-e az ágazati és horizontális kritériumok. A 60 napos kijelölési eljárásban az ágazati kijelölő hatóság és (ha van) az ágazati javaslattevő hatóság felelőssége, hogy megállapítsa az ágazati kritériumok teljesülésének tényét. Emellett fontos részcsелеkmény a horizontális kritériumok⁴⁸ teljesülésének vizsgálata. Ennek érdekében az ágazati kijelölő hatóság szakhatósággént bevonja a hivatásos katasztrófavédelmi szerv központi szervét, a BM Országos Katasztrófavédelmi Főigazgatóságot (a továbbiakban: BM OKF).

A fentiek szerint lefolytatott eljárás határozathozatallal zárul, amelyben az ágazati kijelölő hatóság egy ágazati és egy horizontális kritérium teljesülése esetén kijelöli létfontosságú rendszerelemmé a vizsgált infrastruktúrát. A jogszabályi háttér bővebben a 8. mellékletben kerül kifejtésre.

5.3.3. Energia ágazati szabályozás

Az Lrtv. vhr. rendelkezéseit az energetikai létesítmények tekintetében (az energetikai létesítmény elemének kell tekinteni a technológiai hírközlési és informatikai rendszert is) az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 374/2020. (VII. 30.) Korm. rendeletben (a továbbiakban: energetikai Korm. rend.) foglalt eltérésekkel kell alkalmazni.

Ide tartoznak:

- a villamosenergia-rendszer létesítményei⁴⁹;
- a kőolaj és cseppfolyós szénhidrogén termék szállítóvezetékek és tárolók, a kőolajtermelés és -feldolgozás létesítményei;
- a földgázellátásról szóló törvény szerinti rendszerüzemeltetők, a célvezeték, valamint a normál légköri nyomáson és szobahőmérsékleten gáz halmazállapotú szénhidrogén bányászatához szükséges létesítmények;
- a távhőrendszer létesítményeire a távhőszolgáltatásról szóló törvény szerinti engedélyese.

⁴⁸ 65/2013. (III. 8.) kormányrendelet 1. sz. mellékletében felsorolt kritériumok.

⁴⁹ Kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek.



Az energia ágazatban nevesített ágazati kijelölő hatóságok:

- *villamosenergia-rendszer, valamint az együttműködő földgázrendszer:* Magyar Energetikai és Közmű-szabályozási Hivatal;
- *kőolaj-, földgáztermelés:* bányafelügyelet (kormányhivatal illetékes főosztályaként);
- *kőolajfeldolgozás és -tárolás:* mérésügyi és műszaki biztonsági feladatkörében eljáró fővárosi és megyei kormányhivatal;
- *távhő:* Magyar Energetikai és Közmű-szabályozási Hivatal.

Az energia ágazatban, a villamosenergia-rendszer létesítményei alágazatban kijelölhető *nemzeti* létfontosságú rendszerelemek ágazati kritériumai:

- *villamosenergia-rendszerirányítás tekintetében:* olyan elem, amelynek kiesése esetén az ellátásbiztonság nem tartható fenn, és amely 30 percen belül nem helyettesíthető;
- *villamosenergia-termelés tekintetében:* amely 200 MW és ezt meghaladó névleges teljesítőképességű, illetve a termelő a vizsgálatot megelőző három év villamosenergia-termelése átlagban elérte az 1 TWh-t;
- *átviteli hálózat tekintetében:* amelynek kiesése hatására bármely további elemnek az energetikai Korm. rend. 2. mellékletben meghatározott feszültségszinttől való eltérése a 24 órát meghaladja, és az az adott tevékenység ellátása szempontjából más módon nem pótolható;
- *elosztó hálózat tekintetében:* olyan 1 kV-osnál nagyobb, de legfeljebb 132 kV-os elem, amely kiesésének időtartama (x)
 - a) $24 < x < 48$ óra, és legalább 10 000 felhasználót érint;
 - b) $48 < x < 72$ óra, és legalább 5 000 felhasználót érint;
 - c) $x > 72$ óra, és legalább 2 000 felhasználót zár ki az ellátásból.

5.3.4. Információbiztonsági kötelezettségek

A kijelölt létfontosságú rendszerelemek – így az energia ágazat kijelölt kritikus infrastruktúrái – az Ibtv. hatálya alá tartoznak, így vonatkozik rájuk valamennyi, az információbiztonság növelése érdekében meghatározott kötelezettség.

Ennek megfelelően a kijelölt kritikus infrastruktúrák:

- elektronikus információs rendszereit biztonsági osztályba;
- a szervezetet biztonsági szintbe kell sorolni;
- az elektronikus információs rendszer biztonságáért felelős személyt neveznek ki;
- informatikai biztonsági szabályzatot készítenek.



A jogszabályi követelményeknek történő megfeleléssel kapcsolatosan a 9. melléklet szerinti útmutató nyújthat segítséget.

5.4. Nemzetközi gyakorlat

Az Európai Unió villamosenergia-rendszerekre vonatkozó kibervédelmi szabályozási keretét három jogi aktus adja:

- a CIP irányelv⁵⁰,
- az Európai Unió Kiberbiztonsági Ügynökségről (ENISA) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelet⁵¹, valamint
- a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv⁵² (a továbbiakban: NIS irányelv).

Mindezek keretrendszerként biztosítanak a kritikus infrastruktúrák kiberbiztonságának megteremtéséhez, beleértve a villamosenergia alágazatot is. A nemzetközi tapasztalatok megismeréséhez mintavételelesen négy külföldi modell feldolgozását látta indokoltnak a SeConSys szakmai közössége:

- A *svájci modell* jó gyakorlata, hogy 2050-ig szóló energia stratégia szerint a 2010-es évek közepén kialakításra kerültek az intelligens hálózatok (intelligens mérő rendszerek alkalmazásával), amelyekre alkalmazni szükséges a Szövetségi Energia Hivatal által definiált információbiztonsági követelményrendszert és értékelési módszertant. A svájci Smart Grid Iparági Szövetség vezetésével, az intelligens mérőrendszerek működtetésére és információbiztonsági tanúsítására vonatkozó iránymutatások kerültek létrehozásra. Az okosmérők tanúsítása 2020-tól kötelező, amely ISO/IEC szabvány alapú, és az EU kiberbiztonsági szabályozásával összhangban van. Lásd bővebben a 10. mellékletben.
- Az *észak-amerikai modell* az Amerikai Nemzeti Szabványügyi és Technológiai Hivatal kritikus infrastruktúra biztonsági keretrendszerén belül valósította meg a villamosenergia-rendszer kiberbiztonságát, amely a fizikai biztonságot is magában foglalja.

⁵⁰ A Tanács 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

⁵¹ Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályaon kívül helyezéséről (kiberbiztonsági jogszabály)

⁵² Az Európai Parlament és a Tanács (EU) 2016/1148 IRÁNYELVE a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről



A rendszer és működési folyamatszabványok nem terméket tanúsítanak, hanem piac- és gyártósemleges követelményeket határoznak meg. A rendszerek minősítése az előírás, nem pedig az egyes komponenseké. Az USA Szenátusa elfogadott egy törvényjavaslatot, amely a kiberbiztonsági veszélyek miatt a jelenlegi automatizált digitális rendszerek alternatíváit (elszigetelt rendszerek, kézi tartalék működtetés, analóg rendszerek) kívánja megvizsgálni. Jó gyakorlat, hogy a kiberbiztonságért felelős szervezet számos ingyenes, és nyilvánosan elérhető ajánlást tesz közzé. Lásd bővebben a 11. mellékletben.

- Az *osztrák modellben* a villamosenergia-ipar kiberbiztonságának biztosítása a NIS irányelv implementációjának része. Az osztrák kiberbiztonsági stratégia nagy hangsúlyt fektet az információs és kommunikációs technológiák biztonságára, és a fenyegetésekkel szembeni ellenállóképességük növelésére, amely tevékenységek PPP keretében valósulnak meg. A nemzeti kiberbiztonsági stratégiában meghatározottak ellenőrzésére supervisor team jött létre, amelyben az üzemeltetők és a szabályozó szervezetek is jelen vannak. Tanúsítást a privát szféra szereplői végeznek, és a kormányzati szereplők auditálják. Külön CERT (eseménykezelő központ) működik az energia ágazati szereplők számára. Jó gyakorlat, hogy az osztrák sajátosságok figyelembevétele mellett fenyegetettségi térkép került összeállításra, amely segít a preventív intézkedések végrehajtásában. Lásd bővebben a 12. mellékletben.
- A *német modell* világosan meghatározott, kockázatokkal arányosan kialakított villamosenergia-ipari kritikus infrastruktúra védelmi rendszere egzakt követelményrendszer alapján jelöli ki a kritikus infrastruktúra elemeket. Jó gyakorlat, hogy a túlszabályozottságot kerüli a kialakított rendszer, viszont világos elvárásrendszer van az alapvető kiberbiztonsági jogszabályok által. Az ágazati jogszabályok megfelelően implementálták a nemzetközi szabványok és ajánlások jó gyakorlatait, és a szabályozottság megteremtése érdekében kötelezővé tette azok alkalmazását. A felügyeleti szervek struktúrája és az incidens bejelentés rendszere jól kialakított, ahogy a PPP keretében megvalósuló UP KRITIS⁵³ szakterületi érintettek munkacsoportja és annak működése is. Lásd bővebben a 13. mellékletben.

⁵³ UP KRITIS: Public-Private Cooperation in Critical Infrastructure Protection (köz- és magánszféra együttműködése a kritikus infrastruktúrák védelme terén)



Összességében a jó gyakorlatok bizonyos szegmensei, és a nemzeti szabályozási folyamatok egyes formáinak implementálása számos előnnyel járhat a magyar villamosenergia alágazati szereplők vonatkozásában.



Különösen figyelemreméltónak – és a hazai alkalmazhatóság szempontjából további részletesebb vizsgálatra érdemesnek – tartjuk a német modellt.



5.5. Hazai gyakorlat

Az elmúlt években hatványozottan érezhető volt az Európai Unió törekvése a kritikus infrastruktúrák kibervédelmének megteremtésére. A hazai szabályozási környezet próbálta követni a nemzetközi irányelvekben foglaltakat (CIP irányelv, NIS irányelv), azonban sokáig nem volt kijelölt létfontosságú rendszerelem a villamosenergia alágazatban. A 2019-es év változást hozott a szabályozásban és a kijelölésekben egyaránt, így számos kijelölt létfontosságú rendszerelem kezdte meg az előírt kötelezettségek teljesítését.

5.5.1. Jelenlegi helyzet

Jelenleg az 5.3. pontban összefoglalt, illetve a 8. és 9. mellékletekben meghatározott jogszabályok képezik a szabályozás alapját. Az érintett szervezetek a jogszabályi megfelelés és a hatékony kibervédelem biztosítására elkezdtek a felkészülést, amely a jogszabály által biztosított fokozatosság elvét követve, több éves tevékenység lesz az üzemeltetők részéről.

5.5.2. A szabályozásfejlesztés lehetőségei

A szabályozás fejlesztése elengedhetetlen, mivel számos – az ipari irányító rendszerek sajátosságait jelenleg nem teljeskörűen kezelő – szabályozó áll rendelkezésre. Elengedhetetlen a nemzetközi jó gyakorlatok és ajánlások figyelembevétele, továbbá az Unió szabályozás változásainak a nyomon követése.





Az ipari irányító rendszerek tanúsításának is egyre nagyobb szerepe lesz a jövőben, a beépített védelmi képességek miatt. Ennek hiánya versenyhátrányt jelent majd azon rendszerelem, komponens gyártók vonatkozásában, amelyek nélkülözik a védelmi képességek beépítését az ipari rendszerek moduljaiba, vagy egészébe.



A szabályozásfejlesztés kiinduló helyzetét, a téma szempontjából releváns külföldi és hazai alábbi szabályozások rendszerét az 5. ábra mutatja be. Az ábra szerinti szabályozásokat a kézikönyv egyéb részei ismertetik.

Az 5. ábra szerinti hivatkozások listája:

- [1] ISO/IEC 27001 Information Security Management [ISMS]
- [2] IEC 62443 Industrial Automation and Control System [IACS]
- [3] 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről
- [4] 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
- [5] Security and Privacy Controls for Federal Information Systems and Organizations [SP 800-534]
- [6] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- [7] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- [8] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról
- [9] Nemzeti Energiastratégia 2030, kitekintéssel 2040-ig. Tiszta, okos, megfizethető energia (a Kormány 2020. január 8-i ülésén elfogadott szöveg)
- [10] 2007. évi LXXXVI. törvény a villamosenergiáról
- [11] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról [Ibtv.]
- [12] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről [Lrtv.]



- [13] 1996. évi CXVI. törvény az atomenergiáról
- [14] 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
- [15] 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
- [16] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról [Lrtv. vhr.]
- [17] 374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- [18] 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről
- [19] 118/2011. (VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről
- [20] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről



	Nemzetközi	EU	Magyar
Szabvány	ISMS [1]		
	IACS Security [2]		
Irányelv		CIP irányelv [3]	
		NIS irányelv [4]	
Ajánlás	NIST ajánlás [5]		
Stratégia	Általános		Nemzeti Biztonsági Stratégia [6]
	Kiberbiztonság		Kiberbiztonsági stratégia [7] Hálózati információ biztonsági stratégia [8]
	Energetika		Energiastratégia [9]
Törvény			Villamosenergia tv. [10]
			Ibtv. [11] Lrtv. [12] Atomtörvény [13]
Rendelet	Kormány		Eseménykezelő központok feladat- és hatásköre [14] Elektronikus információs rendszerek biztonsági felügyelete [15] Lrtv. vhr. [16] Energetikai létfontosságú rendszerek [17] Atomenergia fizikai védelem és a kapcsolódó feladatok [18] Nukleáris létesítmények nukleáris biztonsági követelményei [19]
	Minisztérium		41-es BM rendelet [20]

5. ábra: A kiberbiztonsági szempontból mértékadó szabályozások rendszere



6. A villamosenergia-rendszer ICS/SCADA-i gyakorlati kibervédelme

A villamosenergetikai ICS/SCADA rendszerek kiberbiztonságát három alapvető tevékenységcsoport – a megelőzés, az észlelés és a reagálás – szempontjából vizsgáljuk. Először e tevékenységek általános érvényű szempontjait mutatjuk be.

6.1. Általános szempontok

A villamosenergia-rendszer üzemirányítása folyamatos, valós idejű folyamat. A villamosenergetika sajátossága, hogy a rendszer állapota igen gyorsan reagál a vezérlésre. A fogyasztás-termelés egyensúlyát biztosítani kell a megfelelő feszültség viszonyok és az üzleti folyamatok zavartalansága mellett; mindezt sok szereplő (országokon is átívelő) együttműködésével. Ezek megvalósíthatósága napjainkra – és a jövőben egyre nagyobb mértékben – a villamosenergia-rendszer üzemét függővé tette a ICS/SCADA komponensektől. Az ICS/SCADA-k működőképessége önmagában is függ a villamosenergia-rendszertől. Bár a jelen fejezet elsősorban az IT/ICT szektor oldaláról fogalmaz meg ajánlásokat, a SeConSys megközelítésével összhangban minden esetben az OT sajátosságok megfelelő ismerete és figyelembevétele is megjelenik. Az IT/ICT és OT biztonság együtt érvényes, együtt kell kezelni a két területet. Bizonyos esetekben egy OT folyamat módosítása kevésbé támadhatóvá teszi ICT oldalról is a rendszer egészét, illetve a kritikus OT folyamatokhoz különös figyelmet kell szentelni az ICT biztonságára. Ezen felül a sokszereplős és földrajzilag is kiterjedt kapcsolódások miatt a rendszer elosztottnak tekinthető és nincs teljes kontrol felette egyik szereplő részéről sem.

Ahogy a kézikönyv több fejezetében már hangsúlyt kapott, kiemelten fontos az IT és OT szakemberek közötti szoros együttműködés.



A jelen fejezetben tárgyalt technológiai és módszertani javaslatok csak és kizárólag abban az esetben tudnak hatékonyan működni, ha ez az együttműködés az érintett szervezetekben kölcsönösen elfogadott érdekek mentén jön létre és érdemben működik.



6.1.1. Fenyegetés felderítés

A kibertér felől érkező fenyegetések felderítésének (cyber threat intelligence) célja, hogy háttérinformációt nyújtson a kezelőszemélyzetnek megalapozott döntések meghozatalához. Ezáltal a kiberbiztonsági incidenseket megfelelő szakmai kontextusba helyezi, illetve forrásként támogatja a hipotézis generálást az eseménykezelés elején. Ezen kívül lehetőséget biztosít megfelelő reaktív védekező képességek kialakítására egy adott esemény/eseményisor kapcsán.

Mind a *stratégiai* (biztonsági vezetés, szervezeti vezetés), mind a *taktikai* (biztonsági csoportok, hálózati csoportok, esemény kezelő csoportok), mind a *műveleti* (veszélyvadászok, esemény kezelő csoportok, biztonsági vezetés) szervezetek számára elengedhetetlen fontosságú az iparág-specifikus jelentések elkészítése.

Technikai és technológiai ajánlások:

- A megismert fenyegetettség kategóriákba sorolása az alábbi szempontok (és megtörtént esetek) szerint:
 - Érdekelte ellenfelek (pl. Dragonfly⁵⁴)
 - Közvetlen ICS hatás (pl. MiniDuke⁵⁵)
 - Közvetett ICS-hatás (pl. Wannacry⁵⁶)
- A globális fenyegetés felderítési szcénában általánosan elfogadott különböző listák és szabályok használata, amelyek elősegítik a fenyegetettség felismerését. Ilyen források többek között az IoC⁵⁷, Yara⁵⁸, Hash⁵⁹, Url, IP, DNS listák és szabálycsomagok. Ezek használata mind visszatekintő, mind előreutató jelleggel határozottan javasolt. A fenti felsoroláson kívül vannak publikusan nem elérhető iparág specifikus listák is, amelyek használata ugyancsak ajánlott.
- A megfelelő pontosság szempontjából fontos, hogy az összesítés, szűrés szűrése és a meglévő kiberfenyegetés felderítés (CTI⁶⁰) prioritása megvalósuljon a teljesség, a pontosság, a relevancia és az időszűrés szempontjából. Ennek során javasolt, hogy mind az emberileg olvasható (human readable), mind a gépek számára olvasható

⁵⁴ Dragonfly: villamosenergia-rendszer ellen támadást intéző rosszindulatú program

⁵⁵ MiniDuke: A Budapesti Műszaki Egyetemen működő CrySyS káros szoftver elemző labor munkatársainak és az orosz Kaspersky Lab kutatóinak együttes erőfeszítésének köszönhetően 2014-ben felfedezett új és rendkívül veszélyes kémiszoftver.

⁵⁶ Wannacry: 2017-ben elterjedt zsarolóvírus, melyet Észak-Koreának tulajdonítanak.

⁵⁷ IoC: Indicator of Compromise (kompromittálódásra utaló jel)

⁵⁸ Yara: rosszindulatú programok kutatásában és felismerésében használt eszköz

⁵⁹ Hash: lenyomat (előírás szerint képzett bitsorozat)

⁶⁰ CTI: Cyber Threat Intelligence (kiberfenyegetés felderítés)



(repository based) adatok rendelkezésre álljanak, az ehhez szükséges informatikai, feldolgozó és megjelenítő képességekkel együtt.

- Javasolt dedikált ICS „honeypot farm”⁶¹-ok létrehozása, amelyek az ICS-specifikus protokollokat emulálják. Az emulálás során a szektorra jellemző protokollok (Modbus⁶²; DNP3⁶³, OPC⁶⁴, IEC 104⁶⁵, IEC 61850⁶⁶, IEC 60870-5⁶⁷) emulálása is kiemelten javasolt a generikus IP protokollok (HTTP, FTP, távoli elérések, Telnet stb.) mellett.
- A hatékony fenyegetés felderítés (TI⁶⁸) megvalósításának elengedhetetlen részét képezi a képzés. Ennek ajánlott témái pl. a CTI használata a fenyegetés „vadászatban” (mind az automatikus észlelés és megelőzés, mind a kézi használat), az ICS ATT&CK⁶⁹ feltérképezése és historikus elemzése stb.
- Végül kiemelendő a passzív sebezhetőségi hírszerzés fontossága. Javasolt központi adattár építése, ahol a „site-ok” (a feltárt sebezhetőségeket az egymással megosztó szereplők) azokat automatikusan és ütemezett módon, valamint biztonságosan összehasonlíthatják. Figyelmeztetéseket állíthatnak be az eszközeikkel kapcsolatban felmerülő fenyegetésekre vagy CVE⁷⁰-kre.

6.1.2. Kockázateértékelés

Ajánlott a kockázatelemzések és -értékelések belső szabályozásban foglalt kötelezővé tétele, összhangban a jogszabályi követelményekkel.

Az esetek többségében a villamosenergia-ipari vállalatok rendelkeznek kockázatelemzésekkel és -értékelésekkel, viszont ezek ritkán tartalmazzak kiberbiztonsági szempontokat. Fontos, hogy a jövőben az eddigi elemek mellett a kiberbiztonsági kockázatelemzés is a folyamat szerves részét képezze.

Technikai szempontból javasolt a szabványokban leírt, jól bevált módszerek használata. Az elemzések során a védelmi és biztonsági szakértőknek együtt kell elvégezniük a biztonsági kockázateértékelést, figyelembe véve a védelmi biztonsági kockázateértékelési eredményeket

⁶¹ honeypot farm: rosszindulatú kódok algoritmusok elfogására szolgáló csali számítógép „farm”

⁶² Modbus: ipari környezetben alkalmazott adatkommunikációs protokoll

⁶³ DNP3: Distributed Network Protocol 3 (elosztott hálózati protokoll)

⁶⁴ OPC: Open Platform Communication, OLE for Process Control (Platformfüggetlen kommunikáció/Nyílt platformú kommunikáció. Az OLE ipari automatizálásra specializált alkalmazási rendszere.)

⁶⁵ IEC 104: Soros protokoll (RS232) TCP/IP implementációja

⁶⁶ IEC 61850: gyártófüggetlen energetikai adatkommunikációs szabvány

⁶⁷ IEC 60870-5: gyártófüggetlen energetikai adatkommunikációs szabvány

⁶⁸ TI: Threat Intelligence (fenyegetés felderítés)

⁶⁹ ICS ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge (támadói taktikák, technikák és közös tudásbázis)

⁷⁰ CVE: Common Vulnerabilities and Exposures (ismert sérülékenységek és kitettségek)



(amelyek általában rendelkezésre állnak). Az elemzések során kulcsfontosságú mind az IT, mind az OT szempontok együttes és maximális figyelembevétele.

6.1.3. Kiindulópontok, alapesetek felállítása

A biztonsági kiindulási irányelvek képezik a kiberbiztonsági kockázat kezelésének elősegítésére szolgáló politikák, eredmények, tevékenységek, gyakorlatok és ellenőrzések kiindulópontjait, alapeseteit (a baseline⁷¹-okat). Általában széles körű kockázatkezelési politikai célokat fednek le (pl. védelmet nyújtanak a számítógépes fenyegetésekkel szemben, elősegítik a rendellenességek, vagy események észlelését és azokra való reagálást).

Ezen alapelvek alapvetően két csoportba sorolhatók: technikai és nem technikai jellegűekbe.

Mind a technikai, mind a nem technikai baseline-ok kapcsán kulcsfontosságú a folyamatok megléte. Ezek hiánya nagyban megnehezíti a későbbi munkát. Javasolt, hogy ha konkrét szabályozás nem is írja elő, a cégek alkossanak belső szabályokat a baseline-ok kialakítására.

6.1.4. Képzés és tudatosság növelés

Az ICS/SCADA rendszerek kiberbiztonsága kapcsán nem lehet elégszer hangsúlyozni a „humán faktor” kapcsán értelmezhető biztonságtudatosság növelésének és az ehhez szükséges képzéseknek fontosságát. E képzéseket ajánlott összefüggéseiben kezelni. A 6. ábra ajánlás a szakterületi képzések lehetséges rendszerére.

	Biztonságtechnika	Biztonsági események	Biztonságtudatosság az ICS/SCADA-ban	Biztonsági eseményekre adott válasz ICS/SCADA-ban	Általános biztonságtudatosság	Biztonsági eseményekre való reagálás az általános IT-ben
Tervezők és fejlesztők						
Operátorok és karbantartók						
Irodai dolgozók						

6. ábra: A kiberbiztonsági szakterületi képzések ajánlott rendszere

⁷¹ Baseline: kiindulópont, alapeset



6.2. Ajánlások: Megelőzés

A kiberbiztonsági incidensek megelőzését célzó ajánlásokat a következő pontokban foglaljuk össze.

6.2.1. Sebezhetőség vizsgálat

A sebezhetőség vizsgálat célja a gyenge pontok megtalálása a szervezet biztonsági rendszerében. A teljes és megalapozott kép alkotásához ajánlott sebezhetőségi vizsgálat végzése, illetve végeztetése.

Technológiai ajánlások:

- A CVE adatbázis folyamatos nyomon követése. Így még „időben” lehet értesülni az üzemeltetett eszközöket/rendszereket érintő – már felfedezett – sebezhetőségekről.
- Amennyiben az éles rendszerek vizsgálatára nincs lehetőség, úgy ajánlott replika rendszer – vagy legalább néhány meghatározó rendszerelem – megléte penetrációs tesztelési célokra. Javasolt, hogy már a tervezési fázisban tudatosan legyenek megfogalmazva a tesztelésre kialakított rendszerek iránti igények.
- A tesztelés hatókörét a kockázatértékelési eredmények alapján javasolt meghatározni. Az elemzés eredményét ajánlott beépíteni a kockázatkezelési stratégiába.

Szabályozási ajánlások:

- Legyen egységes szabályozási norma a sebezhetőségek értékelésére.
- Az ICS/SCADA komponensek műszaki penetrációs tesztjeit rendszeresen, a jelentős frissítéseket követően pedig minden esetben ajánlott elvégezni.
- Ajánlott a penetrációs tesztet végző csapat (legyen az külső vagy belső) kompetenciájának előzetes ellenőrzése (pl. követelmény a bizonyítvánnyal rendelkező személyzet és a villamosenergetikai ICS/SCADA tapasztalat).
- Ajánlott megkövetelni a beszállítók sebezhetőségének értékelését is.

6.2.2. Konfiguráció- és javításkezelés

A konfiguráció- és javításkezelés a rendszermenedzselés azon területe, amely magában foglalja a többszörös javítás (kódváltoztatás) beszerzését, tesztelését és telepítését egy adminisztrált számítógépes rendszerben. A javításkezelési feladatok magukban foglalják

- a) az aktuálisan rendelkezésre álló javítások listáját,



- b) annak ismeretét, hogy az adott javítás a rendszer mely részeinek megfelelő,
- c) a javítások megfelelő telepítésének biztosítását,
- d) a rendszerek telepítés utáni tesztelését, valamint
- e) az összes kapcsolódó eljárás (pl. például a szükséges konfigurációk) dokumentálását.

Technológiai ajánlások:

- Minden szervezet keresse meg – szükség esetén ehhez tanácsadói támogatást igénybe véve – a számára megfelelő eszközöket a javítás és a konfiguráció kezeléséhez.
- Ajánlott már a rendszerek tervezése, beszerzése során olyan gyártókat választani, amelyek rendszereiket folyamatosan karbantartják és javításokat adnak ki. Ezen javításokat követelje meg a szervezet.
- Ajánlott hangsúllyal figyelembe venni a nem javított – esetenként nem is javítható – ICS/SCADA sebezhetőségeket.

Szabályozási ajánlások:

- Jelenleg még gyakori nézet, hogy „képtelenség a szabályozásokkal követni a technológiát”. E nézet nem tartható tekintve, hogy a (kiber)biztonsági alapelvek jól körül határolhatók, azaz kizárólag a konkrét technikai megvalósítás mikéntje az egyedüli, amit valóban nehéz lenne – és nem is feltétlenül indokolt – törvényi vagy rendeleti szinten követni.
- Ajánlott, hogy a konfiguráció- és javításkezelés témakörben a szabályozó megkülönböztesse az örökölt és az új rendszereket.
- Az örökölt, régebbi (legacy) rendszerek kapcsán ajánlott egyrészt az EoL⁷² szoftver/hardver nyitott internetnek való kitettségéről szóló rendelet megalkotását, másrészt a kötelező készleteltár (és karbantartás) megkövetelését rendeleti szinten.
- Új rendszerek kapcsán ajánlott a beszerzések olyan szabályozása, hogy csak olyan ICS/SCADA eszközöket és rendszereket legyen lehetőség beszerezni, amelyek rendelkeznek megfelelő javításkezelés biztosítására alkalmas megoldásokkal és a gyártó garantálja is ezek támogatását.

⁷² EoL: End of Life (kifutó, üzemideje végén járó hardver/szoftver)



6.2.3. Azonosítás és hozzáférés kezelés, ellenőrzés

Definíció szerint az azonosítás- és hozzáférés kezelés (IAM⁷³) az „üzleti folyamatok, információ és technológia halmaza a digitális identitások kezelésére és használatára”. Ez tehát mindent magában foglal, a jelszókezeléstől az egyszeri bejelentkezésig.

Megtörtént kibertámadások tükrében is kulcsfontosságú az azonosítás- és hozzáférés kezelési rendszer kialakítása. Ajánlott a teljes hozzáférés-kezelési rendszer megvalósítás lehetőségének vizsgálata, majd implementációja.

6.2.4. Határvédelem

A határvédelem célja egy terület (zóna) biztonságosan tartása. Egy biztonsági zóna a szabályok, eljárások, technikai eszközök és technikák összessége, ami lehetővé teszi egy cég adatainak megvédését. A határvédelem olyan fizikai környezetet teremt a vezetés támogatásával, ahol az elektronikus eszközökhöz való hozzáférés szabályai egyértelműen le vannak fektetve és a hozzáférések megfigyeltek.

A villamosenergia-rendszer abból a szempontból speciális, hogy földrajzilag is kiterjedt, elosztott rendszer, így a határvédelmet jóval kiterjedtebben, mélyebben szükséges vizsgálni.

A határvédelem annyira alapvető eleme kell legyen az összes modern villamosenergetikai IT és OT infrastruktúrának, hogy szabályozói oldali fontosságát sem lehet eléggé hangsúlyozni.

Technikai ajánlások:

- Ellenőrizze a fizikai hozzáférést a konzol-port kábelek eltávolításával és a jelszóval védett konzolok vagy virtuális terminálhozzáférés bevezetésével, mindezt megadott időtúllépéseket és korlátozott hozzáférési házirendeket alkalmazva.
- Hozzon létre ACL⁷⁴-eket.
- Használjon VLAN-okat.
- Engedélyezze a port szintű biztonsági beállításokat (port security).
- Engedélyezze a MAC⁷⁵ cím kontrollt.
- Ne használjon "háztartási" hardvereket (lásd VPNfilter).
- Használjon adat diódákat.
- Ne kizárólag a határvédelemre támaszkodjon.

⁷³ IAM: Identity and Access Management (azonosítás- és hozzáférés kezelés)

⁷⁴ ACL: Access Control List (hozzáférési lista)

⁷⁵ MAC: Media Access Control (közeghozzáférés-vezérlés, egyedi hálózati azonosító)



- Használjon mély csomag ellenőrzést (DPI⁷⁶).
- Szűrje a malware-eket a határpontokon.

A konkrét határvédelmi megoldásokra ajánlatos olyan technológiai beszállítót választani, amely megfelelő ismeretekkel rendelkezik mind az IT, mind OT hálózatok biztonságát illetően és ezen képességét bizonyíthatóan alá is tudja támasztani. Emellett az EU törekvéseit figyelembe véve ajánlatos az EU-n belül fejlesztett technológiák alkalmazása.

Amennyiben az ICS/OT infrastruktúra „átlát” a „klasszikus irodai informatikai hálózatba”, (Historian-ERP⁷⁷), akkor oda kötelezően ajánlott a szegmentálás, azaz IT/OT tűzfal implementálása. Célszerű tesztmóddal is rendelkező megoldást alkalmazni, ami segít a forgalmi szabályok tesztelésében anélkül, hogy ez a kritikus kommunikáció véletlenszerű blokkolásával veszélyt jelentene.

A technikai paraméterek figyelembevétele mellett javasolt bevált logikai rendszerek (mint például a Purdue modell) használata.

A Purdue modell lehetővé teszi a szervezetek számára, hogy megtervezzék az adatfolyam útját úgy, hogy adatvonalakat hozzanak létre a meghatározott szinteken és azokon kívül. Ez lehetővé teszi a szervezet számára a megfelelő szabályok kidolgozását a szinteken átnyúló zónák közötti információ áramlás biztonságosabbá tétele érdekében. A biztonsági szintek meghatározásával a biztonsági politikák minden szinten érvényesíthetők a kapcsolódó területek között a kiberbiztonság fenntartása érdekében.

A tűzfal szabályokat rétegelt stratégiával kell felépíteni, a gyártó alapértelmezett szabálykészletével kezdve. A szabálykészletek testre szabása során elemezzük forgalmat, és létrehozunk a konkrét szabálykészleteket, az architektúra, a telepített technológia és a forgalmi minták függvényében. Hoszt szintű szabályokat kell alkalmazni az operációs rendszerek és alkalmazások védelme érdekében.

Részletes technikai ajánlások az OT tűzfalakra:

- Modbus tartalomellenőrzési lehetőségek:

Bármely eszköz, amely hálózati csatlakozással rendelkezik a Modbus vezérlőhöz, potenciálisan megváltoztathatja a vezérlő bármelyik I/O pontját vagy regisztrálhatja az értékeket. Ráadásul használhat olyan funkciókat, amelyeket nem akarunk, hogy használjon (pl. egyszerre több regiszter írása). A Modbus kommunikáció ellenőrzése során az OT mérnökök által meghatározott „megengedett” parancsok listája alapján minden egyes Modbus parancsot és választ ellenőrizni kell.

⁷⁶ DPI: Deep Packet Inspection (mély csomag ellenőrzés)

⁷⁷ ERP: Enterprise Resource Planning (vállalati erőforrás tervezés)



Minden olyan parancsot, amely nem szerepel az „engedélyezett” listán, minden olyan forgalmat blokkolni, naplózni és jelenteni (pl. syslog⁷⁸) kell, amely

- a) nem felel meg a Modbus szabványnak, vagy
- b) bármilyen register vagy coil⁷⁹ hozzáférést megkísérel, vagy amely
- c) kívül esik a megengedett tartományon.

A megoldásnak érdemes ellenőriznie, hogy a Modbus vezérlőparancsok csak jóváhagyott számítógépektől, azaz validált forrásokból származnak-e. A távoli programozással járó „baleseteket” megakadályozásával, a sérült üzenetek blokkolásával a vezérlőrendszer biztonságosabbá és megbízhatóbbá válik.

- DNP3 ellenőrzési lehetőségek:

Jó gyakorlat a DNP3 forgalom monitorozására a valós idejű érvényesség ellenőrzése, amely biztosítja, hogy a végértékek meghaladják a kezdő értékeket. Ha nem haladják meg, akkor a készüléknek el kell dobnia a csomagot, tekintet nélkül annak tartalmára. Így, függetlenül attól, hogy mit tesz a támadó a payload-ba⁸⁰, vagy azt, hogy hogyan próbálta obfuszkálni⁸¹ azt olyan technikákkal, mint a NOP slides⁸². Az ellenőrzések észlelik és blokkolják a támadást. További követelmény, hogy a mérnök meghatározhassa a master/slave eszközpárokat, amelyek között a DNP3 forgalmat engedélyezni kell, és meghatározhassa az engedélyezett DNP3 üzenet típusait és funkciókódjainak listáját. Csak a megfelelően formázott DNP3 forgalom megengedett. A DNP3 érvényesítésének ki kell terjednie a közös fejléc byte mezőkre, a csomaghosszokra és a DNP3 CRC⁸³ érték ellenőrzésekre.

A fentiken kívül javasolt olyan megoldást alkalmazni, amely rendelkezik:

- IEC 104 ellenőrzési lehetőségekkel,
- GOOSE ellenőrzési lehetőségekkel,
- EtherNet/IP ellenőrzési lehetőségekkel,
- OPC ellenőrzési lehetőségekkel,

⁷⁸ syslog: system log (központi naplózás)

⁷⁹ coil: A Modbus esetében az adattípusok többségének elnevezésében közrejátszott, hogy főleg relékkel használták. A coil, azaz tekercs ebben az esetben az egy bites fizika kimenetet jelenti.

⁸⁰ payload: csomagtartalom (adatcsomag üzenet része)

⁸¹ Obfuszkáció: a kommunikáció szándékos elrejtése azért, hogy a kívülállók számára zavaros, kétértelmű vagy nehezen érthető legyen. Szoftverek esetében minél nehezebben lehessen megérteni annak pontos működését úgy, hogy a program helyesen működik.

⁸² NOP slides: Olyan informatikai támadás, mely a NOP, azaz no-operation utasítás egymás utáni többszöri ismétlésével éri el azt a memória-szegmenst, ahol az utasítást végre kívánja hajtani.

⁸³ CRC: Cyclic Redundancy Check (ellenőrző összeg)



- biztonságos távoli konfigurációs lehetőségekkel,
- IEC 61850 mély csomag ellenőrzéssel (DPI).

6.2.5. Behatolás megelőzés

A behatolás észlelő és megelőző rendszer (IDPS⁸⁴) olyan hálózatbiztonsági megelőző megoldás, amely előre megadott szabályok szerint a hálózati forgalomban keresi és akadályozza meg a behatolást és/vagy riasztást küld róla. Az IDPS rendszer tipikusan olyan funkciókat lát el, mint:

- a támadás megállítása,
- a környezet szükséges megváltoztatása (pl.: hálózati eszköz konfigurációjának megváltoztatása),
- a támadás tartalmának megváltoztatása (pl: szanitálja a csomag ártalmas tartalmát),
- a rendszergazda figyelmeztetése,
- a rosszindulatú csomagok kiszűrése,
- a forrásból jövő összes forgalom blokkolása,
- a kapcsolat megszakítása.

Az IPS⁸⁵ és IDS⁸⁶ rendszerek közötti különbség az, hogy míg az IPS rendszerek képesek beavatkozni, reagálni az észlelésre, addig az IDS csak passzívan figyeli a forgalmat.

A közvetlen internetkapcsolattal rendelkező eszközök elé ajánlott IPS eszköz telepítése, különösen azon hálózati szegmensekbe, ahol ICS/SCADA komponensek (is) vannak.

OT-OT és OT-IT közötti tűzfalak szabályrendszerét szegmens specifikusan, az ott fellelhető eszközök tipikus támadásainak és sérülékenységeinek vonatkozásában javasolt összeállítani az OT szakemberek bevonásával.

6.2.5.1. Behatolás megelőzés IT hálózatokban

Az informatikai hálózatok közvetlen internet kijárata elé a ki- és bejövő csomagok vizsgálatára a határvédelmi eszközökben IPS-t ajánlott implementálni. Kifejezetten ajánlott olyan megoldás választása, amelyik képes a Purdue modell (lásd bővebben a 7.1. pontban) szerinti alkalmazás rétegben is dolgozni (az IDS L2-L7 észlel, az IPS funkcionalitás viszont L2-L3 reagál).

⁸⁴ IDPS: Intrusion Detection and Prevention System (behatolás észlelő és megelőző rendszer)

⁸⁵ IPS: Intrusion Prevention System (behatolást megelőző rendszer)

⁸⁶ IDS: Intrusion Detection System (behatolás észlelő rendszer)



Erre számos kereskedelmi termék kapható. Ajánlott, hogy a DMZ-t határoló céleszközök és megoldások különböző gyártótól származó különböző technológiákra támaszkodjanak. Bár a bevezetést ez nagyban nehezíti, de ez a megoldás biztonságtechnikailag lényegesebben magasabb szintet képvisel. A DMZ-ben publikált szolgáltatások elé érdemes célspecifikus megoldásokat alkalmazni, mint például a web alkalmazás tűzfalak, vagy a levelezés védelmi céleszközök.

A hálózati IPS mellett érdemes minden egyes hálózati szegmensbe is IDS eszközt telepíteni. A IDS-t preferáltan hálózati ipszilon osztó (TAP⁸⁷) eszközön, vagy amennyiben ez nem áll rendelkezésre, akkor a forgalom kitükrözésével (SPAN⁸⁸ porton) javasolt megvalósítani.

A legjobb gyakorlat erre a Suricata nyílt forráskódú IDS motor, ami lehetőséget biztosít LAN specifikus szabály rendszer kialakítására (Yara alapon). Ez az incidenskezelés „threat hunting”⁸⁹ szakaszát követő automatizálási feladatokra is tökéletesen alkalmas.

A Suricata GPU⁹⁰ támogatásával számtalan egyéb előny is kiaknázható (pl.: DDoS⁹¹, DoS⁹² elleni védelem).

6.2.5.2. Behatolás megelőzés OT hálózatokban

Az ipari hálózati – esetünkben ICS/SCADA – forgalmak felügyelete kötelező, mivel túlnyomó többségük a különböző alrendszerek között kevésbé vagy egyáltalán nincsen elszigetelve. Ha az eszköz hibás konfigurációja, hardverhiba vagy vírus problémát okoz a hálózat egyik részében, akkor ez másodpercek alatt elterjedhet az egész hálózaton, ezzel akár jelentős kárt is okozva. Még a redundáns biztonsági mentési rendszerek is megbukhatnak egyidejűleg, ha hálózati kapcsolataikat nem védik eléggé.

Az OT hálózatban IPS telepítése szinte semmilyen esetben nem ajánlott. Sokkal inkább az IDS-eket érdemes telepíteni a Purdue modell által definiált zónák közötti és a zónákon belüli forgalomra. A modell az ipar 4.0, 5.0 és az ehhez kapcsolódó technológiák – mint például az 5G – miatt átalakulóban van és javasolt a trendek biztonsági aspektusát is lekövetni.

Az IDPS rendszerek naplózása kiemelt fontosságú, mind megőrzés, mind a felhasználás tekintetében (pl. log elemzés, SIEM⁹³ rendszerek).

⁸⁷ TAP: Test Access Point, olyan hálózati hardvereszköz, mely a hálózati hozzáférést és monitorozást teszi lehetővé.

⁸⁸ SPAN: Switched Port Analyser (port forgalom figyelése, tükrözése, monitorozása)

⁸⁹ threat hunting: fenyegetettség elemzés

⁹⁰ GPU: Graphical Processing Unit (grafikus processzor)

⁹¹ DDoS: Distributed Denial of Service (elosztott, szolgáltatásmegtagadással járó támadás)

⁹² DoS: Denial of Service (szolgáltatásmegtagadással járó támadás)

⁹³ SIEM: Security Information and Event Management (biztonsági információ és esemény kezelés)



Az ipari hálózatokon ajánlott minden kommunikációt áterelni a definiált szabályrendszeren. Minden olyan kommunikációt, amely nem szerepel a megengedett listán, blokkolni, naplózni és jelenteni kell. Ezeknek a megoldásoknak egyaránt támogatniuk kell az IP és nem IP protokollokat. Ajánlott, hogy rendelkezzenek SPI-vel⁹⁴ és OT protokoll esetén lehetőség szerint DPI-vel.

A szabályoknak tartalmazniuk kell az eszközök ismert sebezhetőségeit. A kritikus ICS/SCADA-komponensek folyamatos és hatékony védelme érdekében ezeket rendszeresen frissíteni kell.

Az egyik leggyakoribb IDS program a SNORT.⁹⁵ Az IPS-re és az IDS-re beállított robusztus IT biztonsági szabályoknak több rétege is van. A 14. melléklet néhány alkalmazási példát mutat be az ICS rétegelt tűzfalszabályaira.

6.2.6. Adatbiztonság

Az adatbiztonság az összegyűjtött adatvagyon sérthetetlenségét, integritását, használhatóságát és bizalmasságát lehetővé tevő technológiák és szervezési módszerek összessége. Az adatbiztonság informatikai biztonsági eszközökkel és technológiákkal érhető el.

Technikai ajánlások:

- Amennyiben az üzemeltetés és a technológia megengedi, akkor az érzékeny adatok védelmére ajánlott kriptográfiailag titkosított protokollok alkalmazása (pl. TLS⁹⁶ és SSH⁹⁷ kapcsolat, a titkosítatlan FTP és TELNET helyett).
- Minimum elvárás: jelszavak ne legyenek nyílt szövegben tárolva és küldve.
- Minimum elvárás: a vezetékek nélküli és a nyílt hálózaton keresztüli távoli elérések kriptográfiailag védetten történjenek.

6.3. Ajánlások: észlelés

Az előző pontok szerinti ajánlások maradéktalan megvalósítása ellenére is bekövetkezhet kiberbiztonsági incidens, azaz az esetleges támadó még az intézkedések ellenére is szerezhet hozzáférést a védendő ICS/SCADA-khoz. Kulcsfontosságú ezen esetek észlelése.

⁹⁴ SPI: Stateful Packet Inspection (állapotfüggő csomagfelügyelet)

⁹⁵ Ingyenes, nyílt forrású hálózati behatolás-érzékelő és -megelőző rendszer

⁹⁶ TLS: Transport Layer Security (Titkosítási protokoll, amely az interneten keresztüli kommunikációhoz biztosít védelmet. A TLS az SSL utóda. A TLS és SSL protokollok titkosítják a hálózati kapcsolatok szegmenseit.)

⁹⁷ SSH: Secure Shell (Protokoll, amit egy helyi és egy távoli számítógép közötti biztonságos csatorna kiépítésére fejlesztettek ki.)



Az észlelés fontossága több szempontból is megközelítendő, amelyek egytől-egyig szükségesek ahhoz, hogy az üzemeltető felismerhesse, ha valami nem „oda való” történik a rendszereikben. Elég csak egy APT típusú támadásra gondolni, ahol a behatolók akár évekig is várhatnak a megfelelő pillanatra. A megtörtént esetekkel igazoltan megfelelő észlelési képességek hiányában mindezt teljesen észrevétlenül ténylegesen képesek is megtenni.

Az ipar informatikai fejlődésének elkerülhetetlen velejárója a vezérlő rendszerek internetre történő csatlakoztatása. Az Ipar 4.0 és Ipar 5.0 ezeket – az alapvetően, zárt hálózatba tervezett technológiákat – egyre nagyobb hányadban felhő alapú menedzseléssel valósítja meg. Ennek megfelelően a rendszerek kitettsége nő, amivel arányosan a vállalatok kiberbiztonsága csökken. A villamosenergetikai ICS/SCADA üzemeltetőknek ajánlott a felhő alapú megoldásokkal kapcsolatos biztonsági politika kialakítása.

Az észlelés feladata a fenyegetettségek lehető legkorábbi időben történő felismerése, a belőlük megjelenő kockázatok csökkentése.

6.3.1. Helyzetismeret

A helyzetismeret azt jelenti, hogy az üzemeltető minden időpillanatban pontosan tudja, hogy mi történik a rendszerében (a rendszert tágan értelmezve, tehát informatikai, kommunikációs és villamosenergetikai téren is) és minden elképzelhető helyzetben (beleértve támadások alatti helyzeteket is).

6.3.2. Naplógyűjtés, kezelés és elemzés (SIEM)

A biztonsági naplók információt tartalmaznak az ICS/SCADA komponensekbe való belépésekről, az erőforrás használatról, a fájl módosításról és minden egyéb biztonság szempontból fontos eseményről. Megfelelően beállított audit adatgyűjtés és naplózás nélkül az eseménykezelő csapat gyakran nem tudja eldönteni az esemény fontosságát. Megfelelően beállított naplók segítségével könnyebben el lehet dönteni, hogy egy esemény megtörtént-e, ha igen mi volt a hatása, kiterjedése, és hogyan lehet a jövőben megelőzni a hasonlókat.

A naplógyűjtés kapcsán szabályozói szempontból a legfontosabb a naplózás meglétének megkövetelése.

A szabályzók pontosan definiálják a naplógyűjtést kritikus infrastruktúrák (adott esetben villamosenergia-rendszer) esetén, általánosságban az alábbi technikai követelményekkel:

- Központi naplógyűjtés és kezelés.
- Naplók tárolása és archiválása.



- Riasztást generáló események, eseménysorok meghatározása (use-case-ek).
- Fejlett naplógyűjtő megoldások, amik kezelik az architektúrális kihívásokat.
- Különböző forrásból származó naplók korrelációja.

A naplók feltétlenül szükségesek az utólagos elemzésekhez és ezzel újabb események megelőzéséhez

6.3.3. Rosszindulatú kód (malware) észlelés

A malware bármilyen kód, amelyet számítógépen/rendszeren a felhasználó/üzemeltető beleegyezése nélkül hajt végre nem dokumentált műveleteket. Ez a szándék gyakran rosszindulatú, a nem dokumentált műveletek a legtöbb esetben károsak (pl. vírusok, férgek, trójaiak, hátsó ajtók jogszerű programokban, befecskendezett kódok jogos folyamatokba stb.)

A malwarek kiszűrésének egyik leghatékonyabb módja, a különböző rendszerek között programokat és beállításokat hordozó USB háttértárak rendszeres ellenőrzése. Ezen felül ajánlott azoknak a hálózati forgalmaknak az ellenőrzése is, amelyek nem időkritikusak és átlépik két rendszer határát (amennyiben az ellenőrzés nem befolyásolja a kritikus forgalmakat és nem veszélyezteti az időbeli feltételeket).

Mivel gyakran az ipari hálózatba az irodai hálózaton keresztül kerül be a rosszindulatú kód, ezért az irodai hálózatban minden esetben folyamatos és alapos malware ellenőrzésre, szűrésre van szükség.

6.4. Ajánlások: reagálás

A biztonsági incidens (security incident) egy észlelt esemény (security event), amely egy sikeres támadás következménye. Ennek során az üzleti folyamatokban és a villamosenergia-rendszer üzemirányításában a kritikus folyamatok megállhatnak, károk keletkezhetnek, szélsőséges esetben az üzemvitelben súlyos fennakadások lehetnek. Éppen ezért fontos a megfelelő eseménykezelés, reagálás kialakítása. A villamosenergia-rendszer üzemirányítása esetén a legveszélyesebb támadások nagy valószínűséggel "cross-domain"⁹⁸ típusúak lesznek. Tehát például az infokommunikációs infrastruktúrát, az azt kiszolgáló szervereket, és az üzemirányítási folyamatokat, SCADA rendszert, fizikai erőátviteli elemeket egyszerre támadhatják. Ugyanezen okból az eseménykezelés során különös tekintettel kell lenni a biztonsági szempontokra, hiszen a villamosenergia-rendszerben pl. a meggondolatlan – támadás esetén az ártó szándékú – kapcsolások, műveletek fizikai károkat is okozhatnak, sőt

⁹⁸ cross-domain támadás: különböző típusú informatikai rendszerek közötti, egymásra kölcsönösen ható támadási megoldások



emberéleket is veszélyeztethetnek. Ugyanakkor egy esetleges támadás esetén a rendszert nem lehet leállítani, sőt inkább szinte bármi áron üzemben kell tartani.

Támadás esetén a reagálás célja elsődlegesen a támadási hatás, vagyis a működési zavarok minimalizálása. Ehhez eleve úgy kell a rendszerek működését megtervezni, hogy lehetséges legyen a támadással érintett (az IDS által jelzett) rendszerek elszigetelése az ép rendszerektől. Továbbá – a 6.4.3. pont szerinti forensics szempontjait is szem előtt tartva – meg kell kezdeni a kompromittált eszközök helyreállítását.

A támadás elhárítása után – sőt akár már alatta is – meg kell kezdeni a begyűjtött adatok feldolgozását, értékelését. A rendszer üzemeltetője szempontjából ennek legfontosabb célja az ICS/SCADA üzemének mielőbbi biztonságos helyreállítása, valamint a jövőbeni hasonló események megelőzése. Ehhez a támadás és az abban felhasznált technikák részletekbe menő vizsgálata szükséges. A hatékony reagálás magában foglalja a jövőbeni megelőzés és támadás észlelés folyamataiba való visszacsatolást, azok folyamatos fejleszthetősége érdekében.

A rendszer üzemeltetőinek közvetlen feladatain túllépve a rögzített adatokkal a bűnüldözést (forensics) is támogatni szükséges. Az ehhez szükséges rögzített adatok köre alapvetően azonos az üzem helyreállításához és a megelőzéshez is felhasználtakkal. Azonban ebben az esetben fontos az igazságügyi szakértői felhasználás szempontjainak megfelelő tartalom és forma előállítása.

A támadás elhárítása, az adatok elemzése, a támadás során kihasznált sebezhetőségek azonosítása után az érintett feleknek/részlegeknek egyeztetniük szükséges a reagálás folyamatáról. Ehhez visszajelzési, értékelő rendszert kell kialakítani, amelyben az illetékesek megoszthatják releváns információikat és az ezekkel kapcsolatos megfigyeléseiket.

6.4.1. A reagálás folyamata

A villamosenergetikai ICS/SCADA komponenseket üzemeltető szervezetnek minden pillanatban felkészültnek kell lennie a támadásra. Nem csak a villamosenergia-rendszer ICS/SCADA komponensek megelőző védelmére kell felkészülni már jóval a támadások megtörténte előtt, hanem ki kell alakítani azokat az eljárásokat, amiket behatolás észlelés esetén élesíteni kell.

A támadás kezelését, az arra adandó reagálás alapvető stratégiáját, irányelveit előzetesen rögzíteni szükséges, hiszen előre nem lehet minden támadásra felkészülni. Ezzel együtt az előre definiálható kereteken belüli konkrét reagálás minden esetben fog egyedi – a konkrét helyzet által éppen megkívánt és rögtönzött – elemeket is tartalmazni.

A felkészüléshez, majd egy esetleges támadás hatékony kezeléséhez a 6.1-6.3. pontokban foglalt komplex tevékenységek következetes végrehajtása szükséges.



A támadással érintett, kompromittált ICS/SCADA komponenseket (eszközöket, szervereket stb.) átvizsgálásuk, majd szükség szerinti javításuk, újratelepítésük stb. és tételes tesztelésük után lehet visszaállítani a támadást megelőző állapotukba és üzemükbe.

A támadásra adandó reakció sürgős, a személyzetnek stresszhelyzetben kell dolgoznia, éppen ezért fontos az előzetesen kialakított, jóváhagyott és rendszeresen tesztelt biztonsági eseménykezelési tervben kialakított eljárások, jelentések, kommunikációk megfelelő és folyamatos végrehajtása.

A támadás során, majd annak lezárulta után a rendelkezésre álló adatokat rendszerezve tárolni kell. Ezután kezdődhet meg a támadás részletes elemzése, a támadás során kihasznált sebezhetőségek feltárása. Ennek eredményeként egyrészt a behatolás megelőzéshez és észleléshez új származtatott információk jönnek létre, másrészt a jövőbeli eseménykezelési tréningekhez új szempontok merülhetnek fel, amivel javítható a legközelebbi hasonló eseményre adott reakció hatékonysága.

6.4.2. Villamosenergia-rendszer specifikumok

A villamosenergia-rendszer ICS/SCADA-k működése online, valós idejű folyamat, amelyben nem lehetnek kiesések. Prioritás a fertőzött, támadás alatt álló szerverek elkülönítése, valamint SCADA-t érő támadás esetén a villamos hálózat aktuális állapotával üzembe lépő tartalék rendszer rendelkezésre állása.

A valós idejűség a villamosenergetikai ICS/SCADA komponensek – hangsúllyal a védelmek – esetében a kibervédelmükkel kapcsolatos többlet funkciók ellátása erős performancia-tartalék követelményeket támaszt, mivel pl. az adatok gyűjtése, a logolás, a titkosítás/hitelesítés stb. semmilyen körülmények között sem lassíthatja a normál technológiai reakcióidőket.

Ajánlások:

- A villamosenergia-rendszer ICS/SCADA komponensek üzemeltetőinek biztonsági eseménykezelési szabályzattal és tervvel kell rendelkezniük.
- Ideális esetben a szervezeteknek saját, rendszeresen trenírozott eseménykezelő cross-domain csapattal kell rendelkeznie.
- Támogatni kell a lehető legalaposabb elemzést. Ez az elemzés történhet házon belül vagy kívül is, minden érintett kompetencia terület bevonásával, a cross-domain összefüggések feltárásával.



- Rendszeres eseménykezelő tanfolyamokat és gyakorlatokat (de legalább szimulációs gyakorlatokat) kell tartani. Ezek során az ICS/SCADA komponensek révén minden érintett terület be kell vonni, tehát a villamosenergia-rendszer üzemirányítását végző diszpécser, vagy a szerverpark üzemeltetését végző rendszergazdát épp úgy, mint pl. a villamos védelmeket üzemeltető mérnököt.
- A legjobb gyakorlatok alapján reagálási eljárások, irányelvek készíthetők az ICS/SCADA komponensek üzemeltetésében közvetlenül és közvetve illetékes valamennyi szervezet és személy számára, a szükséges együttműködéseket megjelölve.
- Ajánlott SOAR⁹⁹ rendszer használata.
- Ajánlott a leltár, a hálózati topológia, a függőségi gráf naprakész állapotban tartása.
- Mentések, visszaállási információk, megfelelő konfiguráció kezelés végzendő, illetve készíthető, amelyek révén a visszaállítás hatékonyan végezhető.
- Passzív hálózatfigyelés, amellyel a régi rendszerek esetén is hatékony adatgyűjtés végezhető.
- A támadás során vélhetően érintett hálózatoktól való minél jobb elkülönítés érdekében legyen fizikailag elválasztott menedzsment-hálózat a naplógyűjtésre és a biztonsági beállítások elvégzésére.
- Legyen eljárásrend a támadás elhárítása után az esemény kiértékelésre.
- Az értékelés eredményei beépítendő a megelőzési és észlelési stratégiákba.
- A támadás elhárítása és elemzése után a 6.1-6.3. pont szerinti összes tevékenységet ajánlott tételesen átvizsgálni, értékelni, majd a tanulságokat visszacsatolni, a szükséges folyamat-, szabályozás-, technológia- stb. fejlesztéseket elvégezni.

6.4.3. Számítógépes kriminalisztika (Forensics)

A számítógépes kriminalisztika célja a hibaelhárítás, a megfigyelés, a helyreállítás és az érzékeny adatok védelmének támogatása. Ezen felül bűncselekmény elkövetése esetén a számítógépes kriminalisztika végzi az adatgyűjtést, elemzést és archiválást, amelyet bizonyítékként használhatnak a bíróságon. Ennek előfeltétele, hogy a begyűjtött adatok beazonosítható forrásból származzanak, hitelesek legyenek.

⁹⁹ SOAR: Security Orchestration Automation and Response (olyan szoftvermegoldások halmaza, amely együttesen képes megvalósítani a fenyegetések és sebezhetőségek kezelését, az incidensmenedzsmentet és a biztonsági műveletek automatizálását)



Az adatok volatilitása, a villamosenergetikai technológia, az ICS/SCADA komponensek specialitásai, valamint a berendezéseknek vizsgálat alatti zavartalan működésnek és rendelkezésre állásának követelményei együttesen jelentős kihívást támasztanak a forensics felé.

Mint ilyen, alapvető fontosságú, hogy az incidens bekövetkezése előtt rendelkezésre álljanak és bevezetésre kerüljenek a megfelelő szabályok és tevékenységek, úgy, hogy az esemény reagálásának kivizsgálása után a kriminalisztikai programnak előre meghatározott kiindulópontjai legyenek.

Az eddig felsoroltakon felül rendkívül fontos szempont, hogy a megoldások ne legyenek tolaakodóak. Ellenkező esetben az üzemeltető személyzet meg fogja kerülni azokat, ezzel hatástalanítva őket.

Ugyancsak fontos szempont, hogy semmilyen módon ne befolyásolják az üzleti műveleteket, a szolgáltatási és üzemeltetési stabilitást vagy a vezérlőrendszerek környezetéhez kapcsolódó kritikus funkcionálisat.

Ajánlások:

- Ajánlott forensics végzése, szoros kapcsolatban az eseménykezeléssel.
- Esetleges támadás után ajánlott az azonnali reagálás és a forensics megkezdése.







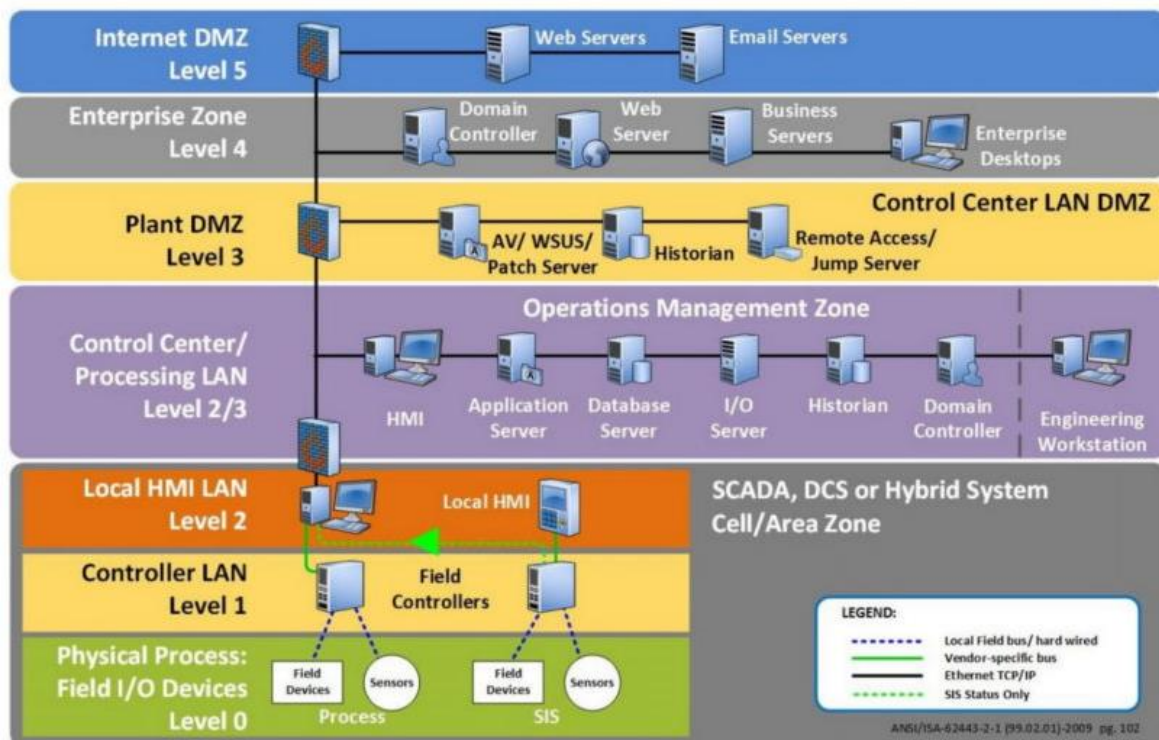
7. Rendszertechnika

Az előző fejezetben foglaltak a villamosenergia-rendszer ICS/SCADA-i kiberbiztonságának szükséges, de nem elégséges feltételei. További feltétel az ICS/SCADA-rendszerek és komponensek kiberbiztonsági szempontoknak is megfelelő felépítése, rendszertechnikája, többszintű védelmi rendszere és illesztése az IT rendszerekhez.

7.1. Architektúra-modell ICS/SCADA-k tervezéséhez: a Purdue-modell

Purdue-modell néven az 1990-es években a Purdue Egyetemen kidolgozott nagyvállalati referencia architektúra modell ISA-99 bizottsága által készített folyamatirányító rendszerek hierarchia-modelljét ismerjük. Jelenleg a legismertebb verziója a SANS Reading Room ICS whitepaper publikációi között érhető el.¹⁰⁰ [7]

Az ICS rendszerekhez kidolgozott Purdue-modell 4 zónát és 5 szintet különböztet meg (egy gyártóvállalat példáján keresztül):



7. ábra: A Purdue modell az ISA ábrázolásában¹⁰¹[8]

¹⁰⁰ L. Obregon. „Secure Architecture for Industrial Control Systems.” SANS Institute. <https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327> (Letöltve: 2020. augusztus 26.)

¹⁰¹ D. Peterson. „Is The Purdue Model Dead?” <https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/> (Letöltve: 2020. augusztus 26.)



Ügyviteli zóna

5. szint: Ügyviteli/vállalati rendszerek

Ebben a zónában helyezkednek el a szervezet ügyviteli IT infrastruktúrájának elemei, a különböző IT rendszerek és alkalmazások. Ebben a zónában mindennaposnak számítanak a VPN-en keresztüli távoli elérések és az internet használata (pl. egyes alkalmazásszerverek licenc-ellenőrzése folyamatos internet-kapcsolatot igényel). Az ebben a zónában elhelyezkedő rendszerek számára a Purdue-modell nem ajánlja közvetlen kommunikációs lehetőséget biztosítani az ICS rendszerekkel, ehelyett egy belső DMZ-n keresztül javasolja lehetővé tenni a hozzáférést az ICS rendszerek hálózatához.

4. szint: Üzleti tervezés és logisztika

A 4. szint gyakran az 5. szintből kerül kialakításra. Itt üzemelnek azok az üzleti rendszerek, amelyek fontos belső folyamatokat támogatnak (ilyenek lehetnek többek között a kapacitás-tervezésben, készlet-nyilvántartásban stb. érintett rendszerek).

Gyártási zóna

3. szint: Helyszíni gyártási műveletek és vezérlés

A Purdue-modell javaslata alapján ezen a szinten üzemelnek azok a rendszerek, amik az üzemirányító rendszerek támogatását biztosítják (pl. hálózati fájlszerverek, általános IT szolgáltatások, mint a DNS¹⁰², DHCP¹⁰³, NTP¹⁰⁴ stb., a mérnöki munkahelyek, a történeti adatokat tároló rendszerek, a jelentések előállítását és ütemezéseket végző rendszerek stb.). Az ezen a szinten üzemelő rendszerek egy DMZ-n keresztül kommunikálnak a Vállalati zóna szintjein működő rendszerekkel. A DMZ-t megkerülő direkt eléréseket célszerű kerülni.

Továbbá a 3. szinten található rendszerek kommunikálhatnak az 1. és 0. szinten található rendszerekkel is (pl. hálózati idősinkronizálás vagy DNS névfeloldás miatt erre szükség lehet).

¹⁰² DNS: A Domain Name System (DNS), azaz a tartománynév rendszer hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára.

¹⁰³ DHCP: Dynamic Host Configuration Protocol (dinamikus állomáskonfiguráló protokoll. A TCP/IP hálózatra csatlakozó hálózati végpontoknak adja meg a hálózat használatához szükséges beállításokat pl. IP-cím, hálózati maszk, alapértelmezett átjáró).

¹⁰⁴ NTP: Network Time Protocol (hálózati idő protokoll. Az órák szinkronizálására szolgáló hálózati protokoll).



Ipari zóna

2. szint: Ipari felügyelet és vezérlés

A 2. szinten működő rendszerek közé olyanok tartoznak, amelyek jellemzően az 1. szinten található rendszerekkel kell kommunikálniuk (ilyenek pl. a vezérlőtermi munkaállomások), illetve amik interfészként szolgálnak az 1. szintű eszközök és a gyártási vagy vállalati zónákban található rendszerek között (pl. monitoring és riasztó rendszerek vagy HMI-ok).

1. szint: Alapvető vezérlés

Ezen a szinten olyan eszközök találhatók, amelyek feladata a folyamatvezérlés biztosítása. Ezek az eszközök fogadják és dolgozzák fel a különböző szenzoroktól érkező adatokat. Ezek az eszközök (többnyire DCS¹⁰⁵-ek, PLC-k, RTU-k) felelősek a folyamatos, szekvenciális, kötegelt és diszkrét vezérlésekért. Ezek az eszközök jellemzően gyártó-specifikus operációs rendszereket/főrmereket futtatnak és a mérnöki munkaállomásokról lehet őket programozni és konfigurálni.

0. szint: Folyamatok

A 0. szinten üzemelnek azok a szenzorok és műszerek, amelyek az ipari folyamatok közvetlen ellenőrzését végzik. Ezeket az eszközök az 1. szinten működő rendszerek vezérlik.

Biztonsági (safety) zóna

Ebben a zónában olyan rendszerek működnek, amelyek az ipari folyamatok biztonsági ellenőrzését végzik és az előre bekonfigurált határértékek elérése vagy átlépése esetén az operátor értesítése mellett beavatkozik a biztonságos állapot helyreállítása érdekében. Ezeket a rendszereket javasolt teljes mértékben izolálni minden más rendszertől (amikor ez az izolálás nem történik meg, akkor olyan incidenseket kockáztatnak, mint amilyen a Triton/TriSIS incidensnél¹⁰⁶ előfordult). [9][10]

¹⁰⁵ DCS: Distributed Control System (osztott intelligenciájú folyamatirányító rendszer)

¹⁰⁶ B. Johnson et. al. „Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure.” Fireeye. <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html> (Letöltve: 2020. augusztus 26.)

Dragos. „TRISIS Malware. Analysis of Safety System Targeted Malware.” <https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf> (Letöltve: 2020. augusztus 26.)



2019 elején többen, több alkalommal (pl. az S4X19 konferencián¹⁰⁷, majd 2020 májusában David Greenfield cikkében is¹⁰⁸) [11] fogalmazták meg azt a kérdést, hogy amint az Ipar 4.0, az IIoT, az ipari felhő megoldások egyre inkább kezdenek teret nyerni, vajon túlhaladottá vált-e a Purdue-modell?

A kérdés oka elsősorban az, hogy a Purdue-modellt egy olyan időszakban dolgozták ki, amikor az ICS/SCADA rendszerek döntő többsége még izoláltan működött és egyáltalán nem, vagy csak minimálisan kapcsolódott az adott szervezet hálózatán kívül működő eszközökkel. Ma, amikor egyre több ICS/SCADA rendszernek kell egyre több egyéb, IT – és gyakran felhő-alapú – rendszerrel rendszeresen, egyes esetekben valós időben kommunikálnia, valóban szükség lehet a Purdue-modell újraértékelésére. A különböző (Purdue-modell szerint 0. és 1. szintű) eszközök, szenzorok, szelepek, áramváltók és szabályozók egyre növekvő funkcionalitása, "intelligenssé" válása, integrálásuk a különböző, szabványos IT és OT protokollokkal (pl. TCP/IP, OPC, Modbus, BacNET stb.) jóval „laposabbá” tette az ICS/SCADA rendszerek hálózatait. Ez pedig azzal jár, hogy kezdenek elmosódni, időnként már el is tűnnek a jól felismerhető határok, amiket az eredeti Purdue-modell alapján a 2., 1. és 0. szintek között még létrehoztak és a köztük lévő szigorú átjárási szabályokat minden körülmények között be is tartattak.

Ráadásul az ICS/SCADA hálózatokban egyre nagyobb arányban jelennek meg a különböző IT eszközök (switch-ek, szerverek és egyéb, korábban csak adatközpontokban használt megoldások), amikkel együtt jár a sávszélességek és a megbízhatósági (reliability) képességek megváltozása is, ami további számítási kapacitásokat igényelhet a folyamatirányítási hálózatok határain. Ezekkel párhuzamosan az IT is egyre gyorsuló ütemben változik, aminek következtében egyes, korábban alaposan tervezett funkciók már külső szolgáltatásként (Everything-as-a-Service) jelennek meg a vállalati IT-ban, aminek szintén hatása lehet az ICS/SCADA rendszerekre. Még ha az ipari felhőszolgáltatások nem is jelentek meg egy szervezet életében, a felhős megoldások használata a vállalati IT-ban tovább növeli az igényt az ICS/SCADA hálózatok és a vállalati hálózatok határára tervezett ipari DMZ iránt, aminek azonban sokkal dinamikusabban kell tudnia alkalmazkodnia a környező hálózatok (elsősorban a vállalati IT hálózatok) változásaihoz. Ez viszont az SDN¹⁰⁹ felé mozgatja a jövő ipari hálózatainak tervezőit is.

¹⁰⁷ D. Peterson. „Is The Purdue Model Dead?” <https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/> (Letöltve: 2020. augusztus 26.)

¹⁰⁸ D. Greenfield. „Is the Purdue Model Still Relevant?” AutomationWorld. <https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant> (Letöltve: 2020. augusztus 26.)

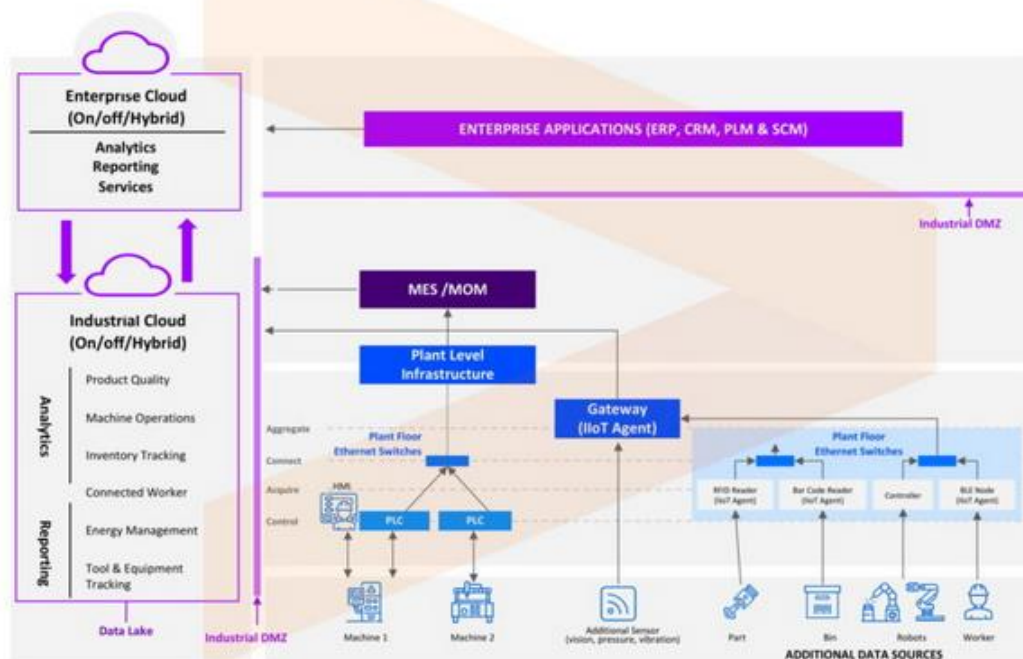
¹⁰⁹ SDN: Software Defined Networking (szoftveresen meghatározott hálózatok. Új hálózatüzemeltetési megközelítés, ami dinamikus, programozhatóan hatékony hálózatkonfigurálást tesz lehetővé, ezáltal növelve a hálózati performanciát és felügyeleti képességeket).



Mindezekre – valamint a különböző iparágak sajátosságai szerinti eltérő avulásra – tekintettel a Purdue-modell felhasználhatósági szintje is más és más lehet. A villamosenergia-szektor ebből a szempontból lassabban változik. Így a Purdue-modell e szektorban inkább tűnik használhatónak, mint olyan területeken (pl. ilyen a termelésirányító rendszereké), ahol az IIoT eszközöket és az Ipar 4.0 fejlesztéseit gyorsabban és szélesebb körben kezdik alkalmazni.

Még a modernebb ICS/SCADA rendszerek és hálózatok esetén sem teljesen használhatatlan a Purdue-modell. Erre bizonyíték Brad Hegrat ipari felhő környezetekre átdolgozott, Purdue-alapú architektúra-modellje (8. ábra) vagy a General Electric és a Dragos whitepaper-sorozatának első részében megjelent Purdue-modell változat¹¹⁰. [12]

CLOUD-ORIENTED INDUSTRIAL ARCHITECTURE



8. ábra: Brad Hegrat felhő-orientált ipari architektúra-modellje¹¹¹

A kihívás egyértelmű: a XX. század teljes mértékben izolált ICS/SCADA rendszerei és a XXI. század első két évtizedének robusztus, jól körülbástyázott, Purdue-modellen alapuló ipari hálózatai után egy újabb, az ipari hálózatok tervezését alapjaiban megváltoztató modell-váltás előtt állunk.

¹¹⁰ Dragos. „Building security to achieve engineering and business requirements.” https://www.dragos.com/wp-content/uploads/SecIndSys_Purdue_GEDragos.pdf (Letöltve: 2020. augusztus 26.)

¹¹¹ D. Peterson. „Is The Purdue Model Dead?” <https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/> (Letöltve: 2020. augusztus 26.)



A Purdue-modell ugyan nem halott, de az általa nyújtott alapokon egy új megközelítésre lesz szükségünk, a villamosenergia-szektor ICS/SCADA rendszereit illetően éppúgy, mint más iparágakban.



Figyelembe véve az ICS/SCADA rendszerek folyamatosan és egyre gyorsabban növekvő kiberbiztonsági kockázatait, ebben a helyzetben sem hibázhatnak az ipari folyamatirányítással foglalkozó szervezetek, amikor a már meglévő vagy újonnan kialakított ICS/SCADA rendszereik hálózatbiztonsági tervezésével foglalkoznak. Értékelniük kell, hogy a saját, egyedi környezetükben, eszközparkjukkal és igényeik szerint a klasszikus Purdue-modell mennyire alkalmazható számukra és amennyiben úgy látják, hogy a különböző IIoT eszközök és felhős (ipari vagy vállalati IT) megoldások használata miatt már nem profitálnak annak használatából, akkor új megoldásokat kell keresniük. Még az sem zárható ki, hogy az egyetlen, általános ICS architektúra modell helyett a jövőben szektor-specifikus modelleket kell kidolgozni.



A SeConSys számára egy, a nemzeti villamosenergia-rendszer jövőjét meghatározó, Purdue-alapú architektúra-modell kidolgozása lehet a közeljövő egyik nagy szakmai kihívása.

7.2. Javaslat a villamosenergia-rendszer ICS/SCADA-k kiberbiztonsági szintjeire

A kézikönyv a villamosenergia-rendszer legnagyobb teljesítményű, legnagyobb energiaáramokat kezelő – így esetlegesen sikeres kibertámadás miatti üzemzavarokkal a legnagyobb zavarokat, károkat okozó – elemeiben (erőműveiben, alállomásokban stb.) üzemelő ICS/SCADA-kra fókuszál.

A kézikönyv készítése folyamatában konzultációk zajlottak a magyar villamosenergia-átviteli és -elosztó hálózat egyes mértékadó szakembereivel a villamosenergia-rendszer legnagyobb teljesítményű, legnagyobb energiaáramokat kezelő elemeinek azonosítására és esetleges kibertámadásuk miatti zavarai miatti várható fogyasztói hatásaik – ezzel a velük kapcsolatban szükséges védelmi intézkedések – prioritásainak meghatározására¹¹². Ezek eredményeként koncepció készülhetett a magyar villamosenergia-rendszer sajátosságaihoz illeszkedő ICS/SCADA kibervédelmi szintek rendszerére.

¹¹² Köszönet Kapás Mihály, Kovács Gábor, Orlay Imre, Oroszki Lajos és Tari Gábor értékes tanácsaiért.





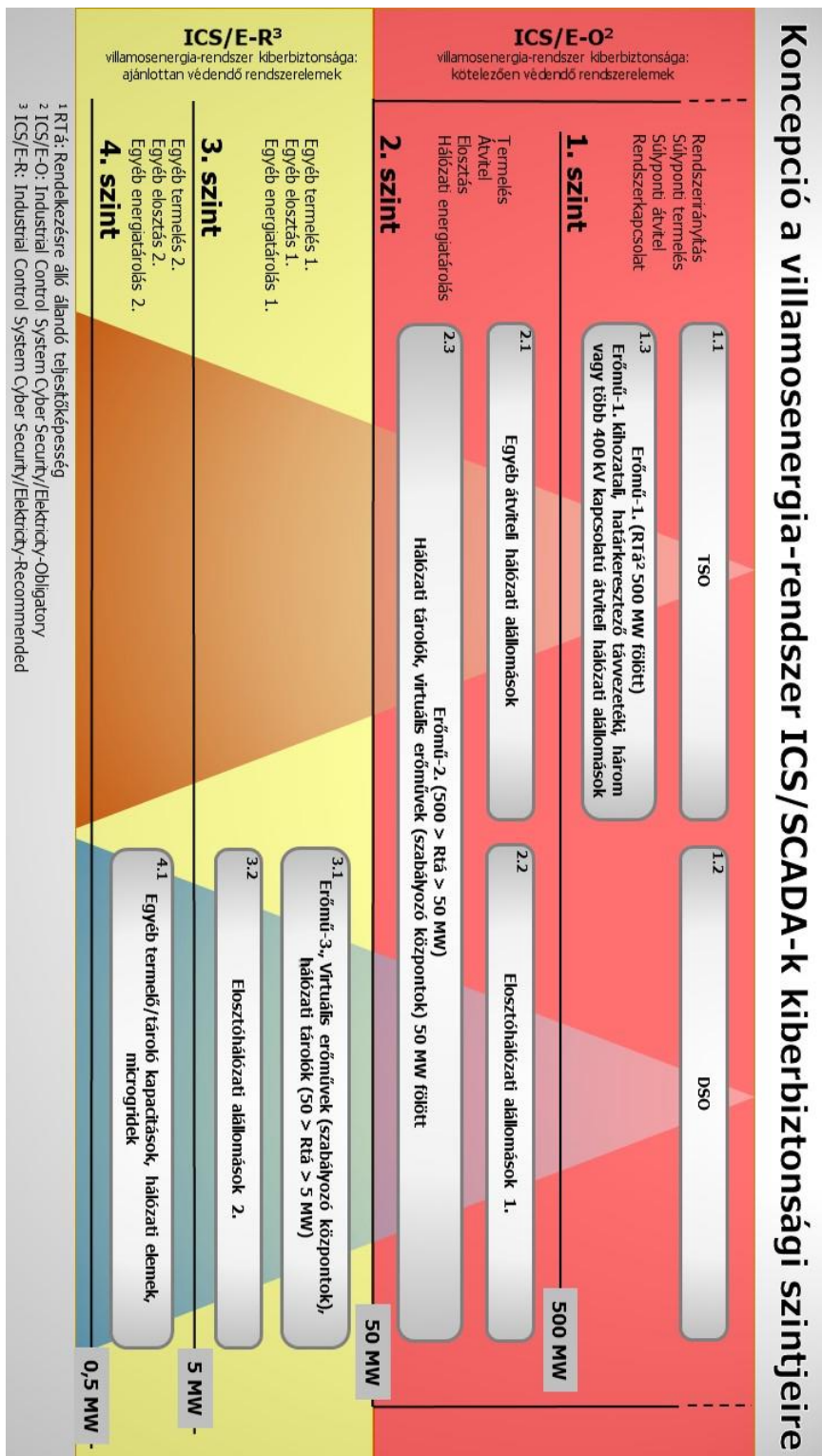
Olyan átlátható és hatékony kiberbiztonsági rendszer kiépítése szükséges, amely a magyar villamosenergia-rendszer sajátosságait is figyelembe véve képes minimalizálni egy esetleges kibertámadás bekövetkezési esélyét, avagy egy mégis megtörtént támadás fogyasztói hatását.



A kiberbiztonsági szintbe sorolásra vonatkozó koncepcióban figyelembe vett ICS/SCADA komponenseket a 4.2. pont tartalmazza.

A koncepció értelmében a villamosenergia-rendszer ICS/SCADA-k kibervédelmét a 9. ábra szerinti négy – két kötelező és két ajánlott – védelmi szintbe célszerű szervezni.





9. ábra: Javaslat a villamosenergia-rendszer ICS/SCADA-k kiberbiztonsági szintjeire¹¹³

¹¹³Köszönet Kapás Mihály, Kovács Gábor, Orlay Imre, Oroszki Lajos és Tari Gábor hasznos tanácsaiért.



- Kötelező, szabályozott, auditált módon védendő a kibertér felől érkező támadásoktól a villamosenergia-rendszer azon elemeinek ICS/SCADA-komponensei (ICS/E-O 1. és 2. szint), amelyek kibertámadás miatti működési zavara átlagosan legalább 50 MW teljesítményt és/vagy 200.000 fogyasztót érint.
- Ajánlott, más módon és helyen szabályozottan védendő a jelzett küszöbértékek alatti ICS-komponensek (ICS/E-O 1. és 2. szint).

A koncepció része, hogy a 2., 3. és 4. kiberbiztonsági szint követelményeitől el lehet térni (pl. védett és létfontosságú fogyasztók, tűz és robbanásveszély stb. esetén), de kizárólag a szigorúbb követelményű szint irányába. Az 1. szint követelményeitől nem lehet eltérni.

Az egyes szinteken belül feltüntetett sorrend az adott szintbe sorolt létesítményekre egységesen meghatározott követelményeknek való megfelelés ajánlott prioritásait jelzi.

Ugyancsak a koncepció része, hogy a régebbi létesítésű, üzemelő villamosenergetikai ICS-ek is szintbe sorolandók, majd az adott szintre előírandóktól való esetleges elmaradás esetén a későbbiekben kidolgozandó határidőre felzárkóztatandók.

Az engedélyesek jogosultak a felsoroltakon túli további objektumokat is bevonni valamely kiberbiztonsági szintre.

Az $R_{tá} = 50$ MW alatti termelő kapacitások kiserőműnek, az akkora, vagy annál nagyobbak nagyerőműnek minősülnek.

Az $R_{tá}^{114} = 5$ MW és 500 MW értékek a magyar villamosenergia-rendszer sajátosságai szerinti célszerű lépcsők.

A telephelyileg, szervezetileg stb. elkülönülő, de egy társasághoz tartozó termelő kapacitások kiberbiztonsági szempontból közös irányításúként tekintendők, azaz a kiberbiztonsági szintbe sorolásukkor az $R_{tá}$ -k összegét kell alapul venni.

A 0,5 MW-nál kisebb teljesítőképességű termelők, tárolók, szabályozóközpontok, microgrid-ek villamosenergetikai kiberbiztonsági szempontból (jelenleg) nem kerülnek besorolásra. De ez nem jelenti azt, hogy ezek kibervédelmi minimum követelményeit ne kellene (másutt, más módon) megfogalmazni.

Az egyes szintek konkrét kibervédelmi követelményeire vonatkozó javaslatokat a SeConSys a folytatódó munka keretében dolgozza ki.

¹¹⁴ RTá: Rendelkezésre álló állandó teljesítőképesség



7.3. Villamosenergetikai ICS/SCADA-k felépítése

A villamosenergia mindennapjaink része. Nem ismert olyan területe a civilizációnak, ahol ne lenne szükség rá. A villamosenergiát – a jelenleg ismert technológiákkal – meghatározó mennyiségben, hosszabb távon (> órák, napok), gazdaságosan nem lehet tárolni, így a megtermelt és az elfogyasztott mennyiségnek, földrajzi, fizikai és időbeli egyensúlyban kell lennie folyamatosan. Ehhez az szükséges, hogy ismerjük a villamosenergia-rendszer állapotát és tudjuk befolyásolni/irányítani. Az erőművekben megtermelt villamosenergia mérésére, a beavatkozásra a hálózati csomópontokban van lehetőség, amelyeket alállomásnak nevezünk. Mélni kell a villamosenergia fizikai paramétereit (feszültség, áram, frekvencia), az irányítást végző készülékek állapotáról is információ kell, valamint e készülékeket vezérelni is kell tudni. Ezeket a feladatokat az alállomási ICS/SCADA-komponensek (védelem és irányítástechnika) végzik. Amennyiben az üzemirányítás nem rendelkezik a villamosenergia-rendszer mindenkori állapotáról megbízható adatokkal akkor üzemirányítani sem tudja azt.

Annak függvényében, hogy az alállomási ICS/SCADA milyen régen került telepítésre, illetve, hogy az adott alállomás hol helyezkedik el a villamosenergia-rendszerben (pl. erőmű mellett, határkeresztező távvezetékét is fogad-e stb.) eltérő a konkrét védelmi és irányítástechnikai rendszer felépítése és az alkalmazott protokollok, de az alapelvek az alábbiak:

- A fizikai paraméterek mérését, az irányító elemek állapotát megadó jelzések begyűjtését és utóbbiak vezérlését a nagyfeszültségű (> 1 kV) ún. primer¹¹⁵ készülékek közelében lévő mezőgépek¹¹⁶ végzik.
- Az adatok összegyűjtését és kiértékelést a fejgép¹¹⁷/RTU végzi, a közöttük szükséges kapcsolatot a hálózati csatolók (multiplexer, switch stb.) teremtik meg.

Az alállomások között 20 éves ICS/SCADA-val működők is vannak, amelyek cseréje folyamatosan zajlik, számos esetben futnak eltérő generációs (10-15-20 év különbséggel) rendszer elemek. Ezekre is mutat példát a 15. melléklet 1. pontja.

A villamosenergia-ellátásban a nagyfeszültségű készülékek jellemző (és sok esetben tervezett) élettartama 20-40 év, az adatgyűjtő és feldolgozó rendszereké 15-20 év.

¹¹⁵ Primer készülék/technológia: a nagyfeszültségű (Magyarországon jellemzően 6, 10, 20, 35, 120, 220, 400 és 750 kV) villamos energia ki/be kapcsolását, irányítását, mérését végző alállomási berendezések

¹¹⁶ Mezőgép: analóg (áram/feszültség) bemeneti és erősáramú be/kimeneti kártyákkal rendelkező mérő, adatgyűjtő, feldolgozó, vezérlő készülék, amely közvetlenül a primer készülékektől kapja az adatokat és vezérli is azokat.

¹¹⁷ Fejgép: az alállomáson a központi adatgyűjtő, feldolgozó, vezérlő és protokoll konverter funkciókat ellátó készülék



Egy jelenlegi technológián alapuló alállomás esetében az adatgyűjtés és a kommunikáció TCP/IP elvű hálózaton keresztül történik, ennek megfelelő protokollokkal.

Minden alállomásnak van legalább egy idő szervere (NTP) amely – általában – az alállomáson van és ezen felül a felsőbb irány (központi ICS/SCADA) biztosít egy másikat. A következő generációs alállomások esetében már az 1 μ s nagyságrendű pontosságú kommunikáció is szükséges lesz egyes eszközök között a PTP¹¹⁸ protokoll alkalmazása miatt.

A villamosenergia-rendszer sok szereplős (lakossági fogyasztók/termelők, ipari fogyasztók/termelők, erőművek, hálózat tulajdonosok/üzemeltetők, DSO/TSO, külföldi TSO-k stb.) és ezeknek mind kell – valamilyen megoldással – csatlakoznia az üzemirányító rendszerhez. Mivel a tulajdonosi/üzemeltetői kör motivációja és szakmai ismerete igen nagy szórást mutat, így meg kell határozni azokat a minimum követelményeket, amelyekkel az előbb felsorolt különböző szereplők csatlakozhatnak a másikhöz. A 15. melléklet 2-5. pontjai mutatják be a magyar villamosenergia-rendszerre jellemző megoldásokat, az ezekre elvárt minimum követelményeket is megfogalmazva.

¹¹⁸ PTP: Precision Time Protocol (IEC 1588-2008 szabvány által definiált időfelbontás és szinkronizációs elv)



Energetikai, informatikai és kiberbiztonsági fogalmak, rövidítések jegyzéke

Fogalom, rövidítés	Kifejtés	Magyar megnevezés
AC	Alternating Current	Váltakozó áram
ACL	Access Control List	Hozzáférési lista
A/D	-	Analóg/digitális átalakítás
administrator		Rendszergazda
API	Application Programming Interface	Alkalmazásprogramozási interfész/felület
APN	Access Point Name	Egyedi hálózatelérési azonosító
APT	Advanced Persistent Threat	Folyamatosan fennálló, tartós fenyegetést jelentő, fejlett támadás
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	Támadói taktikák, technikák és közös tudásbázis
ATT&OT	ATT & CK for Industrial Control Systems	Támadói taktikák, technikák és ipari felügyeleti rendszerek
backdoor	-	Kiskapu, rejtett belépési pont
baseline	-	Kiindulópont, alapeset
BIOS	Basic Input/Output System	Alapvető bemeneti/kimeneti rendszer
bootkit	-	A számítógép indulásakor betöltődő rosszindulatú kód
botnet	Logical collection of Internet-connected devices	Internetre kötött vezérelt eszközök
CERT	Computer Emergency Response Team. Computer Emergency Readiness Team (US)	Eseménykezelő Központ
CISA	Cybersecurity and Infrastructure Security Agency	Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség
coil	-	A Modbus esetében az adattípusok többségének elnevezésében közrejátszott, hogy főleg reléekkel használták. A coil, azaz tekercs ebben az esetben az egy bites fizika kimenetet jelenti.
COTS	Commercial off-the-shelf	Kereskedelmi forgalomban kapható, ún. „dobozos” szoftverek és hardverek
CRC	Cyclic Redundancy Check	Ellenőrző összeg
cross-domain támadás	-	Különböző típusú informatikai rendszerek közötti, egymásra kölcsönösen ható támadási megoldások.
CTI	Cyber Threat Intelligence	Kiberfenyegetés felderítés
Cybersecurity Act	-	Az Európai Unió Kiberbiztonsági Törvénye
CyBOX	Cyber Observable eXpression	Ipari számítógépes rendszerekben dinamikus események, változók és paraméterek ellenőrzését, mérését segítő nyelv
CVE	Common Vulnerabilities and Exposures	Ismert sérülékenységek és kitétségek
DC	Direct Current	Egyenáram
DCS	Distributed Control System	Osztott intelligenciájú folyamatirányító rendszer
DDoS	Distributed Denial-of-Service	Elosztott, szolgáltatásmegtagadással járó támadás
defense in depth	-	Mélyégi védelem
defacing	-	Webtartalom módosítás
DHCP	Dynamic Host Configuration Protocol	Dinamikus állomáskonfiguráló protokoll
DMZ	Demilitarized Zone	Demilitarizált (védett) zóna
DNP3	Distributed Network Protocol 3	Elosztott hálózati protokoll
DNS	Domain Name System	Tartománynév rendszer



DoS	Denial-of-Service	Szolgáltatásmegtagadással járó támadás
Dragonfly	-	Villamosenergia rendszer ellen támadást intéző rosszindulatú program
drive-by-download	-	Letöltés általi támadás
DPI	Deep Packet Inspection	Mély csomag ellenőrzés
DSO	Distribution System Operator	Elosztóhálózati Rendszerirányító
EACMS	Electronic Access Control or Monitoring System	Hozzáférés szabályozási vagy felügyeleti rendszerek (pl. tűzfal, autentikációs szerverek és logmenedzsment megoldások)
ENCS	European Network for Cyber Security	Európai Hálózat a Kiberbiztonságért
ENTSO-E	European Network of Transmission System Operators for Electricity	Európai Villamosenergia-átviteli Rendszerirányítók Szervezete
ENISA	European Union Agency for Cybersecurity	Európai Unió Kiberbiztonsági Ügynökség
EoL hardware/software	End Of Line/Life hardware/software	Kifutó, üzemideje végén járó hardver/szoftver
ERP	Enterprise Resource Planning	Vállalati erőforrás tervezés
exploit/exploitability	-	Kihasználás/kihasználhatóság
forensics	-	Informatikai eszközön vagy rendszerben bekövetkezett események hiteles rekonstrukciója
GPRS	General Packet Radio Service	Csomagkapcsolt, IP-alapú rádiós adatátviteli technológia
GPU	Graphical Processing Unit	Grafikus processzor
Hash	-	Lenyomat (előírás szerint képzett bitsorozat)
HMI	Human Machine Interface	Ember-gép kapcsolati felület
honeypot	-	Csali (mézesbödön) számítógép
honeypot farm	-	Rosszindulatú kódok algoritmusok elfogására szolgáló csali számítógép „farm”
HSR	Highly-available Seamless Redundancy	Nagy megbízhatóságú, fürtös elvű protokoll
IAM	Identity and Access Management	Azonosítás- és hozzáférés kezelés
Ibtv.	-	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
ICS	Industrial Control System	Ipari felügyeleti rendszer
IDS	Intrusion Detection System	Behatolás észlelő rendszer
IDPS	Intrusion Detection and Prevention System	Behatolás észlelő és megelőző rendszer
IEC 104	-	Soros protokoll (RS232) TCP/IP implementációja
IEC 61850	-	Gyártófüggetlen energetikai adatkommunikációs szabvány
IEC 60870-5	-	Gyártófüggetlen energetikai adatkommunikációs szabvány
IED	Intelligent Electronic Device	Intelligens elektronikus eszköz
IoC	Indicator of Compromise	Kompromittálódásra utaló jel
IIoT	Industrial Internet of Things	Az ipari eszközök internete
IoT	Internet of Things	A dolgok („kütyük”) internete
IPS	Intrusion Prevention System	Behatolást megelőző rendszer
IPsec	Internet Protocol Security	IP biztonsági protokoll, Az IP protokollon működő, minden IP-csomagot titkosító és a jogosultságát ellenőrző protokoll



IRP	Incident Response Plan	Incidenskezelési terv
JTAG	Joint Test Action Group	Áramkörvizsgálati módszerekkel foglalkozó szakmai szervezet, illetve az IEEE-1149.1 szabvány által meghatározott módszer az integrált áramkört lapok/rendszerek gyors és automatikus tesztelésére
KDSZ	-	Közzeti Diszpécser Szolgálat
kernel	-	Rendszermag
Kiberbiztonság	-	A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kibertérrel megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.
Kibervédelem	-	A kiberbiztonsági keretrendszerben megvalósított szervezeti és technikai védelmi megoldások összessége
KII	-	Kritikus információs infrastruktúra
lateral movement	-	Oldalirányú mozgás, lépés
Lrtv.	-	Létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény
Lrtv. vhr.	-	A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet
MAEC	Malware Attribute Enumeration and Characterization	Rosszindulatú alkalmazások jellemzőinek részletezése és karakterizációja (leíró nyelv). Lásd még: STIX és TAXII.
MAC	Media Access Control	Közeghozzáférés-vezérlés, egyedi hálózati azonosító
malware	-	Rosszindulatú, kártékony alkalmazás vagy kód
MiniDuke	-	Adobe Reader sérülékenységet kihasználó rosszindulatú alkalmazás vagy kód
MitM	Man-in-the-Middle	Közbeékelődéses támadás
MAVIR	-	Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zrt.
MDLC	Motorola Data Link Communication	Motorola fejlesztésű adatkommunikációs protokoll
Merging Unit	-	Analóg áram és feszültség értékéből IEC 61850 szabványnak megfelelő értéket előállító mérő eszköz
MISP	Malware Information Sharing Platform	Rosszindulatú alkalmazásokkal kapcsolatos információmegosztó felület
Modbus	-	Ipari környezetben alkalmazott adatkommunikációs protokoll
NES	-	Nemzeti Energiatérkép
NIS	The Directive on security of network and information systems (NIS Directive)	Az Európai Parlament és a Tanács 2016/1148 Irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
NOP slides	no-operation slides	Olyan informatikai támadás, mely a NOP, azaz no-operation utasítás egymás utáni többszöri ismétlésével éri el azt a memória-szegmenst, ahol az utasítást végre kívánja hajtani.
NKI	-	Nemzeti Kibervédelmi Intézet
NTP	Network Time Protocol	Hálózati időforrás protokoll



Obfuszkáció	-	Kommunikáció szándékos elrejtése
ODSZ	-	Országos Diszpécser Szolgálat (a MAVIR üzemirányító központja)
OPGW	Optical Ground Wire	Optikai kábelt tartalmazó távvezetési védővezető
OPC	Open Platform Communication/OLE for Process Control	Platformfüggetlen kommunikáció/Nyílt platformú kommunikáció. Az OLE ipari automatizálásra specializált alkalmazási rendszere.
OPC DA	OLE for Process Control Data Access	Az OLE ipari automatizálásra specializált alkalmazási rendszere
OSINT	Open Source Intelligence	Nyílt forrású információszerzés
OSP	Operator Security Plan	Üzemeltetői biztonsági terv
patch/patch-elés	-	Javítócsomag/szoftverfrissítés
payload	-	Csomagtartalom (adatcsomag üzenet része)
PCA	Protected Cyber Asset	Eszköz, ami routolható protokollon keresztül kapcsolódik a rendszerhez
pentest	Penetration testing	Sérülékenységvizsgálat
perzisztencia	-	Tartós fenntartás
PDCA	Plan, Do, Check, Act	Tervezd meg, csináld meg, ellenőrizd, avatkozz be!
phishing	-	Adathalászat
PLC	Programmable Logic Controller	programozható logikai vezérlő
privilege escalation	-	Jogosultsági szint emelés
PRP	Parallel Redundancy Protocol	Párhuzamos redundancia elvű adatgyűjtő protokoll
PTP	Precision Time Protocol	IEC 1588-2008 szabvány által definiált időfelbontás és szinkronizációs elv
RAT	Remote Access Tool	Távoli hozzáférést biztosító program/kód
RBAC	Role-Based Access Control	szerepkör alapú hozzáférés-kezelés
resilience	-	Ellenállóképesség
RKR	-	Rotációs Kikapcsolási Rend
root	-	Gyökér könyvtár. Korlátlan jogosultságú rendszerfelhasználó.
rootkit	-	Saját és más programok jelentését elrejtteni képes, rosszindulatú kód
RSTP	Rapid Spanning Tree Protocol	Gyors hasítófa elvű adatgyűjtő protokoll
RTá	-	Rendelkezésre álló állandó teljesítőképesség
RTU	Remote Terminal Unit	Telemechanikai alközpont
SCADA	Supervisory Control and Data Acquisition	Felügyeleti irányítás és adatgyűjtés
SeConSys	Security of Control Systems	Ipari Irányítástechnikai Rendszerek Biztonsága
SDN	Software Defined Networking	Szoftveresen meghatározott hálózatok
shell	-	Parancssori felület, parancsértelmező
script kiddie	-	Komoly szaktudással nem rendelkező kezdő hacker
side-channel	-	Kerülő út
SIEM	Security Information and Event Management	Biztonsági információ és esemény kezelés
SLO	Security Liaison Officer	Biztonsági összekötő személy
smart grid	okos hálózat	Energiatermelés és -fogyasztás decentralizált menedzselése digitális eszközökkel a stabil, fenntartható, hatékony és megbízható működés érdekében



SNORT	-	Ingyenes, nyílt forrású hálózati behatolás-érzékelő és -megelőző rendszer
SOAR	Security Orchestration Automation and Response	Olyan szoftvermegoldások halmaza, amely együttesen képes megvalósítani a fenyegetések és sebezhetőségek kezelését, az incidensmenedzsmentet és a biztonsági műveletek automatizálását.
SOC	Security Operations Centre	Biztonsági Üzemeltetési Központ
social engineering	-	A pszichológiai befolyásolás, félrevezetés és megtévesztés módszere
SPAN	Switched Port Analyser	Port forgalom figyelése, tükrözése, monitorozása
spear-phishing	-	Célzott adathalászat, konkrét személy/szervezet ellen
SPI	Stateful Packet Inspection	Állapotfüggő csomagfelügyelet
SSH	Secure Shell	Protokoll, amit egy helyi és egy távoli számítógép közötti biztonságos csatorna kiépítésére fejlesztettek ki
SSL	Secure Socket Layer	Titkosítási protokoll, amely az interneten keresztüli kommunikációhoz biztosít védelmet.
STIX	Structured Threat Information eXpression	Strukturált kiberfenyegetés leíró nyelv és formátum a kiberfenyegetésekkel kapcsolatos információk megjelenítésére és átadására
superuser	-	Magas hozzáférési jogosultsággal bíró felhasználói fiók
syslog	system log	Központi naplózás
tamper resistant	-	Jogosulatlan fizikai hozzáférés ellen védett eszköz
TAP	Test Access Point	Olyan hálózati hardvereszköz, mely a hálózati hozzáférést és monitorozást teszi lehetővé.
TAXII	Trusted Automated eXchange of Indicator Information	Biztonságos, automatizált információcsere protokoll a kiberfenyegetésekkel kapcsolatos információk, adatok megjelenítéséhez és HTTPS protokollon történő továbbításához.
threat hunting	-	Fenyegetettség elemzés
TI	Threat Intelligence	Fenyegetés felderítés
TLS	Transport Layer Security	Titkosítási protokoll, amely az interneten keresztüli kommunikációhoz biztosít védelmet.
TMOK	-	Telemechanizált (távvezérelt és -felügyelt) oszlopkapcsoló
token	-	jogosultsági és biztonsági kódgeneráló eszköz
TSO	Transmission System Operator	Átviteli Hálózati Rendszerirányító
Yara	-	Rosszindulatú programok kutatásában és felismerésében használt eszköz
UP KRITIS	Public-Private cooperation in Critical Infrastructure Protection	Köz- és magánszféra együttműködése a kritikus infrastruktúrák védelme terén
URH	-	Ultrarövid hullám (nyílt rádiós jelátviteli technológia)
ÜKE jelzés	-	Üzemkésztség jelzés
watering hole	-	Gyakran látogatott weboldalak támadása
work-around	-	Kerülőmegoldás
WG-R	Working Group on Regulation	Szabályozási munkacsoport
WG-T	Working Group on Technology	Technológiai munkacsoport
WPA2	Wi-Fi Protected Access 2	A vezeték nélküli hálózati rendszerek biztonsági protokollja, amely tartalmazza az IEEE 802.11i szabvány főbb szabályait
zero-day sérülékenység	-	Még nem javított és nem publikált sérülékenység



Ábrajegyzék

1. ábra A SeConSys együttműködés résztvevői (2020. júliusi állapot)

Forrás: szerző

2. ábra A villamosenergia-rendszer ICS/SCADA-komponensei

Forrás: szerző

3. ábra Európai kiberbiztonsági kutatóközpontok

Forrás: Nai-Fovino, I., Neisse, R., Lazari, A. & Ruzzante, G. (2018). European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey. Luxembourg, Publications Office of the European Union, ISBN 978-92-79-92954-0, doi:10.2760/42369, JRC111211.

4. ábra EU-finanszírozás a kutatás és az innováció területén (2021–2027)

Forrás: Európai Bizottság. „EU-finanszírozás a kutatás és az innováció területén (2021–2027)”

5. ábra A kiberbiztonsági szempontból mértékadó szabályozások rendszere

Forrás: szerző

6. ábra A kiberbiztonsági szakterületi képzések ajánlott rendszere

Forrás: szerző

7. ábra A Purdue modell az ISA ábrázolásában

Forrás: D. Peterson. „Is The Purdue Model Dead?”

8. ábra Brad Hegrat felhő-orientált ipari architektúra-modellje

Forrás: D. Peterson. „Is The Purdue Model Dead?”

9. ábra Javaslat a villamosenergia-rendszer ICS/SCADA-k kiberbiztonsági szintjeire

Forrás: szerző

Mellékletek ábrái:

- 1.1. ábra Hatásukban és számukban is növekvő incidensek

Forrás: World Energy Council. „Cyber challenges to the energy transition.”

- 2.1. ábra Az alállomási kapcsolási séma a Pivnichna-i vezénylő monitorán

Forrás: youtube.com/watch?v=AUoiKZBqIo0

- 2.2. ábra Az alállomási 330 kV-os diszpozíció a Pivnichna-i vezénylő monitorán

Forrás: youtube.com/watch?v=AUoiKZBqIo0

- 2.3. ábra Az Enpaszelektro honlapja

Forrás: enpaselectro.com/ua/tehnologii/sistemy-upravleniya.html



2.4. ábra Információk a Pivnichna-i alállomás irányítástechnikájáról

Forrás: enpaselectro.com/ua/tehnologii/sistemy-upravleniya.html

2.5. ábra Pivnichna-i irányítástechnikai rendszer leírása

Forrás: enpaselectro.com/ua/tehnologii/sistemy-upravleniya.html

4.1. ábra Kiberbiztonsági stratégiák ENISA honlapon való szerepeltetése

Forrás: szerző

4.2. ábra Kiberbiztonsági stratégiák érvényességi idői

Forrás: szerző

7.1. ábra Kritikus infrastruktúrák függőségei

Forrás: Rinaldi, S.M. & Peerenboom, James & Kelly, T.K.. (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE. 21. 11 - 25. 10.1109/37.969131.

9.1. ábra Ibtv.-ben megfogalmazott védelmi követelmények

Forrás: szerző

9.2. ábra Az információbiztonság alapfogalmai

Forrás: szerző

9.3. ábra Az Ibtv. szerinti biztonsági osztályba sorolás módszertana

Forrás: szerző

9.4. ábra Az Ibtv. szerinti szintbe sorolás módszertana

Forrás: szerző

10.1. ábra Javaslat egy lehetséges magyar rendszerre

Forrás: szerző

11.1. ábra CIP-010 R3 3.3 követelmény

Forrás: CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments.

11.2. ábra CIP-010 R2-R3 követelmény megsértésének feltétele

Forrás: CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments.

14.1. ábra Alkalmazási példa 1.

Forrás: ICS CERT oktatási anyag

14.2. ábra Alkalmazási példa 2.

Forrás: ICS CERT oktatási anyag

14.3. ábra Alkalmazási példa 3.

Forrás: ICS CERT oktatási anyag



14.4. ábra Alkalmazási példa 4.

Forrás: ICS CERT oktatási anyag

15.1. ábra Régi adatgyűjtő rendszer

Forrás: szerző

15.2. ábra Részben felújított adatgyűjtő rendszer

Forrás: szerző

15.3. ábra Jelenlegi technológiai szintű adatgyűjtő rendszer

Forrás: szerző

15.4. ábra Jövőbeli technológia szintű adatgyűjtő rendszer

Forrás: szerző

15.5. ábra Védelmi jelátvitel direkt optikai szálon

Forrás: szerző

15.6. ábra Védelmi jelátvitel külön jelátviteli berendezésen

Forrás: szerző

15.7. ábra Alállomási RTU - alállomási RTU

Forrás: szerző

15.8. ábra HMKE-SCADA direkt kapcsolat

Forrás: szerző

15.9. ábra HMKE-Aggregátor-SCADA kapcsolat

Forrás: szerző

15.10. ábra Kiserőmű-KDSZ

Forrás: szerző

15.11. ábra Kiserőmű-alállomás erősáramú kapcsolat

Forrás: szerző

15.12. ábra Kiserőmű-alállomás jelátviteles kapcsolat

Forrás: szerző

15.13. ábra SCADA felépítése

Forrás: szerző



Mellékletek





1. melléklet: Incidens katalógus (2020. októberi állapot)

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
1	Salt River Project	USA, Phoenix metropolitan area	1994	Lane Jarret Davis jogosulatlan hozzáférést szerzett egy betárcsázós modemen keresztül az SRP egyes rendszereihez, köztük legalább 5 órán keresztül a Phoenix város tágabb környezetének vízellátásáért felelős SCADA rendszerhez is.	Egy tartalék számítógéphez csatlakoztatott betárcsázós modem	SCADA	Pénzügyi veszteség 40.000 USD, nincs információ a fizikai folyamatokra gyakorolt hatásról	https://www.risidata.com/Database/Detail/salt-river-project-hack
2	US Navy - San Diego-i közműszolgáltatók	USA, San Diego	1999	1999 novemberben az amerikai haditengerészet San Diego-i öböl közelében végrehajtott hadgyakorlata során a haditengerészeti radarok olyan EMI (elektromágneses interferencia) hatást generáltak, ami zavart okozott a San Diego megyei vízmű és a San Diego-i gáz- és elektromos művek ICS rendszereiben használt távkezelte berendezések kapcsolataiban és a távkezelésben.	Vezeték nélküli kommunikáció zavarása (nem szándékos)	SCADA, PLC, RTU	Az érintett alállomásokon vissza kellett állni manuális vezérlésre.	https://www.risidata.com/Database/Detail/navy-radar-shuts-down-scada-systems
3	CA ISO	USA, California	2001	2001-ben a kaliforniai független villamosenergia-ipari rendszerirányító IT rendszereit érte támadás. A támadók két, nem megfelelően tűzfalazott és Internetről elérhető webservert kompromittálásán keresztül fértek hozzá a rendszerirányító belső hálózatához. Az incidens kiváltó okaként alapvetően a nem kellően biztonság tudatos tervezést és kivitelezést tartják, illetve az időkritikus üzleti folyamatok biztonságos működés fölé emelt prioritását	Nem megfelelően szegmentált hálózat, gyenge biztonsági intézkedések Internetről elérhető webserverek esetén	Nem érintett ICS rendszereket	Nem ismert	https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf
4	Blaster worm	USA, Kanada	2003	Egyes források szerint a 2003-as nagy Észak-keleti áramszünet (ami az USA Észak-keleti államai mellett egyes Dél-Kelet-kanadai régiókban is üzemzavart okozott) hátterében a Blaster féregtámadás állt. Bár az incidens utáni elemzések szerint az érintett szolgáltatók ICS/SCADA rendszerei nem Windows operációs rendszeren futottak, de egyes monitoring rendszerek igen. A Blaster ezeket tette használhatatlanná, ami miatt az üzemzavar-elhárításért felelős villamosmérnökök nem tudták időben észlelni és megelőzni a nagy kiterjedésű üzemzavart.	Automatikusan kihasználható Windows sérülékenységen keresztül terjedő féreg	-	Kb. 55 millió fogyasztó maradt villamos áram nélkül hosszabb-rövidebb időre (4 órától két hétig terjedő időszakokról állnak rendelkezésre információk)	https://blogs.scientificamerican.com/observations/expert-a-virus-caused-the-blackout-of-2003-will-the-next-one-be-intentional/

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
5	Stuxnet	Natanz, Irán	2010	A Stuxnet néven ismert autonóm ICS malware az iráni urándúsító infrastruktúra és folyamat megzavarását célzó támadás volt, ami 4 különböző Windows 0-day sérülékenységet használt ki a terjedéshez és a WinCC DLL lecserélésével hajtott végre man-in-the-middle támadást az urándúsító centrifugákat vezérlő PLC-k ellen.	USB adathordozók, automatikus futtatás, szerver kompromittálás, man-in-the-middle	WinCC, PLC	Urándúsítási folyamat szabotálása, urándúsító centrifugák (minimum több 100 darab) fizikai meghibásodása)	https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
6	Havex/ Dragonfly	Európa, USA	2014	ICS rendszerek és ICS fejlesztő/felhasználó európai és Észak-amerikai vállalatok ellen indított, elsődlegesen információszerezésre specializált támadás-sorozat, ami kifejezetten kritikus infrastruktúrákat (elsődlegesen az energia-sektort) és beszállítóikat célozta.	Spear-phising, watering hole, RAT (Remote Access Tool)	A kompromittált gyártók weboldalain elhelyezett ICS szoftvertelepítő fájlokkal telepített rendszerek.	Mivel a támadások célja az információszerezés volt, ezért az incidenseknek a fizikai világra és folyamatokra gyakorolt hatása nem ismert.	https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
7	Calpine	USA	2014	Támadók kompromittálták a Calpine (jelentős szereplő az USA villamosenergia szektorában) szélerőműveket irányító SCADA rendszerének egyes elemeit és manuális szabályozásra állították az automata vezérlést.	Beszállítói lánc támadása (Supply-Chain Attack)	ICS/SCADA	Az incidensnek nem volt közvetlen hatása a villamosenergia-rendszerre.	https://apnews.com/c8d531ec05e0403a90e9d3ec0b8f83c2
8	Malware-támadás ázsiai atomerőművek ellen	Japán, Dél-Korea	2014	Malware-támadás ért egy japán (Monju) és egy Dél-koreai (Korea Hydro and Nuclear Power Plant) atomerőmű vezérlőtermében használt egyes rendszereket.	Malware-támadás	Nem ismert	Nem ismert	http://securityaffairs.co/wordpress/21109/malware/malware-based-attackhit-japanese-monju-nuclear-power-plant.html
9	Ukrán áramszolgáltatók	Nyugat-Ukrajna	2015. december 23.	Támadók 4 Nyugat-ukrajnai áramszolgáltató ICS rendszereit kompromittálva idéztek elő számos alállomáson jelentős üzemzavart, majd törölték a SCADA rendszerek diszkjeit és illegális firmware-frissítésekkel használhatatlanná tették számos RTU-t. A támadók utolsó lépésként DDoS-támadásokkal elérhetetlenné tették az érintett áramszolgáltatók webszervereit és hibabejelentésre használt telefonos ügyfélszolgálatait. A szolgáltatás helyreállítását jelentősen gyorsította az érintett áramszolgáltatóknál az automatizálás alacsony szintje, így képesek voltak gyorsan átállni manuális vezérlésre.	Spear-phising, BlackEnergy, KillDisk	ICS/SCADA, RTU	Mintegy 225.000 fogyasztót és 135 MW teljesítményt érintő áramkimaradás. Az incidensben érintett RTU-k teljes körű cseréje hónapokat (egyes esetekben 4-6 hónapot) vett igénybe.	https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
10	Izraeli közmű-szabályozó hatóság	Izrael	2016	Súlyos kibertámadás érte az izraeli közműszabályozó hatóság több rendszerét. Az incidens részletei nem ismertek.	Nem ismert	-	Nem ismert	https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
11	Malware-támadás német atomerőmű ellen	Németország	2016	Malware-t találtak a Gundremmingen-i atomerőmű rendszereiben. Az erőmű vezérléséért felelős rendszereket az incidens nem érintette.	Nem-célzott malware-támadás, a malware egy hétköznapi kártevő volt, az erőművi rendszerbe történő bejutási módja nem ismert	-	Az incidensnek nem volt közvetlen hatása az erőmű alap funkcióira.	https://securityaffairs.co/wordpress/46708/security/virus-q/gundremmingen-nuclear-plant.html
12	Industroyer/ CrashOverride	Ukrajna, kijevi körzet	2016. december 17.	Az Ukrenergó ukrán rendszerirányító elleni támadás a negyedik ismert, ICS rendszereket célzó támadás és a második, amiben autonóm, ICS rendszer ellen készített malware-t használtak a támadók (az első a Stuxnet volt). Egyes elemzők szerint a támadók célja nem egy sima üzemzavar előidézése volt, hanem azt tervezeték, hogy az üzemzavar előidézése után, amikor az Ukrenergó szakemberei a szolgáltatás helyreállításán dolgoznak, DoS-támadásokkal kiiktatnak több védelmet, majd az így védtelenül maradt alállomási berendezések egy túlterhelés esetén akár végzetes károkat is szenvedhetnek volna, ami akár több hónapos, fél éves, éves áramkimaradásokat is okozhatott volna. Az elemzés szerint ez végül csak azért nem következett be, mert a támadók hibát vétettek a DoS-támadáshoz használt számítógépes kódok fejlesztése esetén.	Industroyer/CrashOverride ICS malware	ICS/SCADA RTU Digitális védelem	200 MW teljesítmény kiesése a villamosenergia-rendszerből (az érintett felhasználók száma ismeretlen)	https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf
13	NotPetya	Ukrajna, Csernobil	2017. június	Az EternalBlue sérülékenységet kihasználó NotPetya ransomware (más források szerint cryptowiper malware) támadása miatt a Csernobili atomerőmű környezetében használt sugárázsmérő rendszer működése ellehetetlenült. Az érintett rendszer működését manuális vezérlésre kellett állítani	Feltételezhetően nem célzott malware-támadás, ami egy 3 hónapja ismert, javítással is rendelkező sérülékenység kihasználására épült.	Mérő- és adatgyűjtő rendszerek	Az erőmű rendszereire az incidensnek nem volt hatása.	https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html
14	Ír villamos-energia ipari rendszer-irányítók	Írország, Észak-Írország	2017. augusztus	Az EirGrid ír rendszerirányító és Észak-írországi leányvállalata, a SONI ellen intéztek támadást ismeretlenek, a becslések szerint 2 hónapig lehallgatva a két villamosenergia-ipari rendszerirányító hálózati forgalmát.	A két érintett szervezet Interneten elérhető hálózati eszközeiről a támadók GRE tunnel alkalmazásával kitérítették a hálózati forgalmat és kb. két hónapon keresztül hallgatták le a két rendszerirányító Internetes kommunikációját.	-	Az incidensnek nem volt ismert hatása a villamosenergia-rendszerre.	https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
15	Támadások az USA villamosenergia-rendszere ellen	USA	2018. július	Az amerikai Belbiztonsági Minisztérium (Department of Homeland Security, DHS) egy publikus webes előadás-sorozatot tartott az USA kritikus infrastruktúrája elleni orosz kibertámadásokról. Az előadás-sorozat egyik újdonsága 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. Erdemes megfigyelni a hasonlóságot a Havex-nél már bemutatott módszerrel, amikor európai ICS gyártók letölthető binárisait cserélték le malware-rel fertőzött változatokra, így támadva a kiszemelt szervezeteket.	Beszállítói lánc támadása (Supply-Chain Attack)	Nem ismert	Az incidenseknek nem volt ismert hatása a villamosenergia-rendszerre.	https://www.us-cert.gov/sites/default/files/c3vp/Russian_Activity_Webinar_Slides.pdf
16	Ransomware-támadás a johannesburgi áram-szolgáltató ellen	Dél-Afrikai Köztársaság	2019. július	Ransomware-támadás érte a johannesburgi áramszolgáltató rendszereit, aminek következtében – bár az áramszolgáltató ICS rendszereit állításai szerint nem érintette az incidens – mégis egyes ügyfeleknél, (akik, hasonlóan a magyar feltöltő kártyás mobil telefont konstrukciót használókhoz hasonlóan hasonló módon) előre fizettek a villamosáramért), hosszabb áramkimaradások voltak.	Ransomware-támadás, ami az áramszolgáltató adatbázisait és más rendszereit tette használhatatlanná	-	A rendelkezésre álló információk szerint az incidens nem érintette a villamosenergia-rendszer irányításáért felelős ICS rendszereket, de az előre fizető felhasználók egy bizonyos hányadánál áramkimaradások voltak	https://www.reuters.com/article/us-safrica-city-power/johannesburg-power-body-hit-by-ransomware-attack-idUSKCN1UK15N
17	DoS-támadás a vezérlő-központ és az állomás közötti kommunikációt biztosító berendezések ellen	USA	2019. szeptember	Az USA nyugati felén található sPower nevű villamosenergia-ipari cég vezérlő központja és távoli, kisebb erőművei közötti kommunikációt biztosító egyik eszköz (egy tűzfal) sérülékenységeit kihasználva támadók DoS-támadással átmenetileg ellehetetlenítették az erőművi állomások távfelügyeletét.	Az internetre csatlakoztatott tűzfal webes adminisztrátori felületének egy ismert, de nem javított hibáját kihasználva folyamatos újraindításokat idéztek elő a támadók	-	A kommunikáció kiesése a felügyeleti funkciók átmeneti degradálódását okozta, de nincs információ ennek nyomán kialakult üzemzavarról vagy fogyasztókat érintő áramkimaradásokról.	https://www.eenews.net/stories/106111289
18	Malware-támadás indiai atomerőmű rendszerei ellen	India	2019. október	Feltételezhetően célzott malware-támadás érte a Kudankulam atomerőművet (KKNPP) Indiában. A malware-t a Dtrack néven ismert, a feltételezések szerint Észak-koreai állami háttérű Lazarus csoporthoz köthető malware-ként azonosították.	A rendelkezésre álló információk szerint a malware a KKNPP ügyviteli hálózatait fertőzte meg, feltehetően Internet-eléréssel rendelkező hostokon keresztül.	Nem ismert	Az incidensnek a KKNPP és az indiai szabályozó szerv közlése szerint nem volt hatása az erőmű irányítástechnikai rendszereire	https://dragos.com/blog/industry-news/assessment-of-reported-malware-infection-at-nuclear-facility/

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
19	Kibertámadás az ENTSO-E ellen	Belgium	2020. március	Támadás érte az ENTSO-E (European Network of Transmission System Operators for Electricity) irodai rendszereit. Az ENTSO-E közleménye szerint a rendszereinek nincs kapcsolata az európai villamosenergia-ipari TSO-k rendszereivel.	Nem ismert.	Nincs	Nem ismert	https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/
20	EDP ransomware-támadás	Portugália	2020. április	Nagyszabású ransomware-támadás és adatlopás érte a portugál központú, multinacionális, gáz és villamosenergia-szektorban tevékenykedő EDP-csoportot. A támadók a RagnarLocker malware-t használták és a fájlok titkosítása mellett az ellopott adatok nyilvánosságra hozásával is zsarolták az EDP-t.	Feltételezhetően fertőzött MS Office dokumentumokban, e-mail csatolmányként érkezett a malware.	Nincs	Kb. 10 TB-nyi adatot loptak el illetve titkosítottak a támadók.	https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/
21	Elexon elleni támadás	UK	2020. május	Közelebbről nem részletezett kibertámadás érte a Nagy-britanniai villamosenergia-piacot működtető Elexon IT rendszereit. A beszámolók szerint az incidensben az Elexon legfontosabb rendszerei nem voltak érintettek.	Nem ismert	Nincs	Egyes rendszereket kb. egy napra le kellett állítaniuk.	https://www.theguardian.com/business/2020/may/14/lights-stay-on-despite-cyber-attack-on-uks-electricity-system https://theenergyst.com/elexon-hit-by-cyber-attack/

Az alábbiakban a megtörtént incidensek különösen fontos elemeit és azok tanulságait emeljük ki.

1. Energetikai vonatkozású incidensek és azok tanulságai

Az egyes országok, régiók villamosenergia-rendszereiben már az 1990-es és 2000-es években széles körben elterjedtek a részben kereskedelmi forgalomban kapható, hagyományos IT komponensekből is épített ICS/SCADA-k. Ezek a megoldások tették lehetővé és megfizethetővé az egyes villamosenergia-ipari szereplők számára a villamosenergia-rendszer egyre nagyobb mértékű helyi, majd távkezelését. Ebben az időben egy szűk szakmai közösségen kívül szó szerint senki nem foglalkozott az ipari folyamatirányító (ICS/SCADA) rendszerek kiberbiztonsági kérdéseivel, nem volt ez másképp a villamosenergia-rendszerekben használt ICS/SCADA-k esetében sem. Ezeket a rendszereket szinte kizárólag villamosmérnökök tervezték, fejlesztették és üzemeltették, szinte kizárólag villamosmérnöki szemmel nézve a rendszereket és azok funkcionális követelményeit. A nem funkcionális követelmények (már amennyiben azok egyáltalán voltak) között a hagyományos kiberbiztonsági szempontok szinte egyáltalán nem szerepeltek, ha esetleg mégis, akkor ezek a szempontok a sértetlenségre és a rendelkezésre állásra korlátozódtak. Olyan követelményekről, mint a szerepkör alapú hozzáférés-kezelés (RBAC¹¹⁹), titkosított és hitelesített kommunikáció, hálózatbiztonsági eszközök és jó gyakorlatok alkalmazása és sok más, a 2000-es évek közepére más, üzleti területeken tevékenykedő szervezetek (pl. pénzügyintézetek) esetében törvényi kötelezettségként megjelenő információ- és IT-biztonsági elvárásrendszerek alkalmazásáról szó sem lehetett. Ha valaki ezt akár csak feltételesen szóba hozta, azonnal heves ellenállásba ütközött (jellemzően az ICS/SCADA-kat üzemeltető, szinte kizárólag villamosmérnöki háttérrel rendelkező mérnökök irányából). Az érvek az ICS/SCADA biztonság témájával foglalkozók számára általában jól ismertek (az alábbiak csak példaként szolgálnak):

- Az ICS/SCADA-k tulajdonképpen nem IT rendszerek, ezért nem is kell őket úgy kezelni, mint egy bármilyen más szervezet IT rendszereit;
- Az ICS/SCADA-k nincsenek összekapcsolva más rendszerekkel, ezért az IT hálózatok irányából nem érhetőek el és ezért nincs is értelme hálózatbiztonsági kérdésekről beszélni;

¹¹⁹ RBAC: Role-Based Access Control (szerepkör alapú hozzáférés-kezelés)



- Az ICS/SCADA-k működése egyedi és specifikus, csak az érti őket, akinek értenie kell és hozzáféréssel kell rendelkeznie ezekhez a rendszerekhez, ezért még ha egy támadó be is tudna jutni az egyébként fizikailag szeparált hálózatban működő ICS-ek valamelyikébe, nem lenne képes észrevétlenül üzemzavarhoz vezető változtatásokat végrehajtani.

A villamosenergia-rendszerben bekövetkezett első – kibertámadásra visszavezethető – üzemzavart a Blaster néven ismertté vált számítógépes féreg 2003-as elszabadulása okozhatta. Ekkor az USA észak-keleti és Kanada dél-keleti államaiban voltak jelentős áramkimaradások. Az üzemzavar utáni vizsgálatok ugyan azt állapították meg, hogy az érintett területek villamosenergia-ellátásáért felelős szervezetek ICS-ei nem Windows-alapú operációs rendszerekre épültek, így azokat a Blaster féreg (ami a fertőzött számítógépek rendszeres újraindulását okozta) közvetlenül nem érintette, azonban az ICS-eket monitorozó rendszerek már Windows-alapúak voltak és érintette is őket a Blaster-támadás. Ennek köszönhetően a Blaster támadása miatt kiesett monitoring rendszerek hiányában a villamosenergia-ellátásért felelős mérnökök nem tudták időben észrevenni azt a kisebb méretű és hatású üzemzavart, aminek az elhárításával még megelőzhető lett volna a nagyobb területre kiterjedő üzemzavar.

A már említett, kis létszámú ICS biztonsági közösség (amelynek jelentős része az USA-ban dolgozott abban az időben) 2006-ra jutott el odáig, hogy az Idaho National Labs közreműködésével egy tesztorozatban próbálhatták bizonyítani azt az állításukat, hogy a villamosenergia-rendszerben használt eszközök ellen végrehajtott kibertámadásokkal is képesek lehetnek egyes berendezéseket használhatatlanná tenni, akár fizikailag károsítani és így végső soron üzemzavart előidézni a villamosenergia-ellátásban. A teszt (ami később Aurora teszt¹²⁰ néven vált ismertté az ICS kiberbiztonsággal foglalkozó szakemberek között) végül a használt transzformátor leégésével és a téma fontosságával érvelők igazának maradéktalan bizonyításával ért véget. Ekkortól beszélhetünk az ICS kiberbiztonságról, mint létező szakterületről. Ennek ellenére a különböző, ICS-eket használó szervezetek továbbra sem vették komolyan a kulcsfontosságú folyamatirányító rendszereiket érintő kiberbiztonsági fenyegetéseket (még akkor sem, ha egyébként a vállalati IT rendszereikhez kapcsolódóan egyébként foglalkoztak információ/IT biztonsági kérdésekkel). Erre egészen 2010-ig várni kellett.

¹²⁰ <https://www.youtube.com/watch?v=LM8kLaJ2NDU>



2. Stuxnet

Annak ellenére, hogy a Stuxnet esetében nem a villamosenergia-rendszer ellen végrehajtott támadásról van szó, mégis máig tartó hatása van az ICS biztonság területén és hivatkozási alap szinte minden, ICS biztonsági témájú kiadványban. Ezért érdemes röviden összefoglalni, hogy pontosan mi is volt a Stuxnet néven ismertté vált ICS malware.

A Stuxnet nyilvánosságra kerülése utáni években számos különböző mélységű és minőségű elemzés foglalkozott a malware és az incidens részleteinek elemzésével. Jelen összefoglaló legnagyobb részben Ralph Langren „How to kill a centrifuge”¹²¹ [13] című munkája alapján készült.

A történetek utólagos rekonstrukciója alapján a Stuxnet fejlesztése valamikor 2004/2005-ben kezdődhetett, míg a bevetésére valamikor 2007/2008 során kerülhetett sor. A történeteket rekonstruálva az derült ki, hogy a támadó elsőként USB-s adathordozókon bejuttatta a Stuxnet-et a célba vett iráni urándúsító létesítmények telephelyein használt, Windows (általában Windows XP) operációs rendszerekbe. A kezdeti fertőzésekhez a malware fejlesztői felhasználtak több Taiwan-i hardver- (és meghajtó szoftver) gyártó cégtől ellopott, a Microsoft által egészen 2010/2011-ig megbízhatónak tekintett és kérdés nélkül elfogadott kód aláíró tanúsítványt. Ezekkel a tanúsítványokkal aláírva a Stuxnet malware binárisait, a támadók elérték, hogy a Windows XP-be épített ellenőrzéseken akadály nélkül átjusson a malware és azonnal futtatható legyen a célba vett számítógépeken, ráadásul mindezt rendszer szintű jogosultsággal tudták tenni. A rendszer szintű jogosultságot felhasználva a malware megkereste az egyes, urándúsításhoz használt centrifugák vezérlésére használt számítógépeken futó WinCC Step7 illesztőprogramot, ami a WinCC és a PLC közötti interfész volt, majd lecserélte a Step7-t egy olyan, saját változatra, amivel a támadók már képesek voltak irányításuk alá vonni a Step7 modult. Az irányítás megszerzése után a támadók előbb rögzítettek egy 21 másodperces normál üzemi időszakot, majd ezt a felvételt elkezdték visszajátszani az urándúsítást felügyelő iráni atomfizikusoknak. Ezután a Stuxnet hozzákezdett fő célja megvalósításához, az urándúsítási folyamat sabotálásához. Ehhez először megfordította az egymás után sorba kötött centrifugák forgási irányát, majd elkezdte az urándúsításhoz szükséges fordulatszámnál jóval magasabb (86400 fordulat/percre), illetve jóval alacsonyabb (120 fordulat/percre) fordulatszámra átállítani a centrifugákat. Ezt a felgyorsítás-lelassítás műveletet egymás után sokszor ismételte a malware, így egyrészt teljesen használhatatlanná téve az urándúsításnál használt urán-hexafluorid gázt, másrészt – bár a Stuxnet alkotóinak egyes elemzők szerint ez valószínűleg nem volt elsődleges célja –

¹²¹ R. Langner. „To Kill a Centrifuge.” The Langner Group. <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf> (Letöltve: 2020. augusztus 26.)



olyan szintű mechanikai terhelésnek tette ki az érintett centrifugákat, hogy azok végül százasaival hibásodtak meg, egyes források szerint a meghibásodott centrifugák száma akár az ezret is elérhette.

A támadók meglehetősen jó munkát végeztek a Stuxnet lopakodó képességeinek fejlesztésekor, mivel az incidensről készített elemzések szerint a malware különböző verziói közel 6 évig működtek anélkül, hogy bárki észrevette volna, akkor is csak azért sikerült azonosítani, mert a Stuxnet végül elszabadult és nem csak az eredetileg célpontként kijelölt létesítményekben fertőzött.

3. Havex/Dragonfly

Valamikor 2013. február és június között mindmáig nem azonosított támadók célzott adathalász támadások keretében malware-fertőzött PDF fájlokat küldtek e-mailben különböző, jellemzően az energia-szektorban dolgozó vezetőknek. A mindennapokban megszokott adathalász támadásokkal ellentétben ezek az e-mailek nagyon jól kidolgozottak és személyre szabottak voltak, így a sikeres támadások aránya jóval nagyobb volt, mint egy átlagos adathalász-támadás esetén, ráadásul a célzottságuk miatt az esetek száma alacsony maradt, ezért közel két éven át a nagy IT biztonsági cégeknek sem tűnt fel.

Ezzel nagyjából egy időben a támadók több, az energiaszektorban működő szervezet weboldalát kompromittálták és ún. watering hole-támadásokat indítottak újabb célpontok ellen. Ezeknek a támadásoknak a célja egy RAT¹²² telepítése volt, hogy hátsó ajtót nyissanak a célba vett rendszereken.

Ezután a támadók három európai ICS gyártó vállalat (német, svájci és belga cégek) rendszereit kompromittálták és módosították a weboldalaikat, ezzel elérve, hogy az ügyfelek az adott cég ICS szoftvereinek egy, a Havex malware-rel fertőzött változatát töltsék le és telepítsék. A fertőzött fájlok 10 naptól 6 hétig terjedő időszakon át voltak elérhetőek a gyártók weboldalain, mielőtt az érintett cégek felfedezték és eltávolították volna őket.

A Havex/Dragonfly támadásokat utólag több neves IT biztonsági cég is részletesen elemezte (emiat is van az esetnek egynél több neve, az F-Secure Havex-ként¹²³ [14], a Symantec Dragonfly-ként¹²⁴ [15] hivatkozik nagyjából ugyanarra a támadói csoportra és támadásokra). Az elemzések alapján a biztonsági kutatók arra a következtetésre jutottak, hogy a támadás

¹²² RAT: Remote Access Tool (Távoli hozzáférést biztosító program/kód)

¹²³ Daavid. „Havex Hunts For ICS/SCADA Systems.” F-Secure.

<https://archive.f-secure.com/weblog/archives/00002718.html> (Letöltve: 2020. augusztus 26.)

¹²⁴ Symantec. „Dragonfly: Western energy sector targeted by sophisticated attack group”. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks> (Letöltve: 2020. augusztus 26.)



célja a megtámadott szervezetek hálózatainak és ICS, valamint IT rendszereinek felderítése volt, ehhez az OPC ipari telekommunikációs szabvány protokollt használták.

A Havex/Dragonfly támadások esetén (hasonlóan a legtöbb kibertámadáshoz) nem sikerült biztosan megállapítani, hogy kik voltak a támadók, bár a támadásokat elemző szakértők többnyire az orosz állami háttérű APT csoportok egyikét tartják felelősnek. Évekkel később történt incidensek után (elsősorban az ukrán villamosenergia-rendszer elleni 2015. és 2016. évi támadások után) olyan elméletek is napvilágot láttak, hogy a Havex/Dragonfly támadások valójában felderítési célú műveletek voltak, amelyek során felmérhették a későbbi, immár a fizikai világra is hatást gyakorló támadások lehetséges célpontjait. Az első ilyen támadásra nem is kellett sokáig várni.

4. Kibertámadás ukrán áramszolgáltatók ellen

2015. december 23-án, helyi idő szerint délután fél négykor a Nyugat-ukrajnai régióban működő Kyivoblenergo áramszolgáltatónál az ügyeletes villamosmérnök diszpécser az észre vette, hogy az elosztóhálózat alállomási távkezelését biztosító számítógépeken a kurzor mozogni kezd és sorban megpróbálja kikapcsolni az egyes alállomásokat – annak ellenére, hogy senki sem nyúlt az egérhez vagy a billentyűzethez.¹²⁵ A támadók 7 db 110 kV-os és 23 db 35 kV-os alállomáson okoztak üzemzavart, ami közel 225.000 fogyasztót hagyott villamos áram nélkül, mindezt a tél közepén.

Az üzemzavar és az áramkimaradások előidézése után a támadók törölték az üzemirányító ICS rendszerek számítógépeinek merevlemezeit, kiemelt figyelmet fordítva arra, hogy néhány, kulcsfontosságú binárist ne csak töröljenek, hanem felül is írjanak, így téve még nehezebbé és hosszabbá a helyreállításukat. Ezzel egy időben az alállomásokon használt RTU-k nagy hányadán olyan, hibás firmware-frissítéseket telepítettek, amikkel az érintett RTU-k végleg üzemképtelenné váltak (és lehetetlenné vált a korábbi, működő firmware helyreállítása is). Amikor ezzel is végeztek, a támadók szolgáltatás-megtagadásos (Denial-of-Service, DoS) támadást indítottak az áramszolgáltató ügyfélszolgálati telefonvonalai és a hibabejelentésre használt weboldalai ellen.

Az csak később derült ki, hogy nem egy, hanem összesen négy, Nyugat-Ukrajna különböző régióinak villamos áram-ellátásáért felelős szolgáltatót és azok több, mint 50 alállomását ért támadás.

¹²⁵ 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>



Az ukrán áramszolgáltatók végül azért tudták néhány óra alatt helyreállítani az áramszolgáltatást, mert az érintett áramszolgáltatók és alállomások esetében az automatizáltság szintje még nem volt nagyon magas, ezért rendelkezésre álltak azok az elektrikusok, akiket az érintett alállomásokra vezényelve kézi vezérlésre tudták átállni és így december 23-án késő estére a legtöbb érintett területen sikerült helyreállítani az áramszolgáltatást. A támadásoknak hosszabb távú hatásai is voltak, a tönkretett RTU-k egy részét még 2016 áprilisában sem tudták kicserélni.

Az ukrán hivatalos szervek nyíltan is az orosz titkosszolgálatokat vádolták a támadásokkal, vitathatatlan bizonyítékokkal azonban nem rendelkeztek. Az incidens után szinte azonnal, már december 23-án ukrán és amerikai állami szervek, valamint IT és ICS biztonsági magáncégek elismert szakértői indultak az incidensek helyszíneire. Az általuk gyűjtött adatok és az azok alapján készült elemzések szerint a támadás 9 hónappal korábban, 2015. márciusban kezdődött. A támadók ekkor makró-vírussal fertőzött dokumentumokat küldtek a célba vett áramszolgáltatók egyes dolgozóinak.



A phishing során a támadó az ukrán energetikai minisztérium hivatalos küldeményeinek tűnő elektronikus levelekkel igyekezett meggyőzni a célpontként kiválasztott társaságok alkalmazottjait. A csali email-hez MS Excel dokumentum volt csatolva, amelybe ágyazott makrónak a címzett általi óvatlan engedélyezése után a címzett gépére települt a BlackEnergy3 malware. A támadó a makro engedélyezésére valódnak tűnő, MS Office figyelmeztetéssel (*„Attention! This document was created in a newer version of Microsoft Office. Macros are needed to display the contents of the document.”*) vette rá a célpontokat.



A makróvírusokkal történő fertőzés annak ellenére sikeres volt, hogy a megcélzott áramszolgáltatók a szakmai jó gyakorlatoknak és ajánlásoknak megfelelően technikai kontrollokkal (csoportházi rendekkel) tiltották a makrók futtatását, azonban a támadók social engineering technikák alkalmazásával elérték, hogy a célba vett felhasználók engedélyezzék a makrók futtatását a számítógépeiken. Az így elinduló makróvírus volt az ún. dropper, ami egy előre belekódolt IP címen elérhető szerverről letöltötte és elindította a BlackEnergy nevű malware-t, ami utána hátsó ajtókat nyitott a megfertőzött számítógépeken. Ezeket a hátsó ajtókat használták a támadók az adott szervezet IT és ICS hálózataiban a további célpontok keresésére. Az első számítógépek kompromittálása után a támadók legitim felhasználói azonosítókat és jelszavakat kerestek (és találtak is), amelyek birtokában újabb rendszereket



tudtak kompromittálni és még több adatot loptak ki az áramszolgáltatók rendszereiből. Ezek a támadás későbbi fázisaiban fontosnak bizonyulhattak az üzemzavar előidézése során.



A támadás során a fogyasztói leágazások kikapcsolásához képest mellékszálak tűnik – holott lehetséges következményeit tekintve kulcsfontosságú volt – az UPS-ek támadása. Ez az UPS-ek távfelügyeleti interfészén keresztül történt. A támadás egyik tanulsága, hogy komolyan kell venni az ilyen távoli elérési felületek kiberbiztonsági kockázataira vonatkozó permanens szakértői figyelmeztetéseket. Ezek a csatlakozási lehetőségek különösen sérülékennyé tehetik a védendő rendszert, ha azok pl. folyamatosan, vagy akár csak a szükséges és elégséges időnél hosszabb ideig elérhetők, avagy rajtuk keresztül külsős, a védendő rendszer üzemeltetőjénél kevésbé szigorú kiberbiztonsági protokoll szerint működő társaság csatlakozhat. Bár az UPS-ek támadása fontos rendszerek működését zavarta meg, de a következmények még súlyosabbak is lehettek volna. A kritikus rendszerek kivétel nélkül UPS alátámasztásúak. Egy az ezekre irányuló masszív kibertámadás akár a megszakítókra vonatkozó kapcsolási jog megszerzése nélkül is – de e joggal együtt különösen! – képes az energiaszolgáltatás folyamatosságának súlyos megzavarására.



A 2015. decemberi ukrán áramszolgáltatók ellen végrehajtott kibertámadásokról 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.¹²⁶ [16]

5. Industroyer/CrashOverride

Majdnem napra pontosan egy évvel később, 2016. december 17-én újabb kibertámadás érte az ukrán villamosenergia-rendszert. Ebben az esetben az Ukrenergo, az ukrán villamosenergia-ipari rendszerirányító Kijev melletti alállomásán (Pivnichna-észak 330/110/10 kV) idéztek elő üzemzavart ismeretlen (de a feltételezések szerint megint csak orosz titkosszolgálati háttérrel rendelkező) támadók. Annak ellenére, hogy a 2016-os támadás az alállomások számában (2015-ben több, mint 50 áramszolgáltatói alállomás volt érintett a

¹²⁶ R. M. Lee, M. J. Assante, T. Conway. „Analysis of the Cyber Attack on the Ukrainian Power Grid.” E-ISAC. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (Letöltve: 2020. augusztus 26.)



2016-os egyetlen alállomással szemben) nem volt összehasonlítható az egy évvel korábbi incidenssel, 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 megjelenése jelentette. Az első elemzést a malware-ről az ESET szlovák IT biztonsági cég készítette, ők nevezték el a malware-t Industroyer-nek. 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.

2019. szeptemberében Joe Slowik, a Dragos Inc. munkatársa egy 16 oldalas elemzést készített¹²⁷ [17], amiben új állításokat fogalmazott meg az incidenssel kapcsolatban. Ez az elemzés nem kevesebbet állít, mint hogy a 2016 decemberi incidens során a támadók célja nem csak az Ukrenergó kijevi alállomásán történő üzemzavar előidézése és az ennek nyomán kialakuló áramkimaradás volt, hanem egyben az alállomási védelmek kiiktatásával (az érintett Siemens SIPROTEC védelmekben megtalálható volt egy még 2015-ben azonosított sérülékenységgel, ami miatt DoS-támadással használhatatlanná lehetett tenni az érintett berendezéseket) egy jóval nagyobb eszközparkot érintő pusztító támadás végrehajtása. Joe Slowik feltételezései szerint a támadók arra készültek, hogy az üzemzavar előidézése után, amikor az Ukrenergó szakemberei a szolgáltatás helyreállításán dolgoznak, DoS-támadásokkal kiiktatnak több védelmet, majd az így védtelenül maradt alállomási berendezések egy túlterhelés esetén akár végzetes károkat is szenvedhettek volna, ami akár több hónapos, fél éves, éves áramkimaradásokat is okozhatott volna. Az elemzés szerint ez végül csak azért nem következett be, mert a támadók hibát vétettek a DoS-támadáshoz használt számítógépes kódok fejlesztése során.

¹²⁷ J. Slowik. „CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack.” Dragos. <https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf> (Letöltve: 2020. augusztus 26.)





Az ICS-CERT 2015. július 21-én ICS biztonsági javaslatot hozott nyilvánosságra a Siemens SIPROTEC 4 és SIPROTEC Compact védelmeinek, valamint EN100 Ethernet kártyáinak sérülékenysége kapcsán azt követően, hogy egy orosz szakember felfedezte, majd bejelentette azt a Siemensnek, amely ennek nyomán firmware frissítést adott ki. A felfedezett sérülékenység kihasználásával az érintett védelmekben szolgáltatásmegtagadás (DoS) lett volna előidézhető, amelynek következtében a védelmek nem lettek volna képesek ellátni védelmi funkciójukat. A DoS után a védelmek működőképessége csak helyszíni újraindításukkal lett volna helyreállítható. Arra vonatkozóan viszont nincs információ, hogy a Pivnichna-i alállomás SIPROTEC védelmein a támadás időpontjáig végrehajtották-e a firmware frissítést. Az elemzések szerint a malware megkísérelte a SIPROTEC védelmek támadását, a DoS kiváltását, amelynek nyomán azok „firmware frissítés” módba váltottak volna. Ez azonban a védelmek korlátozott erőforrásai (főleg memóriája) miatt egyben a védelmi képességek elvesztését is jelentette volna.

A védelem nélküli visszakapcsolás magában hordozhatta a hálózati elemek súlyos károsodásának a veszélyét. Szándéka szerint a támadó ezzel a taktikával a megszakítók kikapcsolásával okozott kiterjedt ellátatlanság mellé egy második, a hálózat fizikai károsodásának a lehetőségét is magában hordozó támadási lépcsőt is beiktatott. A támadó mondhatni a kezelőszemélyzet ellen tervezett ún. túlterheléses támadást végrehajtani arra alapozva, hogy a mielőbbi visszakapcsolás miatti időszűkében a kezelőszemélyzetet hibára kényszerítse.



Jelentős különbség volt a 2015-ös és 2016-os incidensek között, hogy a 2015-ös incidensnél a támadók malware-eket még csak a kezdeti számítógép-fertőzésekhez és a kompromittált eszközök törléséhez használták fel, de magát az üzemzavart manuálisan idézték elő. Ezzel szemben a 2016-os támadás során bevetett moduláris malware nagymértékben automatizált volt, így a támadóknak kevésbé – szinte egyáltalán nem – kellett manuálisan beavatkozniuk az üzemzavar előidézéséhez – ugyanakkor ez lehet az oka annak is, hogy nem sikerült nagyobb károkat okozniuk a célba vett alállomás rendszereiben.

A moduláris felépítés miatt az Industroyer/CrashOverride malware-t kisebb változtatásokkal fel lehet használni tulajdonképpen bármilyen más ICS elleni támadásnál is. A 2016-os ukrán incidensből származó malware-minta a 101-es (IEC 60870-5-101), 104-es (IEC 60870-5-104),



IEC 61850-es és OPC DA¹²⁸ protokollokat ismerte, de a támadásról és a malware-ről megjelent, kifejezetten színvonalas elemzések¹²⁹ [18][19][20] alapján a támadóknak nem okozhat megoldhatatlan problémát más ICS-ek által használt protokoll ismeretét is belekódolni.

Az Industroyer/CrashOverride malware a negyedik, célzottan ICS-ek ellen tervezett malware (a Stuxnet, a BlackEnergy és a Havex után), egyben az első ismert malware, amit kifejezetten a villamosenergia-rendszer elleni támadásra hozták létre. Veszélyességét a modularitása és a nagyfokú autonóm működése emeli magas szintre. A Stuxnet után az Industroyer/CrashOverride volt a második olyan, ICS-eket célzó malware, ami emberi beavatkozás nélkül volt képes megzavarni az ICS-ekkel vezérelt fizikai folyamatokat.

2017 során a szakértők több nyilvános előadásban¹³⁰ [21] és cikkben¹³¹ [22] fogalmaztak meg olyan véleményeket (köztük Marina Krotofil, egy ukrán származású, Amerikában élő ICS biztonsági szakértő is), amelyek szerint az ukrán villamosenergia-rendszert ért támadások gyakorlatilag élesben végrehajtott tesztek voltak, itt próbálták ki az ismeretlen támadók az ipari (elsősorban közüzemi) célpontok elleni támadásokhoz használható eszközeiket és technikáikat.

6. További kibertámadások villamosenergia-ipari rendszerek ellen

2015-ig sem szakmai körökben, sem a sajtóban nem kaptak hangot azok a kiberbiztonsági incidensek, amik közvetett vagy közvetlen hatással voltak egyes villamosenergia-ipari szervezetekre.

Kézzel fogható bizonyítékok nem álltak és nem állnak rendelkezésre, de a 2003-as amerikai áramszünetet több neves IT biztonsági szakember is a Blaster féreg-támadásra vezeti vissza.¹³² [23]

¹²⁸ OPC DA: OLE for Process Control Data Access (Az OLE ipari automatizálásra specializált alkalmazási rendszere)

¹²⁹ R. M. Lee, M. J. Assante, T. Conway. „Analysis of the Malware Reportedly Used in the December 2016 Ukrainian Power System Attack” E-ISAC. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf (Letöltve: 2020. augusztus 28.)

A. Cherepanov, „Win32/Industroyer: a new threat for industrial control systems.” Eset. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf (Letöltve: 2020. augusztus 28.)

Dragos. „CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations” https://www.dragos.com/wp-content/uploads/SecIndSys_Purdue_GEDragos.pdf (Letöltve: 2020. augusztus 28.)

¹³⁰ K. Zetter. „The Ukrainian Power Grid Was Hacked Again.” Vice. https://www.vice.com/en_us/article/bmykn4/ukrainian-power-station-hacking-december-2016-report (Letöltve: 2020. augusztus 28.)

¹³¹ A. Greenberg. „How an Entire Nation Became Russia's Test Lab for Cyberwar.” Wired. <https://www.wired.com/story/russian-hackers-attack-ukraine/> (Letöltve: 2020. augusztus 28.)

¹³² M. Moyer. „Expert: A Virus Caused the Blackout of 2003. Will the Next One Be Intentional?” Scientific American. <https://blogs.scientificamerican.com/observations/expert-a-virus-caused-the-blackout-of-2003-will-the-next-one-be-intentional/> (Letöltve: 2020. augusztus 28.)



2015. december 21-én (két nappal az ukrán áramszolgáltatók elleni támadás előtt) jelent meg a Las Vegas Sun cikke¹³³ [24] az USA egyik legjelentősebb villamosenergia-ipari vállalata, a Calpine ellen még 2014-ben végrehajtott kibertámadásról. A támadók nem csak a cég vállalati rendszereit kompromittálták, hanem a szélerőművet vezérlő SCADA rendszer egyes elemeihez is hozzáférést szereztek és az egyik automata működésre konfigurált komponenst is át tudták állítani kézi szabályozásra.

2016. januárban a Times of Israel publikált egy cikket¹³⁴ [25], ami szerint az izraeli közműszabályozó hatóság több rendszerét érte súlyos támadás.

2016 októberében jelentek meg a sajtóban információk atomerőművek ellen végrehajtott kibertámadásokról. 2014-ben a publikált¹³⁵ [26] információk¹³⁶ [27] szerint a Japánban található Monju és a Dél-koreai Korea Hydro and Nuclear Power Plant ellen történtek támadások, 2016-ban pedig a Nemzetközi Atomenergia Ügynökség tisztviselője beszélt egy német (egyes források¹³⁷ [28][29] szerint a gundremmingeni) atomerőműben történt kiberbiztonsági incidensről.

2017 júliusában a Cisco-n belül működő Talos biztonsági labor publikált részleteket több ún. template injection¹³⁸ támadásról, amik egy része az amerikai villamosenergia-szektor egyes szervezeteit érte. Nevesítve a Wolf Creek-i atomerőmű és az amerikai Energiaügyi minisztérium lehettek a célpontok. Az érintettek egyaránt azt állították, hogy a támadók „csak” az ügyviteli hálózataikhoz szereztek hozzáférést.

¹³³ G. Burke, J. Fahey. „AP Investigation: U.S. power grid vulnerable to foreign hacks.” Las Vegas Sun. <https://lasvegassun.com/news/2015/dec/21/ap-investigation-us-power-grid-vulnerable-to-forei/> (Letöltve: 2020. augusztus 28.)

¹³⁴ T. Staff. „Steinitz: Israel’s Electric Authority hit by ‘severe’ cyber-attack.” The Times of Israel. <https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/> (Letöltve: 2020. augusztus 28.)

¹³⁵ P. Paganini. „Malware based attack hit Japanese Monju Nuclear Power Plant.” Security Affairs. <http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html> (Letöltve: 2020. augusztus 28.)

¹³⁶ P. Paganini. „Nuclear plant in South Korea hacked.” Security Affairs. <http://securityaffairs.co/wordpress/31416/cyber-warfare-2/nuclear-plant-south-korea-hacked.html> (Letöltve: 2020. augusztus 28.)

¹³⁷ P. Paganini. „Virus discovered at the Gundremmingen nuclear plant in Germany” Security Affairs. <https://securityaffairs.co/wordpress/46708/security/virus-gundremmingen-nuclear-plant.html> (Letöltve: 2020. augusztus 28.)

A. Shalal. „IAEA chief: Nuclear power plant was disrupted by cyber attack.” Reuters. <https://in.reuters.com/article/nuclear-cyber-idINKCN12A1P1> (Letöltve: 2020. augusztus 28.)

¹³⁸ Bővebben ld. <https://portswigger.net/web-security/server-side-template-injection> és https://portswigger.net/kb/issues/00200308_client-side-template-injection

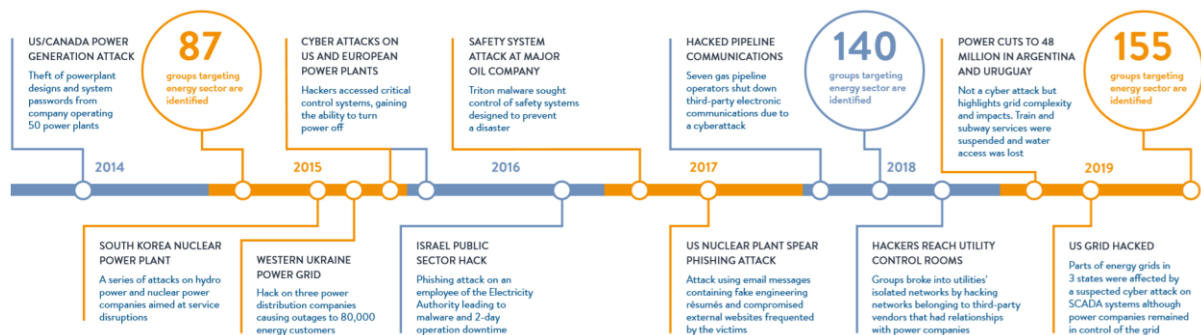


2017. augusztus 6-án jelent meg az ír Independent-ben egy cikk¹³⁹ [30], ami szerint az EirGrid ír rendszerirányító és észak-írországi leányvállalata, a SONI ellen intéztek támadást ismeretlenek, a becslések szerint 2 hónapig lehallgatva a két villamosenergia-ipari rendszerirányító hálózati forgalmát.

2018 júliusában az amerikai Belbiztonsági Minisztérium egy publikus webes előadás-sorozatát tartott az USA kritikus infrastruktúrája elleni orosz kibertámadásokról¹⁴⁰. 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. Érdekes megfigyelni a hasonlóságot a Havex-nél már bemutatott módszerrel, amikor európai ICS gyártók letölthető binárisait cserélték le malware-rel fertőzött változatokra, így támadva a kiszemelt szervezeteket.

2019. július végén a johannesburgi áramszolgáltató rendszereit érte ransomware-támadás, aminek következtében – bár az áramszolgáltató ICS-eit állításaik szerint nem érintette az incidens mégis – egyes ügyfeleknél, akik a feltöltő kártyás mobil telefont használókhoz hasonló módon előre fizettek a villamos áramért, hosszabb áramkimaradások voltak.

2019. szeptember közepén ismét az USA villamosenergia-rendszerének egyik szervezete elleni támadásról jelentek meg részletek.¹⁴¹ [31]



1.1. ábra: Hatásukban és számukban is növekvő incidensek¹⁴² [32]

¹³⁹ C. McMahon. „Exclusive: EirGrid targeted by 'state sponsored' hackers leaving networks exposed to 'devious attack'.” Independent.ie. <https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html> (Letöltve: 2020. augusztus 28.)

¹⁴⁰ Az előadás prezentációja a US-CERT weboldalon érhető el: https://www.us-cert.gov/sites/default/files/c3vp/Russian_Activity_Webinar_Slides.pdf

¹⁴¹ B. Sobczak. „Report reveals play-by-play of first U.S. grid cyberattack.” E&E News. <https://www.eenews.net/stories/1061111289> (Letöltve: 2020. augusztus 28.)

¹⁴² World Energy Council. „Cyber challenges to the energy transition.” https://www.worldenergy.org/assets/downloads/Cyber_Challenges_to_the_Energy_Transition_WEC MMC 2019.pdf (Letöltve: 2020. augusztus 28.)





Senkit nem téveszthet meg, hogy a 2015. és 2016. évi ukrajnai támadások óta nem fordult elő hasonló tömegű fogyasztói ellátatlanságot okozó kibertámadás. A kritikus infrastruktúrák – ezen belül a villamosenergia-rendszer – elleni támadások folyamatosan és növekedő számban zajlanak. Nem az a kérdés, hogy lesz-e újabb, jelentős fogyasztói ellátatlanságot okozó támadás, hanem az, hogy mikor lesz, hol lesz és hány fogyasztót fog érinteni. A kézikönyv célja a magyar kitettség csökkentésének a szakmai támogatása.



2. melléklet: A villamosenergia-rendszer kiberbiztonsága és az OSINT¹⁴³

1. Előzmény

Az ukrán villamosenergia-rendszer elleni, az 1. mellékletben részletesen bemutatott – de főleg a 2016. december 17-ei – kibertámadások elemzései azt valószínűsítik, hogy a támadó felkészülését nyílt forrású információk is jelentősen segíthették. Így a biztonságos villamosenergia-ellátás amúgy is összetett feltételrendszere új elemmel, a nyílt forrású információk körének az áttekintésével és szükség szerinti szűkítésével is kiegészítendő. Ez feladatot ró a stakeholderek-re.

Egy kibertámadás szempontjából elsődlegesen fenyegetett, azaz legjobban védendő szervezetek a villamosenergetikai ICS/SCADA rendszereket és berendezéseket tervező, gyártó, létesítő, üzemeltető társaságok, valamint egyre növekvő mértékben ezek beszállítói.

A kibertámadások előkészületeinek egyik meghatározó eleme a nyílt forrású információszerzés (OSINT), ami lehet passzív és aktív. Passzív OSINT esetén a támadó közösségi oldalakon, weboldalakon, fórumokon, újságokban elérhető, azaz publikus, minden feltétel nélkül, bárki által elérhető, megismerhető információkat gyűjt, amelynek ténye és végrehajtója többnyire rejtve tud maradni. Aktív OSINT esetén a támadó gondosan megtervezett és anonimizált módon végzi a célpont társaság hálózatának, informatikai rendszerének a felderítését.

2. Az OSINT technikák villamosenergetikai relevanciája



Az OSINT elleni eredményes védekezés előfeltétele, hogy a védekezők – adott esetben a villamosenergetikai társaságok vezetői – tisztában legyenek az ellenük bevethető OSINT technikákkal. Ezek látszólag kevés, önmagukban szinte használhatatlannak tűnő információmorzsához juttatják a támadót. A villamosenergetikai társaságok illetékes vezetőinek felelőssége annak felismerése, hogy hozzáértő támadó e nyílt forrású töredék információk komplex elemzésével a támadáshoz nagyon is fontos információk birtokába juthat.



A kritikus infrastruktúrák – közte hangsúllyal a villamosenergia-rendszer – kiberbiztonsága szempontjából szenzitív információk védelme óhatatlanul más jogok korlátozásával jár. Ugyanakkor az önvédelem minden állam alapvető és elidegeníthetetlen joga.

¹⁴³ Köszönet Droppa Béla és Kocsis Tamás értékes tanácsaiért.



A villamosenergetikában is alkalmazható néhány OSINT technika (a teljesség igénye nélkül):¹⁴⁴ [33]

2.1. Célszemélyek azonosítása

A támadási előkészületek első lépése a megtámadni tervezett villamosenergetikai célponthoz közvetlenül, vagy – akár áttételeken keresztül is – közvetve kapcsolódó személyek azonosítása, akik aztán további előkészületi lépések (pl. adathalászat) alkalmas célpontjai lehetnek. Ennek elsődleges forrásai mindenekelőtt a népszerű közösségi alkalmazások. A 2015. december 23-ai ukrajnai kibertámadás egyik fontos tanulsága, hogy a támadó számára messze nem csak a megcélzott villamosenergetikai társaság informatikusai lehetnek alkalmas célszemélyek, hanem pl. üzemirányítók. A támadás során a támadó az üzemirányítók személyazonosító adatait megszerezve hajtott végre ellátatlanságot okozó kapcsolásokat. A támadó e személyazonosító adatokat az ukrán energetikai minisztériuméhoz megtévesztésig hasonló adatkérő csatlévelek küldése nyomán szerezte meg.¹⁴⁵

Lehetőségek a célszemélyek azonosítására:

a. Közösségi alkalmazások

A megtámadni tervezett villamosenergetikai társasághoz tartozó, vagy kapcsolódó célszemélyek azonosításának az immár „hagyományos” forrásnak tekinthető Facebook, Instagram stb. mellett mindenekelőtt a LinkedIn, mint kifejezetten szakmai közösségi alkalmazás lehet alkalmas területe.

Magyarországon adottak a jogi feltételek a munkahelyi adatok közösségi médiában való közzétételének, azaz akár a munkavállaló személyiségi jogainak szükséges mértékű korlátozására¹⁴⁶, a közzé nem tehető adatok körének meghatározására. A munkaviszonyra vonatkozó adatok szabályellenes közzététele fegyelmi vizsgálatot alapozhat meg.

b. Előadások, szakmai publikációk

Az előadások, szakmai publikációk mind az előadók, szerzők neve, beosztása, mind az általuk közzé tett szakmai információk szempontjából a támadó hasznos információforrásai lehetnek.

¹⁴⁴ D. R. Hayes, „Using Open Source Intelligence for Risk Assessment to the U.S. Power Grid” presented at the 15th International Conference e-Society 2017, Budapest, Hungary, Apr. 10–12, 2017.

¹⁴⁵ D. E. Whitehead, K. Owens, D.s Gammel, J. Smith. „Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies.” presented at the Power and Energy Automation Conference, Spokane, WA, USA, March 21–23, 2017 [34]

¹⁴⁶ A Munka Törvénykönyvéről szóló 2012. évi I. törvény



Amennyiben az információ nem minősül minősített adatnak, vagy üzleti titoknak, úgy jogszabályi rendelkezés hiányában is a szervezet vezetőjének joga annak meghatározása, hogy a kritikus infrastruktúráról hol és milyen adat jelenhet meg.

c. Netes szakmai fórumok

E fórumokon, „bennfentes” szakmai közegben pl. a munkahelyénél aktuálisan megoldásra váró informatikai problémák megosztásával nagyobb az esélye olyan információk óvatlan közreadásának, amelyek segítséget nyújthatnak egy a cége elleni támadás megtervezésében, a lehetséges sérülékenységek azonosításában.

2.2. Célszervezet hardver és szoftver elemeinek beazonosítása

Míg a fentebb sorolt technikákkal a támadó a „ki által?” kérdés megválaszolásához találhat nyilvánosan elérhető információkat, addig más technikák a „mit” kérdés megválaszolásában segíthetik.

a. Karrier információk

Gyakran a villamosenergetikai társaságok is élnek az üres álláshelyek honlapjaikon való megjelenítésének lehetőségével. Informatikai pozíciók meghirdetése esetében a szükséges ismeretekre, elvárt gyakorlatra vonatkozó információk is hasznosak a támadónak, mivel képet adnak az adott villamosenergetikai társaságnál használatban lévő operációs rendszer(ek)ről, alkalmazásokról stb., így ezek ismeretében tudja hatékonyabbá tenni a támadást.

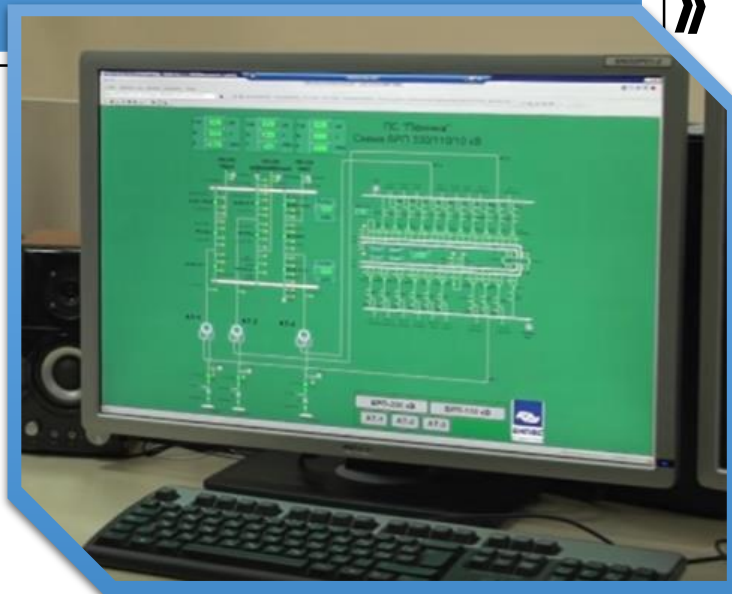
Az állashirdetéseknek nincsen jogszabályban meghatározott kötelező minimum vagy maximum tartalmi eleme, azaz az abban megjeleníthető információk körét szintén a szervezet vezetője jogosult korlátozni.

b. Fényképek, videók

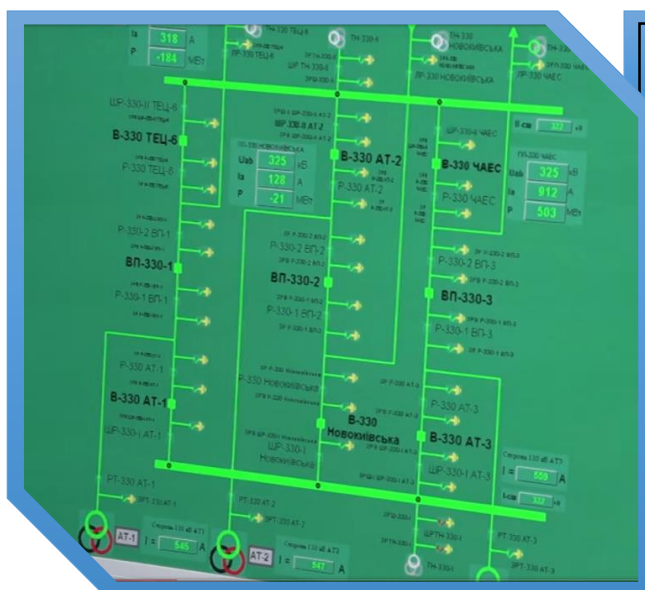
A Stuxnet vírus kapcsán megjelent elemzések egyik tanulsága, hogy akár egy energetikai létesítményben végzett óvatlan propaganda fotózás is milyen hihetetlen mennyiségű és érzékenységgű információhoz juttathat egy támadót.



A 2016. december 17-ei ukrajnai kibertámadás kapcsán még évekkel később is érdemes rákérteni az érintett Pivnichna (észak) 330/110/35 kV átviteli hálózati alállomásra. A 2010-es évek közepén az alállomáson felújítás zajlott, amelyre az Ukrenergo büszke volt, egyebek mellett sajtóbejárást is szervezett. Erről a YouTube-on „Прес-тур на ПС 330 кВ "Північна" (Sajtó bejárás a Pivnichna-i 330 kV-os alállomáson) címmel egy 2015. szeptember 15-én feltöltött videó található.¹ Ezen 00:23 percnél megjelenik a teljes alállomási primer diszpozíció:



2.1. ábra: Az alállomási kapcsolási séma a Pivnichna-i vezénylő monitorán



Aztán 01:00 percnél megjelenik a 330 kV-os részletes diszpozíció is:

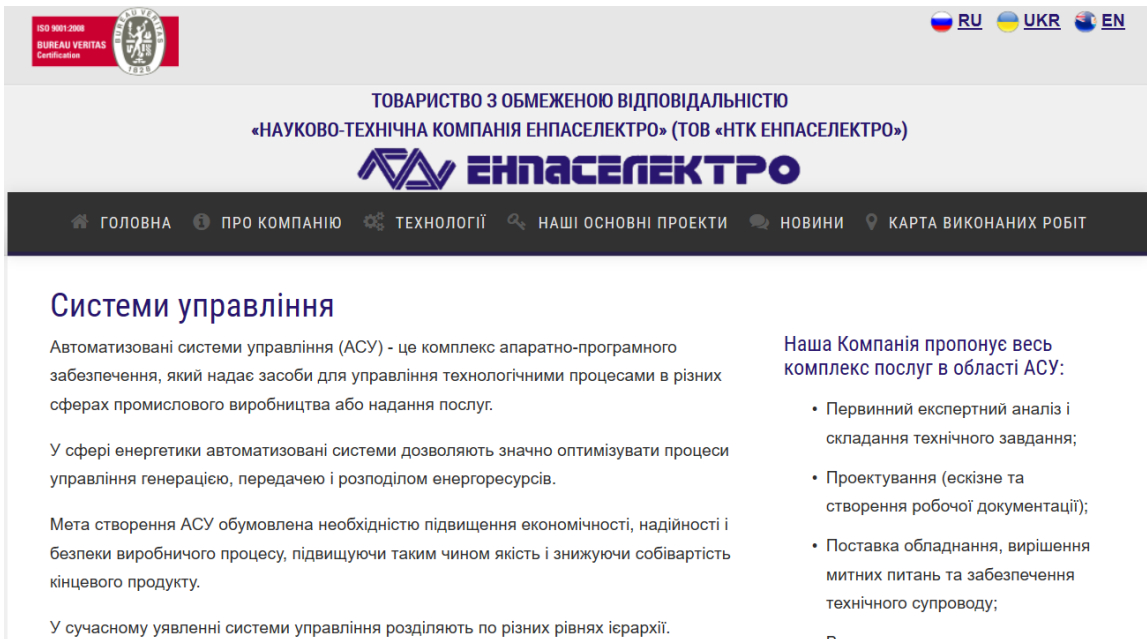


2.2. ábra: Az alállomási 330 kV-os diszpozíció a Pivnichna-i vezénylő monitorán



c. Honlapok

Ukrán nyelvet beállítva a Google-n és rákeresve a „Північна 330/110/10 підстанції схема” kifejezésre egyebek mellett elérhető a 2.3. ábra szerinti tervező cég honlapja:

The screenshot shows the website of ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «НАУКОВО-ТЕХНІЧНА КОМПАНІЯ ЕНПАСЕЛЕКТРО» (ТОВ «НТК ЕНПАСЕЛЕКТРО»). The website features a navigation bar with links: ГОЛОВНА, ПРО КОМПАНІЮ, ТЕХНОЛОГІЇ, НАШІ ОСНОВНІ ПРОЕКТИ, НОВИНИ, and КАРТА ВИКОНАНИХ РОБІТ. The main content area is titled "Системи управління" (Control Systems) and describes automated control systems (АСУ) for industrial production. It mentions that these systems allow for significant optimization of processes in the energy sector, such as generation, transmission, and distribution of energy resources. The website also lists services offered by the company, including expert analysis, project design, and equipment supply.

2.3. ábra: Az Enpaszelektro honlapja¹⁴⁷

¹⁴⁷ <https://enpaselectro.com/ua/tehnologii/sistemy-upravleniya.html>



A honlapon a 2.4. ábra szerinti részletes információk találhatóak a Pivnichna-i alállomásról:



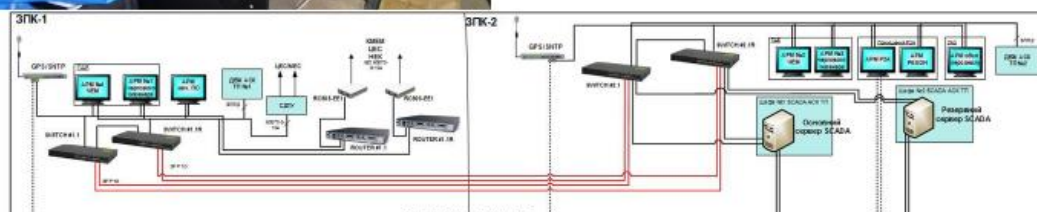
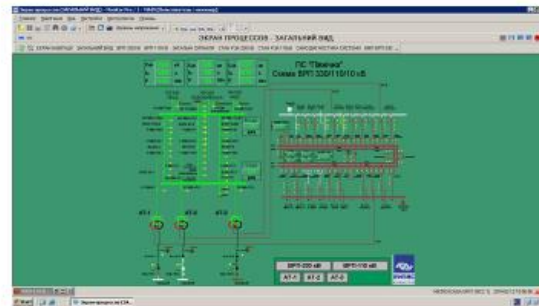
ГОЛОВНА ПРО КОМПАНІЮ ТЕХНОЛОГІЇ НАШІ ОСНОВНІ ПРОЕКТИ НОВИНИ КАРТА ВИКОНАНИХ РОБІТ

Реалізовані проекти

2012-2014 рік - Розширення та реконструкція ПС 330/110/10 кВ "Північна" в частині: Автоматизована система управління технологічними процесами ПС 330/110/10 кВ "Північна"

Комплекс робіт :

- Проектування (стадія П і РД);
- Поставка обладнання системи АСУТП (сервери, комунікаційне обладнання, RTU);
- Монтаж і збірка шаф системи;
- Налаштування мережі системи;
- Налаштування серверного обладнання та RTU;
- Створення бази даних системи;
- Створення інтерфейсів системи;
- Налаштування комунікацій між різними апаратами управління в енергосистемі;
- Підготовка виконавчої документації;
- Сервісне обслуговування системи;



2.4. ábra: Információk a Pivnichna-i alállomás irányítástechnikájáról



A példák igazolják, hogy óvatlan alvállalkozói kommunikációval egy potenciális támadó számára milyen, az OSINT keretében jól kutatható szenzitív adatok válhatnak elérhetővé.

Hazai viszonyok között a kritikus infrastruktúra üzemeltetője az általa kötelezően készítendő ún. üzemeltetői biztonsági tervben rögzítendő eljárásrend szerint a beszállítóval kötött beszállítói szerződésben (illetve felektől függően egyéb megnevezésű, de ilyen tartalmú dokumentumban) korlátozhatja a megjeleníthető adatokat. E korlátozások rögzítése és következetes érvényesítése az adott kritikus infrastruktúra vezetésének felelőssége.

d. Beszállítói referencialisták

A potenciális támadó számára értékes információk forrása az informatikai beszállítók által esetenként honlapjaikon is közzétett referencialista. Az adott beszállító termékjellemzőinek az ismeretében a támadó képet tud alkotni pl. egy adott villamosenergetikai társaságnál fellelhető informatikai megoldásokról.

A 2.5. ábra a befejezett projektek bemutatása keretében ad közre érzékeny információkat a Pivnichna-i alállomás irányítástechnikai rendszeréről.



General description

The project is based on IEC61850 standard. The modern relay protection and automation equipment manufactured by ABB, GE and Siemens, fully integrated into automation control system, were installed in the substation.

Substation automation control system is based on MicroSCADA Pro 9.3 software. The system implements algorithms for control of switching devices and interfaces to monitor the status of the main substation equipment.

Provided information exchange facilities between the substation and power system dispatch center. After the system installation our specialists provided training for substation and power system personnel, as well as continue to provide service support.

2.5. ábra: Pivnichna-i irányítástechnikai rendszer leírása

A szerződő felek a szerződésben a jogszabályok adta keretek között minden, számukra lényeges kérdésről jogosultak rendelkezni, a beszállítói, valamint titoktartási kötelezettségek körében feltüntetni. Kritikus infrastruktúra esetében a szerződésben helye van a szenzitív adatok megjelenítési korlátozásának is.

e. Berendezések publikus hardver, szoftver és paraméterezési leírásai. Termékkatalógusok

A villamosenergetikai társaságok informatikai beszállítói esetenként a honlapjaikon is elérhetővé teszik termékeik hardver, szoftver és paraméterezési leírásait. Ez kitűnő lehetőség



a támadónak, hogy részletes információkat szerezzen a megtámadni kívánt eszközről, rendszerről. Ezzel esetenként maguk a beszállítók segítik elő megrendelőjük megtámadását.

A jogi helyzet azonos a 2.2.d. pontban írtakkal.

f. Tenderkiírások

Egy hosszú távra tervező támadó számára hasznos információforrásul szolgálhatnak a villamosenergetikai cégek informatikai beszerzéseire vonatkozó nyilvános tenderfelhívások. Ezekből a támadó képet alkothat arról, hogy az adott cégnél idővel milyen informatikai megoldások jelenlétével számolhat.

Jogilag kényes kérdés, mivel nyilvános és önmagukban értékkel nem bíró információk gyűjtésével és célirányos feldolgozásával létrejövő származtatott információ minősítési szintjét érinti úgy, hogy a tender kiírójának úgy kell óvnia a biztonságát, hogy közben a verseny tisztaságát és nyíltságát sem veszélyeztetheti. Bár a jogszabályi keretek adottak, de az egyébként nyílt adatok biztonsági érdekből nem nyilvánossá minősítésének még nincs gyakorlata. Ennek megtörténteig a támadó lépéselőnyben marad.

2.3. Célhálózat gyenge pontjainak azonosítása: hálózati topológia

Hozzáértő támadó számára a nyilvánosan elérhető villamos hálózati topológiák is hasznos adatforrások. Ezek bármely módon való elérhetővé tétele segítheti a támadót a támadni tervezett hálózat megismerésében, a lehetséges gyenge pontok azonosításában, priorizálásában, végül a támadási célpont meghatározásában.

Jelenleg még nincsenek átfogó és általánosan elfogadott megoldások az OSINT technikák révén a villamosenergia-rendszert fenyegető kockázatok kezelésére. De már önmagában e technikák veszélyeinek a felismerésével, majd a kockázatot hordozó információk körének a fokozatos korlátozásával is nehezíthető a potenciális támadó felkészülése, ezzel is csökkentve egy esetleges kibertámadás esélyét.

3. OSINT célú alkalmazások

Az OSINT elsődleges terepe az internet. A nyílt forrásokon alapuló, előző pontban vázolt információk megszerzését számos, akár ingyenesen is elérhető OSINT alkalmazás segíti. Már ezek is impresszív mennyiségű és minőségű információ összegyűjtésére alkalmasak. Ennek tükrében a villamosenergetikai társaságok illetékes vezetőinek különösen indokolt észben tartania, hogy egy akár állami háttérrel, azaz jelentős erőforrásokkal is rendelkező támadó számára nem lehet akadály sem az ingyeneseknél is lényegesen több és érzékenyebb információ gyűjtésére alkalmas fizetős eszközök beszerzése, sem pedig fejlett, rejtett vagy



titkos információgyűjtő eszközök alkalmazása, vagy akár egyedi eszköz kifejlesztése.^{148 149} [35]

Néhány példa a széles körben használt OSINT alkalmazásokra: Shodan, Censys, theHarvester, Recon-ng, OSINT Framework, GHDB (Google Hacking Database), Maltego, Spiderfoot.

4. Az OSINT elleni védekezés lehetőségei

Az OSINT elleni eredményes védekezés elsődleges feltétele rendszeres képzés és tréning révén a megvédendő társaság vezetőinek és alkalmazottainak magas szintű biztonságtudatossága. További előfeltétel a nyílt forrású információk körének, mindenekelőtt az adott társaság „digitális lábnyomának” a szűkítése. Ennek érdekében célszerű rendszeres társasági önellenőrzések, sérülékenységvizsgálatok végzése; az IP-címek és tartományok blokkolása; az elérhetővé teendő dokumentumok publikáció előtti előzetes biztonsági ellenőrzése (pl. a metaadatokra is kiterjedően); a társasággal kapcsolatban a beszállítók anyagaiban megjelenő információk ellenőrzése, a szenzitívek törltetése.¹⁵⁰ [36]

Hangsúlyozni kell, hogy az eredményes OSINT elhárítás csak a társaság vezetőinek és alkalmazottainak közös erőfeszítésével biztosítható. A villamosenergetikai társaságoknak – mint a kritikus infrastruktúrák között is kiemelt fontosságú rendszerek üzemeltetőinek – az OSINT kockázatok ismeretében célszerű az alapoktól áttekinteniük a róluk nyílt forrásból elérhető információk körét, majd szükség szerinti szigorításokkal szűkíteniük azt.

5. Összegzés

Miközben a villamosenergia-rendszer elsődleges célpontnak számító társaságai fokozatosan erősítik a kiberbiztonságukat, a támadók figyelme e társaságok általában alacsonyabb védelmi szintű beszállítói felé fordul és rajtuk keresztül próbálnak bejutni az elsődleges célpontok rendszereibe. Emiatt szigorodó követelményeket kell támasztani a beszállító társaságoktól megkövetelendő kiberbiztonság, így az OSINT által náluk elérhető, a megrendelő számára érzékeny információk körének szűkítése tekintetében is.

A támadók rendszerirányítók, illetve egyéb kapcsolódó szervezetek iránti növekvő érdeklődése is figyelmet érdemel.

¹⁴⁸ The Recorded Future Team. „What Is Open Source Intelligence and How Is it Used?”. <https://www.recordedfuture.com/open-source-intelligence-definition/> (Letöltve: 2020. augusztus 28.)

¹⁴⁹ <https://github.com/jivoi/awesome-osint>

¹⁵⁰ J. Elder. „Open Source Intelligence (OSINT) for OT: What adversaries can learn about your organisation and what you can do.” Applied Risk. <https://applied-risk.com/resources/osint> (Letöltve: 2020. augusztus 28.)



Az ilyen jellegű szervezetek azért is hasznos célpontok a villamosenergia-rendszer potenciális támadóinak, mert egyetlen sikeres támadással több villamosenergetikai cég sikeres támadását elősegítő érzékeny információkhoz is hozzájuthatnak.¹⁵¹ [37]

¹⁵¹ Dragos. „Energy Organizations Continue to be Compromised Globally.” <https://www.dragos.com/blog/industry-news/energy-organizations-continue-to-be-compromised-globally/> (Letöltve: 2020. augusztus 28.)



3. melléklet: Fenyegetettségi térkép

1. Összegzés

A fenyegetettség-térkép (Threat landscape) egy adott domain-t, esetünkben a villamosenergia alágazatot, kiemelten a létfontosságú rendszereket, rendszerelemeket veszélyeztető fenyegetettségek, a kapcsolódó támadó profilok/modellek és a támadási trendek gyűjteménye, katalógusa. A térkép több szintű lehet, a támadás-kategóriákat, támadási vektor-típusokat átfogó felső szintű elemzéstől a konkrét támadásokat, azok eszközeit tárgyaló részletes analízisig terjedhet. A kézikönyv az alágazat szempontjából releváns kibertámadás-típusokat, típus támadásokat áttekintő jelleggel tárgyalja. Az elemzés a fenyegetettségeket és trendeket elsődlegesen a támadási vektorok és az egyes támadó profilok, modellek (aktorok) alapján mutatja be, konkrét támadási módszerekre, metódusokra részleteiben nem tér ki. A dokumentum nem tárgyalja azon, környezeti (elemi, természeti csapások, ökológiai hatások), illetve társadalmi (háború, lázadás, terror-cselekmény stb.) eredetű fenyegetettségeket, tényezőket, amelyek nem specifikus, kiberbiztonsági fenyegetettségként értékelendők.

A fenyegetettség-térkép első fejezete a domain szempontjából releváns támadási vektorokat, biztonsági problémákat, kihívásokat áttekintő jelleggel tárgyalja. A második fejezet a domain szempontjából releváns támadó profilokat/modelleket, azaz a szóba jöhető aktorokat mutatja be. A komplex, átfogó fenyegetettség-térkép harmadik eleme a domainben történt konkrét támadások feldolgozása (a támadók, módszerek és következmények áttekintése), amely a SeConSys keretében végzett munka során már áttekintésre, elemzésre került, így e helyütt külön nem térünk ki rá.

2. Támadási vektorok

2.1. Sérülékenységeket kihasználó támadások

A sikeres támadások mindig valamilyen, a megtámadott rendszerben található (egy vagy több) sérülékenység kihasználására épülnek. A sérülékenységek a rendszer minden szintjén, illetve a rendszert üzemeltető szervezet működésében is megtalálhatóak. Lehetnek:

- fizikai,
- logikai jellegűek,
- a szervezet eljárásrendjeivel, működési- és munkafolyamataival kapcsolatosak, vagy
- humán természetűek.



A *fizikai sérülékenységek* a rendszer fizikai védelmi megoldásaiban található hibák. Ilyenek lehetnek az egyszerűen nyitható zárok, az őrzés nélkül hagyott bejáratok, a folyosón elhelyezett, bárki által hozzáférhető hálózati eszközök és csatlakozók, az elektromágneses árnyékolás hiánya stb. Ezen sérülékenységek a fizikai támadás és behatolás különböző formáit teszik lehetővé.

A *logikai sérülékenységek* a számítógépes (köztük az ICS/SCADA) rendszerekben található hibák, amelyek logikai szintű támadásokat tesznek lehetővé. Logikai sérülékenységek előfordulhatnak tervezési és implementációs szinten, mind a rendszert alkotó hardver elemekben, mind pedig a szoftver komponensekben. Egy alkalmazásban található programozói hiba szoftvert érintő implementációs szintű sérülékenységnak tekinthető, míg egy kriptográfiai protokoll Man-in-the-Middle¹⁵² támadást lehetővé tevő hibája tervezési szintű sérülékenység.

A szervezet *eljárásrendjeiben, működési- és munkafolyamataiban található sérülékenységek* olyan procedurális hibák, amelyek kihasználása nagymértékben segítheti a rendszer elleni fizikai és logikai támadások kivitelezését. Ilyen hiba lehet pl., ha a rendszeres jelszócsere nem kikényszerített, ha egyetlen rendszergazda hozzáférhet minden kritikus rendszerhez, ha a felvételi eljárásban nem ellenőrzik a jelentkezők megbízhatóságát, ha nincs előírva, hogy egy alkalmazott munkaviszonyának megszűnésekor haladéktalanul vissza kell vonni minden hozzáférési jogosultságot stb.

A *humán erőforrást érintő hibák* kihasználása ugyancsak segítheti a rendszer elleni fizikai és logikai támadásokat. Ilyen típusú hiba pl. a személyzet anyagi megbecsülésének alacsony szintje, vagy egyéb, a személyzet elégedetlenségét növelő hiányosság, amely csökkenti a szervezet iránti lojalitást, zsarolhatóvá teszi az alkalmazottakat. Szintén ebbe a kategóriába tartozó hiba, ha a szervezet elmulasztja a biztonságtudatosság kialakítását és szinten tartását.

A sérülékenységek létezésével folyamatosan számolni kell. A szervezetek és az általuk használt fizikai és logikai (számítógépes) rendszerek felépítése többnyire komplex, nehezen átlátható, ami hibalehetőséget rejt magában. Ráadásul a technológia fejlődésével a rendszerek komplexebbé válása figyelhető meg, amely komplexitás általában nem teszi lehetővé a kimerítő hibakeresést (tesztelést) vagy a hibamentesség formális úton történő bizonyítását. A sérülékenységek folyamatos jelenléte annak is köszönhető, hogy a rendszereket emberek tervezik és implementálják, általában szoros határidők és limitált költségvetés mellett. Valamennyi sérülékenység azonosítása és kijavítása lehetetlen, a sérülékenységek létezését tehát el kell fogadni, azaz folyamatosan törekedni kell a sérülékenységek azonosítására, az ismert sérülékenységekkel kapcsolatos kockázatok felmérésére és az arányos

¹⁵² MitM: Man-in-the-Middle (Közbeékelődéses támadás)



ellenintézkedések megtételére, ami a sérülékenység teljes megszüntetését, áthidaló megoldások bevezetését, vagy adott esetben a sérülékenység változatlanul hagyását és a kockázat elviselését, vagy nem technikai eszközökkel történő módon (pl. biztosítás kötésével) történő kezelését egyaránt jelentheti.

Ismert az a sérülékenység, amely már azonosításra került, ugyanakkor a legtöbb sérülékenység nem azonosított. Az ismert sérülékenységeket két osztályra bonthatjuk aszerint, hogy a sérülékenységgel kapcsolatos információk publikusan elérhetőek vagy sem; ha egy felfedezett sérülékenységhez kapcsolódó információk publikusan elérhetőek, akkor *publikusan ismert sérülékenységről* beszélhetünk. A nem publikusan ismert sérülékenységeket *zero-day sérülékenységeknek* nevezzük. A publikusan ismert sérülékenységekkel kapcsolatos információk a támadók számára is elérhetőek. Egy sérülékenységgel kapcsolatos adatbázis bejegyzés tartalmazza az érintett rendszerek specifikációját, a sérülékenység rövid leírását, becsült hatását és kihasználhatóságát (exploitability¹⁵³), valamint referenciákat a sérülékenység javítását biztosító megoldásokra és eszközökre.

Az ipari rendszerek szempontjából fontos a Shodan kereső rendszer¹⁵⁴, amely az interneten elérhető beágyazott eszközöket térképezi fel és tartja nyilván. Segítségével a támadó potenciálisan sérülékeny beágyazott eszközöket azonosíthat egy adott földrajzi környezetben. A támadó információt kap az így megtalált eszközökön futó szolgáltatásokról (nyitott portokról), azok esetlegesen hibás konfigurációjáról (pl. default jelszó beállítás), a rendszerekre és eszközökre vonatkozó publikusan ismert sérülékenységekről és az alkalmazható exploitokról. A kereső segítségével a támadó SCADA és egyéb ipari folyamatirányítási rendszerekhez tartozó, az interneten elérhető beágyazott eszközöket is kereshet. A publikusan ismert sérülékenységekkel kapcsolatos információk természetesen a rendszerek üzemeltetői számára is rendelkezésre állnak. Ennek ellenére a legtöbb sikeres támadás mégis sérülékenységeket használ ki.

Az ismert sérülékenységek megszüntetésének hiánya jellemzően üzemeltetői vagy gyártói hanyagságból fakad. Ha a sérülékenység javítása a gyártó érdekkörébe tartozik, az üzemeltető kénytelen megvárni, amíg a gyártó a hibát javítja, ám a javításig ki van téve a sérülékenység kihasználásából származó veszélynek. Az ipari termelő és gyártó létesítmények esetében továbbá számolni kell azzal is, hogy az üzemeltető – bár technikailag képes lenne rá – szándékosan nem javít ki egy ismert hibát, mivel a javítás olyan változtatást jelentene a rendszerben, amelyet alapos tesztelés, hatáselemzés, és adott esetben egy felügyelő szervezet formális jóváhagyása vagy engedélye nélkül nem lehet végrehajtani. Amikor egy sérülékenység nem szüntethető meg azonnal, olyan áthidaló (work-around) megoldásokat kell

¹⁵³ exploitability: kihasználhatóság

¹⁵⁴ <https://www.shodan.io>



alkalmazni, amelyek a rendszer szolgáltatásait nem befolyásolják, de a sérülékenység potenciálisan káros hatásait minimalizálják.

A fejlettebb technikai tudással rendelkező támadók folyamatosan keresik a még nem ismert sérülékenységeket. A támadó számára nagy előnyt jelent, ha korábban még nem azonosított sérülékenységet talál, mivel a zero-day sérülékenység nincs kijavítva, így a támadó nagy valószínűséggel sikeresen és többnyire észrevétlenül tudja azt kihasználni. Mivel a kihasználható sérülékenységek azonosítása technikailag nehéz feladat, amely speciális és mély tudást igényel, ugyanakkor a zero-day sérülékenységek nagy értéket képviselnek a támadók számára, ezért a sérülékenység-keresés jövedelmező üzleti tevékenység. A zero-day sérülékenységeket kihasználó exploit-okat jobbra célzott támadásokban használják a támadók. A célzott támadások jól kidolgozottak és egy szűk csoportra szabottak, ezért a támadó lebukásának valószínűsége kicsi. Ha idővel a támadást mégis detektálják és sikerül kideríteni, hogy milyen publikusan nem ismert sérülékenységeket használt ki a támadó, akkor a zero-day sérülékenységből publikusan ismert sérülékenység lesz. Ugyanakkor egy ilyen frissen publikussá vált sérülékenység még mindig sokáig használható marad, mivel javítása nem mindenhol történik meg azonnal, akár évekig kihasználható biztonsági rést jelenthet.

Hosszabb ideje publikusan ismert sérülékenység esetén elképzelhető, hogy már publikáltak egy, a sérülékenységet kihasználó exploit-ot, azt a támadók által használt fórumokon „forgalomba hozták”, esetlegesen a támadók önállóan fejlesztették ki az eszközt. Exploit keretrendszerek (pl. Metasploit framework) online, ingyenesen is elérhetőek, léteznek speciális, kifejezetten SCADA sérülékenységeket kihasználó exploit-okat tartalmazó exploit csomagok is.

2.2. Fizikai behatolás

A fizikai behatolás, mint támadási vektor, elsődlegesen nem kiberbiztonsági kérdés, ugyanakkor meg kell említeni két olyan esetet, amikor a fizikai és a logikai biztonság összemosódik. Az első az az eset, amikor a támadó fizikailag hozzáfér egy programozható rendszerhez. A fizikai hozzáférés általában erősebb, komolyabb következményekkel járó logikai támadást tesz lehetővé. Ha pl. a rendszerelem egy szerver vagy egy hálózati eszköz, akkor a fizikai hozzáférés konzol szintű elérést biztosít, ami a szerveren vagy hálózati eszközön végzett műveletek egy bővebb halmazát jelenti a távoli hozzáféréshez képest. A fizikai hozzáférés a rendszerelem gyártója által specifikált interfészek megkerülését is lehetővé teheti. A beágyazott eszközök (pl. fejlesztési és tesztelési célból) sokszor rendelkeznek JTAG¹⁵⁵

¹⁵⁵ JTAG: Joint Test Action Group (áramkörvizsgálati módszerekkel foglalkozó szakmai szervezet, illetve az IEEE-1149.1 szabvány által meghatározott módszer az integrált áramkört lapok/rendszerek gyors és automatikus tesztelésére)



interfészszel, ám ez az interfész általában a kész terméken már nem elérhető.

Fizikai hozzáférés esetén a JTAG interfész reaktiválható, hozzáférhetővé tehető, így közvetlenül elérhetővé válik az eszköz memóriája, illetve megfigyelhető belső működése.

Általában, ha a rendszerelem, eszköz nem kifejezetten bontásellenálló (tamper resistant), akkor a fizikai hozzáférés a támadó számára lehetővé teszi a rendszerelemen tárolt adatok (beleértve bizalmas információk, mint jelszavak és kriptográfiai kulcsok) kiolvasását, valamint a rendszerelemen, eszközön futó programok módosítását is. A fizikai hozzáférés, még a bontásellenálló eszközök esetén is előnyöket jelent a támadó számára, mert lehetővé teszi olyan ún. side-channel¹⁵⁶ információk (pl. pontos időzítések, áramfelvétel) megfigyelését, amelyek a távoli támadó számára nem elérhetőek, viszont logikai támadások alapjául szolgálhatnak.

A második eset, amikor a fizikai védelmi rendszerek programozható számítógépes rendszereket is tartalmaznak. Tipikus példa a beléptető rendszer, amely alapvetően egy fizikai behatolás védelmi rendszer, ám a belépő kártyák, a kapuknál található kártyaolvasók, a belépési jogosultságokat tároló szerver és az annak elérését biztosító hálózat lényegében egy számítógépes rendszert alkotnak. Hasonlóan, egy folyamatos megfigyelést biztosító kamera rendszer, az ahhoz tartozó archív tárolókkal, keresési funkciót biztosító szerverekkel, megjelenítő képernyőkkel és az összeköttetést biztosító hálózattal lényegében egy számítógépes rendszer, amely fizikai védelmi funkciókat lát el. A fizikai behatolás ebben az esetben nem mint támadási vektor merül fel, hanem mint egy, a fenti számítógépes rendszerek valamelyike ellen sikeresen kivitelezett logikai támadás nem kívánt következménye. Más szavakkal a fenti rendszerek kompromittálása lehetővé teheti vagy megkönnyítheti a támadó számára a védett objektumba történő fizikai behatolást, csökkentheti a behatolás által kiváltott ellenintézkedések hatékonyságát.

2.3. Hálózati behatolás

A számítógépes rendszerek ritkán működnek teljesen izolált környezetben; a legtöbb rendszerre inkább az a jellemző, hogy kommunikációs hálózatokon vagy dedikált csatornákon keresztül összeköttetésben állnak más belső alrendszerekkel, külső beszállítók, partnerek számítógépes rendszereivel, vagy akár publikus távközlő hálózatokon keresztül vagy az internet felől is elérhetőek. Hálózati behatolásról akkor beszélünk, amikor a támadó ezen kapcsolatokat kihasználva, jellemzően távolról kompromittálja a rendszert.

¹⁵⁶ side-channel: kerülő út



A hálózati behatolás tipikus példája, mikor a támadó egy kívülről elérhető hálózati szolgáltatásban fedez fel kihasználható hibát, és megfelelő inputok segítségével távolról átveszi egy belső rendszerkomponens felett az irányítást. Általában már az is támadásnak minősül, ha a támadó nem tudja átvenni az irányítást, de az általa kívülről bejuttatott inputok hatására a rendszer hibás szolgáltatást nyújt, vagy nem tudja biztosítani az elvárt szolgáltatásminőséget. A hálózati behatolás lehetséges másik formája, amikor a rendszer hálózaton keresztül történő távoli hozzáférést biztosít hitelesített felhasználók vagy szolgáltatások számára, és a támadó a távoli hozzáféréshez szükséges hitelesítő információkat szerzi meg, amelyek segítségével valamely legitim felhasználó vagy szolgáltatás nevében tud távolról belépni a rendszerbe. A támadáshoz szükséges hitelesítő információhoz a támadó többféle módon is hozzájuthat, egyszerű jelszavak használata esetén megpróbálhatja a jelszót kitalálni, kipróbálhat ismert jelszavakat, vagy egy előre szerkesztett szótár szavait és azok egyszerű kombinációit, esetleg kimerítő kereséssel végig próbálgathatja az összes lehetséges jelszót. Kriptográfiai hitelesítés esetén megpróbálhat hibát keresni az alkalmazott protokollban. Ez általában valamilyen Man-in-the-Middle (MitM) típusú támadást igényel, ahol a támadó beékelődik a szerver és a legitim felhasználó közé, így lehallgathatja, valamint tetszőlegesen manipulálhatja a szerver és a felhasználó között zajló kommunikációt. A fentiek mellett, a támadó social engineering módszerek útján is hozzájuthat hitelesítő adathoz, pl. rávehet egy legitim felhasználót arra, hogy mondja el neki a jelszavát.

A hálózati behatolások elleni hatékonyan megelőzési és érzékelési módszerek kombinációjával lehet védekezni. Létfontosságú vagy különösen magas fokú üzembiztonságot igénylő rendszerek – mint amilyenek a villamosenergia-ipari ICS/SCADA-k – esetében azonban nagyobb hangsúlyt kell fektetni a megelőzésre, mert üzembiztonsági szempontból egyes szolgáltatások legcsekélyebb mértékű kiesése sem tolerálható. A megelőzés és érzékelés együttes érvényesítését szolgálja a hálózat szegmentálására épülő mélységi védelem elvének érvényesítése.

2.4. A támadók behatolás utáni lépései

Privilegium-szint emelés (privilege escalation¹⁵⁷): miután a támadó sikeresen bejutott a rendszerbe, általában további lépéseket kell tennie célja eléréséhez. A bejutás többnyire olyan rendszerelemen keresztül történik, ami kihasználható sérülékenységgel rendelkezik, de általában nem ez a rendszerelem a támadó végső célpontja, csak a hozzáférés első lépcsőfoka. A támadó sok esetben nem rendszergazda, csak korlátozott jogosultságokkal és lehetőségekkel rendelkezik, ezért gyakori, hogy a bejutás után privilegium szint emelést hajt

¹⁵⁷ privilege escalation: jogosultsági szint emelés



végre és rendszergazda (root¹⁵⁸, superuser¹⁵⁹, administrator¹⁶⁰) jogosultságot szerez. A privilégium szint emelés a kompromittált rendszerelem operációs rendszerében található további sérülékenységek kihasználásával érhető el.

A privilégium szint növelésének másik lehetséges útja a bejutás utáni jogosultságok felhasználása olyan információk gyűjtésére, amelyek lehetővé teszik még több jogosultság megszerzését.

Perzisztencia biztosítása: megfelelő jogosultságok birtokában a támadó konfigurációs beállításokat végezhet és programokat telepíthet a rendszerben. Sokszor az első dolog, amire a támadó ezt a képességét felhasználja a folyamatos jelenlét (perzisztencia) biztosítása. Ennek eszköze lehet olyan backdoor-ok¹⁶¹ telepítése, amelyek lehetővé teszik, hogy a támadó később is be tudjon távolról lépni a rendszerbe. Ennek érdekében a támadó elindíthat egy hálózati szolgáltatást, ami távoli hozzáférést biztosít, vagy létrehozhat egy új felhasználói fiókot, amelynek segítségével a rendszerben esetleg már eleve létező távoli hozzáférés lehetőséget tudja kihasználni. Megfelelő konfigurációs beállításokkal a támadó elérheti, hogy a kiskaput biztosító szolgáltatások, programok, vagy program modulok akkor is elinduljanak vagy betöltődjenek, ha időközben a rendszert kikapcsolták és újraindították. A támadó mindemelett olyan rosszindulatú programokat (rootkit¹⁶²-eket) telepíthet, és konfigurációs beállításokat végezhet, mellyel elrejtetheti jelenlétét.

Oldalirányú mozgás (lateral movement¹⁶³): ha a támadó megszerezte a megfelelő jogosultságokat, biztosította a folyamatos és rejtett jelenlétét, megkezdheti a rendszer feltérképezését, további, immár belső információk gyűjtését, a támadás szempontjából érdekes rendszerelemek azonosítását és kompromittálását. Ez a folyamat az oldal irányú mozgás (lateral movement), amelynek célja a támadás célpontjául szolgáló rendszerelem elérése és kompromittálása. Oldalirányú mozgás közben a támadó hasonló eszközöket használ, mint az első bejutás alkalmával, de ebben a fázisban már több jogosultsággal, adott esetben teljes rendszer szintű adminisztrátori jogosultsággal rendelkezik. A jogosultságok birtokában és/vagy sérülékenységeket kihasználva további támadó eszközök telepíthetőek, vagy a meglevők frissíthetőek, illetve információ gyűjthető és konfigurációs beállítások végezhetőek. Az oldalirányú mozgás során a támadó olyan belső protokollokat is támadhat vagy kihasználhatja azok hibáit, amelyek a rendszeren kívülről nem láthatóak.

¹⁵⁸ root: gyökér könyvtár. Korlátlan jogosultságú rendszerfelhasználó.

¹⁵⁹ superuser: magas hozzáférési jogosultsággal bíró felhasználói fiók

¹⁶⁰ administrator: rendszergazda

¹⁶¹ backdoor: hátsóajtó

¹⁶² rootkit: saját és más programok jelentését elrejtteni képes, rosszindulatú kód

¹⁶³ lateral movement: oldal irányú mozgás



2.5. Kártékony programok használata

A támadó a támadás során több szinten alkalmazhat kártékony programokat céljai elérése érdekében. Az első behatolás alkalmával általában olyan kódot juttat a rendszerbe (inputként vagy legitim tartalomba rejtve), amely biztosítja a távoli hozzáférés lehetőségét.

Ez tipikusan minimális méretű kód, ami a rendszerben eleve meglevő funkciókat aktivál (pl. elindít egy shell-t¹⁶⁴ és létrehoz egy hálózati kapcsolatot). Ennek segítségével a támadó aztán újabb és komplexebb kártékony modulokat tud a rendszerbe juttatni, amelyek célja lehet a privilégium szint növelés, a perzisztencia biztosítása, a védelmi funkciók (pl. antivírus szoftverek) kikapcsolása, a támadó jelenlétének elrejtése, az információgyűjtés, vagy valamilyen szabotázs jellegű akció végrehajtása (pl. adatok törlése vagy rejtjelezése).

A kártékony programokat korábban vírus, féreg, és trójai kategóriákba sorolták, de a kódok ma már nehezen kategorizálhatók így. A modern kártékony programok, malware-k¹⁶⁵ moduláris felépítésűek, új modulokkal rugalmasan bővíthetők, és általában távolról vezérelhetők. A modulok lehetnek önállóan futtathatóak, már futó folyamatokba (pl. böngészőbe vagy rendszerfolyamatokba) betölthető könyvtárak vagy bináris programrészek, vagy az operációs rendszerbe beépülő komponensek is. A távoli vezérléshez szükséges kommunikáció általában rejtjelezett és valamilyen fedő forgalomba ágyazott, amelyet a tűzfalak tipikusan átengednek.

A kártékony programnak lehetnek önálló terjedést megvalósító funkciói, de sok kártékony kód egyáltalán nem terjed magától – vagy mert a támadó szorosan kontrollálni akarja a terjedést (pl. egy célzott támadás esetén), vagy mert más módon éri el nagy számú áldozat megfertőzését (pl. egy populáris weboldalon keresztül). A jellemzően használt disztribúciós módszerek a következők:

- e-mail: a kártékony program e-mail csatolmányként érkezik vagy az e-mail-ben található egy link, és arra rákattintva a felhasználó egy olyan weboldalra kerül, ahonnan a kód (is) letöltődik. A csatolmány magától nem fut le a rendszerben, a fertőzéshez a felhasználót rá kell venni arra, hogy nyissa meg (vagy végrehajtható állományok esetében indítsa el) a csatolmányt. Célzott támadás esetén az e-mail olyan ún. spear-phishing¹⁶⁶ levél, amely kifejezetten az áldozatra szabott, akár személyes információkat is tartalmazhat, ezért nagy a valószínűsége, hogy a megcélzott személy megnyitja majd a csatolmányt.

¹⁶⁴ shell: parancssori felület, parancsértelmező

¹⁶⁵ malware: rosszindulatú, kártékony alkalmazás vagy kód

¹⁶⁶ spear-phishing: célzott adathalászat, konkrét személy/szervezet ellen.



- drive-by-download: a malware egy weboldalon van elhelyezve és a támadó valamilyen módon ráveszi az áldozatot az oldal meglátogatására. Mikor az oldal letöltődik a kártékony program is végrehajtásra kerül az áldozat gépén. A végrehajtás első fázisa a böngészőn belül zajlik, ám a böngésző vagy az operációs rendszer valamilyen sérülékenységet kihasználva a kártékony kód végül a hoszt számítógépet is megfertőzi.
- watering hole: technikailag megegyezik a drive-by-download támadással. A különbség az, hogy a támadó nem közvetlenül veszi rá az áldozatot a weboldal meglátogatására, hanem olyan oldalon helyezi el a kártékony tartalmat, amit a potenciális áldozatok nagy valószínűséggel maguktól is meglátogatnak. Ez lehet egy populáris web site, vagy kifejezetten erre a célra létrehozott áldozat.
- fertőzött adathordozó: A kártékony program közvetlenül az adathordozón, az adathordozón tárolt valamelyik állományban (pl. egy PDF vagy DOC fájlban), vagy az adathordozó boot szektorában található. Az áldozatnak meg kell nyitnia a fertőzött fájlt, el kell indítania a kártékony programot, vagy bootolnia kell az adathordozóról ahhoz, hogy a kártékony program aktivizálódjon.

A kártékony kód által megvalósított funkciók és a kód minősége (kifinomultsága) a támadó technikai tudásától és anyagi erőforrásaitól függ. A script kiddie jellegű támadó tipikusan mások által fejlesztett kártékony programot használ, esetleg megpróbálja azt átkódolni, újracsomagolni, hogy a szignatúra alapú anti-vírus szoftverek ne ismerjék fel. Egy ilyen malware-t adott esetben egy hagyományos anti-vírus szoftvernél fejlettebb védelmi eszköz képes lehet detektálni. Az állam által szponzorált támadók viszont tipikusan saját kártékony programot fejlesztenek, illetve saját fejlesztésű malware platform segítségével hoznak létre különböző, a céljaiknak megfelelő variánsokat. Az ilyen malware-t jellemzően még a fejlettebbnek mondható eszközök sem detektálják, sőt egyre több malware detektálja azt, ha védelmi eszközök próbálják detektálni működésüket (ez esetben jellemzően passzív maradnak). A PLC-ket és RTU-kat ugyanúgy meg lehet fertőzni kártékony programokkal, mint asztali PC-ket, laptop-okat, vagy tablet-eket. Sőt, a beágyazott eszközök még nagyobb veszélynek vannak kitéve, mert hagyományosan kevesebb figyelmet szenteltek ezeknek az eszközöknek a biztonsági szakemberek, csak most kezdik megérteni, hogy az a környezet, amiben ezeket az eszközöket használják, nem teljesen zárt, azaz ezek az eszközök is támadások célpontjai lehetnek.

Az elmúlt években megnövekedett az olyan kártékony programok száma, amelyek nem felhasználói vagy az operációs rendszer kernel¹⁶⁷ szintjén futnak, hanem a számítógépen vagy beágyazott eszközön futó firmware-t módosítják. PC-k esetében pl. malware támadás

¹⁶⁷ kernel: rendszermag



célpontja lehet a BIOS¹⁶⁸, mert az ebben található programkód az, amit a hardver boot-oláskor először lefuttat. A BIOS-ban elhelyezett kártékony kód, az ún. bootkit¹⁶⁹, általában tetszőleges módosítást tud végezni a boot-olási folyamat során később betöltésre kerülő szoftvereken, pl. az operációs rendszer betöltő programján és magán az operációs rendszeren, és hagyományos eszközökkel nagyon nehéz detektálni.

Az USB-n csatlakozó eszközök (akár egy pendrive, egér, billentyűzet), lényegében beágyazott mikro-számítógépek, amelyeken valamilyen firmware fut, ami felülírható. A firmware számára rendelkezésre álló memória korlátos mérete korlátozza egy ilyen malware képességeit, az azonban elképzelhető, hogy az USB eszköz mikrokontrollerjének firmware-ében rejtőző malware kártékony kódot injektálhat az USB eszköz számítógépen futó driver programjába annak valamilyen hibáját kihasználva, ezzel akár a számítógép teljes kompromittálását is lehetővé téve. Ennek jelentős hatása lehet az ipari folyamatirányítási rendszerekre, köztük a villamosenergia-ipari létesítményekre, hiszen az USB adathordozón keresztül történő adat és program mozgás bevett szokás ezen a területen is.

Kártékony funkció, pl. hátsóajtó, nemcsak utólag kerülhet egy rendszerbe. Elméletileg, a rendszer vagy a rendszer egyes komponenseinek tervezője vagy megépítője is rejthet nem dokumentált funkciókat a rendszerbe, amelynek lehetnek káros hatásai. Bár adott esetben ennek kockázata alacsony lehet, az elvi lehetőség fennáll. Ráadásul, a nem dokumentált funkciók elrejtése több szinten is történhet, a hardvertől, az azt közvetlenül felügyelő firmware-en át, egészen a rendszeren futó szoftverekig. Minél alacsonyabb szinten van elrejtve egy nem dokumentált, potenciálisan kártékony funkció, annál nehezebb azt detektálni (egy chip szinten elhelyezett hardver backdoor praktikusán detektálhatatlan a végfelhasználók számára, de egy nagyméretű szoftver bináris verziójában szintén igen nehezen detektálható egy nem specifikált funkció). A problémát súlyosbítja, hogy a modern szoftverek számos, harmadik fél által készített program könyvtárat vagy egyéb modult tartalmaznak. Ezek intenzív használatának praktikus okai vannak, ha a licenz engedi, akkor érdemesebb egy már elkészített, létező kódot átvenni, mint ugyanazt a funkciót újra implementálni. Ez nemcsak felgyorsítja a fejlesztést, de jelentősen csökkentheti a költségeket is. Általában, a létező programkönyvtárak használata a szoftver minőségét is javíthatja, mert a fejlesztés az új funkciókra fókuszálhat, nem kell időt fordítani azon funkciók megvalósítására, amelyeket már létező könyvtárakban implementáltak.

¹⁶⁸ BIOS: Basic Input/Output System (alapvető bemeneti/kimeneti rendszer)

¹⁶⁹ bootkit: a számítógép indulásakor betöltődő rosszindulatú kód



Az is valószínű továbbá, hogy a könyvtárat olyan fejlesztő készítette, aki kifejezetten ahhoz a területhez ért, és jobb minőségben oldotta meg a feladatot, mint a szoftverfejlesztő cég programozói tennék. Ugyanakkor, mindez kockázatot is jelenthet, ha a felhasznált programkönyvtár készítőjéről nem sok információ áll rendelkezésre. A felhasznált könyvtárak és modulok készítői implicit módon a beszállítási lánc részévé válnak, és ugyanúgy implementálhatnak rejtett funkciókat a kódban, mint a rendszer építője.

2.6. Kriptográfiai sérülékenységek kihasználása

Az adatok átvitel vagy tárolás során történő védelmének eszközei a kriptográfiai algoritmusok és protokollok. Kriptográfiai módszerek használhatók felhasználók és szolgáltatások hitelesítésére, hálózati kommunikáció lehallgatás és módosítás elleni védelmére, adattárolón tárolt adatokhoz történő hozzáférés korlátozására, programkódok hitelesítésére és integritásvédelmére, és több egyéb feladatra. Nyílt rendszerek védelme lényegében elképzelhetetlen kriptográfiai eszközök alkalmazása nélkül. A kriptográfia, mint a védelem egy láncszeme, hatással van a teljes rendszer biztonságára. Általában azonban az mondható el, hogy a megfelelő erősségű és körültekintően implementált kriptográfiai mechanizmusok az erősebb láncszemek közé tartoznak, és viszonylag kevés kriptográfiai sérülékenység és azt kihasználó támadás ismert. Jelenleg egyszerűbb feladatnak tűnik a kriptográfiai algoritmust futtató számítógép vagy beágyazott eszköz kompromittálása, mint a kriptográfiai algoritmus feltörése. Ugyanakkor, a mélyebb technikai tudással rendelkező, elsősorban állam által szponzorált támadók esetében a kriptográfiai támadásokat sem lehet kizárni. A legtöbb gyakorlatban használt kriptográfiai algoritmus biztonsága nincs abszolút értelemben bizonyítva, ezért bármikor előfordulhat, hogy valaki az eddig ismert támadásoknál egy jóval hatékonyabb támadást talál egy adott algoritmus ellen.

2.7. Protokoll és API hibák kihasználása

A több rendszerelem együttműködésének és kommunikációjának szabályait leíró elosztott algoritmust protokollnak nevezzük. A protokollokat általában a résztvevők programjának és a kommunikációban használt üzenetek formátumának megadásával definiáljuk. Egy protokoll résztvevői lehetnek szoftvermodulok, amelyek az együttműködés során egymás funkcióit felhasználják, meghívják. A szoftvermodulok más modulok által meghívható funkcióinak halmazát API-nak nevezzük. Az API tehát az az interfész, amin keresztül a szoftvermodul szolgáltatásokat tud biztosítani más modulok számára.

A protokollokban és az API-kban található sérülékenységek tervezési szintű hibák, amelyek a rendszert támadhatóvá tehetik, ugyanakkor javításuk nehezebb, mint az implementációs szintű hibák javítása, mivel egy protokoll vagy API módosítása a rendszerben mélyebb szintű



változtatásokat igényel, és ezeknek a változtatásoknak kiterjedtebb hatása lehet az egész rendszerre.

Egy széleskörben használt protokoll pl. a TLS – vagy korábbi változata az SSL¹⁷⁰ – amely távoli felek között hoz létre biztonságos kommunikációs csatornát. A protokoll lehetővé teszi, hogy a távoli felek egymást hitelesítsék, megegyezzenek az alkalmazni kívánt kriptográfiai algoritmusokban, létrehozzanak egy közös mestertitkot, majd abból a kommunikáció védelmére használt kriptográfiai algoritmusok számára kulcsokat deriváljanak, és végül, az algoritmusok és a kulcsok felhasználásával, a felek üzeneteik bizalmasságának és integritásának megőrzésével tudjanak egymással kommunikálni. Számos egyéb, a TLS/SSL-hez hasonló biztonsági protokoll létezik, pl. SSH, IPsec¹⁷¹, WPA2¹⁷² stb. Ezek különböző hálózati rétegekben működnek, vagy valamilyen speciális feladatot látnak el. Ezen protokollokat intenzíven használják a modern számítógépes rendszerek. A legtöbb széleskörben használt protokollban az évek során számos hibát találtak, amelyek javítása újabb protokoll verziókat eredményezett, és az ezekre való áttérés sokszor gyakorlati problémákba ütközött, vagy egyes környezetekben nem valósulhatott meg. A rendszerek így egy-egy protokoll több verzióját is támogatják, ami további komplikációkhoz és támadási lehetőségekhez vezetett.

A protokollok elleni támadásoknak több fajtája létezik. A támadás célja lehet egy protokoll-résztevő megszemélyesítése, a protokoll által létrehozott közös kulcs megszerzése, egy régebben használt (és potenciálisan már kompromittált) korábbi kulcs elfogadtatása a résztvevőkkel, vagy a résztvevők kommunikációja során átküldött, kriptográfiailag védett üzenetek szisztematikus feltörése, észrevétlen módosítása, visszajátszása vagy hamis üzenetek előállítás. A támadóról általában azt feltételezzük, hogy tetszőlegesen be tud avatkozni a felek közötti kommunikációba, ami általában MitM támadót jelent, aki fizikailag vagy logikailag ékelődik be a protokoll-résztevők közé. Az alkalmazott kriptográfiai algoritmusokat általában ezen a szinten biztonságosnak tekintjük, azaz azt feltételezzük, hogy a támadó protokollhibákat keres, vagyis nem magukban az algoritmusokban, hanem abban keresi a kihasználható sérülékenységet, ahogyan az algoritmusokat a protokoll egymással kombinálja.

¹⁷⁰ SSL: Secure Socket Layer (titkosítási protokoll, amely az interneten keresztüli kommunikációhoz biztosít védelmet. Az SSL a TLS elődje.)

¹⁷¹ IPsec: Internet Protocol Security (IP biztonsági protokoll, Az IP protokollon működő, minden IP-csomagot titkosító és a jogosultságát ellenőrző protokoll.)

¹⁷² WPA2: Wi-Fi Protected Access 2 (A vezeték nélküli hálózati rendszerek biztonsági protokollja, amely tartalmazza az IEEE 802.11i szabvány főbb szabályait.)



A protokollokhoz hasonlóan biztonsági API-kkal is számos környezetben találkozhatunk. Ezekben a széleskörben használt biztonsági API-kban is előfordultak hibák, amelyek javítása az API-k újabb és újabb verzióihoz vezetett.

API-k esetében a támadó olyan, a tervező által előre nem látott módon hívja meg az API függvényeit, hogy végül kompromittálja a rendszert (pl. hozzájut egy kulcshoz, amit közvetlenül az API-n keresztül nem lenne szabad elérnie, megszerez egy hitelesítő token¹⁷³, amit közvetlenül az API-n keresztül nem tudna elérni, végrehajt egy műveletet, amihez egyébként nem lenne jogosultsága, vagy egyszerűen hibás működést vagy leállást idéz elő az API által védett szoftver modulban).

2.8. Social engineering, phishing

A technikai jellegű támadások mellett nagyon hatékony a humán felhasználók ellen irányuló támadások köre. Sokan a humán felhasználókra úgy tekintenek, mint az informatikai és irányítástechnikai rendszerek biztonságának leggyengébb láncszemeire. Ez abban a tekintetben igaz, hogy hiába alkalmazunk technikailag erős biztonsági megoldásokat, ha a felhasználók nincsenek felkészítve ezek megfelelő használatára, vagy az ezekkel kapcsolatos titkos paraméterek biztonságos kezelésére. Egy képernyőre ragasztott cetlire vagy táblára felírt jelszó pl. könnyű hozzáférést biztosít a védett rendszerhez egy támadó számára akár a technikai szempontból legerősebb biztonsági megoldások mellett is.

A humán felhasználók elleni támadásokat social engineering támadásoknak nevezzük. Ezek egy alcsoportját alkotják a phishing¹⁷⁴ támadások, amelyekben a támadó a felhasználók számára hamis információt tartalmazó e-mail-t küld vagy weboldalt jelenít meg, ezzel megtévesztve és rávéve őket valamilyen kompromittáláshoz vezető lépésre. Tipikus példa, mikor a támadó olyan e-mail-t küld a felhasználónak, amiben arról tájékoztatja, hogy valamilyen okból (pl. karbantartás vagy fiók adatok ellenőrzése) be kell lépnie a támadó által célzott rendszerbe, ám az e-mail nem az igazi rendszerre mutató linket tartalmaz, hanem egy támadó által birtokolt, az eredetihez mindenben hasonlító weboldalra mutat. Ha a gyanútlan támadó ezen az oldalon megkísérli a belépést, akkor közvetlenül a támadónak küldi el az igazi rendszerhez történő hozzáféréshez szükséges fiókazonosítót és jelszót.

A social engineering támadások hatékonyságát a támadók úgy növelik, hogy minden rendelkezésre álló forrást felhasználnak a rendszerrel és a felhasználókkal kapcsolatos információk gyűjtésére.

¹⁷³ token: jogosultsági és biztonsági kódgeneráló eszköz

¹⁷⁴ phishing: adathalászat



2.9. Belső támadó vagy szerződéses partner felől érkező támadás

A belső fenyegetettséget olyan támadók testesítik meg, amelyek valamilyen legitim hozzáféréssel rendelkeznek a szervezet számítógépes rendszereihez és adataihoz, és ezt a hozzáférést rosszindulatúan használják fel a rendszer és/vagy az adatok kompromittálására.

A kompromittálás általában a bizalmasság, integritás, és rendelkezésreállítás hármas valamelyikének megsértését jelenti (pl. a támadó bizalmas adatokat szivárogtat ki, vagy elérhetetlenné teszi a rendszer egyik szolgáltatását). A támadó elsősorban az elégedetlen munkatárs támadómodellnek megfelelő entitás lehet (azaz egy aktuális vagy egy közelmúltban elbocsátott munkatárs, aki még mindig rendelkezik hozzáférési jogosultságokkal) vagy a szervezet egy beszállítója, amely egy őt ért támadás következtében kompromittálódott, és a támadó a beszállító hozzáférési jogosultságait, hálózati kapcsolatait felhasználva támadja a szervezet számítógépes rendszerét.

A belső fenyegetettséget megtestesítő támadó több tekintetben is erősebb, mint más támadó típusok, és ezért nagy kihívást jelent. Először is már rendelkezik valamilyen hozzáférési jogosultsággal és ez több lehetőséget biztosít a rendszer kompromittálására, mint ami egy külső támadó rendelkezésére áll. Másrészt jóval több információval rendelkezik a rendszerről, mint egy külső támadó: nemcsak magát a rendszert ismerheti jól, hanem annak gyengeségeit is. A technikai jellegű információk és hibák mellett, a belső támadó ismerheti a szervezet biztonsági szabályzatait és eljárásrendjeit, illetve azok gyengeségeit, valamint személyes kapcsolatait lehetnek a szervezet más alkalmazottjaival, amiket kihasználhat. A belső támadó valamilyen szintű fizikai hozzáféréssel is rendelkezhet a rendszerhez. A fentiek együtt jóval több lehetőséget biztosítanak egy belső támadó számára nemcsak egy sikeres támadás kivitelezéséhez, hanem a támadás tényének, nyomainak elrejtéséhez, s így a kompromittált állapot kiterjedt ideig történő fenntartásához is.

A leggyakrabban előforduló belső munkatárs által elkövetett támadások az információ-lopás (beleértve a szellemi tulajdont képző információkat), a megszerzett bizalmas információk illetéktelen felhasználása (ami magában foglalja a személyes adatok nyilvánosságra hozását is), és rosszindulatú programok (vírus, backdoor) alkalmazása.

A belső fenyegetettséghez tartoznak a beszállítók, illetve az egész beszállítási lánc felől érkező támadások is. A beszállítási láncba tartozó bármely beszállító felől érkező támadás a beszállítás bármely fázisában. Mivel a számítógépes rendszerek komplexek, ezért számos beszállító termékeit tartalmazzák, mind hardver mind szoftver szinten. Ezek a termékek tartalmazhatnak szándékosan elhelyezett hibákat vagy kikapukat (backdoor), amelyek így már a rendszer építése során bekerülhetnek a rendszerbe. Később, az üzemeltetés és a karbantartások során szintén részt vehetnek beszállítók a munkában, akik különböző szintű



hozzáférést kapnak a rendszerhez, a különböző eszközökhöz, és alkalmuk lehet azokat kompromittálni, vagy azokban későbbi támadás során kihasználható hibákat elhelyezni. A fenti támadások ugyanakkor nem feltétlenül történnek a beszállító tudtával: a veszély elsősorban az, hogy egy külső támadó az alvállalkozó rendszerét kompromittálva, nevében és jogosultságaival hajthat végre káros következménnyel járó műveleteket a beszállító által kiszolgált szervezet rendszerében.

A támadó számára ez általában azért kedvelt stratégia, mert a beszállítók között sok a kisebb cég, amelyek kevesebbet tudnak biztonságra költeni és ezért sérülékenyebbek, mint a nagyobb szervezetek.

3. Támadó profilok

3.1. A támadó profilok/modellek osztályozásának alapjai

A számítógépes, illetve ipari irányítási rendszereket fenyegető támadások forrása sokféle lehet, ezért célszerű az egyes támadók alábbi szempontok alapján történő osztályozása:

- *Motiváció:* az egyik legalapvetőbb osztályozási szempont. A jelentősebb támadói csoportok tevékenysége mögött jellemzően gazdasági, társadalmi, vagy politikai okok húzódnak, az egyéni elkövetők motivációja ugyanakkor többnyire személyes, vagy azt akarják megmutatni, hogy technikailag képesek egy adott támadást végrehajtani, vagy személyes bosszúból támadják az őket ért, vélt vagy valós sérelem forrását. A motiváció hatása jelentős a támadás célpontjának kiválasztására, a támadás hátterére, stratégiai céljára (pl. ipari kémkedés, szabotázs, fizikai vagy anyagi károkozás, hírnévsértés stb.). A stratégiai cél elérése érdekében a támadó konkrét technikai célokat tűzhet ki (pl. bejutás a támadott rendszerbe, jogosultságok szerzése, információlopás; a támadott szervezet weboldalának feltörése és a webtartalom módosítása; személyes adatok lopása és eladása, közzététele stb.).
- *Az információszerzés mélysége:* a technikai célok elérése érdekében a támadó megtervezi és végrehajtja a támadást, amelynek fontos eleme a támadást megelőző, illetve a támadás során folytatott információszerzés mélysége. A támadás sikere nagymértékben függ a megtámadott rendszerről rendelkezésre álló információtól, ezért a támadók általában – képességeiktől függően – megpróbálnak a lehető legtöbb, a rendszer általános felépítésére, az elérhető szolgáltatásokra, az alkalmazott hardver és szoftver eszközök típusára és konfigurációs beállításaira, a hálózati topológiára, az alkalmazott hálózati technológiákra, illetve az alkalmazott biztonsági mechanizmusokra vonatkozó információhoz hozzájutni. Ugyancsak fontos a kapcsolódó ismert sérülékenységek, esetleg az azok kihasználását lehetővé tévő konkrét exploit technikák,



illetve a rendszer felhasználóiról és jogosultságaikról rendelkezésre álló információk ismerete is. Ipari folyamatirányítási rendszerek esetén hasznos lehet továbbá a rendszer által vezérelt fizikai folyamat jellemzőinek és a kapcsolódó kontroll algoritmusoknak az ismerete. Jellemzően különbséget szokás tenni az ún. külső és belső támadók között, ugyanakkor ez a felosztás meglehetősen leegyszerűsítő.

A két kategória között alapvető különbség, hogy a külső támadó általában csak publikusan elérhető információkhoz jut hozzá, míg a belső támadó bizonyos mennyiségű nem publikus, belső információhoz is hozzáfér. Ezek a belső információk és a hozzáférési lehetőségek ugyanakkor sokfélék lehetnek. Belső támadó lehet egy korlátozott hozzáférési jogosultságokkal és technikai ismeretekkel rendelkező munkatárs, egy a folyamatirányítási rendszerért felelős mérnök (kiterjedt technikai ismeretekkel és a rendszer működésével kapcsolatos belső információkkal, de korlátozott hozzáférési jogosultságokkal), vagy akár egy rendszergazda (kiterjedt hozzáférési jogosultságokkal, de az irányítási rendszerre vonatkozó korlátozott technikai ismeretekkel). Belső támadónak számíthat továbbá egy beszállító vagy az üzemeltetéshez technikai támogatást nyújtó külső partner is, ha birtokában van belső információknak, esetleg bizonyos szintű hozzáféréssel is rendelkezik. A leegyszerűsítés további problémája, hogy nem tudja kezelni azt a gyakori esetet, amikor egy külső támadó a támadás kivitelezése közben belsővé válik (pl. kártékony program telepítésével, jogosultságok megszerzésével, belső munkatársak megzsarolásával, beszállítók rendszereinek kompromittálásával stb.). Célszerűbb ezért a támadókat aszerint megkülönböztetni, hogy milyen mélységben képesek a rendszerre vonatkozó információk megszerzésére. Ezzel a belső információk és hozzáférési lehetőségek sokfélesége és az információszerzés dinamikus jellege is kezelhető.

- *A technikai tudás mélysége:* a technikai tudás egyrészt az információszerzés mélységének növelése szempontjából lehet fontos, másrészt a technikai tudás az, amelynek segítségével a publikusan elérhető és a rendszerről megszerzett belső információk sikeres támadássá alakíthatók. Ipari folyamatirányítási rendszerek esetén, a számítógépes rendszerek alatt programozható rendszereket értünk, azaz a technikai tudás nemcsak a hagyományos irodai környezetben használt eszközök működésének, gyengeségeinek, és kompromittálási lehetőségeinek ismeretére terjed ki, hanem magában foglalja ugyanezt az ipari környezetben használt beágyazott eszközök és szoftverek tekintetében is.



- A támadó rendelkezésére álló *anyagi erőforrások mennyisége*: az anyagi erőforrások jelentőségét elsősorban azok információszerzésre és a technikai tudás mélységének növelésére való felhasználhatósága adja. Nagyobb anyagi erőforrásokkal rendelkező támadók könnyebben tudnak információt szerezni (pl., beépüléssel, zsarolással, technikai dokumentáció megszerzésével, social engineering technikák kiterjedtebb használatával, vagy akár hírszerzési módszerek alkalmazásával), és könnyebben férnek hozzá a támadáshoz szükséges technikai tudáshoz (szakemberek megfizetésével vagy saját kompetenciák kifejlesztésével). A nagyobb anyagi erőforrások mindemellett fejlettebb támadó eszközök és módszerek alkalmazását is lehetővé teszik (pl. zero-day exploit-ok alkalmazása, kriptográfiai kulcsok kompromittálása stb.).

3.2. Jellemző támadó profilok

A fenti általános szempontok figyelembevételével, a villamosenergia alágazat létesítményeit fenyegető támadók a következő tipikus támadó modellekbe sorolhatók:

- *Script kiddie*: korlátozott technikai tudással, információval (és információszerzési lehetőséggel) és anyagi erőforrásokkal rendelkező magányos külső támadó. Motivációja elsődlegesen az önkifejezés és -megvalósítás. Mivel technikai tudása és anyagi erőforrásai korlátozottak, a támadáshoz jellemzően mások által kifejlesztett módszereket és eszközöket használ fel. Arra ugyanakkor képes lehet, hogy ezeket a módszereket és eszközöket újszerű módon integrálja, kombinálja. A fenti limitációk miatt, a támadás célpontját nem előre megtervezett stratégia mentén, hanem inkább opportunista módon választja, többnyire nem az a lényeges számára, hogy ki a célpont, hanem az, hogy a célpont az elérhető eszközök és információk segítségével könnyen kompromittálható legyen. Ennek megfelelően a támadás sikerének oka általában a támadott rendszert üzemeltető szervezet hanyagsága, amelynek következtében a rendszerben könnyen kihasználható hibák maradnak. Fontos ugyanakkor, hogy a script kiddie által felhasználható, publikusan elérhető információk és eszközök mennyisége folyamatosan növekszik, folyamatosan kerülnek megosztásra újabb és újabb sérülékenységek és exploit technikák, illetve új információmegosztó fórumok is megjelennek. Egy-egy régebbi támadó eszköz vagy exploit technika elavulhat a technológia fejlődésével, ennek üteme azonban az ipari, így a villamosenergia-ipari létesítmények tekintetében lassabb, mert ezekben a létesítményekben, a hosszú életciklus modell miatt, sokszor régi technológiát használnak. Mindez azt jelenti, hogy hosszabb távon a script kiddie támadó technikai képességeinek folyamatos növekedésével kell számolni. A script kiddie alacsony kockázatot jelent a villamosenergia-ipari létesítmények programozható rendszereire, mert motivációja nem



kifejezetten ezekre a rendszerekre irányítja figyelmét, valamint limitált információval, technikai tudással, és anyagi erőforrásokkal rendelkezik. A létesítmények tipikusan elavult technológiája, az elérhető támadó eszköztár folyamatos bővülése, valamint a létesítmények rendszereinek üzemeltetése során esetlegesen mutatkozó hanyagság azonban növelheti ezt a kockázatot.

- *Elégedetlen munkatárs/beszállító:* a magányos támadó tipikus esete az elégedetlen munkatárs, beszállító, akinek motivációja szintén személyes jellegű. Sokkal veszélyesebb, mint a script kiddie, mert célpontja egy konkrét szervezet vagy intézmény, motivációja általában átgondolt stratégiai cél definiálására ösztönzi, amelynek elérése érdekében konkrét technikai célokat határoz meg.

Több információval rendelkezik vagy több információt képes megszerezni, mint egy script kiddie, ismerheti a rendszeráltalános felépítését, egyes alrendszerek működéséről, konfigurációjáról, és hozzáférési lehetőségeiről akár részletes információi is lehetnek; szerepkörétől függően különböző szintű hozzáférési jogosultságokkal rendelkezhet. Emellett személyes kapcsolatban állhat a rendszer többi felhasználójával, üzemeltetőjével, karbantartójával, a beszállítókkal, amit további információk és jogosultságok megszerzésére használhat fel. Technikai tudásának mélysége változó, nagymértékben függ szerepkörétől, ipari folyamatirányítási környezetben ismerheti a kontrollált fizikai folyamat jellemzőit, tudhatja milyen beállítások vezethetnek katasztrofális vagy jelentős anyagi kárral járó következményekhez, ismerheti az alkalmazott fizikai eszközök korlátait, hibáit, érzékeny pontjait. Anyagi erőforrásai általában korlátozottak, de ezt kompenzálja információszerző képességének és technikai tudásának mélysége. Jelentős kárt okozó támadások végrehajtására is képes lehet, ezért jelentős mértékű kockázatot jelent. Mivel motivációja jellemzően személyes, az irracionális viselkedés sem zárható ki. A kockázatot mérsékeli, hogy általában egyedül tevékenykedik, nem rendelkezik jelentős anyagi erőforrásokkal, és ezért többnyire csak az általa közvetlenül megszerezhető információk és saját technikai tudásának megfelelő támadást hajt végre.

- *Hacktivist csoportok:* a hacktivist csoportok általában laza szerveződésű, eltérő szintű technikai tudással rendelkező, amatőr hacker-ből állnak. Motivációjuk általában valamilyen társadalmi vagy politikai ideológia védelme és/vagy terjesztése. Ez határozza meg a támadás célpontját és stratégiai célját, de az is előfordul, hogy a célpont kiválasztása és a stratégiai cél kijelölése opportunistá elemeket is tartalmaz (néha könnyen kompromittálható rendszereket támadnak meg, amelyet utólag a támadást társadalmi vagy politikai küzdelme érdekében végrehajtott, előre eltervezett akciónak állítanak be). Ha a célpont kiválasztását és a stratégiai cél kijelölését a csoportok eredeti



motivációja határozza meg, akkor azok gyakran valamilyen, a motivációval összefüggésbe hozható aktuális társadalmi vagy politikai eseményre reflektálnak, tevékenységük tehát inkább akciószerű, és nem hosszútávú stratégiához igazodik. Alapvetően külső támadók, általában semmilyen vagy nagyon kevés belső információval rendelkeznek a támadott rendszerről. Anyagi erőforrásaik limitáltak, ezért információszerző képességük is korlátozott, alapvetően technikai módszerekkel és eszközökkel, a támadás kivitelezése közben próbálnak több információt gyűjteni a támadott rendszerről és hozzáférési jogosultságokat szerezni. Technikai tudásuk tagjaik tudása határozza meg, így a csoportok tudása széles skálán mozog. Jellemzően van néhány magas technikai tudással rendelkező tagjuk, ám a csoport nagy része alacsony, script kiddie-hez hasonló szintű technikai tudással rendelkező amatőr.

- A hacktivisták csoportok hangadói kapcsolatban állhatnak kiberbűnözői csoportokkal vagy maguk is tagjai lehetnek kiberbűnözői szervezeteknek, amelyek segítségét és magasabb szintű technikai tudását alkalmanként igénybe vehetik. A hacktivisták csoportok anyagi erőforrásai korlátozottak, egyrészt a laza szerveződés nem teszi lehetővé, hogy a csoportok strukturált módon erőforrásokat halmozzanak fel, másrészt általában nem rendelkeznek külső szponzorral. A hacktivisták csoportok korlátozott információszerző képessége és technikai tudása valószínűleg nem elegendő katasztrofális következményekkel járó kibertámadások végrehajtásához, valószínűbb, hogy politikai vagy társadalmi üzeneteiket weboldalak lebénításával és módosításával (de-face) próbálják elérni (ld. Anonymous). Ugyanakkor nem hagyható figyelmen kívül, hogy kis komplexitású támadásoknak is lehetnek előre nem tervezett negatív mellékhatásai.
- *Terrorista szervezetek:* tendenciózusnak mondható, hogy terrorista szervezetek az eszköztárukat egyre inkább számítógépes rendszerek ellen használható támadó eszközökkel bővítik, ezek ugyanakkor egyelőre leginkább a hagyományos eszközök kiegészítésére (információszerzésre, a fizikai támadások hatásainak felerősítésére stb.) szolgálnak. A terrorista szervezetekre a determináltság és sokszor az irracionalitás jellemző, ami különösen veszélyessé teszi ezen támadókat. Motivációjuk általában politikai vagy vallási ideológiára épül, amelynek nevében szinte mindenre képesek. Stratégiai céljaik átgondoltak, elsősorban média figyelemre és a civil lakosság megfélemlítésére és elbizonytalanítására törekszenek. Célpontjaikat (amelyek sokszor civil létesítmények) tudatosan választják. Anyagi erőforrásaik számottevőek lehetnek, amelynek felhasználásával jelentős mennyiségű belső információt képesek szerezni a megtámadni kívánt rendszerről. Technikai tudásuk egyelőre nem túlságosan mély, de határozottan mélyülő tendenciát mutat. A terrorista szervezetek sok esetben modern eszközrendszerrel rendelkeznek és intenzíven használják az internetet on-line tudásbázis



készítésére és tagjaik kiképzésére is. Aggasztó tendencia továbbá a terrorista szervezetek és a hagyományos bűnszervezetek kooperációja. A villamosenergiái-ipari létesítmények ellátási láncban betöltött szerepük miatt akár közvetlen célpontjai is lehetnek terrorista támadásoknak. A terrorista szervezetek jelentős kockázatot, komoly fenyegetést jelentő támadók.

- *Kiberbűnöző szervezetek:* elsődleges motivációjuk a gazdasági haszonszerzés, amelynek érdekében, átgondolt stratégiai célok mentén, nagyszabású, térben és időben kiterjedt támadási kampányokat hajtanak végre. Mivel a potenciális haszon az áldozatok számával arányos, ezért a támadási kampányok általában nagyszámú áldozattal járnak, amelynek jelentős része egyéni felhasználó.

Az egyéni felhasználók elleni támadások célja lehet személyes adatok (pl. hitelkártyaszám) gyűjtése az áldozatok rendszereiből, vagy különböző szolgáltatásokhoz tartozó hozzáférési jogosultságok (pl. felhasználónév – jelszó párok) megszerzése. Felhasználói adatok és fiók információk nagy mennyiségben szerezhetők be különböző on-line szolgáltatók számítógépes rendszereiből is, ezért ezen rendszerek is a kiberbűnöző szerveződések célpontjai. A megszerzett információk közvetlenül felhasználhatók haszonszerzésre, vagy értékesíthetők. A támadások másik tipikus célja az irányítás átvétele nagy mennyiségű számítógép felett, és a kompromittált számítógépek ún. botnet-be szervezése. Az információhoz hasonlóan, a botnet által nyújtott számítási kapacitás és támadói potenciál közvetlenül felhasználható haszonszerzésre (pl. spam kampány vagy DDoS támadás végrehajtásához), vagy a botnet bérbe adható más támadói csoportoknak. Végül támadási cél lehet hozzáférhetetlenné tenni az áldozat számára a saját adataihoz történő hozzáférést. Ekkor a haszonszerzés tipikusan zsarolás útján történik. Mára kialakult egy jól működő illegális gazdasági ökoszisztéma, amely lehetővé teszi személyes adatok, botnet kapacitás, és egyéb támadó eszközök (pl. exploit információk és kártékony programok, valamint kártékony programok fejlesztésére alkalmas egyedi eszközök vagy teljes keretrendszerek) értékesítését, bérbeadását. Ez az illegális ökoszisztéma biztosítja a kiberbűnözői szervezetek számára a támadói tevékenység gazdasági haszonná alakításának lehetőségét. Az ökoszisztéma a legális gazdasághoz hasonló versenyre ösztönzi az egyes szereplőket, ami az innováció motorja. Nem véletlen, hogy drasztikus ütemű fejlődés tapasztalható a kiberbűnözői eszközök kifinomultságában és hatékonyságában, és gyors az adaptálódás az új számítástechnikai platformok és biztonsági mechanizmusok megjelenésére. A sikeres kiberbűnöző szervezetek számottevő információszerző képességgel, illetve jelentős anyagi erőforrásokkal rendelkezhetnek, amely növeli az információszerző képesség és a technikai tudás mélységét.



A villamosenergia-ipar létesítményei tekintetében a kiberbűnözői csoportok kétféleképpen jelenthetnek kockázatot: egyrészt, támadó eszközeiket vagy technikai tudásukat pusztán haszonszerzés céljából eladhatják vagy bérbe adhatják más támadói csoportoknak, pl. terrorista szervezeteknek vagy akár valamely állam által szponzorált támadói csoportnak is; másrészt, közvetlenül is indíthatnak támadást az iparág különböző létesítményei, szervezetei, vagy azok beszállítói ellen, elsősorban értékesíthető információk megszerzése, vagy a létesítmény működéséhez szükséges adatokhoz, rendszerekhez történő hozzáférés megakadályozása, és ennek zsarolásra történő felhasználása céljából. Bár a kiberbűnözői szervezet fejlett információszerző képességgel és mély technikai tudással rendelkezik, ezért veszélyes támadónak minősül, motivációja a villamosenergia-ipar létesítményei elleni támadásra limitált, mivel egyelőre ennél egyszerűbben képes hasznot termelni.

- *Idegen állam által támogatott támadó csoport:* motivációját, stratégia céljait, és támadásainak célpontjait a támogató állam kormányzatának politikai céljai határozzák meg. Jellemző stratégiai cél az ipari, politikai, vagy katonai céllal folytatott kémkedés, valamilyen szabotázs akció végrehajtása (amelynek tipikus fókusza az áldozat informatikai és távközlési rendszereinek megbénítása, adatvesztés előidézése), kiberfizikai rendszerek esetében fizikai kár okozása, illetve egy fizikai támadás támogatása, hatékonyságának és hatásának növelése. Az idegen állam által támogatott támadó csoport erősen motivált, világos stratégiai célokkal rendelkezik, és ezek elérése érdekében tudatosan választja célpontjait és technikai céljait. A korábban elemzett támadó csoportoktól megkülönbözteti szervezettsége és erőforrásgazdagsága. Ez teszi számára lehetővé információszerző képességének és technikai tudásának mélyítését, valamint komplex, térben és időben nagy kiterjedésű támadások precíz előkészítését és hatékony végrehajtását. Információszerző képessége túlmutat minden korábban elemzett támadó csoport képességein, hiszen az nemcsak informatikai eszközökre és a szokásos social engineering technikákra korlátozódik, hanem hagyományos hírszerzői módszerekre és tevékenységekre is támaszkodhat. Technikai tudása is mélyebb, mert anyagi erőforrásai komplex kutatási és képzési programok végrehajtását teszik lehetővé számára. Ennek megfelelően az idegen állam által támogatott támadó csoportra jellemző a kifinomult és fejlett, nem ritkán mások által még teljesen ismeretlen támadási módszerek és eszközök alkalmazása.

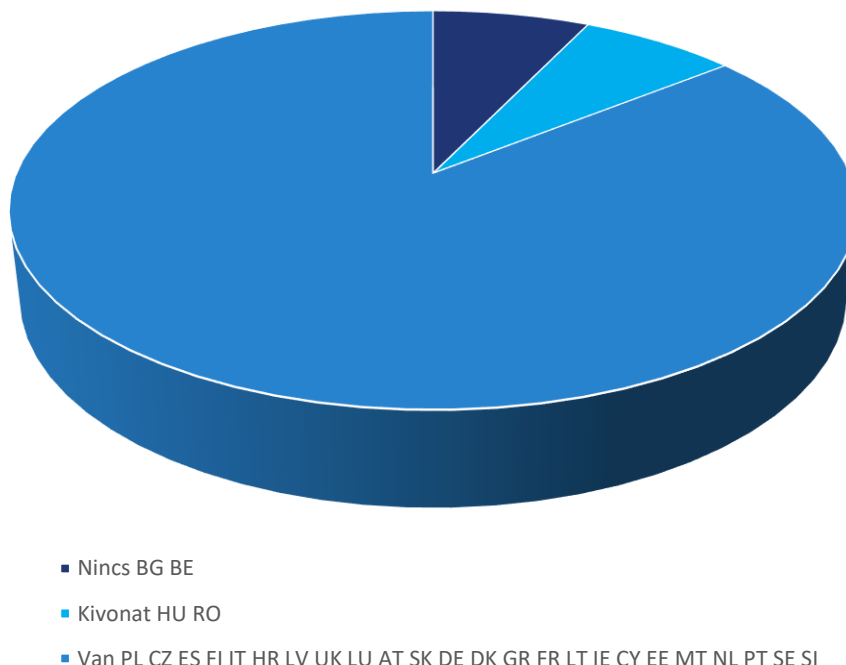


4. melléklet: Az Európai Unió tagállamainak nemzeti kiberbiztonsági stratégiái vizsgálatának és a magyar kiberbiztonsági stratégia elemzésének összefoglaló jelentése

A villamosenergia alágazati szereplők kiberbiztonságának biztosítása minden esetben meghatározott célok mentén kialakított stratégia által kellene, hogy megvalósuljon. Ehhez egy megfelelően felépített nemzeti kiberbiztonsági stratégiára lenne szükség, amely meghatározza az elérendő célokat, a megvalósítás módját és eszközeit- valamint határidejét, illetve a felelősöket, továbbá a visszaellenőrzés eszközrendszerét.

Az előzőkre tekintettel az EU tagállamok kiberbiztonsági stratégiáinak vizsgálata során szerzett tapasztalatok alapján készült jelen dokumentum. Nem minden stratégia hatályos jelenleg a vizsgált dokumentumok közül, így előfordulhat, hogy emiatt nem említene bizonyos védelmi feladatokat.

Az ENISA honlapjára feltöltött nemzeti kiberbiztonsági stratégiákat vizsgálva megállapítható, hogy összesen 2 stratégia nincs meg angol nyelven. Belgium és Bulgária nem rendelkezik angol nyelvű nemzeti kiberbiztonsági stratégiával.



4.1. ábra: Kiberbiztonsági stratégiák ENISA honlapon való szerepeltetése

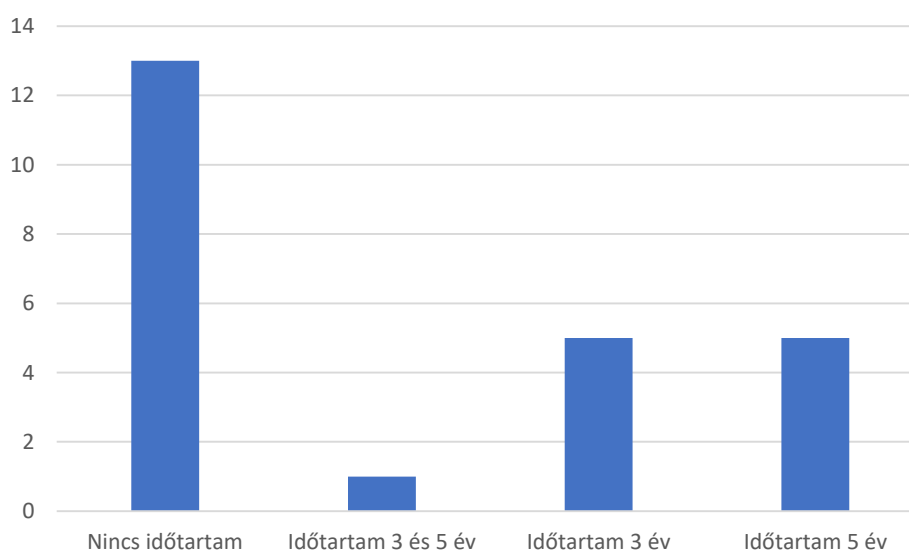


A magyar stratégia egy „kivonat”, amely mellett Románia is egy ilyen hasonló kivonatot tett közzé az ENISA honlapján (a vizsgálat során előzőekre tekintettel a belga, a bolgár, a román és a magyar stratégia nem került bele a vizsgálati adatokba). A magyar kivonat nem tesz említést az energia ágazat, és a villamosenergia-szolgáltatók kibervédelméről. A kritikus infrastruktúrák védelme érintőlegesen említésre kerül, de a kijelölt létfontosságú rendszerelemek kibervédelmi stratégiája a dokumentumban nem kerül kifejtésre.

A dokumentum nem határoz meg konkrét célokat és feladatokat, inkább egy vízió érzetét kelti az olvasóban. A napjainkban elterjedt ellátási láncokat kihasználó kibertámadások elleni védelemmel kapcsolatos feladatokat is nélkülözi a Nemzeti Kiberbiztonsági Stratégia. A NATO, EU és egyéb nemzetközi szervezettel történő együttműködés megemlítésre kerül, ahogy a PPP (Public Private Partnership) is. A szaknyelv által használt kifejezések magyarázatát a dokumentum nem tartalmazza.

A mai napig hatályos és érvényben lévő Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat (word vagy pdf dokumentumként) mindössze 5 oldal. A Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján kihirdetett stratégia 29 oldal. Az ehhez kapcsolódó intézkedési terv további 25 oldalon részletezi a feladatokat. Eközben az EU tagállamainak stratégiái átlagosan 31 oldalt tesznek ki, egységes szerkezetben.

A stratégiák vizsgálata során (24 stratégia került áttanulmányozásra) megállapításra került, hogy a 11 nemzet meghatározott időtartamra fogalmazta meg a stratégiáját, míg 13 ország nem határozott meg időtávot a stratégia alkotása során. Azon nemzetek közül, amelyek határoztak meg időtartamot, 1 nemzet 3 és 5 éves stratégiát készített, 5 nemzet 3 évest, és szintén 5 nemzet 5 éves stratégiát alkotott.



4.2. ábra: Kiberbiztonsági stratégiák érvényességi idői



Konkrét elérendő célokat 17 nemzet fogalmazott meg, míg 7 nemzet víziót, alapelveket definiált a saját kiberbiztonsági stratégiájában.

A kritikus infrastruktúrák védelméről csupán egyetlen stratégia nem tett említést, vagyis a nemzeti létfontosságú rendszerek védelme egy kivétellel mindenhol prioritásként van kezelve, ha csak említés szinten is.

Napjaink egyik legnépszerűbb kibertámadási formája az ellátási láncok kapcsolatait kihasználó támadások, amellyel szemben való védekezés fontosságát csupán 8 stratégia tartotta fontosnak megemlíteni.

A nemzetközi együttműködést (NATO, EU) a 24 stratégiából csupán 5 nem említi, ennek azonban a NATO tagság hiánya is oka lehet.

Az állami és nem állami szereplők együttműködését mindössze 2 dokumentum nem tartotta fontosnak megemlíteni, 22 stratégia kiemelten kezeli, hogy minden érintett szereplő együtt határozza meg a védelem kialakításának módját.

A nemzeti kiberbiztonsági stratégiák 50%-a használ külön kifejezés gyűjteményt és magyarázatot, amely nagyon fontos annak érdekében, hogy az olvasó megértse, hogy miről is szól pontosan egy stratégia. Egy hétköznapi ember által olvasva magyarázatok nélkül érdektelenné válhat egy ilyen dokumentum, amelynek a következménye a tudatosság nélkülözése is lehet, amely egy döntéshozó esetében beláthatatlan következményekkel járhat.

A villamosenergia alágazati szereplők kiberbiztonságát 13 db stratégia kezeli valamilyen formában, a további 11 db említést sem tesz róla. Az újabb stratégiák már a NIS irányelv szerinti feladatokat is említik, illetve beépítik a stratégiába. A 13 db stratégia közül a dán szektor specifikusan kezeli a kritikus infrastruktúrák kibervédelmét külön felelős minisztériumok részére meghatározott feladatok által.

A dán ágazati stratégia¹⁷⁵ [38] kialakításában a legfontosabb magán szereplők is részt vettek, így a dán példát tekintve a felelős Energiaügyi Minisztérium mellett a DANSK Energy, az Energinet a Dansk Fjernvarme, a DINEL, Radius és a HOFOR is.

Az audit, és a visszaellenőrzés rendszere a 2010-es évek végén megjelent stratégiák szerves részét képezik.

További jó gyakorlat a nemzeti kibervédelmi stratégiák vonatkozásában, hogy a saját nemzet kibervédelmi helyzete is meghatározásra kerül a globális kibervédelem rendszerében, és az ehhez rendelt feladatok szintén. Van olyan stratégia, amely 2011-től már a klímaváltozás hatásait is prognosztizálva, az ebből eredő hatásokkal is számol a kibervédelem területén.

¹⁷⁵ Danish Ministry of Defence. „New sectoral strategies to prepare society for cyber attacks.” <https://www.fmn.dk/eng/news/Pages/New-sectoral-strategie-stop-repare-society-for-cyberattacks.aspx> (Letöltve: 2020. augusztus 28.)



A 2019-20-as év COVID-19 világjárvány rávilágít arra is, hogy egy globális pandémiás helyzet hatásai is meghatározók a kibervédelemben.

Javasolt lenne a magyar stratégiát is meghatározott időtartamra (3 vagy 5 év) meghatározni, és vagy ebben a dokumentumban, vagy egy külön villamosenergia kibervédelmi stratégiában meghatározni az elérendő célokat, a megvalósítás módját és eszközeit- valamint határidejét, illetve a felelősöket, továbbá a visszaellenőrzés eszközszerkezetét. Érdemes lenne nagy hangsúlyt fektetni a PPP-re. Szükséges lenne a szakma által használt kifejezések magyarázata is a dokumentumban.

Fontos, hogy a stratégiában megjelenő feladatok visszamérhető legyenek, ennek a rendszerét is ki kell dolgozni. Nem elég a feladatokat meghatározni, mellyel bizonyos célokat kíván a nemzet a kibervédelem területén elérni a villamosenergia alágazat vonatkozásában, hanem egy supervisor team általi megvalósulás ellenőrzés keretrendszere is részét kellene, hogy képezze a nemzeti kiberbiztonsági stratégiának.

A jelenlegi formában az ENISA honlapon megjelenő magyar kibervédelmi stratégia nem mutat jól a többi stratégia mellett. Javasolt lenne egy olyan stratégia megalkotása, amely meghatározott elképzeléssel bír a villamosenergia alágazati szereplők kiberbiztonságának megvalósításáról, megfelelő formában megszerkesztve, és naprakészen kezeli a folyamatosan felmerülő problémákat a kiberbiztonság területén.

A 2020 év elején megjelent Nemzeti Energiastratégiában új elemként megjelent kiberbiztonsági fejezetet olvasva megállapítható, hogy az a Nemzeti Kiberbiztonsági Stratégiát nem említi, azzal nincs kapcsolatban.

Az ENISA interaktív térképén jeleníti meg a nemzeti kiberbiztonsági stratégiákat.¹⁷⁶

A jelenleg hatályos 1139/2013. (III. 21.) Korm. határozat stratégia (NKS) és a 1838/2018. (XII. 28.) Korm. határozat alapján nyilvánosságra hozott hálózati és információs rendszerek biztonságára vonatkozó Stratégia¹⁷⁷ (a továbbiakban: Új stratégia) egyaránt elemzésre kerül.

A stratégia kibervédelmi vonatkozásainak elemzése:

1. A célok megfelelően kifejtésre kerülnek az új stratégiában. A gyermekvédelem, oktatás tudatosság, K+F, PPP, mint célok megfelelően definiáltak.
2. A régi NKS elavult, és az egyéb szakterületet érintő szabályozók követését nem hivatott elősegíteni. Az Új stratégia még nem került hivatalosan kiadásra, de már elavult (példa: BM OKF, mint eseménykezelő központ).

¹⁷⁶ <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>

¹⁷⁷ <https://nki.gov.hu/wp-content/uploads/2020/11/Strat%C3%A9gia-a-h%C3%A1l%C3%B3zati-%C3%A9s-inform%C3%A1ci%C3%B3s-rendszerek-biztons%C3%A1g%C3%A1ra.pdf>



3. A célok a korábbiakban említettek szerint kifejtésre kerülnek az Új stratégiában, azonban nem volt meghatározva az, hogy azt milyen módszerrel kívánjuk elérni, illetve ki az 56 megfogalmazott intézkedésnek a felelőse, és hogy mikorra kell a feladatokat megvalósítani (ütemezés). Ez a hiányosság azóta pótlásra került.¹⁷⁸
4. Az ENISA honlapján fentlévő magyar kiberbiztonsági stratégia nem fest jó képet az ország kibervédelméről. Egy megfelelően felépített stratégia angol nyelven megfogalmazva jobb képet mutatna a hazai kibervédelem rendszeréről az alapok bemutatása által. Ha ez még nem változik egy ideig, javasolt lenne a kiegészítése a Nemzeti Energiastratégiában megjelent kiberbiztonsági résszel.
5. Az NKS egyáltalán nem említi, az Új stratégia pedig bemutatja, hogy jelenleg milyen szabályozói vannak a rendszernek. A jelenlegi szabályozás és gyakorlat azonban jelenleg nem kezeli a villamosenergia alágazati szereplők kibervédelmét, amely a Nemzeti Energiastratégiában 2020 év elején megjelent. Az Új stratégia megfogalmazása szerint Magyarország területére terjed ki. A nemzetközileg összekapcsolt villamosenergia-rendszerek így nem teljeskörűen kezeltek, ezáltal nem lehet azt mondani, hogy a magyarországiak teljeskörűen kezelve lennének.

Az európai kritikus infrastruktúrák (többek között villamosenergia) azonosításának hiánya indította el a DG HOME általi ECI (Európai Kritikus Infrastruktúra védelmi) direktíva (CIP irányelv) megújítását, az előző hiányosságra tekintettel. A határokon átnyúló rendszerek azonosítása létfontosságú érdek, főleg a minden kritikus infrastruktúra alapját képező villamosenergia-rendszerek tekintetében.

Az EU alapvető szolgáltatásként definiálta a villamosenergia alágazat által biztosított szolgáltatásokat, és meghatározta a szereplők pontos körét is a NIS irányelv vonatkozó mellékletében. A DG CNECT az a felelős Főigazgatóság, amely dolgozott az alapvető szolgáltatást nyújtók kiberbiztonsági szabályozásának megfelelőségén.

2018 év elején a két Főigazgatóság (DG HOME és DG CNECT) felismerte, hogy a CIP irányelv felülvizsgálata és a NIS irányelv készítése párhuzamosan, párbeszéd nélkül zajlott, így duplikáció és egyéb (pl. azonosítási) problémák merültek fel. A párbeszéd megindult, az eredménye feltételezhetően a NIS 2.0-ban fog megjelenni.

Jelenleg az alapvető szolgáltatást nyújtók a villamosenergia alágazatban a kijelölt létfontosságú rendszerelemek.

¹⁷⁸ A részletes intézkedési terv elérhető az alábbi link megnyitásával:
<https://2015-2019.kormany.hu/download/3/6d/b1000/Int%C3%A9zked%C3%A9si%20terv%202020-2022.pdf#!DocumentBrowse> linken.



Meg kell jegyezni, hogy az Ibtv. és a végrehajtására kiadott 41/2015. BM rendelet nem kezeli az alágazati sajátosságokat, ezért vagy új energia ágazati végrehajtási rendelet lenne szükséges (pl.: NIST 800-82 alapon), vagy a 41/2015. BM rendelet bővítése, és a kivétel rendszerek kidolgozása. (Ez más ágazatokat érintő probléma is pl.: víz, egészségügy stb.)

6. Együttműködések mind a két stratégiában említésre kerülnek, azonban azok elvárt eredményei nem kerülnek megfogalmazásra. Pontosan azonosítani kellene, hogy mi az elvárás a NATO-val történő együttműködés, vagy a PPP kapcsán, és ehhez határidőket és felelősöket rendelni, illetve a megvalósulást érintő ellenőrzési rendszert. A megvalósulás hiányának vagy nem megfelelőségének kellene generálnia a stratégia felülvizsgálata utáni módosítását.
7. A kiberkoordinátornak rendkívül fontos szerepe lenne az Új stratégiában megfogalmazott intézkedések végrehajtásában. Az Nemzeti Kiberbiztonsági Koordinációs Tanáccsal együtt lehetne egy supervisor-i feladatkörrel ellátott szereplő, illetve a villamosenergia alágazati szereplők döntéshozóival és/vagy szakembereivel együttesen.
8. Az intézkedések (56 db) határidővel ellátottak, azonban nem szabad figyelmen kívül hagyni azt sem, hogy a meghatározott idő elteltével a stratégiát felül kellene vizsgálni, és fejleszteni kellene. Erre vonatkozóan nem tartalmaz rendelkezést egyik stratégia sem.
9. A kiberfenyegetések folyamatosan fejlődnek, ahogy a támadások számai is világszerte. A szabályozás, illetve az elvileg alapját képező stratégia kiadásának hiánya egy olyan idő szakadékot eredményez, amely a megfelelő védelem kialakítását nagy mértékben hátráltatja.
10. A Nemzeti Energiastratégiában megjelenő kiberbiztonsági rész rövid helyzetképet és intézkedési javaslatokat határoz meg a villamosenergia alágazati szereplők vonatkozásában.

Összefoglalva a stratégia elemzést elmondható, hogy konkrétumok kellene a villamosenergia alágazati szereplők kiberbiztonságának megteremtése érdekében, a vízió és a felületes stratégiai célok helyett. Határidők, felelősök, visszaellenőrzési keretrendszer, folyamatos stratégia fejlesztés. A villamosenergia alágazat sajátosságait nem nélkülözheti a nemzeti kiberbiztonsági stratégia, mert annak a következménye a nem teljeskörű kibervédelem kialakítása lesz. Ehhez az NKS és a Nemzeti Energiastratégiában megjelent kiberbiztonsági részt összhangba kell hozni. A stratégia elsődleges célja az kell, hogy legyen, hogy kezelje szabályozás szempontjából a villamosenergia-ipari szereplők helyzetét a kor kiberbiztonsági kihívásainak megfelelően, mert a jelenlegi stratégiai környezet és a szabályozás erre nem alkalmas teljeskörűen.



5. melléklet: A 2020. évi Nemzeti Energiastratégia kiberbiztonsági vonatkozásai

A kormány 2020. januárjában elfogadta az új Nemzeti Energiastratégiát.¹⁷⁹ Ennek a korábban hatályoshoz képest lényeges újdonsága, hogy önálló fejezetben (13. Kiberbiztonság) ad hangsúlyt az energetikai létesítmények – így a villamosenergia-rendszer – kiberbiztonságának.

A fejezet a kiberbiztonságot a nemzetbiztonság egyik legfontosabb elemeként, szuverenitásunk megőrzésének egyik feltételként határozza meg és célul tűzi ki a kiberbiztonság általános szintjének lehető legmagasabbra emelését.

A fejezet röviden értékeli a villamosenergia-rendszert a kibertér felől érő kihívásokat. Helyesen rámutat a régebbi, az aktuális kihívásoknak megfelelni képtelen technológiai megoldások kiberbiztonsági kihívásaira.

A stratégia intézkedési javaslatokat is megfogalmaz:

1. Szektorális kiberbiztonsági követelményrendszer

A feladat abból fakad, hogy jelenleg a magyar villamosenergia-rendszerben érintett jelentősebb szervezetek nem tartoznak a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.) hatálya alá, azaz – a stratégia készítésének idején még – nem lettek létfontosságú rendszerelemmé kijelölve. Ezzel összhangban a létfontosságú rendszerek és létesítmények védelmével kapcsolatos jogszabályi környezetet úgy kell átalakítani, hogy a küszöbértékek lehetővé tegyék a jelentősebb szervezetek létfontosságú rendszerelemmé történő kijelölését. Javasolt az érintett szakmai szervezetek bevonásával a szektorális sajátosságok figyelembevételével a hatályos kiberbiztonsági követelményrendszer – a 2013. évi L. törvény (Ibtv.) és a 41/2015. BM rendelet – követelményeinek módosítása (figyelembe véve azt is, hogy a 41/2015. BM rendelet egyes rendelkezései a villamosenergia-iparban használt ICS és SCADA rendszerek esetén nem értelmezhetőek, vagy nem alkalmazhatóak e rendszerek működési/felhasználási sajátosságai miatt).

Üdvözlendő javaslat a megelőző, érzékelő és reagáló képesség folyamatos javítása a követelményrendszer meghatározásával, célirányos gyakorlatok szervezésével, támogatási eszközök megteremtésével. A 41/2015. (VII. 15.) BM rendelet mellékleteiben foglalt kontrollkörnyezet bizonyos – az adott ágazati üzemeltetés szempontjából releváns kontrollok kiemelésével – elemeiből üzemeltetőre szabott egyedi kontrollrendszert szükséges kialakítani.

¹⁷⁹ Nemzeti Energiastratégia 2030, kitekintéssel 2040-ig. Tiszta, okos, megfizethető energia (a Kormány 2020. január 8-i ülésén elfogadott szöveg)



A módosítás értelmében az információbiztonsági hatóság az adott üzemeltető számára irányadó kontrollkörnyezet elemeiben egyedi összetételű követelményrendszert engedélyezhet az üzemeltető kockázatelemzése alapján. A kijelölések megtörténtek és jelenleg a megfeleléssel kapcsolatos feladatok végrehajtása zajlik.

2. Szektorális kiberbiztonsági információ megosztás

Az energiaszektorban érintett jelentősebb szervezetek között hatékonyabbá kell tenni az információ megosztást mind hazai, mind nemzetközi szinten. A stratégia értelmében a magyar energiaszektorban érintett jelentősebb szereplők (energiatermelők, -szolgáltatók, rendszerirányítók) közötti, rendszeres információ megosztást kormányzati koordinációval kívánják elindítani. Ennek keretében szükséges kialakítani a releváns villamosenergetikai vonatkozású kiberbiztonsági információk automatizált megosztásának lehetőségeit is.

3. Gyorsreagálású egység felállítása incidenskezelésre

A stratégia értelmében az egység helyszíni támogatást nyújt az egyes szereplők számára kiberbiztonsági incidensek esetén (nyomrögzítés, fenyegetés-elemzés, hálózatbiztonsági monitoring, incidenskezelés, különböző támadói eszközök és módszerek elemzése).

4. Humánerőforrás kérdések

A stratégia helyesen foglal állást, hogy a kiberbiztonsági helyzet javításához (vagy legalább a kiberbiztonsági kockázatok szintjének további romlásának megelőzéséhez) a legfontosabb intézkedésnek a kiberbiztonsági tevékenységek képzett és tapasztalt szakemberekkel történő folyamatos ellátását tartjuk.

Összegezve: a stratégia nagy előrelépés, hogy önálló fejezetként, hangsúllyal jelenik meg benne az energetikai kiberbiztonság témája. Ugyanakkor a kiberbiztonság fejlesztése nem szerepel a stratégia szerinti zászlóshajó projektek között.

A kézikönyv 5.2. pontja szerintiék ráerősítenek, terjedelmében és mélységében is kifejtik a hatályos Nemzeti Energiastratégiában foglaltakat.



6. melléklet: A 2020. évi Nemzeti Biztonsági Stratégia kiberbiztonsági vonatkozásai

A Kormány a 1163/2020. (IV. 21.) határozatával elfogadta Magyarország Nemzeti Biztonsági Stratégiáját. Ebben a Kormány elkötelezettségét fejezi ki azzal, hogy 2030-ra Magyarország Európa 5, a világ 10 legbiztonságosabb országainak egyikévé váljon. Ehhez meghatározza, hogy a kibertér felőli biztonság alapvető értéke hazánkunk, amelyet fenntartani és erősíteni szükséges.

A nemzeti létfontosságú infrastruktúra védelmét a stratégia megfelelően megoldottnak tekinti. A hibrid támadásokkal szembeni ellenállóképességről is említést tesz a Kormányhatározat, valamint a hibrid fenyegetések növekvő üteméről. Ugyanakkor megjegyzi, hogy fejleszteni szükséges az információs és kiberhadviselés elleni védekezés rendszerét. A hibrid hadviselés elleni nemzeti – valamint az elsősorban az Európai Unió és az Észak-atlanti Szerződés Szervezete (NATO) keretein belül a többnemzeti – válaszadási képesség fejlesztése Magyarország érdeke.

A stratégia említést tesz a kiberbiztonsági kapacitás folyamatos fejlesztéséről, és a hazai szervezetek dolgozóinak körében tapasztalható alacsony információbiztonsági tudatossági szintről.

Az energia ágazaton belül a villamosenergia arányának jelentős növekedését vizionálja a stratégia, azonban Magyarország energia ellátásbéli kiszolgáltatottságát is taglalja. A folyamatos energiaellátás kritikus fontosságú az egyének és a gazdaság szempontjából is, ezért az energiaellátás rendkívüli jelentőségű. Az energiapolitika céljai az energia szuverenitás, az energiabiztonság megerősítése, valamint az energiatermelés dekarbonizációja, mindez az energiainport csökkentése mellett.

A Kormányhatározatban kiemeli a növekvő számú APT támadásoknak, a kiberbűnözői csoportok aktivizálódásának, az elektronikus információs rendszerek sérülékenységeinek veszélyeit.

A kibervédelem területén a kutatás és fejlesztés kiemelt figyelmet érdemel, ennek hangot ad a Nemzeti Biztonsági Stratégia.

A közműszolgáltatók elleni kibertámadásokat kiemelt biztonsági kockázatként kezeli Magyarország, ahogy az energiainportban bekövetkezett fennakadásból fakadó ellátási válsághelyzet létrejöttét is.

A stratégia célul tűzi ki a hibrid fenyegetések elleni hatékony fellépést, valamint a kiberbiztonság garantálását, hogy a nemzeti létfontosságú információs infrastruktúra zavartalanul működhessen. Ugyancsak cél a kiberképességek fejlesztése, a hibrid fenyegetések megelőzése, felderítése és elhárítása.



7. melléklet: A 2020. május 1-jei elnöki rendelet és annak háttere

1. A rendelet

2020. május 1-jén „Executive Order on Securing the United States Bulk-Power System” címmel az Egyesült Államok elnöke rendeletet adott ki, melyben az USA villamosenergia-rendszerét fenyegető veszélyek miatt országos vészhelyzetet hirdetett ki.¹⁸⁰ A rendelet általánosságban a 69 kV, vagy annál nagyobb névleges feszültségű villamos hálózati és erőművi berendezésekre, valamint azok felügyeleti rendszereire vonatkozik. Az érintett berendezések egyebek mellett nagytranszformátorok, turbinák és generátorok, megszakítók, szabályozó transzformátorok, fojtók, kondenzátorok, csatoló kondenzátorok és nem utolsó sorban relévédelmi és mérő berendezések, ipari felügyeleti rendszerek.

A rendelet indoklása szerint az USA ellenérdekű felei egyrészt egyre inkább törekednek az USA villamosenergia-rendszere sebezhetőségeinek a kihasználására (beleértve kibertámadásokkal is), másrészt további sebezhetőségeket igyekeznek kiépíteni. Ezt az USA nemzetbiztonságának, kritikus infrastruktúráinak, gazdaságának zavartalan villamosenergia-ellátása szempontjából elfogadhatatlannak ítélik. A rendelet katasztrofális hatásokat felvető lehetőségként nevezi meg a külföldi tervezésű, fejlesztésű, gyártású villamos hálózati berendezések eddigi beszerzési és alkalmazási gyakorlatát, valamint az ilyen berendezések és rendszerek külföldiek általi tulajdonlását, irányítását. Bár a rendeletben az USA kifejezi a befektetések szabadságában való további érdekelttségét, de ezt a továbbiakban egyensúlyba kívánja hozni az ország nemzetbiztonsági érdekeivel.

Az USA területén tiltottá válik a rendelet értelmében hatálya alá tartozó bármely olyan külföldi érdekelttségű villamosenergetikai áruk beszerzése és telepítése, amelyek nem felelnek meg egy az egyebek mellett az energiaügyi, belügy, védelmi és kereskedelmi miniszterektől, a nemzeti hírszerzési igazgatóból álló munkacsoport által kialakítandó követelményeknek. Egyebek mellett:

- azonosítani kell a korábban külföldi tervezésben, fejlesztésben, gyártásban létrejött villamos hálózati rendszerelemeket,
- ajánlásokat kell kidolgozni az ilyen elemek mielőbbi elkülönítésére, megfigyelésére vagy cseréjére,
- meg kell határozni azokat a kritériumokat is, amelyek alapján egy a jövőbeni beszerzések során alkalmazandó lista készíthető az előminősített, kockázatot hordozó villamosenergetikai berendezésekről és azok beszállítóiról.

¹⁸⁰ White House. „Executive Order on Securing the United States Bulk-Power System.” [39] <https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/> (Letöltve: 2020. augusztus 28.)



A munkacsoport egyebek mellett értékeli a nemzetbiztonsági szempontoknak az energiabiztonsági és kiberbiztonsági politikába való beépítéséhez használt módszereket és kritériumokat. A végrehajtás részletei a rendelet kiadásától számított 150 napon belül kerülnek meghatározásra.

2. Háttér és lehetséges következmények

A rendelet egyszerre tekinthető váratlannak és egyben a hatályba léptetési amerikai politika logikus következményének. Váratlan abból a szempontból, hogy kiadásának nem volt szélesebb szakmai körben nyilvánosan érzékelhető előjele, továbbá mindeddig nem is került nyilvánosságra az USA villamosenergia-rendszerét az addigiakon túli ért olyan kiemelkedő incidens, ami indokolhatná egy ilyen kemény intézkedés akkori meghozatalát. Ugyanakkor az USA villamosenergia-rendszerét az elmúlt években főleg a kibertér felől ért, folyamatosan növekedő számú fenyegetés tükrében számítani lehetett valamilyen szövetségi szintű intézkedésre. Ennek a mostaninak külön súlyt ad, hogy ilyen magas szinten, azaz elnöki rendelet formájában került kiadásra.

Az USA-t a kibertér felől érő fenyegetésekre adandó válasz első komolyabb jele a CISA¹⁸¹, mint illetékes ügynökség által 2017. október 20-án kiadott riasztás volt.¹⁸² Ez még csak általánosságban utalt az USA energetikai és egyéb kritikus infrastruktúráját érő fejlett és rendszeres fenyegetésekre. Aztán fél év múlva, 2018. április 16-án a CISA újabb riasztást adott ki. Ez már címében is konkrét, hálózati eszközöket és rendszereket érintő orosz, állami hátterű kiberfenyegetést nevesít.¹⁸³

Egyes közlések a kínai JHSP transzformátorgyártó egyik USA-ba szállított és ott lefoglalt transzformátort említik a lehetséges előzmények között.¹⁸⁴ [40] Amerikai szakmai berkekben vita bontakozott ki a Purdue modell szerinti 0. – és esetleg 1. – szint elemeit veszélyeztethető új típusú fenyegetésről, amely az ezekbe (pl. transzformátorra szerelt szenzorokba, avagy transzformátor felügyeleti elektronikába) még a gyártó által beépített hátsóajtók formájában jelenik meg.¹⁸⁵ [41]

¹⁸¹ CISA: Cybersecurity and Infrastructure Security Agency (Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség)

¹⁸² Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors, <https://www.us-cert.gov/ncas/alerts/TA17-293A>

¹⁸³ Alert (TA18-106A): Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, <https://www.us-cert.gov/ncas/alerts/TA18-106A>

¹⁸⁴ S. Varghese. „US seized Chinese-built transformer – but nobody knows why.” IT Wire. <https://www.itwire.com/government-tech-policy/us-seized-chinese-built-transformer-%E2%80%93-but-nobody-knows-why.html> (Letöltve: 2020. augusztus 30.)

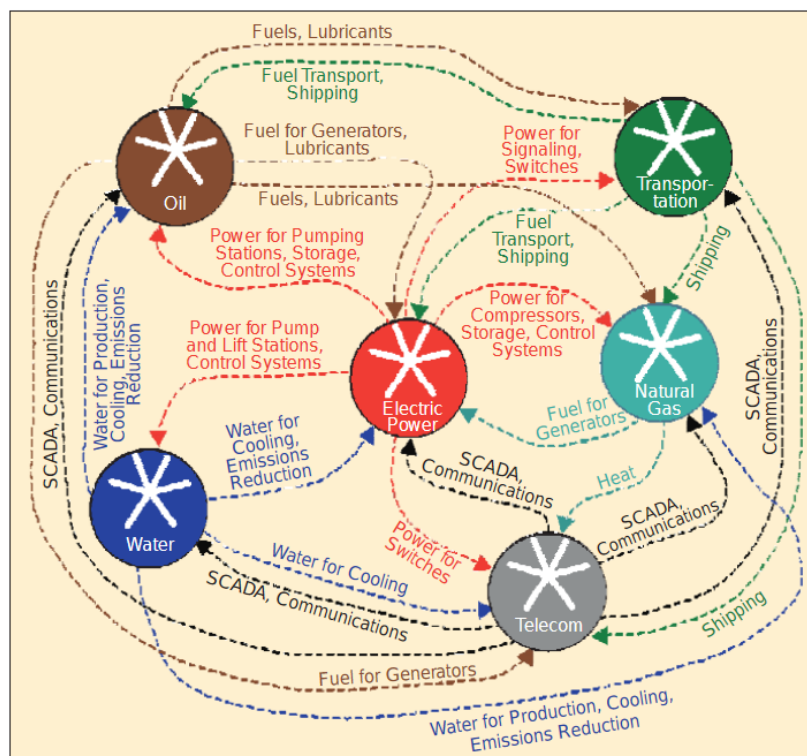
¹⁸⁵ J. Weiss. „ICS cyber security is the second coming of the Maginot Line – and the Chinese have breached it.” EnergyCentral. <https://energycentral.com/c/ics-cyber-security-second-coming-maginot-line-%E2%80%93-and-chinese-have-breached-it> (Letöltve: 2020. augusztus 30.)



A villamosenergia-rendszer szempontjából veszélyt jelenthet, ha a támadó a hátsóajtón keresztül át tudja venni az ún. szabályozó transzformátorok fokozatkapcsolóinak a vezérlését, avagy az érzékelőkkel a valóstól eltérő kapcsolókészülék állásjelzéseket, illetve mérési értékeket tud küldetni a védelmek és/vagy a SCADA felé, ezzel azok téves működését, akár fizikai károsodását okozhatja. Ez utóbbi felhívja a figyelmet a hihetőségvizsgálati funkció várható felértékelődésére, avagy általánosságban a villamosenergia-rendszer ellenálló képessége erősítésének a szükségességére.

A rendelet létrejötte és tartalma beleillik az USA Trump elnök hatalomra kerülése óta folytatott, „America first” szlogennel összegezhető politikájába. A rendelet logikusan következik az USA-nak a kínai Huawei kommunikációs hálózati eszközeivel kapcsolatban tett drasztikus, Kínával nyíltan konfrontatív, a két nagyhatalom közötti konfliktust kiváltó lépéseiből.

A mostani rendelet arra utal, hogy az USA nagyon komolyan veszi a zavartalan villamosenergia-ellátás fontosságát. A civilizáció jelenlegi, minden eddiginél szélesebb körben különféle digitális technológiákat alkalmazó – sőt arra ráutalt – fejlettségi fokán hangsúlyosan igaz, hogy a kritikus infrastruktúrák működése egyértelműen a villamosenergia-rendszer zavartalan működésének függvénye. A függést jól mutatja a 7.1. ábra.



7.1. ábra: Kritikus infrastruktúrák függősége¹⁸⁶

¹⁸⁶ Rinaldi, S.M. & Peerenboom, James & Kelly, T.K.. (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE. 21. 11 - 25. 10.1109/37.969131.



A függőségi rendszer tükrében egyre inkább kijelenthető, hogy a villamosenergia-rendszer a legkritikusabb kritikus infrastruktúra. E logikával összhangban e rendelettel az USA kinyilvánítja, hogy a villamosenergia-rendszer biztonságát nemzetbiztonsági kérdésnek tekinti. A rendeletben foglaltak tükrében az USA határozott lépéseket kíván tenni annak érdekében, hogy megelőzze a korábban a Huawei esetében komolynak ítélt azon veszélyt, hogy valamely idegen hatalom befolyást gyakorolhasson az USA valamely kritikus infrastruktúrájának működésére, megbízhatóságára.

A rendeletnek szakmailag is figyelemre méltó eleme a külföldi eredetű kockázatot hordozható rendszerelemek mielőbbi azonosítására, elkülönítésére, megfigyelésére vagy cseréjére vonatkozó előírás. Ez a technológiák mai fejlettségi szintjén példa nélküli, azaz megvalósítása óriási szakmai és jelentős erőforrásokat kívánó gyakorlati kihívás lesz, messze ható tanulságok mellett.

A nyilvánosan elérhető információk alapján az elnöki rendelet a Huawei esettel ellentétben nem egy az USA és Kína közötti konkrét konfliktus folyamánya. A rendelet szövege nem nevesít konkrét országot. Azt a jóval átfogóbb szándékot tükrözi, hogy az USA a továbbiakban egyetlen külföldi ország vonatkozásában sem szándékozik kockázatnak kitenni országa villamosenergia-rendszerét. Az USA globális súlya ismeretében ez a szándék érthető. Kiemelkedő erőforrásai révén az USA képes is lehet arra, hogy hazai érdekeltségű tervezőkkel, gyártókkal, létesítőkkel, üzemeltetőkkel ki tudja szolgálni az ország villamosenergia-rendszerének igényeit. Az e szándékot támogató konkrét intézkedések 150 nap elteltével derülnek ki.

Közismert, hogy Yokogawa gyártmányú hamisított távadók kerültek az USA-ba és beépítésre is kerültek.¹⁸⁷ [42] 2020-as fejlemény, hogy olyan kínai gyártmányú óriástranzformátor került leszállításra az USA-ba, amelynek átvételi vizsgálatai „oda nem való” elektronikát derítettek fel. Ezt követően a transzformátor nem került beépítésre.¹⁸⁸ [43]

3. Hazai hatások

Az elnöki rendelet minden bizonnyal más országokat is hasonló lépésekre fog készíteni. Ugyanakkor korlátos azon országok száma, amelyek az USA-hoz hasonlóan a villamosenergia-rendszer valamennyi kritikus elemét és rendszerét saját maguk képesek biztosítani.

¹⁸⁷ J. Weiss. „An Assessment of Presidential Executive Order 13920 – Securing the United States Bulk-Power System.” Control Global. <https://www.controlglobal.com/blogs/unfettered/an-assessment-of-presidential-executive-order-13920-securing-the-united-states-bulk-power-system/> (Letöltve: 2020. augusztus 30.)

¹⁸⁸ J. Weiss. „Emergency Executive Order 13920 – Response to a real nation-state cyberattack against the US grid.” Control Global. <https://www.controlglobal.com/blogs/unfettered/emergency-executive-order-13920-response-to-a-real-nation-state-cyberattack-against-the-us-grid/> (Letöltve: 2020. augusztus 30.)



Ez minden bizonnyal felértékeli az ezen elemek tervezői, gyártói, létesítői, üzemeltetői által a jövőben nyújtandó biztonsági garanciák kérdését.

Hazánk nincs abban a helyzetben, hogy villamosenergia-rendszere védelmében az USA-hoz hasonló mélységű lépéseket tegyen. Ugyanakkor az amerikai elnök rendelete talán elősegíti azt, hogy az eddiginél nagyobb hangsúlyt kapjanak az egyéb kritikus infrastruktúrák villamosenergia-ellátástól való – szakmai berkekben egyébként köztudott – függőségei, de főleg a fenyegetések növekvő számával és súlyával összhangban álló (kiber)biztonsági szint garantálásához szükséges komplex intézkedések és ezek esetleges nemzetbiztonsági vonatkozásai.



Az elnöki rendeletnek nem látszanak a magyar villamosenergia-rendszert érintő azonnali és jelentős hatásai. Hosszabb távon annál inkább. Egyetlen ország, így Magyarország sem vállalhat fel olyan kockázatot, hogy kulcsfontosságú berendezései felett ne rendelkezzenek 100%-os felügyelettel.



Az idegen eredetű hozzáférések megelőzése és megakadályozása egyebek mellett a szabályozási, beszerzési, tervezési, gyártási, létesítési, üzembehelyezési, üzemeltetési keretek célirányos átalakítását teheti szükségessé. Átfogó rendszert kellhet kiépíteni a kompromittált berendezések, hardver és szoftver elemek, akár chip-ek kiszűrésére. Mindezt intenzív kutatás-fejlesztésnek kellhet támogatnia.



8. melléklet: A hatályos hazai szabályozási környezet bemutatása

Jelen melléklet áttekintő jelleggel mutatja be a hazai kiberbiztonsági szabályozás energetikai ágazatra irányadó rendelkezéseit. A SeConSys platform WG-R munkacsoportja villamosenergia-rendszer kiberbiztonságával összefüggésben végzett szakértői munkája részeként készült elemzés célja a releváns hazai normatív szabályanyag számbavétele és rövid bemutatása. Az elemzés nem minősül jogi tanácsadásnak.

A dokumentum az általános, szektorfüggetlen jogszabályokat, illetve az ágazati, szektorspecifikus normákat a normák tartalmát kifejtő végrehajtási rendeletekkel egységben tárgyalja *(az adott törvényt közvetlenül a releváns végrehajtási rendeletei követik)*. A jogszabályok feldolgozása a SeConSys céljainak megfelelően történt, így az elemzés kizárólag a vizsgált joganyag releváns rendelkezéseire szorítkozik.

Az elemzésben az alábbi jogszabályok kerültek feldolgozásra:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
 - 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
 - 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
 - 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Lrtv.)
 - 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról (Lrtv. vhr.)
 - 374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 2007. évi LXXXVI. törvény a villamosenergiáról



- 1996. évi CXVI. törvény az atomenergiáról
 - 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről
 - 118/2011. (VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről

1. A hatályos joganyag bemutatása

1.1. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

személyi/szervezeti hatály	• 2. § (1) bekezdésében felsorolt állami- és önkormányzati szervek, intézmények • a 2. § (1) bek. szerinti szervek számára adatkezelést végzők • a jogszabály alapján a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói • az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek (<i>a továbbiakban együttesen: létfontosságú infrastruktúrák</i>)
szabályozási kör	a jogszabály hatálya alá tartozó szervezetek elektronikus információs rendszerei (<i>hálózatok, eszközök/eszközcsoporthok és digitális adatok; a továbbiakban: EIR</i>)
releváns főbb rendelkezések	• információbiztonsági követelmények rögzítése: ▪ a törvény hatálya alá tartozó EIR-ek teljes életciklusában meg kell valósítani és biztosítani kell: ◦ az EIR-ben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint ◦ az EIR és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét;



- a védelem érdekében a kapcsolódó rendeletben (*41/2015 BM rendelet*) meghatározott olyan logikai, fizikai és adminisztratív intézkedéseket kell bevezetni, amelyek támogatják:
 - a megelőzést és korai figyelmeztetést,
 - az észlelést,
 - a reagálást, valamint
 - a biztonsági események kezelését;
- a kockázatarányos védelem érdekében a rendszereket biztonsági osztályba, a szervezetet, illetve az EIR-ek fejlesztését, üzemeltetését végző, azok üzemeltetéséért, információbiztonságáért felelős szervezeti egységeket biztonsági szintbe kell sorolni;
- a besorolásokat felül kell vizsgálni;
- a biztonsági osztályokhoz, szintekhez rendelt követelmények teljesítése a szervezet vezetőjének felelőssége;
- az EIR-ek biztonságáért felelős személyt kell kinevezni, vagy megbízni;
- informatikai biztonsági szabályzatot kell kiadni;
- a védelmi feladatokat és felelősségi köröket oktatni kell;
- rendszeres kockázatelemzést, ellenőrzést, auditokat kell lefolytatni;
- biztosítani kell az EIR eseményeinek nyomon követhetőségét;
- biztonsági esemény (*a továbbiakban: incidens*) bekövetkezése esetén gondoskodni kell a gyors és hatékony reagálásról, az incidens kezeléséről;
- közreműködő igénybevétele esetén megfelelő szerződéses kikötések (*SLA*) alkalmazandóak;
- az incidensekről, azok kockázatairól az érintetteket tájékoztatni kell;



- a norma rögzíti a szervezet vezetőjének felelősségét, az EIR biztonságáért felelős személy feladatait, kinevezésének feltételeit, valamint az EIR biztonságával összefüggő hatósági *(köztük az IBSZ-ekkel és besorolásokkal kapcsolatos nyilvántartási; ellenőrzési; intézkedés)* és eseménykezelési feladatokat és jogköröket;
- az érintett EIR-ek sérülékenységvizsgálatával, incidensek kivizsgálásával összefüggő jogi feltételeket;
- a kapcsolódó kormányzati koordinációs és központi oktatás-képzési hatásköröket

releváns kapcsolódások

- Lrtv.
- VET
- 65/2013. Korm. rendelet
- 187/2015. Korm. rendelet
- 271/2018. Korm. rendelet
- 41/2015. BM rendelet

hivatkozás

<https://net.jogtar.hu/jogszabaly?docid=a1300050.tv>

1.2. 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

személyi/szervezeti
hatály

- az EIR biztonsági felügyeletét ellátó hatóság (NBSZ Nemzeti Kibervédelmi Intézet, a továbbiakban: NBSZ NKI)

szabályozási kör

kapcsolódó hatósági feladatok, eljárások, jogkövetkezmények

releváns főbb
rendelkezések

- hatósági feladatok, eljárásrend;
- regisztráció és nyilvántartásba vétel;
- az érintett szervezetek kötelezettségei (tájékoztatás, az EIR-ek biztonságáért felelős személy kijelölése);
- jogkövetkezmények, bírságtételek



1.3. 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

személyi/szervezeti hatály	• eseménykezelő központok • sérülékenységvizsgálatot végző gazdálkodó szervezetek • Lrtv. ágazati szereplők
szabályozási kör	Incidentskezelés, sérülékenységvizsgálat
releváns főbb rendelkezések	• eseménykezelő központok feladata- és hatásköre; • incidensek bejelentése; • Lrtv. hatálya alá tartozó szervezetek önkéntes bejelentése; • incidenskezelés, műszaki vizsgálat szabályai; • sérülékenységvizsgálat szabályai
releváns kapcsolódások	• Ibtv. • 41/2015. BM rendelet
hivatkozás	https://net.jogtar.hu/jogszabaly?docid=A1800271.KOR

1.4. 41/2015 (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

személyi/szervezeti hatály	• az Ibtv. hatálya alá tartozó szervezetek
szabályozási kör	a rendelet az Ibtv-ben meghatározott biztonsági osztályba és szintbe sorolás követelményeit, valamint az egyes biztonsági osztályokhoz tartozó adminisztratív, fizikai és logikai intézkedéseket határozza meg, sorolja fel
releváns főbb rendelkezések	• meghatározza a biztonsági osztályba sorolás ismérveit; • meghatározza a biztonsági szintbe sorolás ismérveit;



- rögzíti, jelleg (*adminisztratív, fizikai, logikai*) és cél szerint kategorizálja, illetve biztonsági osztályhoz rendeli a védelmi intézkedéseket (*pl. adminisztratív intézkedések: IBSZ, EIR-ért felelős személy, nyilvántartások, engedélyezés, kockázatelemzés, beszerzés, üzletmenet folytonosság tervezése, eseménykezelés, személyi biztonság, tudatosság és képzés; fizikai intézkedések: engedélyezés, belépés ellenőrzése, hozzáférések felügyelete, riasztó és felügyeleti berendezések, áramellátás, tűzvédelem, hőmérséklet és páratartalom ellenőrzés, szállítás; logikai védelmi intézkedések: rendszerkapcsolatok, tervezés, beszerzés, biztonsági elemzés, tesztelés, képzés és felügyelet, konfigurációkezelés, karbantartás, adathordozók védelme, azonosítás és hitelesítés, hozzáférés ellenőrzése, rendszer és információ sértetlenség, naplózás, rendszer- és kommunikáció védelem*);
- taxatív felsorolja a biztonsági követelményeket;
- ha a szervezet csak az EIR meghatározott elemeit vagy funkcióit üzemelteti vagy használja, a rendelet előírásait kizárólag ezen elemek, funkciók tekintetében kell teljesíteni

releváns kapcsolódások

- Ibtv.
- 271/2018. Korm. rendelet

hivatkozás

<https://net.jogtar.hu/jogszabaly?docid=a1500041.bm>

1.5. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Lrtv.)

személyi/szervezeti
hatály

- a jogszabály mellékletében, illetve végrehajtási rendeleteiben meghatározott ágazati és horizontális kritériumok alapján azonosított és kijelölt létfontosságú rendszer elemek (*az ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszer eleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és*



	<i>vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna) üzemeltetői</i>
szabályozási kör	a jogszabály hatálya alá tartozó ágazatokban működő üzemeltetők nemzeti és európai létfontosságú rendszerelemei
releváns főbb rendelkezések	• az infrastruktúrák azonosítási vizsgálata és kijelölési eljárása; • üzemeltetői biztonsági terv kidolgozásának előírása; • biztonsági összekötő személy foglalkoztatásának kötelezettsége; • incidens bejelentési kötelezettség előírása az NBSZ NKI felé;
releváns kapcsolódások	• Ibtv. • 65/2013. Korm. rendelet • 374/2020. Korm. rendelet • 271/2018. Korm. rendelet • 41/2015. BM rendelet
hivatkozás	https://net.jogtar.hu/jogszabaly?docid=A1200166.TV
<i>1.6. 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról (Lrtv. vhr)</i>	
személyi/szervezeti hatály	• Lrtv. hatálya alá tartozó szervezetek; • javaslattevő, kijelölő és ellenőrző hatóság(ok)
szabályozási kör	lehetséges létfontosságú rendszerelemek azonosításának és kijelölésének szabályai, kötelezettségek
releváns főbb rendelkezések	• a lehetséges létfontosságú rendszerelemek azonosítási vizsgálata, az azonosítási jelentés tartalma; • a nemzeti/európai létfontosságú rendszerelemmé történő kijelölés tartalma, a kijelölés visszavonása;



- a biztonsági összekötő személy képesítési követelményei és foglalkoztatásának feltételei;
- az üzemeltetői biztonsági terv és tartalmi elemei;
- az ellenőrzés szabályai (*az informatikai biztonsági megfelelés is vizsgálatra kerül*);
- szankcionálás szabályai;
- nyilvántartás és adatbiztonság szabályai;
- együttműködés szabályai;
- komplex gyakorlat szabályai;
- alapvető szolgáltatást nyújtó szereplők azonosításának egyéb szabályai;
- a horizontális kritériumok tartalma;
- üzemeltetői biztonsági terv felépítése;
- alapvető szolgáltatások jegyzéke;
- bírságtételek.

releváns kapcsolódások

- Lrtv.
- Ibtv.
- 374/2020. Korm. rendelet
- 41/2015 BM rendelet

hivatkozás

<https://net.jogtar.hu/jogszabaly?docid=A1300065.KOR>

1.7. 374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

személyi/szervezeti
hatály

- energetikai létfontosságú rendszerelemek üzemeltetői

szabályozási kör

az energetikai létfontosságú rendszerek és létesítmények azonosítása, kijelölése, kijelölésének visszavonása és védelme

releváns főbb
rendelkezések

- azonosítási vizsgálatra kötelezettek,
- kijelölő hatóságok;



- az európai létfontosságú rendszerelemek ágazati kritériumai;
- a nemzeti létfontosságú rendszerelemek ágazati kritériumai;
- jelentős zavar mértéke;
- alapvető szolgáltatásokhoz tartozó küszöbértékek;
- rendkívüli eseményekre vonatkozó részletes ágazati szabályok.

releváns kapcsolódások

- Lrtv.
- 65/2013. Korm. rendelet

hivatkozás

<https://net.jogtar.hu/jogszabaly?docid=A2000374.KOR&searchUrl=/gyorskereso%3Fkeyword%3D374/2020>

1.8. 2007. évi LXXXVI. törvény a villamos energiáról (VET)

személyi/szervezeti
hatály

- villamosenergia piac szereplői (*VET 2. § - atomerőmű esetében az Atomtv. szabályaival összhangban*)

szabályozási kör

a villamosenergia termelése, átvitele, elosztása, kereskedelme, fogyasztása, továbbadása,

a villamosenergia-rendszer irányítására,

a villamosmű, az összekötő és a felhasználói berendezés, termelői vezeték, magánvezeték és a közvetlen vezeték építése, üzemeltetése, használatbavétele, fennmaradása és megszüntetése,

a törvény hatálya alá eső természetes személyek, jogi személyek közötti jogviszonyokra

releváns főbb
rendelkezések

- a felhasználók biztonságos és zavartalan villamosenergia-ellátása kiemelt közérdek;
- számlázás zártági feltételei (*jogosulatlan hozzáférés kizárása, adatmódosítás elleni védelem – a számlázási rendszernek meg kell felelnie az általános információbiztonsági zártági követelményeknek is, ennek érdekében adminisztratív, fizikai és logikai intézkedésekkel*)



kell biztosítani az általános információbiztonsági zártági követelmények teljesülését); a megfelelést tanúsító szervezet által történő, a számlázási informatikai rendszerre vonatkozó tanúsítással kell igazolni (a számlázási rendszerre vonatkozó követelmények teljesülése kizárólag informatikai biztonsági funkciókat megvalósító szoftvertermékek és -rendszerek elfogadott hazai vagy nemzetközi informatikai biztonsági módszertanon alapuló tanúsítására akkreditált tanúsító szervezet által kiállított tanúsítvánnyal igazolható); a számlázási rendszer információbiztonsági megfeleltetéséről az engedélyes az Ibtv. rendelkezéseinek megfelelő módon köteles gondoskodni (az egyedi számlázó szoftver forráskódszintű elemzése is előírás); a jogszabály a tanúsító szervezetekkel szembeni követelményeket is meghatározza

releváns kapcsolódások

- Ibtv.
- 41/2015 BM rendelet

hivatkozás

<https://net.jogtar.hu/jogszabaly?docid=A0700086.TV>

1.9. 1996. évi CXVI. törvény az atomenergiáról (Atomtv.)

személyi/szervezeti hatály

- nukleáris létesítmény és radioaktív hulladék-tároló engedélyesek;
- atomenergia alkalmazók

szabályozási kör

az atomenergia békés célú alkalmazása, a kapcsolódó jogosultságok és kötelezettségek

releváns főbb rendelkezések

- a fizikai védelem szabályai (tervezési alapfenyegetettség, mélységében tagolt védelem)

releváns kapcsolódások

- 190/2011. Korm. rendelet
- 118/2011. Korm. rendelet

hivatkozás

<https://net.jogtar.hu/jogszabaly?docid=99600116.TV>



1.10. 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről

személyi/szervezeti
hatály

- rendelet 1. §-ban foglalt felsorolás szerint

szabályozási kör

alkalmazott, tárolt, valamint szállított radioaktív sugárforrás és nukleáris anyag;

feldolgozott, tárolt, valamint szállított radioaktív hulladék;

radiológiai következmények szempontjából jelentős rendszer és rendszerelem;

a létesíteni tervezett és üzemelő nukleáris létesítmény;

a létesíteni tervezett és üzemelő átmeneti és végleges radioaktív hulladék-tároló; továbbá

a fix és mobil telepítésű ionizáló sugárzást létrehozó, radioaktív anyagot nem tartalmazó berendezések

releváns főbb
rendelkezések

- tervezési alapfenyegetettség meghatározása;
- programozható rendszer fogalmának meghatározása (olyan funkcionális eszköz vagy struktúra, amely alkalmas számítási, kommunikációs, automatizálási, vezérlési, ellenőrzési feladatok ellátására, ezen belül:
 - a létesítmény technológiájához kapcsolódó irányítástechnikai rendszerek,
 - a fizikai védelmi rendszerek,
 - a nukleáris biztosítéki rendszerek,
 - a radioaktív anyag nyilvántartási rendszerek, valamint
 - a létesítmény technológiájához közvetlenül nem csatlakozó olyan nukleáris biztonsági, fizikai védelmi, nukleáris biztosítéki és radioaktív anyag nyilvántartási rendszerek, amelyekhez, valamint az azokban tárolt, kezelt adatokhoz, információkhoz engedélyesi felelősség kapcsolódik;
- a programozható rendszerek védelmi működése nem befolyásolhatja a nukleáris biztonsági, fizikai védelmi,



nukleáris biztosítéki vagy radioaktív anyag nyilvántartási funkciók működőképességét;

- a programozható rendszerek védelmi követelményeinek meghatározása:
 - a programozható rendszerekben tárolt és kezelt adatok bizalmosságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer sértetlenségének és rendelkezésre állásának kockázatarányos biztosítása,
 - a rendszerek tervezése során el kell készíteni azok védelmi zónamodelljét (*a rendszereket azok nukleáris biztonsági-, fizikai védelmi-, nukleáris biztosítéki- és radioaktív anyag nyilvántartási funkciója rendelkezésre állási fontossága, valamint a bennük tárolt adatok és információk bizalmosságára, sértetlenségére és rendelkezésére állására vonatkozó elvárások szerint szintekbe, majd a vonatkozó védelmi követelmények alapján védelmi zónákba kell sorolni*); a különböző zónákhoz a fontosság szerint eltérő védelmi követelményeket kell meghatározni;
 - a programozható rendszerek védelmének felépítését és működését leíró védelmi tervet kell készíteni;
 - a védelmi tervében meg kell határozni mindazokat a műszaki, és adminisztratív védelmi intézkedéseket, amelyek alkalmazása biztosítja a programozható rendszerek védelmét a szándékolatlan károkozás és a tervezési alapfenyegetettségben meghatározott kibertámadásokkal szemben, a tervnek meg kell alapoznia és fenn kell tartania a mélységi védelem stratégiáját, hogy minden esetben biztosított legyen a szándékolatlan károkozások vagy a tervezési alapfenyegetettségben meghatározott kibertámadások mielőbbi érzékelése, kezelése (*következményeinek csökkentése, a sérülékenységek javítása*) és a normál működés helyreállítása;
 - a védelmi tervnek legalább az alábbiakra kell kitérnie:
 - fizikai és logikai hozzáférések,
 - konfigurációkezelés,



- azonosító- és jelszókezelés, jogosultságkezelés,
 - biztonsági javítások és szoftverfrissítések,
 - hordozható eszközök és mobil adathordozók használata,
 - vezeték nélküli készülékek és hálózatok,
 - távoli hozzáférés, adminisztrálás és karbantartás,
 - eseménykezelés, incidenskezelés, mentés és helyreállítás,
 - a fenyegetettségek és sérülékenységek felderítésére, elemzésére, dokumentálására és ezek kezelésére vonatkozó eljárások, valamint
 - rendszeres auditok és felülvizsgálatok,
 - programozható rendszerek jegyzéke,
 - a védelmi intézkedések megvalósíthatósága,
 - folytonos üzemvitel, rendszerek biztonsági mentése,
 - a rendszerek védelmével összefüggő változáskezelés, életciklus;
 - rendszeres felülvizsgálatokat kell végrehajtani;
 - kockázatelemzést kell készíteni a jogszabályban meghatározott gyakorisággal;
 - a programozható rendszerek védelmének felügyeletére a létesítmény legfelső vezetésének közvetlenül alárendelt szervezetet kell létrehozni vagy kijelölni;
 - képzés és gyakorlat szabályai;
 - tesztelés és karbantartás szabályai
- releváns kapcsolódások
- Atomtv.
 - 118/2011. Korm. rendelet
 - OAH FV-18. sz. útmutató

hivatkozás

<https://net.jogtar.hu/jogszabaly?docid=A1100190.KOR>



1.11. 118/2011. (VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről

személyi/szervezeti hatály • létesíteni kívánt, valamint a már üzemelő nukleáris létesítmények, azok rendszerei és rendszerlemei, a nukleáris létesítménnyel kapcsolatos tevékenységet végzők

szabályozási kör a rendelet 1. § (1) bekezdése szerint

releváns főbb rendelkezések a mélységében tagolt védelem 5 szintjének meghatározása, összetevői definiálása (a programozható irányítástechnikai rendszerek funkcióinak alrendszerekhez rendelése során alkalmazni kell a mélységben tagolt védelem elvét);

meghatározza a programozható irányítástechnikai rendszerekre irányadó követelményeket:

a nem biztonsági, vagy az alacsonyabb biztonsági osztályba sorolt funkciók nem építhetők be egy biztonsági osztályba sorolt, vagy magasabb biztonsági osztályba sorolt alrendszerbe;

különböző biztonsági osztályba sorolt programozható irányítástechnikai rendszerek közötti kapcsolat esetén igazolni kell, hogy az alacsonyabb osztályba sorolt rendszer a magasabb osztályba sorolt rendszer működését nem befolyásolja;

azonos biztonsági osztályba sorolt programozható irányítástechnikai rendszerek közötti kapcsolat esetén igazolni kell, hogy az egyik rendszer hibája a másik autonóm biztonsági funkcióinak teljesítését nem gátolja

releváns kapcsolódások • Atomtv.
• 190/2011. Korm. rendelet

hivatkozás <https://net.jogtar.hu/jogszabaly?docid=A1100118.KOR>

2. A szabályozás elemzése

A hatályos jogi szabályozás elsődleges igazodási pontja, központi eleme az ISO/IEC 27001-es szabvány (*Information technology – Security techniques – Information security management systems – Requirements*) és a NIST SP 800-53r4 ajánlás (*Security and Privacy Controls for*



Federal Information Systems and Organizations) fogalomrendszerére és megközelítésére épülő Ibtv.

A törvény nem egyenszilárd szabályozást ad, az egyes intézkedések kibontásában, részletezettségében eltérnek (*ennek oka a jogalkotás környékén keresendő*). A normaszövegben erőteljes hangsúlyt kap a hatósági hatáskörök tárgyalása. A jogszabályban kifejtett intézkedések és tevékenységek a pre-de-co elvre épülnek, vagyis a megelőzésre, észlelésre és reagálásra. A jogalkotó a kiberbiztonság (*a bizalmasság, sértetlenség és rendelkezésre állás együttese*) teljeskörű, a folyamatos, zárt, nyomon követhető és kockázatokkal arányos védelem valamennyi elemére kiterjedő szabályozásra törekedett. A törvényt végrehajtási rendelete, a biztonsági osztályba és szintbe sorolás ismérveit példálódzó módon kifejtő, a védelmi intézkedések katalógusát taxatív (*kimerítő, de részben redundáns*) felsorolás formájában feldolgozó 41/2015 BM rendelet tölti meg gyakorlati tartalommal.

Alapvetően szerencsés, a túlszabályozottság elkerülését és az egységes fogalomhasználatra épülő keretrendszer kialakítását biztosító megközelítésnek tekinthető az egy jogszabály köré szervezett, hivatkozásokra épülő szabályozásra törekvés. Az információbiztonsági joganyag, az Ibtv., mint központi kiberbiztonsági norma köré szervezése ugyanakkor nehézséget is jelent, gyakorlati tapasztalatok alapján a hatóság irányában jelentkező kötelezettségek, valamint azok komplexitása és erőforrásigénye visszatartják a szervezetek vezetőit az intézkedések bevezetésétől.

Az energetikán (és a villamosenergia ágazaton) belül – részben sajátos szabályozási tárgya, illetve a szabályozás tárgya által jelentett sajátos kockázatok alapján – a nukleáris terület kiberbiztonsági aspektusai tekinthetőek a leginkább kidolgozottnak. A zónamodell alkalmazása összhangban áll a nemzetközi szinten széles körben alkalmazott, IEC 62443 (*Industrial Network and System Security*) ipari-kiberbiztonsági szabvánnyal (*és alapvető elvei tekintetében nem tér el az osztályba sorolástól*).



A hazai szabályozás hiányossága leginkább az ipari, kifejezetten az irányítástechnikai sajátosságok figyelmen kívül hagyásában jelentkezik, e téren a már meglévő szabályozás módszerére és fogalomhasználatára épülő, egyedi, de teljeskörű szabályozás bevezetése jelentene előrelépést.



9. melléklet: Útmutató a létfontosságú rendszerelemmé kijelölt villamosenergia alágazati szereplők jogszabályi megfeleléséhez

1. Kötelezettségek

Kiindulási alap: az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 114/2008/EK irányelv (CIP irányelv), és az abban foglalt tagállami kötelezettségek:

- *energia és közlekedés ágazat prioritásként történő kezelése;*
- *sebezhetőségi pontok meghatározásának kötelezettsége (hazai szabályozásban ez a kockázatbecslésen alapuló azonosítási jelentés készítésében jelenik meg, amit az Lrtv. ír elő);*
- *azonosítás és kijelölés folyamatának meghatározása (hazai szabályozásban ez az üzemeltető által végrehajtott azonosítási vizsgálatként és a hatóságok által lefolytatott kijelölési eljárásként zajlik az Lrtv. 2. §-a szerint);*
- *horizontális kritériumok tagállami átvétele és értelmezése (hazai szabályozásban összesen 6 horizontális kritériumot vizsgálnak, amelyek az Lrtv. vhr. 1. mellékletében szerepelnek);*
- *ágazati kritériumok tagállami szintű megfogalmazása (hazai szabályozásban ágazati kormányrendeletekben találhatóak, villamosenergia alágazat kapcsán a 374/2020. (VII. 30.) kormányrendelet 4. §-ban);*
- *üzemeltetői biztonsági terv készítési kötelezettség meghatározása (hazai szabályozásban az Lrtv. írja elő és az Lrtv. vhr. 2. mellékletében szereplő tartalmi követelmények szerint készül);*
- *biztonsági összekötő személy alkalmazásának kötelezettsége (hazai szabályozásban az Lrtv. írja elő és az Lrtv. vhr. 6. §-a szerinti feltételeknek kell teljesülnie).*

Hazai szabályozási keret: irányadó jogszabály a 2013 márciusában hatályba lépett, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.) és annak végrehajtási rendelete (Lrtv. vhr.), illetve a 2020 júliusában megújult az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 374/2020. (VII. 30.) kormányrendelet is.



A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.):

- általános érvényű eljárási szabályokat tartalmaz külön a nemzeti és az európai létfontosságú rendszerelemek kijelölésére vonatkozóan;
- hivatalból induló eljárásként definiálja a kijelölést, amely az azonosítási jelentés üzemeltető általi benyújtását követően indul;
- megállapítja az alapvető szolgáltatásokat nyújtó szereplők azonosításának folyamatát;
- kijelenti, hogy a kijelölés (és az alapvető szolgáltatást nyújtó szereplőként történő azonosítás) fő felelőse az ágazati kijelölő hatóság;
- nyilvántartó hatósági feladatokat állapít meg, amelynek végrehajtásához *üzemeltetői kötelezettségeket* társít: Lrtv. 5. §;
- ellenőrzés koordinációjával kapcsolatos feladatokat a BM Országos Katasztrófavédelmi Főigazgatósághoz delegálja: Lrtv. 8. §;
- *üzemeltetői biztonsági terv* készítésének kötelezettségét és annak körülményeit állapítja meg a kijelölt üzemeltető részére: Lrtv. 6. § (1);
- *biztonsági összekötő személy* alkalmazásának kötelezettségét állapítja meg a kijelölt üzemeltető részére: Lrtv. 6. § (14).

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.):

- *azonosítási jelentés* készítésének szabályai, újra-azonosítás: Lrtv. vhr. 2. §;
- kijelölés/visszavonás részletszabályai: Lrtv. vhr. 4-5. §;
- *biztonsági összekötő személy* képesítési követelményei és foglalkoztatásának feltételei: Lrtv. vhr. 6. §;
- *üzemeltetői biztonsági terv* egyéb szabályai: Lrtv. vhr. 7. §;
- *ellenőrzések* rendje: Lrtv. vhr. 8. §;
- *szankcionálás*: Lrtv. vhr. 9. §;
- nyilvántartó hatóság meghatározása (BM OKF), kapcsolódó *üzemeltetői kötelezettségek*: Lrtv. vhr. 10. §;



- *együttműködés és rendkívüli események kezelésének szabályai*: Lrtv. vhr. 11. §;
- *komplex gyakorlat szabályai*: Lrtv. vhr. 12. §;
- *alapvető szolgáltatást nyújtó szereplőkkel* kapcsolatos egyéb szabályok: Lrtv. vhr. 12/A. §;
- horizontális kritériumok: Lrtv. vhr. 1. melléklet;
- *üzemeltetői biztonsági terv* tartalmi elemei: Lrtv. vhr. 2. melléklet;
- alapvető szolgáltatások jegyzéke: Lrtv. vhr. 3. melléklet;

Az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 374/2020. (VII. 30.) Korm. rendelet (a továbbiakban: Energia vhr.)

- *kijelölő hatóságok* nevesítése ágazatonként, villamosenergia ágazat tekintetében a *Magyar Energetikai és Közmű-szabályozási Hivatal*: Energia vhr. 3. § a);
- európai és nemzeti létfontosságú rendszer elemek ágazati kritériumainak meghatározása, villamosenergia ágazatban: Energia vhr. 4. § a) és 5. §;
- *jelentős zavar értelmezése a villamos energia ágazatban*: Energia vhr. 9. §;
- *alapvető szolgáltatásokhoz tartozó küszöbértékek a villamos energia ágazatban*: Energia vhr. 13. §;
- *biztonsági összekötő személy képesítési követelményei*: Energia vhr. 17. §.

Információbiztonsági vetület: Az energia ágazat kijelölt kritikus infrastruktúrái az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartoznak, így vonatkozik rájuk valamennyi, az információbiztonság növelése érdekében meghatározott kötelezettség és kapcsolódó jogszabály. Mindezek végrehajtása szorosan kapcsolódik a NIS irányelv (2016/1148 Irányelv) követelményrendszeréhez, amely az alapvető szolgáltatást nyújtó szereplők vonatkozásában is érvényesítendő biztonsági intézkedéseket írt elő a tagállamok részére. Ilyen a hatékony kockázatmenedzsment kialakítása, az incidens bejelentési kötelezettség, illetve az egyenszilárd információbiztonságra törekvés.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.):

- *alapvető elektronikus információbiztonsági követelmények*: Ibtv. 5-6. §;
- elektronikus információs rendszerek *biztonsági osztályba sorolása*: Ibtv. 7-8. §;



- elektronikus információs rendszerrel rendelkező szervezetek *biztonsági szintjének meghatározása*: Ibtv. 9-10. §
- érintett *szervezetek további kötelezettségei* (felelősségi körök, informatikai biztonsági szabályzat készítése, kockázatelemzés, ellenőrzés-audit stb.): Ibtv. 11-13. §
- *EIR felelős* feladatai: Ibtv. 13. §;
- hatósági feladatok: Ibtv. 14-16. §;
- eseménykezelés: Ibtv. 19-20. §;
- szankcionálás: Ibtv. 16. § (2)-(3).

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 vhr.):

- elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságok meghatározása: Hatósági vhr. 2. §;
- *létfontosságú rendszerek elektronikus információs rendszereinek biztonsági felügyeletét ellátó hatóság*: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet.
- hatósági eljárás általános jellemzői: Hatósági vhr. 3-5/A. §;
- hatósági feladatok: Hatósági vhr. 6-10/E. § és 12. §;
- *kijelölt rendszerelem kötelezettségei*: Hatósági vhr. 11. §
- *jogkövetkezmények*: Hatósági vhr. 13. §

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: Eseménykezelési vhr.):

- *biztonsági események bejelentése* a nemzeti CSIRT (Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által működtetett eseménykezelő központ) részére: Eseménykezelés vhr. 8-13. §;
- nemzeti CSIRT feladatai és hatásköre: Eseménykezelés vhr. 2-5. §;
- más eseménykezelő központok és feladataik: Eseménykezelés vhr. 6-7. §



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

- *biztonsági osztályba sorolás* szempontjai: BM rendelet 1. melléklet;
- *biztonsági szintbe sorolás* szintjei: BM rendelet 2. melléklet;
- *besorolási útmutató és védelmi intézkedések táblázatai* a biztonsági osztály megállapításához: BM rendelet 3. melléklet;
- *adminisztratív, fizikai és logikai biztonsági követelmények*: BM rendelet 4. melléklet.

Az Irányelvet kiegészíti a 2019 áprilisában kiadott 2019/553 számú Bizottsági ajánlás, az *energia ágazatban érvényesítendő kiberbiztonságról*, amely kifejezetten a valós idejű követelményekre, az áttételes hatásokra, valamint az örökölt és korszerű technológia kombinálására fókuszál.

2. Kötelezettségek teljesítése

a. A biztonsági összekötő személy alkalmazása

Az Lrtv. 6. § (14) bekezdése kötelezően előírja, hogy minden létfontosságú rendszer üzemeltetőjének gondoskodnia kell biztonsági összekötő személy foglalkoztatásáról, és a tevékenységéhez szükséges feltételek folyamatos biztosításáról. A biztonsági összekötő személy alkalmazásának költségei az üzemeltetőt terhelik (Lrtv. 7. §). A feladat ellátásával a Munka Törvénykönyve szerinti rendelkezéseknek megfelelően olyan, már a szervezetnél dolgozó személy is megbízható, aki megfelel a követelményeknek.

Minden ágazatra érvényes, hogy biztonsági összekötőnek csak büntetlen előéletű személy jelölhető ki, aki az Lrtv. vhr. 6. §-ában felsorolt képesítések valamelyikével, illetve a vonatkozó ágazati kormányrendeletben meghatározott képzettséggel rendelkezik.

A büntetlen előéletre vonatkozó követelmény teljesülését a biztonsági összekötőnek kell igazolnia, ami a hatósági ellenőrzések keretében – a bűnügyi nyilvántartási rendszerből történő adatigényléssel – ellenőrizhető.



b. A biztonsági összekötő bejelentésének szabályai

A kijelölő hatóság a szervezetre vonatkozó kijelölő határozatban felhívja az üzemeltető figyelmét az Lrtv. által meghatározott, biztonsági összekötő személy alkalmazására vonatkozó kötelezettségére. A kijelölő hatóság az üzemeltetői biztonsági terv elkészítésének határidejét adja meg a kijelölő határozatban, ez érvényes a biztonsági összekötő személyre is, tekintettel arra, hogy a biztonsági összekötő személy nevét és elérhetőségeit az üzemeltetői biztonsági terv is tartalmazza.

A biztonsági összekötő személy megbízásáról tájékoztatni kell a nyilvántartó hatóságként eljáró BM Országos Katasztrófavédelmi Főigazgatóságot (BM OKF) az alábbi adatok rendelkezésre bocsátásával:

- természetes személyazonosító adatok,
- telefonszám, e-mail cím,
- szakirányú végzettség és a végzettséget igazoló okirat sorszáma,

Fontos kötelezettség, hogy az üzemeltető a BM OFK által nyilvántartott adatokban bekövetkezett változásokról 72 órán belül tájékoztatja a nyilvántartó hatóságot.

c. A biztonsági összekötő személy képzési követelményei az energia ágazatban

Az Energia vhr. 17. §-a szerint az energia ágazatban kijelölt létfontosságú rendszerelemek esetében olyan biztonsági összekötő személyt lehet alkalmazni, aki *szakirányú műszaki szakon szerzett felsőfokú végzettséggel is* rendelkezik.

Ezen kívül, az Lrtv. vhr. 6. §-a tartalmazza azokat a további képzéseket, amelyek valamelyikének birtokában a biztonsági összekötő személy feladatai elláthatók:

- védelmi igazgatási, katasztrófavédelmi vagy rendészeti igazgatási szakon szerzett felsőfokú végzettség,
- tűzvédelmi, iparbiztonsági, polgári védelmi szakmai irányú rendészeti szervezői szakképzés, vagy ezzel egyenértékű végzettség,
- iparbiztonsági szaktanfolyami végzettség,
- iparbiztonsági szakon szerzett felsőfokú végzettség, vagy
- a katasztrófavédelem hivatásos szerveinél legalább 5 év iparbiztonsági szakterületen szerzett gyakorlat;



Foglalkoztatható továbbá olyan személy, akit korábban rendvédelmi szerv által, a rendvédelmi szerv alaptevékenységébe tartozó feladatok ellátása körében legalább öt évig foglalkoztattak és felsőfokú végzettséggel rendelkezik, amennyiben igazolni tudja az Lrtv. vhr. 6. § (3) bekezdésében foglalt mentesülésnek történő megfelelést.

d. A biztonsági összekötő személy feladatai

Az Lrtv. 6. § (14) a-b) szerint a biztonsági összekötő személy feladata a kapcsolattartás az üzemeltető és a kijelölési eljárásban részt vevő hatóságok között, illetve az üzemeltetői biztonsági terv kidolgozása. Ennek keretében az alábbi tevékenységeket látja el:

- *Kapcsolattartás*
 - ágazati kijelölő hatósággal
 - hatósági eljárásban résztvevő egyéb szervekkel
 - katasztrófavédelemmel
- *Azonosítási jelentés készítése*
 - kijelölést követő 5 év után [Lrtv. vhr. 2. §. (8)],
 - kijelölés visszavonásának alátámasztásaként [Lrtv. vhr. 2. §. (2) a.]
- *Kockázatelemzés/kockázatértékelés lefolytatása*
- Hatóságokkal történő *együttműködés a folyamatban lévő hatósági eljárásban* (pl.: hiánypótlások)
- *Ellenőrzések* szervezésében és lebonyolításában történő részvétel
- *Gyakorlatok* tervezésében és végrehajtásában történő közreműködés
- Üzemeltető *adatszolgáltatási kötelezettségének teljesítése*
- *Rendkívüli eseménykezelésben, illetve a következtetések megállapításában* való közreműködés [Lrtv. vhr. 11. §. (6) e.)]
- *Üzemeltetői biztonsági terv* készítése, felülvizsgálata, aktualizálása

e. Üzemeltetői biztonsági terv készítése, gondozása

A kijelölt nemzeti létfontosságú rendszerelem üzemeltetőjének az ágazati kijelölő hatóság határozatában kitűzött határidőig ki kell dolgoznia az üzemeltetői biztonsági tervét.



Az Üzemeltetői Biztonsági Terv (ÜBT) akumulálja a rendszerelemet fenyegető legfőbb tényezőket, vizsgálja és értékeli valamennyi elemének sebezhetőségét, gyenge pontjait, továbbá azok kiesésének effektusait, konzekvenciáit, a működéshez nélkülözhetetlen források helyettesíthetőségét, áttekinti a szándékos károkozás által okozható problémákat, illetve ezekre vonatkozóan részletes kockázatelemzést tartalmaz.

A 2020. július 31-től hatályos, módosított Lrtv. vhr. 2. melléklete részletes, tételes felsorolásban rögzíti az ÜBT elvárt tartalmi elemeit, ezáltal nyújtva mankót az elkészítésben résztvevő személyeknek, szervezeti egységeknek, külső partnereiknek. Jelen fejezet célja, hogy támogassa az ÜBT kidolgozásának munkafolyamatát.

Az ÜBT kidolgozása nem egyszemélyes munka: a működés feltételei, valamint a kockázati kategóriák is széleskörűek, amelyek nem határolhatók le egyetlen szervezeti egységre. Javasoljuk tehát valamennyi érintett szakterület (pl.: biztonsági, üzemeltetési, humán stb.) koordinált bevonását az ÜBT kidolgozásának folyamatába.

Fontos leszögezni, hogy bizonyos formai követelményekre is figyelemmel kell lenni a kidolgozás során, amelyek az alábbiak:

Az üzemeltetői biztonsági tervet írásban kell elkészíteni – ügyelve a formai követelmények betartására is – és a kijelölő hatóság részére eredeti (az üzemeltető és a biztonsági összekötő személy által aláírt) példányban elektronikus úton kell benyújtani. A térképeket elektronikus adathordozón is be lehet nyújtani.

Egységes borítólap a főbb információk szerepeltetésével:

- az üzemeltető szervezet megnevezése,
- a létfontosságú rendszerelem pontos megnevezése,
- verziószám,
- a dokumentum kiadásának dátuma, mely a kijelölő hatóság általi elfogadás dátuma kell, hogy legyen.

Egyedi belső aláíró lap:

- saját logó és bélyegző szerepeltetésével,
- a dokumentum szervezeten belül aláírásra jogosult személy jóváhagyásának helye.

Verziókövetés:

- a dokumentumon elvégzett valamennyi módosítás tételes jegyzéke,
- pontos dátummal,
- a változtatást végrehajtó személy megnevezése, aláírása.



Tartalomjegyzék:

- megfelelően részletes,
- a kereshetőséget elősegítő,
- a fejezetek és alfejezetek címei a Vhr-ben rögzítettekkel azonosak legyenek a jobb átláthatóság érdekében.

Rövidítések jegyzéke, szómagyarázat:

- az ágazati specifikumoknak, valamint a már bevezetett szervezetszabályozó eszközöknek (pl.: BCP/DRP) megfelelően a dokumentumban gyakran előfordulnak általános, illetve egyedi rövidítések is.
- A fentiek egyértelműsítése ideális esetben az ÜBT első fejezeteiben jelenik meg.

Megfelelő méretarányú és felbontású térképek, képek alkalmazása:

- A térképvázlat vagy helyszínrajz tartalmazza a kijelölt rendszerelem egészét, és olyan méretarányú legyen, amely a megfelelő eligazodást biztosítja. A megfelelő paraméterek megtartása érdekében akár object-ként beillesztve.

Figyelemmel az Lrtv. 6. § (4) bekezdésére, az ÜBT, vagy azzal egyenértékű biztonsági dokumentáció nem nyilvános!

- A fentiek rögzítése a dokumentumban kulcsfontosságú.
- Az ÜBT tartalmi követelményeinek tételes számbavétele, rövid indokolása segíthet megérteni azok elvárt adattartalmát.

Általános bemutatás:

Egy bevezető fejezetben az üzemeltető rögzíti a kijelölt létfontosságú rendszerelem, valamint önmaga azonosításához szükséges adatait, elérhetőségeit (pontos cím hiányát földrajzi koordináta is pótolhatja);

- rögzítésre kerülnek a biztonsági összekötő személy adatai, elérhetőségei;
- a szervezet általános bemutatása során ki kell térni annak tevékenységére, irányítási rendszerére, illetve a kijelölt rendszerelem védelmével kapcsolatos célkitűzéseire – ami leginkább egy általános politika-jellegű, elhivatottságot rögzítő leírás –, valamint a horizontális és ágazati kritériumok teljesülésének vizsgálatára.
- a szervezeti és vezetési struktúrát, a vezető tisztviselőket, illetve felelősségi köreiket javasolt szervezeti ábra, illetve döntési fa mellékelésével bemutatni.
- a személyzetre vonatkozó adatok – aktuális létszám, az üzemszerű működéshez szükséges minimális létszám, saját munkavállalók, külső, szerződéses munkavállalók



szerinti bontásban – mellett javasolt bemutatni azokat a speciális munkaköröket, amelyek a működés szempontjából kritikusak. Fenti adatok a kockázatelemzés elkészítése során kiemelt jelentőséggel bírnak.

- a kijelölt rendszerelem tevékenységének áttekintő bemutatása során kiemelt figyelmet kell fordítani a normál működés paramétereinek (pontos adatok, tanúsítványok mellékelésével) ismertetésére, valamint a beszállítói lánc bemutatására (termékek, szolgáltatások, illetve a partner megnevezése, megkötött szerződésekre való hivatkozás). Fontos figyelemmel lenni a beszállítói lánc azon elemeire, amelyek a kijelölt létfontosságú rendszerelem folyamatos, elvárt szintű működését nagymértékben befolyásolják (kiesésük esetén a normál működés veszélyeztetett). A fenti speciális esetekben a beszállító cég adatait, elérhetőségeit, a szerződés garanciáit, beszállítói audit részleteit szükséges a lehető legnagyobb mélységben bemutatni. Fentiekén túl a kijelölt rendszerelem tevékenysége, az általa nyújtott szolgáltatás által befolyásolt ágazatok, alágazatok bemutatása is szükséges.

A teljesült ágazati és horizontális kritériumok szerinti hatások bemutatása a kijelölt rendszerelem vonatkozásában: részelemek, folyamatok bemutatása a teljesített kritériumok feltűntetésével.

A kijelölt létfontosságú rendszerelem belső auditálási, vezetőségi átvizsgálási rendszerének bemutatása során törekedni kell egy átfogó kép kialakítására, amelyből megismerhető lesz a belső auditok, átvizsgálások rendszere (időszakosság, auditorok személye és képzettsége, dokumentációja).

A változások, változtatások követési és kezelési rendszerének bemutatása a fentiekben ismertetett belső auditok és vezetőségi átvizsgálások eredményeként megvalósított intézkedések mentén történjen. Ezek mellett fontos ismertetni a change management során tett védelmi intézkedéseket is.

A kijelölt rendszerelem környezetének bemutatása:

Elsődleges szempont a kijelölt rendszerelem térbeni elhelyezése, amelyhez lehetőség szerint a legtöbb adatot szükséges mellékelni – pl. természetben hely (pontos cím), helyrajzi szám, koordináták –, amelyhez mellékelni szükséges a megfelelő felbontású helyszínrajzokat, alaprajzokat, műholdas-, vagy egyéb képeket.

A bemutatás során a kijelölt rendszerelem légtérének, valamint a környezetében lévő, a működésére befolyással bíró üzemek (veszélyes üzemek, gyárak, erőművek) pontos ismertetése is elengedhetetlen, csakúgy, mint a természeti környezet, valamint az ebből adódó geológiai-, hidrológiai-, illetve meteorológiai jellemzők és hatásaik – biztonságos működés szempontjából történő – számbavétele. Fenti adatok a kockázatelemzés elkészítése során kiemelt jelentőséggel bírnak.



A kijelölt rendszerelem bemutatása:

Jelen fejezet során szükséges részletesen bemutatni a kijelölt rendszerelem normál működési rendje során a folyamatos, elvárt szintű működést biztosító rendszereket, alrendszereket, eszközöket, berendezéseket, technológiai és karbantartási folyamatokat, műveleteket.

Fentiekre figyelemmel elsődleges cél a normál működés folyamat-szemléletű, teljes körű bemutatása a szükséges erőforrások (és kapacitásaik), illetve tartalékaik ismertetésével, kitérve a tartalék eszközök, berendezések, szolgáltatások üzembe helyezésének folyamatára/szabályaira/időszükségleteire, valamint a visszaállítás szabályaira/folyamataira.

A normál működés ismertetését követően a minimálisan elvárt működés folyamata, erőforrásai is kerüljenek bemutatásra a fenti keretrendszer mentén.

Jelen fejezetben kerüljenek ismertetésre a kijelölt létfontosságú rendszerelem helyszínrajzai, komponensei, illetve a hozzá tartozó rövid ismertető (pl. létesítményen belüli épületek, helyiségek stb.)

A telephelyet kiszolgáló infrastruktúra:

A telephely működése tekintetében releváns közműszolgáltatások (elektromos áram, vezetékes gáz, közüzemi ivóvíz és szennyvíz, távhő, infokommunikációs hálózat) felsorolását követően ismertetni kell azok biztosításának specifikumait:

- szolgáltató (szolgáltatási szerződés paramétereinek ismertetése mellett),
- bekötési pontok,
- területi ellátottság,
- karbantartások és javítások bemutatása, különös tekintettel azok gyakoriságára, valamint a tevékenységre gyakorolt hatására,
- kapcsolattartás módja, szabályozottsága,
- telephelyen belüli ellátottság (hálózat) bemutatása,
- a rendeltetésszerű működéshez szükséges minimum szolgáltatási szint, illetve a szolgáltatás kiesésének működésre gyakorolt hatásának bemutatása,
- a fentiekén túl ismertetni szükséges a rendszerelem működése szempontjából nélkülözhetetlen szolgáltatások kiesése esetén alkalmazandó tartalék, vagy alternatív rendszerek paramétereit (kapacitás adatokkal), működését, üzembe helyezésének szabályozottságát.



Kiemelt figyelmet kell fordítani a kijelölt létfontosságú rendszerelem működésében releváns infokommunikációs szolgáltatások, illetve informatikai rendszerek, eszközök, hálózatok bemutatására (hálózati topológia csatolásával). Ezalatt értendők a fizikai hálózatok, belső hálózatok, vezeték nélküli hálózatok tételes bemutatása, az elektronikus információs rendszerek ismertetése (alkalmazásokkal kiegészítve), kiemelve a fentieknek a létfontosságú rendszerelem működésében betöltött szerepét, kiesésük hatásait, visszaállításuk/helyettesítésük lehetséges módjait.

A kijelölt rendszerelem felépítésének, elemeinek, részletes tevékenységének, termelési, működési folyamatainak bemutatása:

A létfontosságú rendszerelem tevékenységének ismertetése során törekedni kell a részletes, kapacitásadatokkal kiegészített, teljes körű leíró bemutatásra.

A tevékenységekre vonatkozó legfontosabb technológiai/műveleti/munkafolyamatok bemutatása során ki kell térni a tevékenység céljára, a rendeltetésszerű működéshez szükséges erőforrásokra (humán, technikai/technológiai, anyagi), harmadik féltől igénybe vett szolgáltatás(ok)ra, valamint a kiszolgáló infrastruktúra és a technológiai/műveleti/munkafolyamatok kapcsolódási pontjainak részletes bemutatására. Szükséges megjelölni az előbb felsoroltak azon minimális szintjeit, amelyekkel még a rendeltetésszerű működés fenntartása garantálható.

A tevékenységekre vonatkozó legfontosabb karbantartási folyamatok bemutatása során a tervezés részleteire, valamint a belső, illetve külső fél által végzett karbantartásokra is figyelemmel kell lenni.

A lehetséges veszélyt jelentő anyagok, berendezések számbavétele során az alábbiakat kell feltüntetni:

- bemutatása,
- kezelése/szállítása/tárolás,
- megsemmisítése/elszállítása.
- belső és külső tájékoztatási rendszerek bemutatása két szempontrendszer szerint kell, hogy történjen: normál időszaki, valamint válságkommunikációs stratégiák és eljárásrendek ismertetése szükséges. Szükséges bemutatni a külső (harmadik féltől igénybe vett) tájékoztatási rendszereket/eszközöket/szolgáltatásokat.
- (itt kiemelhető az EDR kapcsolódás, amelynek alapját a kormányzati célú hálózatokról és a vonatkozó eljárásrendekről szóló 346/2010. (XII. 22.) Korm. rend. 34. § (3) bekezdése adja).



- A felügyeleti és biztonsági szervezetek, eszközrendszerük, működésük (kiszervezett, harmadik féltől igénybe vett szolgáltatás esetén a szerződés részletei is!) ismertetése az alábbiakra kiterjedően:
 - biztonsági szolgálat bemutatása,
 - elsősegélynyújtó és mentőszervezetek bemutatása,
 - munkavédelmi szervezet(ek) bemutatása,
 - tűzvédelmi szervezet(ek) bemutatása,
 - környezetvédelmi szervezet(ek) bemutatása,
 - műszaki biztonsági szolgálat(ok) bemutatása,
 - katasztrófa elhárítási szervezet(ek) bemutatása,
 - távfelügyeleti és monitoring hálózat(ok) bemutatása (minimum elvárás a rendszerben lévő jelző és érzékelő eszközök tervrajzon való feltüntetése és a dokumentumhoz történő csatolása),
 - beléptető és behatolás jelző rendszer(ek) bemutatása (minimum elvárás a rendszer által védett helyszínek tervrajzon való feltüntetése és a dokumentumhoz történő csatolása),
 - zárt láncú kamerás megfigyelő rendszer(ek) bemutatása (minimum elvárt a kamerák és diszpécserközpontok elhelyezési rajza, a kamerák által lefedett területek jelölésével),
 - tűzjelző rendszer(ek) bemutatása (minimum elvárás a rendszer által védett helyszínek, eszközök és diszpécser központok tervrajzon való feltüntetése és a dokumentumhoz történő csatolása),
 - tűzoltó rendszer(ek) bemutatása (minimum elvárás a rendszer által védett helyszínek, eszközök tervrajzon való feltüntetése és a dokumentumhoz történő csatolása),
 - egyéb a rendszerelem biztonságát szavatoló eszköz/rendszer/szolgáltatás bemutatása (amennyiben releváns, tervrajzon való feltüntetése és a dokumentumhoz történő csatolása).

Kockázatok azonosítása, értékelése, kezelése:

- az üzemeltető által fenntartott kockázat menedzsment rendszer bemutatása,
- felelősségi körök bemutatása,
- kockázatkezelési módszertan bemutatása.



- kockázatok tételes azonosítása, értékelése során minimális elvárás, hogy a jogszabályban rögzített kockázati elemeknek/tényezőknek szerepelniük kell. Ezeken felül szükséges kiegészíteni egyéb ágazati specifikumokkal.

Szükséges a kockázati lista kiegészítése a kijelölt rendszerelem kölcsönösen függő (interdependens) kapcsolódásai és az azokból adódó kockázatok azonosításával és értékelésével (a kijelölt rendszerelem kiesése milyen más ágazatokra, szervezetekre, személyekre van hatással).

A következő lépésben meg kell határozni a kockázatok valószínűsíthető okait, a bekövetkezéskor prognosztizálható negatív hatásait, az okozott kárértéket.

A felmerült kockázatok értékelése táblázat készítése a bekövetkezési valószínűség, a veszélyeztető hatások szintje és harmadik fél felé fennálló kitettség alapján, lehetőleg az alábbiak szerint:

- a bekövetkezési valószínűség lehet: nagyon ritka, ritka, alkalmankénti, gyakori, nagyon gyakori;
- a veszélyeztető hatások szintje lehet: elhanyagolható, alacsony, közepes, magas, katasztrofális;
- a kitettség az alábbi értékeket kaphatja: nincs kitettség, egy fél felé van kitettség, több fél felé van kitettség.

Fentiek közül az utóbbi, a kitettség értékelése szorulhat magyarázatra, mely arra irányul, hogy előfordulnak olyan szolgáltatások (pl. közmű, infokommunikációs, vagy informatikai), melyeket a létfontosságú rendszerelem harmadik féltől vesz igénybe, és melyek kieséséből adódó kockázatok kezelésére – azok nélkülözhetetlen jellegéből adódóan – kiemelt figyelmet kell fordítania például megfelelő garanciákat biztosító SLA-k kötésével, vagy új partnerek bevonásával.

A kockázatelemzés- és kezelés bemutatására a BM Országos Katasztrófavédelmi Főigazgatóság által publikált módszertan biztosít megfelelő keretet. A táblázat kitöltése során az üzemeltető a feltárt kockázati tényezőket a Vhr. szerinti kockázati fő- és alkategóriákba sorolja azok eredetének tekintetében. Következő lépésként az üzemeltető ismerteti a kockázatot, bemutatja annak hatásait, illetve értékeli azt a hármas szempontrendszer segítségével. A kapott kockázati érték alapján meghatározza az alkalmazandó védelmi intézkedés(ek)e)t. A kockázatsökkentő (védelmi) intézkedés részletes ismertetését követően meg kell állapítani annak státuszát, illetve – amennyiben még nem került megvalósításra az adott intézkedés, úgy felelőst és határidőt kell hozzá rendelni. A folyamat harmadik stádiumában részletesen kell ismertetni a megvalósított intézkedést, meg kell adni az új



értékeket, valamint nyilatkozni szükséges az intézkedés fellelhetőségéről. A maradványkockázatot és a kockázatcsökkenést a táblázat számolja ki.

Kockázatkezelés alatt a kockázatok értékelésére készített táblázat kiegészítése értendő, a kockázat kezelésére/elfogadására/áthárítására tett intézkedésekkel.

A rendkívüli események meghatározása során törekedni kell a megfelelő definíciók, határértékek meghatározására, illetve minimum tartalmi követelményként az alábbiakat fel kell tüntetni: az esemény megnevezése, mértéke, bejelentési rend, alkalmazandó eljárásrend.

A kijelölt rendszerelem védelmének eszközrendszere rendkívüli esemény bekövetkezése esetén:

- a rendszerelem védelmét biztosító általános intézkedés(ek) bemutatása;
- a rendszerelem védelmét biztosító speciális intézkedés(ek) bemutatása azonosított kockázatonként;
- a rendszerelem védelmét biztosító, a rendkívüli esemény(ek) során alkalmazandó eljárásrend(ek) bemutatása;
- rendkívüli esemény kezelésében résztvevő szervezeti egységek felsorolása;
- kijelölt rendszerelem védelmére rendszeresített felszerelések és a vezetéshez, a döntéshozzához szükséges folyamatok és infrastruktúrák bemutatása az alábbiak érintésével:
- a vezetői állomány rendkívüli esemény esetén történő értesítésének eszközrendszere;
- a vezetői állomány rendkívüli esemény esetén történő értesítésének eljárásrendje;
- a dolgozók rendkívüli eseménykori riasztásának eszközrendszere;
- a dolgozók rendkívüli eseménykori riasztásának eljárásrendje;
- a rendkívüli esemény következményeinek csökkentését végző saját eszközeinek és erőforrásainak alkalmazása;
- vezetői irányítás folyamata;
- döntési kompetenciák, felelősségek;
- üzemfolytonos működés minimum szintjéhez szükséges feltételek és intézkedések;
- üzemfolytonos működés normál szintjéhez szükséges feltételek és intézkedések;
- üzemfolytonos működés helyszíni, illetve távoli munkavégzéshez szükséges feltételek és intézkedések.



Komplex gyakorlatok céljának, elvárásainak ismertetése:

Amennyiben az üzemeltető a rendkívüli események bekövetkezési valószínűségének vagy a hatások csökkentésére gyakorlatot tart, annak rendszerét, elemeit, folyamatait, értékelését itt lehet bemutatni.

A fent felsorolt általános javaslatok megfontolása mellett az ÜBT elkészítése során javasolt egyeztetni az ágazati kijelölő hatósággal, valamint a BM Országos Katasztrófavédelmi Főigazgatósággal az esetlegesen felmerülő kérdések tisztázása céljából.

3. A kijelölt létfontosságú rendszerelemek üzemeltetőinek elektronikus információs rendszereikkel kapcsolatos kötelezettségei:

a. A hatóság kijelölő határozatának véglegessé válásától számított 60 napon belül a szervezetnek elektronikus úton be kell jelentkeznie a hálózati és információs rendszerei biztonságának felügyeletét ellátó hatóságnál, amely során:

- megadja a szervezet azonosításához szükséges adatokat, amelyek az alábbiak:
- hivatalos név,
- adószám,
- székhely pontos címe,
- aláírásra jogosult személy adatai – vezetői szinten;
- kijelöli a szervezet elektronikus információs rendszereinek biztonságáért felelős személyt (a továbbiakban: IBF/EIR felelős), aki felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Feladat- és felelősségi körét az Ibtv. 13. § részletezi;
- továbbá megküldi ezen kijelölt személy jogszabályban előírt adatait:
- személyes adatok (azonosítás céljából),
- kapcsolattartási adatok (elérhetőségek),
- kompetenciák (végzettség, szakmai tapasztalat).

b. 90 napon belül meg kell küldenie a hatóság részére a szervezet informatikai biztonsági szabályzatát (a továbbiakban: IBSZ)

Az IBSZ kezelése és vizsgálata során a hatóság megállapítja, hogy az abban foglalt védelmi intézkedések milyen mélységben teljesítik a BM rendelet kontrollkörnyezetét. Fentieken túl a



biztonsági osztályba- és szintbe sorolás megállapítására irányuló hatósági eljárás során a megküldött osztályba- és szintbe sorolás űrlapokon jelöltek alátámasztására is szolgálnak.

Előfordulhat, hogy a szervezeten belül kialakított információbiztonsági irányítási rendszer bizonyos elemei nem az IBSZ-ben, hanem valamilyen, az IBSZ-hez kapcsolódó, egyéb szervezetszabályozó eszközben kerültek rögzítésre. Ebben az esetben valamennyi ilyen dokumentumot az IBSZ-hez csatolva szükséges megküldeni a hatóság részére.

Fentiek mellett a dokumentum nyilvántartása a kormányzati eseménykezelő központ munkáját is segíti egy esetlegesen bekövetkező biztonsági esemény (incidens) kezelése során. Az adott szervezet védelmi intézkedéseinek, információbiztonsági kontrollkörnyezetének ismerete a bejelentés és az effektív beavatkozás megkezdése közötti időintervallum szignifikáns csökkenését eredményezheti.

Az előzőekkel összhangban az IBSZ-ben alapvetően rögzíteni szükséges az alábbiakat:

- az Ibtv-vel összehangolt felelősségi köröket – vezető (Ibtv. 11. §) és IBF (Ibtv. 13. §) tekintetében;
- a hatósággal és az eseménykezelő központtal történő kapcsolattartás – mind megfelelőség, mind hatékony eseménykezelés tekintetében – szabályait, amelyeknek alapját szintén az Ibtv. képezi;
- a szervezet, mint kijelölt létfontosságú rendszerelem által használt elektronikus információs rendszerek felsorolását, kiemelve a működés szempontjából kritikus rendszereket, létfontosságú információs rendszerelemeket;
- a biztonsági osztályba- és szintbe sorolás – hatóság határozatában megállapított – eredményeit [Ibtv. 7. § (3) és 10. § (8)];
- továbbá az IBSZ-hez kapcsolódó információbiztonsági dokumentáció (eljárásrendek, szabályzatok, egyéb dokumentáció) felsorolását.

c. Biztonsági osztályba sorolás és biztonsági szint megállapítása

Kiindulási alap: az energia ágazat villamosenergia alágazatának kijelölő hatósága (MEKH) által kiadott kijelölő határozat véglegessé válásától számított egy éven belül a kijelölt létfontosságú rendszerelemnek vizsgálatot kell folytatnia az Ibtv. rendelkezései alapján, a következők szerint:

- *Ibtv. 2. § (2) c) pont alapján a kijelölt létfontosságú rendszerelemekre vonatkoznak az Ibtv. által előírt kötelezettségek, így az*



- Ibtv. 5-6. §-ok szerinti alapvető elektronikus információbiztonsági követelményeket teljesíteni kell

ZÁRT	TELJES KÖRŰ	FOLYTONOS	KOCKÁZATOKKAL ARÁNYOS
az összes releváns fenyegetést figyelembe vevő védelem	védelmi intézkedések a rendszer összes elemére kiterjednek	változó körülmények és viszonyok ellenére megszakítás nélkül valósul meg	kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel

9.1. ábra: Ibtv.-ben megfogalmazott védelmi követelmények¹⁸⁹

- Ibtv. 7-8. § alapján a létfontosságú rendszereknél *található elektronikus információs rendszerek biztonsági osztályba sorolását* el kell végezni, illetve mindez *alapján* az
- Ibtv. 9-10. §-nak megfelelően a *szervezet biztonsági szintjét* meg kell határozni.

Biztonsági osztályba sorolás

Annak érdekében, hogy a létfontosságú rendszerek elektronikus információs rendszerei, és az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs *rendszereket* be kell sorolni *egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából, kockázatelemzés alapján*. Mindehhez *általános irányelveket* biztosít a *BM rendelet 1. melléklete*, amely a biztonsági osztályok értelmezését segíti azzal, hogy az egyes osztályok tekintetében a bekövetkező káresemények mértékét és lehetséges következményeit foglalja össze.

A kockázatelemzés ki kell terjedjen az elektronikus információs rendszerek *vagyonelemeinek felmérésére*, hogy meghatározható legyen a védelem tárgya.

A különböző vagyonelemek tekintetében *meg kell határozni*, hogy milyen *sebezhetőség* jellemző rájuk, milyen *fenyegetéseknek* vannak kitéve IT, infrastrukturális, környezeti, humán, társadalmi, politikai, gazdasági stb. szempontból. Meg kell határozni az *elfogadható kockázatokat*, amelyekkel a rendszer „együtt tud élni”, amelyek a működését jelentős mértékben nem befolyásolják, illetve azokat a *kockázatokat*, amelyek *nem elfogadhatók* a szervezet számára, és intézkedéseket kell fogyanatosítani az adott kockázat csökkentésére. Végül fel kell tártani a *maradványkockázatokat* is, amelyek további értékelésre szorulnak.

¹⁸⁹ Forrás: Saját szerkesztés



Az elektronikus információs rendszerek *osztályba sorolása* a fenti szempontok alapján, *ötfokozatú skálán történik*, a rendszerben kezelt adatoktól és az elektronikus információs rendszer funkcióitól függően. *Kritikus infrastruktúrák tekintetében* (rendeltetésükből és létfontosságú jellegükből adódóan) a szabályozás a *rendelkezésre állást követeli meg* elsődlegesen¹⁹⁰ a bizalmasság – sértetlenség – rendelkezésre állás hármas szempontrendszerét nézve. A szempontok az alábbiak szerint értelmezhetőek az elektronikus információs rendszerekre:

BIZALMASSÁG	SÉRTETLENSÉG	RENDELKEZÉSRE ÁLLÁS
adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel	adat tartalma és tulajdonságai az elvárttal megegyeznek, tehát az elvárt forrásból származik (hiteles) és a származás ellenőrizhető (letagadhatatlan)	annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek

9.2. ábra: Az információbiztonság alapfogalmai

Az elvégzett vizsgálatok alapján meghatározható az egyes elektronikus információs rendszerek *aktuális* (vizsgálat időpontjában jellemző) és *írányadó* (jogsabály alapján elérendő) biztonsági osztálya, amelynek meg kell felelni, és amelyhez társított követelményeket teljesíteni szükséges. Mindennek módszertana a következők szerint foglalható össze:

BIZTONSÁGI OSZTÁLYBA SOROLÁS MÓDSZERTANA

1. A fenti szempontokat vizsgálva meg kell állapítani „hol tart jelenleg a szervezetünk”, minden egyes információs rendszerét tekintve külön-külön.
2. Meg kell állapítani az információs rendszereinkben kezelt adatok, a szervezet funkciója és védelmi képességei alapján az **AKTUÁLIS biztonsági osztályt/osztályokat**.
3. Jogsabályi előírások alapján az adott rendszerre vonatkozó **ELÉRENDŐ biztonsági osztályt** fel kell mérni (hova kell eljutni?) – cselekvési tervet kell készíteni ennek elérésére.
4. Úgy kell kialakítani és fejleszteni a védelmi struktúrát, hogy az megfeleljen a jogsabályokban előírtaknak, vagyis adott időn belül el kell érni az írányadó biztonsági osztályt

9.3. ábra: Az Ibtv. szerinti biztonsági osztályba sorolás módszertana

¹⁹⁰ BM rendelet, 1. melléklet 1.1.2. alapján.



Az egyes *biztonsági osztályokhoz* a BM rendelet 3. sz. mellékletében meghatározott követelményrendszer (*adminisztratív, a fizikai és a logikai intézkedések*) társul, amelynek teljesítésével az adott biztonsági szint abszolválható. Ilyen intézkedések a teljesség igénye nélkül:

- *adminisztratív* védelmi intézkedések: pl. a szabályzatok, a biztonságért felelős személyek kinevezése, nyilvántartások, kockázatelemzés, dokumentációk, eljárásrendek megléte, üzletmenet-folytonosság tervezése, oktatás, képzés stb.
- *fizikai* védelmi intézkedések: pl. a rendszerhez és az eszközökhöz történő hozzáférés szabályozása, ellenőrzése, felügyelete, az áramellátás biztosítása, tűz-, víz-, egyéb károk elleni védelem, karbantartás stb.
- *logikai* védelmi intézkedések: pl. a biztonsági elemzések, tesztelések, konfigurációkezelés, frissítések, naplózások, az adathordozók védelme, azonosítás, hitelesítés, vagy a kommunikáció védelme.

Amennyiben a vizsgálat eredményeként az adott rendszereink vonatkozásában megállapított irányadó biztonsági osztály magasabb, mint az aktuális, akkor cselekvési tervet kell készíteni az Ibtv. 8. § (5) bekezdésnek megfelelően. A következő biztonsági osztályba lépés az Ibtv. 8. § (3) bekezdése alapján két év alatt kell biztosítani, vagyis az elektronikus információs rendszerre vonatkozó védelem elvárt erősségének eléréséhez a létfontosságú rendszernek lehetősége van arra, hogy a biztonsági intézkedéseket a fokozatos elérés elve mentén teljesítse. Így tehát az első vizsgálatkor megállapított biztonsági osztályt alapul véve, minden egyes következő, magasabb biztonsági osztályhoz rendelt biztonsági intézkedések kivitelezésére két év áll rendelkezésre.

Az egyes elektronikus információs rendszerek biztonsági osztályba sorolását *legalább 3 évente* – vagy szükség esetén soron kívül – *felül kell vizsgálni* és dokumentálni kell. Soron kívüli biztonsági osztályba sorolást abban az esetben szükséges végezni, ha rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése mindezt indokolja. A biztonsági osztályba sorolást a szervezet vezetőjének kell jóváhagynia.

Az elektronikus információs rendszerek osztályba sorolását az NBSZ NKI által közzétett ún. *OVI tábla segíti*, amely – kitöltési útmutatóval együtt – letölthető.¹⁹¹

A besorolást a *hatóság rendelkezésére kell bocsátani* annak érdekében, hogy a Hatósági vhr. felhatalmazása alapján ellenőrizze azt, és az ellenőrzés eredménye alapján döntést hozzon annak megfelelőségéről. A besorolás mellé *csatolni szükséges* a biztonsági osztályba sorolással érintett rendszerek rövid leírását, amely kifejezetten a kijelölt létfontosságú rendszer

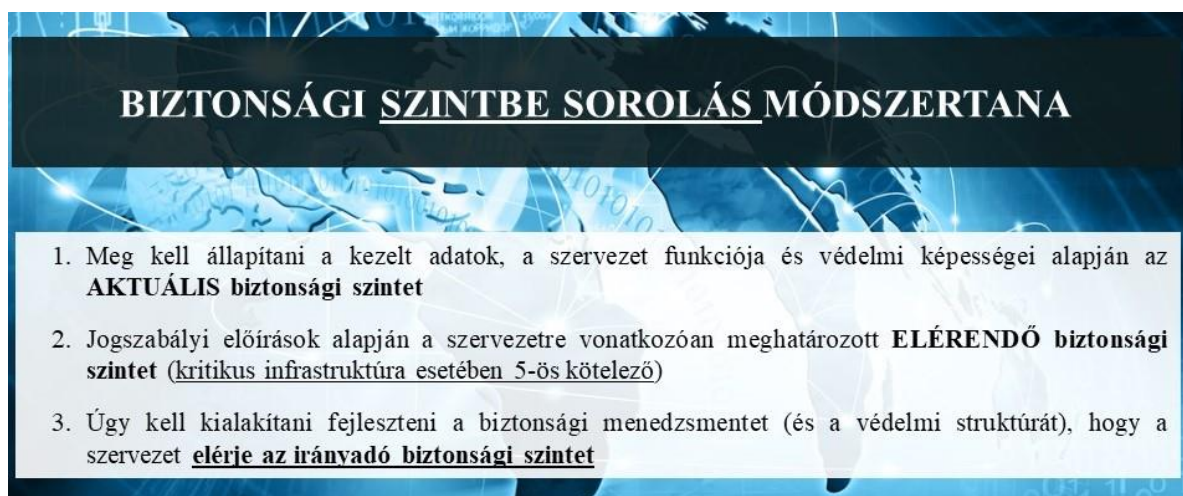
¹⁹¹ <https://nki.gov.hu/hatosag/tartalom/urlapok/>



tevékenységét érintő funkciójukat, szerepüket, illetve meghibásodásuk, kiesésük következményeit mutatja be.

Biztonsági szint meghatározása

A létfontosságú rendszer elektronikus információs rendszereinek biztonsági osztályba sorolása alapján, a *kockázatokkal arányos, költséghatékony védelem kialakítása érdekében* a szervezetet vagy szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük (biztonsági menedzsmentjük) alapján biztonsági szintbe kell sorolni.



BIZTONSÁGI SZINTBE SOROLÁS MÓDSZERTANA

1. Meg kell állapítani a kezelt adatok, a szervezet funkciója és védelmi képességei alapján az **AKTUÁLIS biztonsági szintet**
2. Jogszabályi előírások alapján a szervezetre vonatkozóan meghatározott **ELÉRENDŐ biztonsági szintet** (*kritikus infrastruktúra esetében 5-ös kötelező*)
3. Úgy kell kialakítani fejleszteni a biztonsági menedzsmentet (és a védelmi struktúrát), hogy a szervezet **elérje az irányadó biztonsági szintet**

9.4. ábra: Az Ibtv. szerinti szintbe sorolás módszertana

Az elektronikus információs rendszerrel rendelkező szervezet/szervezeti egység biztonsági szintje a szervezet *biztonsági menedzsmentjének fejlettségét, érettségét méri*, és szintén egy *ötfokozatú rendszerben* állapítható meg. A leggyengébb szint (1-es) azt jelenti, hogy a szervezetnél ugyan vannak az információbiztonságot érintő intézkedések, de a folyamatok ad hoc jellegűek, és folyamatszabályozás szempontjából sem ellenőrzöttek. A biztonsági szintek emelkedésével (2-es, 3-as, 4-es, 5-ös) párhuzamosan a folyamatokra is egyre inkább a szabályozottság, az ellenőrzöttség, a számon kérhetőség jellemző, illetve az eljárások magasabb szinten oktatottak, teszteltek, mérhetők, auditáltak.

A biztonsági szint konkrét megállapítását a *BM rendelet 2. sz. melléklete* segíti, amelyben minden szintre vonatkozóan megtalálhatóak azok az alapvető követelmények, amelyek egy-egy szint megvalósításához szükségesek. Ennek a mellékletnek az 5. pontja szerint a *létfontosságú rendszerek tekintetében az 5. szint teljesítése irányadó*.

A jelenleg hatályos jogszabályi környezet lehetőséget biztosít arra, hogy az illetékes hatóság mérlegelési jogkörében az 5-ös biztonsági szintnél alacsonyabb besorolást állapítson meg.



Az ún. eltérési engedélyhez az üzemeltetőnek kell kérelmet benyújtania és abban igazolnia, hogy az alacsonyabb biztonsági szinthez tartozó követelmények teljesítése nem veszélyezteti a rendelkezésre állás, a bizalmasság és a sértetlenség szempontjaiból teljeskörű védelmet.

Az elektronikus információs rendszer szintbe sorolását az NBSZ NKI által közzétett ún. *SZVI tábla segíti*, amely – kitöltési útmutatóval együtt – letölthető.¹⁹²

¹⁹² <https://nki.gov.hu/hatosag/tartalom/urlapok/>



10. melléklet: Svájci modell

1. Rövid bemutatás

Svájc (Svájci Konföderáció) egy tartományokból álló szövetségi köztársaság. Erős hagyományai vannak a politikai és katonai semlegesség terén, de a nemzetközi együttműködés terén is. Számos nemzetközi szervezet székhelye.

A svájci félig-közvetlen demokrácia alapelve, hogy a hatalom a néptől származik. Ez azt is jelenti, hogy a nép fenntartja magának a két alapvető jogot, a szavazatit és a választásit. A kormányok, és a törvényhozók feladatát nem a hatalom gyakorlójaként határozza meg, hanem a közügyek működtetőjeként. Ők a közösséget a nép alkalmazottjaiként szolgálják, hogy ezzel is könnyítsék azok mindennapi munkáját.

Az 1999. évi alkotmány szerint a kantonokat (tartományokat) mindazok a hatáskörök megilletik, amelyeket nem utaltak tételesen a szövetség hatáskörébe. A kétkamarás svájci parlament – a Szövetségi Gyűlés – a legfőbb államhatalmi szerv. Az egyik kamara az Államtanács 46 tagját (minden kantonból 2 tag, minden „fél-kantonból” 1) minden kantonban közvetlenül választják, míg a másik kamarát a 200 tagú Nemzeti Tanácsot arányos képviseleti rendszerben, közvetlenül választják. Így érvényesülnek a konszociális demokrácia térségi és nemzeti (etnikai) alapelvei. Mindkét ház képviselőinek mandátuma 4 évre szól. A Parlament mindkét házának, a Svájci Államtanácsnak és a Svájci Nemzeti Tanácsnak azonos jogköre van minden tekintetben, beleértve a jogalkotást.

2. Szereplők

A villamosenergia piacon többszáz szolgáltató osztozik. Két szervezet fogja össze a piaci szereplők jelentős részét. A több mint 400 tagot számláló svájci villamosenergia társaságok szövetsége (VSE¹⁹³) a villamosenergia előállításában, szállításában, elosztásában és kereskedelmében érintett vállalatokat, míg a svájci smart grid iparági szövetség (SWISSMIG¹⁹⁴) a gyártókat, megoldásszállítókat tömöríti.

Szabályozási oldalról a svájci Szövetségi Energia Hivatal¹⁹⁵ (SFOE = The Swiss Federal Office of Energy vagy BFE = Bundesamt für Energie) a felelős. A szervezet a DETEC (Federal Department of the Environment, Transport, Energy and Communications) minisztérium keretein belül működik.

¹⁹³ <https://www.strom.ch/de>

¹⁹⁴ <https://www.swissmig.ch/>

¹⁹⁵ <https://www.bfe.admin.ch/bfe/en/home.html>



3. Előzmények

3.1. A villamosenergia-ellátásról szóló törvény (StromVG)

A szabályozási környezet alapja a 2007-es villamosenergia-ellátásról szóló törvény¹⁹⁶ (Stromversorgungsgesetz vagy röviden StromVG). Célja a biztonságos villamosenergia-ellátás és a versenyképes villamosenergia-piac feltételeinek megteremtése. A törvényt az alkotmány 91. cikke¹⁹⁷ alapján alkották meg. A törvény 30. cikke három fontos bekezdést is tartalmaz. A Szövetségi Tanács kiadja a szükséges végrehajtási rendeleteket, a technikai és adminisztratív szabályozásba bevonja az SFOE-t, illetve privát szervezeteknek is lehetőséget ad a részvételre a megvalósításban.

3.2. 2050-ig szóló Energiastratégia

A Szövetségi Tanács 2011-ben a fukushimai katasztrófa után fogadta el a Szövetségi Energia Hivatal (SFOE) segítségével létrehozott 2050-ig szóló energiastratégiát.¹⁹⁸ A fő mozgatórugó a nukleáris energia fokozatos megszüntetése az energiaellátás „környezetbarátabbá” tétele. Ennek megvalósítása erős központi kormányzati koordinációt és „vezérlő” stratégiát igényelt és igényel ma is. A jogszabályalkotás és az Európában élenjáró agilis szabályozás ennek az ambiciózus tervnek a megvalósítását szolgálja. 2013-ban már el is fogadták az első intézkedéscsomagot az energiastratégia alapján. Ennek megfelelően a StromVG-t is felülvizsgálták, és módosították.

3.3. Az Energia rendelet (StromVV)

A StromVG alapján még 2008-ban megszületett az Energia rendelet¹⁹⁹ (Stromversorgungsverordnung vagy röviden StromVV). Az új energiastratégia alapján komoly előkészítő munka kezdődött. Ennek eredményeképpen 2018-ban egy komoly ráncfelvarráson esett át a rendelet is, amelyet elsősorban az okosmérési technológia motivált.

Az SFOE elismerte az intelligens hálózatok jelentőségét Svájc számára, és 2010-ben közzétette a svájci intelligens hálózatokról szóló állásfoglalását. A Smart Meter Impact Assessment (2012) arra a következtetésre jutott, hogy az intelligens mérési rendszerek pozitív költség-haszon arányt mutatnak a svájci gazdaság számára. A 2013-2016-as időszakban a szövetségi kormány és az SFOE energiakutatói tervei támogatták az elektromos hálózatok intelligens hálózatok felé történő fejlesztését.

¹⁹⁶ <https://www.admin.ch/opc/de/classified-compilation/20042411/index.html>

¹⁹⁷ <https://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a91>

¹⁹⁸ <https://www.bfe.admin.ch/bfe/de/home/politik/energiestrategie-2050.html>

¹⁹⁹ <https://www.admin.ch/opc/de/classified-compilation/20071266/index.html>



A rendelet 8b. cikke foglalkozik az adatbiztonsággal. Előírja, hogy csak olyan intelligens mérőrendszerek használhatók a jövőben, amelyek információbiztonsági megfelelőségét sikeresen tesztelték. A hálózatüzemeltetőknek és a gyártóknak alkalmazniuk kell az SFOE által definiált biztonsági követelményrendszert és értékelési módszertant. A rendelet egyúttal kijelölte a svájci Szövetségi Metrológiai Intézetet²⁰⁰ (Federal Institute of Metrology = METAS) a vizsgálatok elvégzésére. A METAS a feladatot vagy annak részeit harmadik felekre bízhatja.

4. Szabályozás jelenlegi állapota

A kormányzat által motivált szabályozás megalkotásába az iparági szövetségek is aktívan bekapcsolódtak az SFOE támogatására. A VSE és a SWISSMIG 2018-ban közösen adták ki a SWISSMIG vezetésével készített iránymutatásukat az intelligens mérőrendszerek működtetésére és információbiztonsági tanúsítására vonatkozóan.²⁰¹

A StormVV rendelet alapján a METAS-Cert 2019. július 1-től kezdte meg a Smart Metering eszközök adatbiztonságának megfelelőségértékelését és tanúsítását az újonnan kidolgozott vizsgálati metodológia²⁰² alapján. Az újonnan beszerzett okosmérők esetén a kötelező tanúsítás alkalmazásának hatályát elhalasztották 2020. január 1-jére.

5. Prüfmethodeologie - Információbiztonsági tanúsítási és értékelési módszertan

A módszertan alapjául a Common Criteria (ISO/IEC 15408) szolgált. Az alkotók szándéka szerint annak egy könnyített részét használja fel és egészíti ki egy speciális területtel. A Prüfmethodeologie megalkotásakor az ESMIG (The European Smart Energy Solution Providers²⁰³) által készített, akkor még nem publikált Protection Profile-ből (védelmi profilból) szövegszerű részeket is átvettek. Ezt a Protection Profile-t az új európai Kiberbiztonsági jogi aktus (Cybersecurity Act) követelményeivel összhangban a CEN-CENELEC-ETSI smart meter szabványosítási koordinációs csoport gondozta.

A SWISSMIG által összeállított vizsgálati módszertannak két fontos melléklete van.

- RL-DSP-CH_A1_1045 [A1]: Az intelligens mérő rendszerek (iMS) tanúsítási követelményeit foglalja össze. Ezek alapvető követelmények az iMS komponenseire, ezáltal a gyártókra is. A követelményeket a fő komponensek architektúrájában, valamint funkcionalitásában fogalmazzák meg.
- RL-DSP-CH_A2_1045 [A2]: Az intelligens mérő rendszerekkel kapcsolatos funkcionális követelmények megfogalmazása az iMS üzemeltetői számára.

²⁰⁰ <https://www.metas.ch/metas/de/home/dl/datensicherheitspruefungen.html>

²⁰¹ <https://www.strom.ch/de/media/6404/download>

²⁰² <https://www.swissmig.ch/wp-content/uploads/2019/07/PruefMethodologie-V21.pdf>

²⁰³ <https://esmig.eu/news/first-harmonised-european-approach>



A módszertan az iMS rendszerek biztonsági szempontból történő ellenőrzésére készült, magába foglalja az intelligens mérő berendezésekkel szemben megfogalmazott követelményeket.

A fő komponenseket mindig rendszerben kell vizsgálni, éppen ezért egy értékeléshez legalább egy okosmérő és a vele kommunikáló háttér rendszer (Head End System) szükséges.

6. Kapcsolódás egyéb szabványokhoz

A vizsgáló laboratóriumnak ISO/IEC 17025, valamint vagy ISO/IEC 27001, vagy Common Criteria, vagy egyéb ezekkel egyenértékű akkreditációval és releváns IoT biztonságértékelési tapasztalattal kell rendelkeznie.

Az intelligens mérőrendszerre vonatkozó követelmények biztonsági elemzéssel azonosított kockázatainak kezelésére szolgálnak, és a nemzetközileg elismert ISO/IEC 27002/27019 biztonsági keretrendszer alapján hozták létre. Kiválasztották azokat a témákat, ellenőrzéseket és kritériumokat, amelyekkel meghatározták az intelligens mérési rendszer megvalósításához, bevezetéséhez és működéséhez szükséges minimum követelményeket.

7. Tapasztalatok

Az egyedi svájci modell megalkotásának elsődleges célja az volt, hogy a Common Criteria tanúsításhoz képest egy gyorsabb, és költséghatékonyabb rendszert hozzanak létre. Az eddigi tapasztalatok alapján ezt a célt egyelőre nem sikerült megvalósítani. A folyamatban sok a bizonytalanság, a követelményrendszer hol túl általános (nehéz megállapítani a megfelelést a követelményeknek), hol túl konkrét (adott implementációra utal, és fölöslegesen korlátozza a gyártókat a lényeges követelmények alkalmas megvalósításában)

A tanúsítónak (METAS-Cert) rövid ideje volt felkészülni, és nem építettek több évtizede hatékonyan működő tanúsítási sémákra (pl. Common Criteria sémák)

A gyártóknak a speciális követelmények miatt komoly energiával egy „csak svájci” tanúsítást kell szerezniük, amelyet nem tudnak újra felhasználni. A tényleges tanúsítási folyamat így a vártnál lassabb és jóval költségesebb lett.

Értékelő laborként, az iparági szereplőkkel szorosan együtt dolgozva úgy látjuk, hogy ezeket a tapasztalatokat érdemes komolyan megfontolni egy alkalmas magyar rendszer megalkotásakor. A lehetséges maximális mértékig célszerű bizonyított és kölcsönös nemzetközi elfogadást biztosító szabványokra és sémákra alapozni.

Nem véletlen, hogy a gyártók európai szintű szervezetében (ESMIG) az unióval együttműködve a Common Criteria alapján javasolják a kölcsönös elfogadást biztosító tanúsítást.



A kölcsönös elfogadás lehetősége a magyar gyártók számára is elemi érdek, hogy a magyar követelményeknek való megfelelés rögtön európai szintű üzleti lehetőséget teremtsen számukra.

A kritikus infrastruktúrát üzemeltető európai szervezeteket tömörítő ENCS²⁰⁴ 2019. júliusában tette közzé az intelligens mérőrendszerek beszerzésekor érvényesítendő információbiztonsági követelményrendszerét.²⁰⁵

Amennyiben egy termék rendelkezik az ESMIG által javasolt védelmi profilnak megfelelő tanúsítással az automatikusan megfelel az ENCS követelményrendszernek, és a svájci elvárásoknak is. Bár Svájcban az egyedi dokumentálási követelmények miatt egyelőre még némi „papírmunkára” szükség van. A METAS-Cert-tel megkezdődött az egyeztetés, hogy a jövőben az említett Common Criteria tanúsítvány további teendő nélkül elegendő legyen.

8. Adaptáció Magyarországon

A lakossági és ipari közmű/energia fogyasztók számára szükséges egy biztonságos és intelligens — okos energiafelhasználás-menedzsmentet lehetővé tevő — közmű felügyeleti és mérési rendszer.

A svájci modellben egy olyan keretrendszert választottak, ami kevésbé szigorú, mint a Common Criteria, de használja azokat a lényeges biztonsági követelményeket, amelyek alkalmazásával biztonságosabbá tehetőek a termékek.

A minisztérium az iparági szövetség ajánlását elfogadva, az alapján hozta létre a jogszabályt és határozta meg a szereplőket. Az iparági szövetség a keretrendszert definiálta.

A keretrendszer által kitűzött cél a 8-10 hét alatt lefolytatott sikeres termékértékelés, amelyeket követően a termékek bizonyítottan megfelelnek a követelményeknek. Ezt a követelményt egyelőre nem sikerült elérniük.

A svájci modell tapasztalatai és az abban érintett gyártókkal, iparági szakemberekkel való egyeztetés alapján azt látjuk, hogy a Common Criteria használata egy alacsonyabb megbízhatósági szinttel, és az ISO 27000-es szabványcsalád alkalmazása lehet a jelenleg legalkalmasabb megoldás a magyar szabályozás számára.

- Teljesen összhangban van az új európai információbiztonsági szabályozás követelményeivel.
- Jelenleg is kölcsönös nemzetközi elfogadást biztosít a gyártóknak.
- Összhangban van az ENCS ajánlásával.

²⁰⁴ ENCS: European Network for Cyber Security (Európai Hálózat a Kiberbiztonságért)

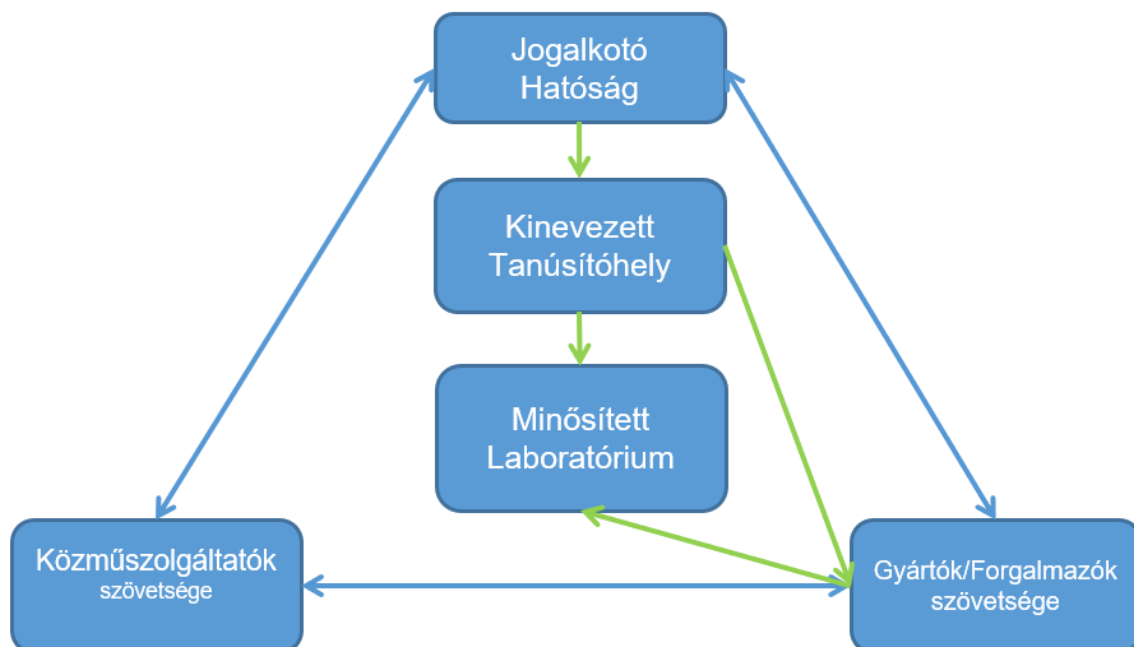
²⁰⁵ <https://encs.eu/encs-document/smart-meter-security-requirements/>



- Kidolgozott, évtizedesen bizonyított módszertanok, és szakemberek állnak mögötte (tanácsadók, értékelők, tanúsítók).
- Abevezetése a sémákat belülről ismerő tanácsadó(k) bevonásával haladéktalanul megkezdhető.

A hazai rendszer bevezetésére a becslésünk jogszabályalkotással, publikálással, iparági egyeztetésekkel együtt 8-16 hónap bevezetési idő a projekt indításától kezdve.

Első lépésként egy megvalósíthatósági tanulmányt készítenénk az EU-ban a kritikus infrastruktúra biztonsági szabályrendszerét, CyberSecurity Act-et, valamint a magyarországi helyzet bemutatását, illetve a svájci modell tapasztalatait is magában foglalva, s ezt aztán a döntéshozó elé tudnánk terjeszteni.



10.1. ábra: Javaslat egy lehetséges magyar rendszerre

A bevezetés során célszerűnek látjuk, hogy legyen egy mintaprojekt, amely a már kialakított magyar modell alapján elvégzett értékelés. Így a rendszer bevezetése elején kiszűrhetőek az esetleges problémás területek, ezáltal csiszolható a rendszer.

Jelenleg egy versenyelőnyös helyzet alakítható ki, ha egy gyorsan megvalósítható, költséghatékonyan kialakított rendszert állítunk össze.

Javaslatunk szerint nemzetközi mintára, az érintett európai szervezetek által kidolgozott szabványokra és ajánlásokra, kipróbált módszertanokra, és a hazai tudásbázisra épüljön a magyar okos mérés biztonságát nyújtó minősítési és tanúsítási rendszer.



11. melléklet: Észak-amerikai modell

1. Rövid bemutatás

Az alábbiakban ismertetett szabályozás kifejezetten villamosenergia-iparra, és annak is az átviteli hálózati "nagybani" részére készült, a biztonságos rendszerüzemeltetés részeként definiálja a kiberbiztonsági szabályokat. A korábbi önkéntes működési mód örökségeként egyes szabályozások eléggé fel vannak puhítva, dokumentálási kötelezettségen nem mennek túl, azonban rendszer szemléletűek és a frissített verzióban a NIST kritikus infrastruktúra biztonsági keretrendszernek való megfelelést valósították meg. Nagy előnye a szabályozásnak, hogy kiforrott, hiszen az észak-amerikai rendszer 2007 óta ezeknek megfelelően működik.

2. Szabályozás jelenlegi állapota

A North American Reliability Corporation (NERC) felel a villamos alaphálózat, erre csatlakozó erőművek és fogyasztók biztonságos üzemeléséért. Általános üzemi szabályzatok része a NERC CIP (Critical Infrastructure Protection), amelyen belül 11 db jelenleg alkalmazandó és 5 db jövőbeli kötelezettséget előíró szabvány van érvényben, emellett 2 db elfogadás alatt van. A rendszert folyamatosan javítják és bővítik, egyes szabványoknál már a hetedik verziónál tartanak, míg az ellátási lánc kockázatértékelés (CIP-013) most kerül első kiadásra. 2013-tól az egységes szemléletű CIP v5 programban mindegyiket felülvizsgálták, üzemeltetési tapasztalatokat is figyelembe véve.

3. Szabályozás háttere, kapcsolat más direktívákkal

NERC 2005-ig önkéntes szervezet volt, akkor Energy Policy Act definiálta az Energy Reliability Organization szerepet és kötelezővé teszi a NERC tagságot USA-ban, valamint a NERC szabványoknak megfelelést 2007-től. Kanadában hasonló törvények alapján szintén kötelező a csatlakozás. Mexikó Baja California része szintén alkalmazza a szabályozást. A CIP v5 felülvizsgálat egyik célja volt a NIST Framework for improving Critical Infrastructure Cybersecurity²⁰⁶-nek való megfelelés. Utóbbi minden részterülete azonosítható az ISO 27001, NIST SP-800-53, ISA-62443, CIS CSC, COBIT szabványok és ajánlások pontjaiban. Mint keretrendszer gyakorlatiasabb megközelítést képvisel az ISO62443-hoz képest.

²⁰⁶ <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>



4. Jogszabályi komplexitás

A rendszer üzemeltetés szabályai közé illesztették be a kiberbiztonsági és fizikai biztonsági előírásokat. Emiatt nagyon erősen real-time üzemeltetés fókuszú, a villamosenergia és tartalék piaccal való kapcsolat lényegében nincs definiálva. Csak az alaphálózathoz ("bulk electricity"), csatlakozó erőművekre és felhasználókra vonatkozik, elosztóhálózatra nem. Részletes követelmények a kiberbiztonság minden területére, fizikai biztonságot is beleértve. Minden követelmény objektív, mérhető és harmadik fél által ellenőrizhető. Egyértelmű követelmények vannak definiálva a megfelelésre és a különböző súlyosságú megsértésre, erre példa a mellékelt ábrán látható CIP-010 R3 által előírt új rendszer/eszköz üzembehelyezése előtt elvégzendő sérülékenységvizsgálat.

CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.

11.1. ábra: CIP-010 R3 3.3 követelmény

Megjegyzés: EACMS: Electronic Access Control or Monitoring System (*hozzáférés szabályozási és felügyeleti rendszer*)



PCA: Protected Cyber Asset (minden olyan eszköz, ami routolható protokollon keresztül kapcsolódik a rendszerhez)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	Medium	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	Long-term Planning and Operations Planning	Medium	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

11.2. ábra: CIP-010 R2-R3 követelmény megsértésének feltétele

Mint látható, az R3 követelmény súlyossági besorolása kicsit formális; enyhe megsértés a 15 hónapon túli teljesítés, erős pedig a 21 és 24 hónap közötti. A legerősebb szint érthető: ha nincs egyáltalán ilyen vizsgálat vagy a feltárt sérülékenységek kezelése nincs dokumentálva (ez a beszűrt ábrán terjedelmi okokból már nem látszik). Ugyanakkor a 11.2. ábra felső részén látható R2 követelményre (amely a baseline konfigurációtól való eltérés ellenőrzését írja elő legalább 35 naponként) nincs ilyen fokozatosság, ha nem történik meg, az automatikusan a leg súlyosabb megsértést eredményezi.



Az egyes követelmények magyarázata is a szabvány része, a fent bemutatott R3 követelményhez részletesen leírja, hogy mit tekint aktív/papír alapú sérülékenységvizsgálatnak:

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well - documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery – A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification – A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review – A review of security rule – sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review – Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery – Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.



5. Szabványok, termék, rendszer, vagy folyamat tanúsítás követelményei

A NERC CIP szabványok rendszer és működési folyamat szabványok, terméket nem tanúsítanak, piac és gyártó semleges követelményeket határoznak meg. A szabványok kialakítása az ANSI (American National Standards Institute) által akkreditált folyamattal történik, széleskörű alkalmazói részvétellel. A CIP v5 verziónál lényeges változás, hogy egyes funkciókat ellátó részrendszereket (Bulk Electric System Cyber System) kell minősíteni és ezekre teljesíteni a követelményeket és nem az egyes komponensekre (CIP-002-5.1a 6. fejezet).

6. Megfelelési kööttségek egyes szabványoknak, vagy adott szabványra épülés

Hatályos szabványok:

CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	Related Information
------------------------------	--	-------------------------------------

CIP-003-6	Cyber Security - Security Management Controls	Related Information
---------------------------	---	-------------------------------------

CIP-004-6	Cyber Security - Personnel & Training	Related Information
---------------------------	---	-------------------------------------

CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	Related Information
---------------------------	---	-------------------------------------

CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Related Information
---------------------------	---	-------------------------------------

CIP-007-6	Cyber Security - System Security Management	Related Information
---------------------------	---	-------------------------------------

CIP-008-5	Cyber Security - Incident Reporting and Response Planning	Related Information
---------------------------	---	-------------------------------------

CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems	Related Information
---------------------------	---	-------------------------------------



[CIP-010-2](#) [Cyber Security - Configuration Change Management and Vulnerability Assessments](#) [Related Information](#)

[CIP-011-2](#) [Cyber Security - Information Protection](#) [Related Information](#)

[CIP-014-2](#) [Physical Security](#) [Related Information](#)

Jövőben hatályos:

[CIP-003-7](#) [Cyber Security — Security Management Controls](#) [Related Information](#)

[CIP-005-6](#) [Cyber Security — Electronic Security Perimeter\(s\)](#) [Related Information](#)

[CIP-008-6](#) [Cyber Security — Incident Reporting and Response Planning](#)

[CIP-010-3](#) [Cyber Security — Configuration Change Management and Vulnerability Assessments](#) [Related Information](#)

[CIP-013-1](#) [Cyber Security — Supply Chain Risk Management](#) [Related Information](#)

Az egyes szabványoknál külön-külön van definiálva, hogy milyen entitásokra vonatkozik az adott szabvány, ez az átláthatóságot nehezíti. Egyes elosztóhálózaton megvalósított funkciókra is kiterjed bizonyos szabványoknál, pl. a 300MW-nál nagyobb fogyasztás korlátozást végző automatikus terheléshedobási rendszer is CIP-002 szerint.

7. Helyi különböző előírások, direktívák, politikai vetület

Az USA kontinentális és szövetségi jellegéből következően a NERC az ACER, ENTSO-E és nemzeti hatóságok számos feladatát és jogkörét egyesíti. A Regional Entities az egyes szabályozási területeken működő helyi szervezetek, ezekhez a NERC delegálja a jogköröket és feladatokat. Kanadában a tartományi kormányzatok hatósági szervei ellenőrzik a betartást, de a követelmények egységesek. Friss hír, hogy az USA Szenátusa elfogadott egy törvényjavaslatot, amely a kiberbiztonsági veszélyek miatt a jelenlegi automatizált digitális



rendszerek alternatíváit (elszigetelt rendszerek, kézi tartalék működtetés, analóg rendszerek) kívánja megvizsgálni.²⁰⁷ [44]

8. Hatósági jogkörök, hatósági funkciók

A Federal Energy Regulation Commission egy kormányzati ügynökség, amely USA-ban felügyeli a NERC-et, de a rendszer kialakításának és ellenőrzésének felelőssége NERC-hez van rendelve. Kanadában ezt a tartományi kormányzatok gyakorolják. NERC tartja fenn a Compliance Monitoring and Enforcement programot, ennek része a Regional Entity-k megfelelési programja, ezek a szervezetek auditálják az üzemeltetőket. A FERC és NERC hatásköreinek megosztásáról jelenleg is vita van, egyes törvényalkotói kezdeményezések a szövetségi hatóság jogköreit kívánják kiterjeszteni²⁰⁸ [45], egyrészt az elosztóhálózatra is kiterjesztve, másrészt a kritikus helyzetekben történő gyorsabb reakció érdekében.

9. Egyéb fontos megjegyzés

Az európai és magyar szabályozási környezetbe a teljes modellt nem lehet átültetni az eltérő hierarchia miatt, de a követelményeket leíró NERC CIP szabványok használata quick win lehetőség és jól illeszkedik az ISO27001-27019 szabványokhoz, azonban figyelemmel kell lenni az elosztóhálózati sajátosságokra is.

²⁰⁷ A. King. „Senate Passes King Bill Protecting Energy Grid from Cyber-Attacks.” U.S. Senate. <https://www.king.senate.gov/newsroom/press-releases/senate-passes-king-bill-protecting-energy-grid-from-cyber-attacks> (Letöltve: 2020. augusztus 30.)

²⁰⁸ Energy Central Community. „FERC versus NERC.” Energy Central. <https://energycentral.com/c/iu/ferc-versus-nerc> (Letöltve: 2020. augusztus 30.)



12. melléklet: Osztrák modell

1. Rövid bemutatás

Ausztria kiberbiztonsági stratégiáját 2013-ban adták ki és jelenleg is ez a stratégia van hatályban.

A villamosenergia-ipar kiberbiztonságának biztosítása a NIS irányelv implementációjának a része. Az irányelvben meghatározott ágazatok információbiztonságát hivatott szolgálni a törvény.

2. Szabályozás jelenlegi állapota

A Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozattal (a továbbiakban: NKS) szemben erősebben jelen van benne a kibertámadások politikai vetülete, mind védelmi, mind támadási szempontból, vagyis a kibertérben zajló politikai tevékenységek jelentősége megjelenik benne. Az NKS jogi aktus, az osztrák stratégia nem jogi aktusként került kiadásra, hanem az az Osztrák Köztársaság Kancellária által kiadott dokumentum.

Az osztrák stratégia nagy hangsúlyt fektet az információs és kommunikációs technológiák biztonságára, és a fenyegetésekkel szembeni ellenállóképességük növelésére. A PPP is célként került meghatározásra a dokumentumban. Tartalmaz feladatot a dokumentum kiberbiztonsági irányítási csoport létrehozására vonatkozóan, amely az ezzel kapcsolatos nemzeti és nemzetközi feladatok ellátását segíti elő, és ellenőrzi azt. A kiberkrízis menedzsment megteremtése szintén megvalósítandó cél, a katasztrófavédelemmel, kritikus infrastruktúrákkal és egyéb releváns szervezetekkel egyetemben.

A kritikus infrastruktúrák külön részt kaptak, illetve a velük kapcsolatos kiberbiztonsági feladatok.

Az oktatáson is nagy hangsúly van, ahogy a kiberbiztonsági kutatás-fejlesztés megvalósításán is. A melléklet tartalmaz egy kiberbiztonsági kockázati mátrixot, amely hasznos dolog a szervezeti és a nemzeti kockázatelemzés szempontjából egyaránt.

A jogi szabályozás terén elmondható, hogy információbiztonsági törvény (NIS törvény) ki van adva, de a hozzá kapcsolódó rendelet még nem került kiadásra, de hamarosan ez is meg fog történni.

A stratégiára vonatkozóan létrehoztak egy supervisor team-et, akik a stratégia megvalósulását hivatottak ellenőrizni. 12 tagból áll, akiket az üzemeltetők delegálnak.



3. Szabályozás háttere, kapcsolat más direktívákkal

A rendelkezésre álló információk és dokumentumok alapján megállapítható, hogy a NIS irányelv és a GDPR kapcsolat megvan az osztrák információbiztonsági törvényben. Különbség a magyar szabályozáshoz képest, hogy az Ibtv. klasszikus információbiztonsági törvény, míg a NIS törvény specifikusan az adott ágazatokra koncentrál, amelyet az irányelv meghatároz.

Létezik rendszer tanúsítás az osztrákoknál, amelyet a privát szféra szereplői végeznek, és a CSC (Cyber Security Center in the Federal Ministry of the Interior), mint kormányzati szereplő auditálja azt.

4. Jogszabályi komplexitás

Az energia ágazat mindhárom alágazatára vonatkozóan tartalmaz a NIS törvény előírásokat, de ezt egyetlen jogi szabályozóban teszi meg.

5. Szabványok, termék, rendszer, vagy folyamat tanúsítás követelményei

Lásd a 3. alcímnél.

6. Megfelelési kööttségek egyes szabványoknak, vagy adott szabványra épülés

Lásd a 3. alcímnél.

7. Helyi különböző előírások, direktívák, politikai vetület

A CERT-ek vonatkozásában különbözőség, hogy külön Energia ágazati CERT áll rendelkezésre az ágazati szereplők számára. (3 nemzeti CERT – MilCERT, GovCERT, és Energy CERT) Megelőző, és önkéntes megközelítéssel dolgoznak, szektor specifikus know-how-kat dolgoznak ki. Az ágazati szereplők között információmegosztás működik megbízható környezetben.

8. Hatósági jogkörök, hatósági funkciók

A NIS törvény hatálya alá tartozó szervezetek kiválasztását a szövetségi kancellária határozza meg. A biztonsági incidenseket a vállalatoknak jelenteniük kell az Energy-CERT számára, amely továbbítja az incidens bejelentést a CSC-nek. A CSC ellenőrzi a magán tanúsító szervezeteket is, amelyek igazolják a szövetségi kancellária által kiválasztott cégek megfelelőségét. Ezeket a tanúsítványokat be kell nyújtani a CSC-nek.



9. Egyéb fontos megjegyzés

2 évenként programokat indítanak nemzeti szinten PPP együttműködés keretében a jelenlegi kritikus infrastruktúra védelmi rendszer ellenállóképességének javítása érdekében. A jelenleg végfázisában lévő projekt a digitális rádiós eszközök üzemeltetésének kritikus infrastruktúra védelmi céljait és a rendszert használó csoportokat vette górcső alá. A kommunikáció lehetőségeit és fajtáit vizsgálják szektoronként külön és együtt is.

Az osztrákok (Austrian Institute of Technology) modellezik az ágazatok közötti összefüggéseket a kockázatok és a tovább gyűrűző hatások vonatkozásában, amelyet egy ún. CERBERUS projekt keretében valósítanak meg.²⁰⁹

²⁰⁹ <https://www.syssec.at/en/projekte/cerberus>



13. melléklet: Német modell

1. Rövid bemutatás

A létfontosságú rendszerek jellemzően nem önmagukban álló, és értelmezhető entitások, hanem szorosan illeszkednek egy tágabb, elsősorban európai műszaki, technológiai, üzleti, jogi és politikai környezetbe. Emiatt is többszörös jelentőséggel bír a nemzetközi szabályozói környezet, és különösen Németország, mint az egyik meghatározó szereplő példájának vizsgálata. A létfontosságú rendszerek (kritikus infrastruktúrák), kibervédelmének német rendszerére a KRITIS név alatt hivatkozunk. Ez egyesíti a KRITIS keretrendszert, illetve az adott területet kiegészítő egyéb ágazati szabályozásokat. Ebben az összefoglalóban ebben az értelemben mutatjuk be a németországi szabályozási környezetet, a KRITIS-t.

2. A szabályozás alapja

A szabályozás alapja a 2015 júliusában hatályba lépett BSI törvény (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) BSI-Gesetz). A BSIG kinyilvánítja az állam felelősségvállalását és demonstrálja, hogy a szabályozó hogyan járhat élen a kritikus infrastruktúrák védelmében, ahol a modern társadalom a legkevésbé engedheti meg a hibákat. Kereteket teremt az állampolgárok, a gazdaság és az állami adminisztráció biztonságának garantálásához.

A kijelölt koordináló és felügyelő szervezet a BSI (Bundesamt für Sicherheit in der Informationstechnik) a Német Szövetségi Információbiztonsági Hivatal.

A kritikus infrastruktúrát üzemeltető szervezeteknek, az energetika, telekommunikáció, közlekedés, egészségügy, vízgazdálkodás, élelmiszeripar és a pénzügyi szolgáltatások esetében fenn kell tartaniuk egy "state-of-the-art" minimális információbiztonsági szintet az NIS irányelvvel összhangban, amit kétfévente felülvizsgálnak, illetve tájékoztatniuk kell a jelentős információbiztonsági incidensekről a BSI-t.

3. Érintett szervezetek

Az atomerőműveket és a telekommunikációs szolgáltatókat már a BSIG egységesen a törvény hatálya alá sorolja. Egyéb esetben a BSIG törvény alapján (10. szakasz 1. bekezdés) a KRITIS-rendelet (BSI-Kritisverordnung vagy BSI-KritisV) definiálja a törvény hatálya alá tartozó kritikus infrastruktúra elemeket, illetve szereplőket. Itt szektorspecifikus küszöbértékeket határoztak meg, amely alapján eldönthető, hogy egy adott tevékenység a törvény hatálya alá tartozik-e. Az 1. melléklet 3. része rögzíti az energetikai ágazat résztvevőit egy hierarchikus struktúrában. Mindegyikkel szemben megállapítja az értékelés módszerét, és a hozzá tartozó küszöbértéket, ami fölött a törvény hatálya kiterjed az érintett résztvevőre.



Pl. 1. Energiaellátás / 1.1. Áramellátás / 1.1.1. Erőmű kategória esetén amennyiben a névleges elektromos teljesítmény MW-ban meghaladja a 420-as értéket, akkor az adott erőmű a törvény hatálya alá tartozik. A 420 MW értékkel több helyen találkozunk. Itt a számítás alapja az volt, hogy 500.000 ember éves átlagos áramfogyasztásának kiszorgálását biztosítja körülbelül 420 MW névleges teljesítmény.

A további fejezetekben az egyéb területek hasonló mutatóit definiálja a rendelet. A 2. mellékletben a vízügy területén. Itt is az 500.000 fő a küszöbértékek számításának alapja. Pl. az 2. Ivóvízellátás / 2.2. Ivóvízfeldolgozás / 2.2.1. Ivóvízfeldolgozó vízmű esetén évi 22 millió m³ feldolgozott ivóvíz a küszöbérték.

A rendelet hatálybalépését követően az érintett szereplőknek 2 év türelmi idejük van a felkészülésre. A 3.5 millió német cégből a rendelet közvetlenül egy-két ezret érint.

Összességében elmondhatjuk, hogy egy nagyon világos szerkezetű, könnyen érthető és az 500.000 fős korláttal egy kockázatarányos rendszert alakítottak ki. Az azonos vagy nagyon hasonló struktúrájú rendszer magyarországi bevezetését célszerűnek tartjuk. A türelmi idő növelését 3-5 évre indokoltnak látjuk. Különösen annak fényében, hogy az Európai Unió egy összehangolt kvantum-technológián alapuló infrastruktúra kialakításán dolgozik a kritikus infrastruktúrák biztonságának fokozására, amelyhez Magyarország is csatlakozott.

4. UP KRITIS

A SeConSys együttműködéshez hasonlóan létezik egy public-private-partnership kezdeményezés az UP KRITIS a kritikus infrastruktúrák üzemeltetői, az ilyen szervezetek iparági szövetségei és az érintett kormányzati szervek között. 2007 óta ágazatok szerinti (áram, gáz, internet-infrastruktúra stb.), illetve egyéb szakterületi (követelmények a beszállítóknak, auditálás és szabványosítás stb.) munkacsoportban folyik a tevékenység. 2017-re 400 fölötti résztvevője lett a szakmai közösségnek.

5. Mi az operátorok feladata?

A kritikus infrastruktúra operátorokra vonatkozó előírásokat a BSIG 8. szakasza tartalmazza általánosságban.

- 8.a. alapján az operátoroknak alkalmas "state-of-the-art" szervezeti- és műszaki intézkedéseket kell bevezetniük, amelyekkel garantálni tudják informatikai rendszereik, komponenseik és folyamataik elérhetőségét, integritását, hitelességét és bizalmasságát. Az intézkedések megfelelőségét pedig legalább kétfévente alkalmas biztonsági auditokkal, felülvizsgálatokkal vagy tanúsítvánnyal kell igazolniuk.
- 8.b. 3. bekezdés alapján egy kontakt pontot kell kijelölniük a BSI felé, amelyen keresztül bármikor elérhetőnek kell lenniük.



- 8.b. 4. bekezdés alapján azonnal jelenteniük kell a BSI felé a jelentős biztonsági incidenseket. A BSI alkalmas informatikai válságkezelő központot működtet a krízishelyzetek hatékony menedzselésére.

6. Ágazatspecifikus szabványok

A BSIG 8.a. szakasz 2. bekezdés szerint az iparági szereplők ágazatspecifikus "state-of-the-art" biztonsági szabványokat határozhatnak meg. Ezek összefoglaló neve B3S (Branchenspezifische Sicherheitsstandards). A BSI kérés esetén eldönti, hogy ezek a szabványok megfelelnek-e a jogszabályi előírásoknak, és alkalmazhatóak-e a megfelelőségértékelési folyamatban. Ezen ágazatspecifikus szabványok listája elérhető a BSI oldalán.

A BSIG 8.a hatálya bizonyos területekre nem terjed ki, ott közvetlen ágazati szabályozás létezik pl. Az EnWG (Gesetz über die Elektrizitäts- und Gasversorgung, Energiewirtschaftsgesetz) az energetikai hálózatok esetén, de ilyen a nyilvános telekommunikációs hálózatok esete is. Ezekre a területekre a Szövetségi Hálózati Ügynökség (Bundesnetzagentur - BNetzA) állította össze az alkalmazandó szabványok katalógusát. Az energia szektor BSI-KritisV hatálya alá eső szereplőinek többek közt az ISO / IEC 27001-nek megfelelő irányítási rendszer működtetését írják elő az ISO / IEC 27002 és ISO / IEC 27009 figyelembevételével. Az operátornak a BNetzA felé is ki kell jelölnie egy kapcsolattartót, aki tájékoztatja az ügynökséget a BSIG szerinti BSI kapcsolattartóhoz hasonlóan az IT biztonsági követelményeknek való megfelelés állapotáról, illetve a súlyos biztonsági incidensekről.

7. Megfelelőségértékelés, tanúsítás

A BSI kiadott az operátoroknak és a tanúsítóknak egy útmutatót (Orientation Guide to Verification According to § 8a, Para. 3, BSI Act) arról, hogy a megfelelőségértékelésnek, illetve a tanúsításnak hogyan kell történnie.

A tanúsító szervezetek, illetve azok szakemberei felé is komoly elvárásokat támasztanak. A tanúsítás a meglévő nemzeti (DAkKS) akkreditáció bázisán egy speciális kiegészítő követelményrendszer teljesítését várja el a szolgáltatótól és annak ellenőrzésére való képességet a tanúsítótól.



»

A KRITIS rendszer azon alapállásból készült, hogy a világ legbiztonságosabb rendszerét hozza létre a kritikus infrastruktúrák védelmére. Ehhez sikerült széleskörű szakmai együttműködést kialakítani, és kevés átfedéssel a meglévő ágazati szabályozásokkal összhangban megalkotni és bevezetni a szabályozást. Ugyanakkor sikerült elkerülni a túlszabályozást és kezelhető rendszert kialakítani, ésszerű belépési küszöbökkel. Ez is bizonyítja, hogy a SeConSys hasonló fókuszált előkészítő munkájával jó úton jár. A megfelelő kormányzati támogatás és elköteleződés szükséges a továbblépéshez, a hatékony védelmi keretrendszer kialakításához.

«

Az ágazati szabályok (B3S) kellő alapossággal egészítik ki a nemzetközi szabványokat alapul vevő általános követelményrendszert. Ezt a struktúrát javasoljuk Magyarország esetében is alkalmazni.



14. melléklet: SNORT alkalmazási példák

1. példa²¹⁰

SNORT-szabály, ami szerint, ha a HMI a vezérlőtől eltérő bármely eszközzel kommunikál, akkor az IDS a zöld üzenetben megadott riasztást küldi:

IDS Implementation

SNORT rule dissection

```
alert ip [10.0.10.20, 10.0.10.30] any <> ![10.0.10.15] \
  any (msg:"ALERT - HMI communicating with another \
  node"; sid:1000001;)
```

alert	= action type
ip	= protocol (TCP, UDP, IP, etc.)
[10.0.10.20, 10.0.10.30] any	= source IP(s) and port
<>	= direction
![10.0.10.15] any	= destination IP(s) and port
sid:1000001;	= signature ID

14.1. ábra: Alkalmazási példa 1.

- A felső sorban kék színű „riasztás” van. Ez azt mondja a SNORT-nak, hogy riasztást hozzon létre.
- Ezután a protokoll típusa piros.
- Ezt követi a csomag kék forráscíme és portja. Ez azonosítja a „trigger”.
- A csomag iránya piros színű. Ebben az esetben a szabály mindkét irányba utazó csomagokra vonatkozik.
- A következő parancs (kék szín) a célcím és a port.
- Végül a riasztás aláírási azonosítója (vörös szín).

²¹⁰ ICS CERT oktatási anyag



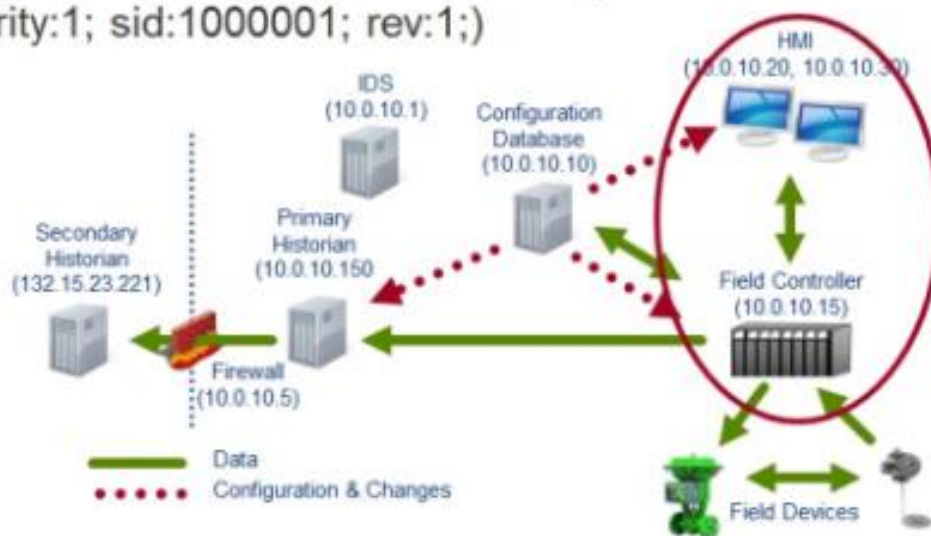
2. példa

Kommunikáció "terepi" vezérlők és HMI között:

IDS: HMI to Field Controllers

SNORT example rule

- alert ip [10.0.10.20, 10.0.10.30] any <> ![10.0.10.15] any \ (msg:"ALERT - HMI communicating with another node"; \ priority:1; sid:1000001; rev:1;)



14.2. ábra: Alkalmazási példa 2.

Valószínű, hogy a támadó felderítést végez és egyéb próbákat tesz, hogy enumerálja a hálózatot, annak eszközeit stb. Ezek olyan rendellenes tevékenységek, amelyekre a megfelelően megtervezett szabályrendszer riaszt. Az ICS egyik fő jellemzője a csomópontok közötti meglehetősen jól megalapozott kommunikáció, azaz az ICS csomópontok kiszámítható – ezért rendellenesség esetén jól detektálható – adatfolyamokkal rendelkeznek.

Amint a példa bemutatja, a HMI elsősorban a vezérlővel kommunikál, így ha egy másik csomópont megpróbál kommunikálni a HMI-vel, akkor alkalmas szabály létrehozásával riasztás generálható.



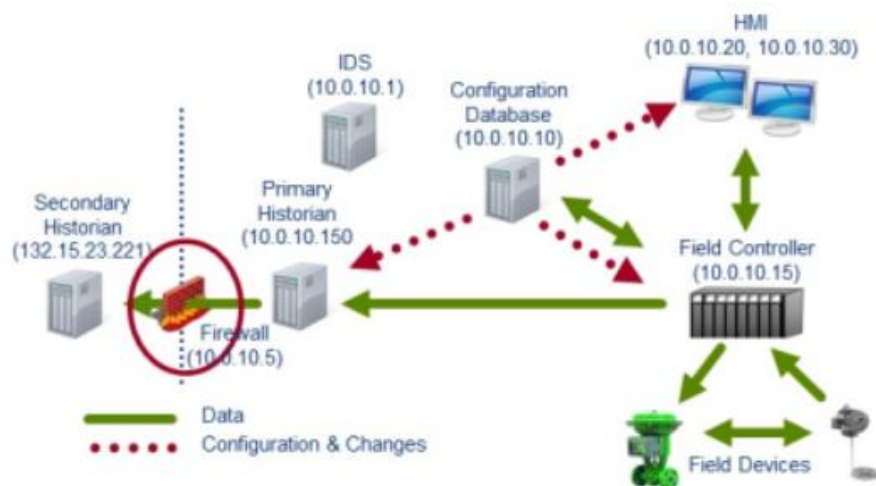
3. példa

Példa a nem megfelelő tűzfal szabályra:

IDS: Improper Firewall Ports

SNORT example rule

- alert ip any any <> 10.0.10.5 80 (msg:"ALERT - Firewall \ access attempted from port 80"; priority:1; sid:1000003; rev:1;)



14.3. ábra: Alkalmazási példa 3.

A tűzfal figyelésére is kidolgozhatunk szabályokat. Ez a szabály pl. akkor generál riasztást, ha bármilyen kommunikáció zajlik a tűzfallal a 80 portján (TCP). „Valaki” megpróbál ezen a porton „beszélni” a tűzfalhoz, miközben azt csak a 443 porton lehet elérni. Ez figyelmeztethet, ha „valaki” megkísérli megnézni vagy megváltoztatni a tűzfal konfigurációját.



4. példa

A megtévesztés alapú IDS rendszerek építése a védekezés szintjének magas szintjét képviseli. Mivel a beruházási (CAPEX) költség relatív elhanyagolható és inkább a szakértelem a domináns, ezért olyan cégnél, ahol jelen van a megfelelő kompetencia, ott érdemes párhuzamos ágon előrehaladni vele.

Számos ilyen megoldás létezik, mint pl:

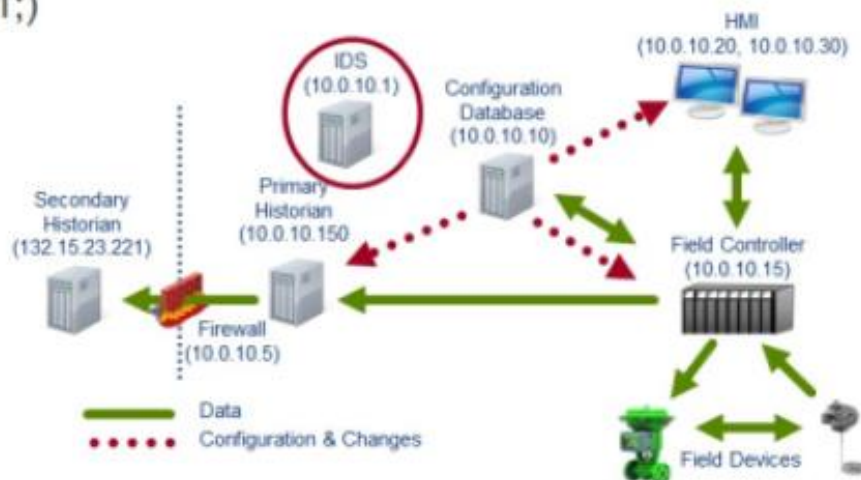
- Honeytoken-ek
- DNS honeypot-ok
- Honeyapp-ek
- ICS Honeypot-ok
- Teljes honeynet-ek
- Fake persona-k
- Purdue Decoy rendszerek

Az alábbi példa egy igen általános esetet mutat be:

IDS: IDS to Nothing

SNORT example rule

- alert ip 10.0.10.1 any <> any any (msg:"ALERT - IDS is \ communicating with another node"; priority:1; sid:1000002; \ rev:1;)



14.4. ábra: Alkalmazási példa 4.



A hálózati honeypot célja az, hogy értesítse a hálózati rendszergazdát arról, ha egy másik eszköz megkísérel kommunikálni a vele. Ez jó jelzés arra, hogy a támadó valószínűleg szkenneli a hálózatot. Ebben a példában a 10.0.10.1 IP-című IDS-kiszolgáló hálózati honeypot-ként működik.



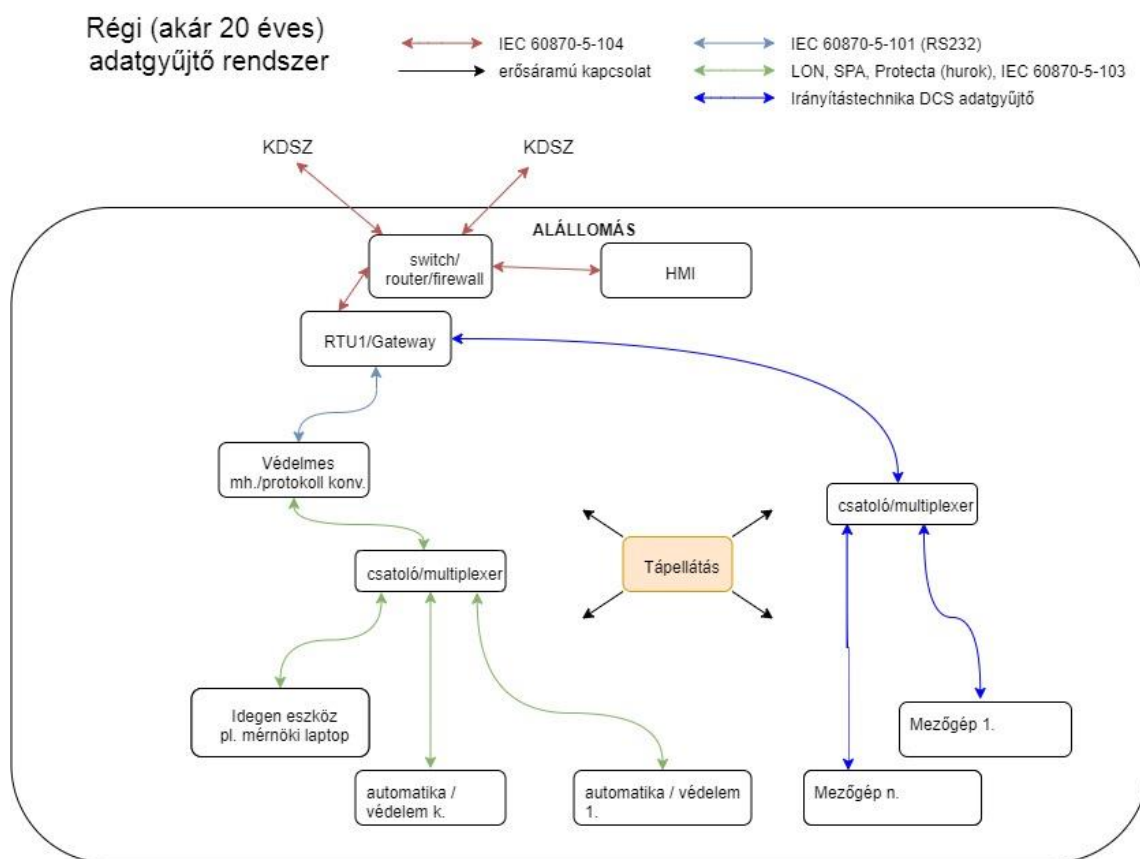
15. melléklet: Villamosenergetikai ICS/SCADA-k felépítése

1. Alállomási adatgyűjtők

Az alállomási adatgyűjtő elemek közötti kommunikáció számos tényezőtől függ (pl. alállomás primer felépítése, feszültségszint, tulajdonos stb.) de a legjelentősebb az, hogy mikor létesült az alállomás és volt-e azóta a szekunder rendszere felújítva.

1.1. Régi alállomás és általános elvek

Egy megközelítőleg 20 évvel vagy korábban létesült és nem rekonstruált alállomás kommunikációs hálózatát mutatja a 15.1. ábra.



15.1. ábra: Régi adatgyűjtő rendszer



Ebben a rendszerben a védelem/automatika és az irányítástechnikai (mezőgép) hálózat el van különítve egymástól. Mindegyik saját csatolóval rendelkezik, amely az alkalmazott (gyártó specifikus) protokollhoz igazodik még fizikai kialakításában is (műanyag- vagy üvegszál optika, csavart érpár). A védelem/automatika készülékek információi a védelmes munkahely/protokoll konverterben gyűlnek össze és ezek továbbítják (a leggyakrabban IEC 60870-5-101 protokollon) az alállomási fejgéphez (RTU). Az irányítástechnikai mezőgépek közvetlenül a fejgéphez csatlakoznak, amely összesíti, feldolgozza és tovább küldi a megfelelően szűrt adatokat a felső (master) irányoknak IEC 60870-5-104 protokollon. Az alállomáson elhelyezett switch/router/firewall-hoz csatlakozik az alállomást teljeskörűen felügyelő helyi megjelenítő (HMI). A KDSZ két – a legtöbb esetben – független útvonalon (lehetőleg más fizikai felületen pl. OPGW²¹¹, rádiós átvitel) keresztül kapja az adatokat szintén IEC 60870-5-104 protokollon. A felső irányok ilyen struktúrájú felépítése minden alállomásra jellemző, beleértve az IEC 60870-5-104 használatát.

Adatgyűjtési és távfelügyeleti szempontból a tápellátás (AC²¹², DC²¹³ és szünetmentes AC) gyakran elhanyagolt része az alállomásnak. Amennyiben a tápellátásban kiesés következik be (meghibásodás, avagy támadás következtében) az alállomás egésze kerül veszélybe, mivel ez biztosítja:

- primer készülék/technológia esetében a működtetéshez szükséges tápellátást és az adatgyűjtéshez szükséges segédüzemi feszültséget,
- szekunder készüléknél/technológiánál²¹⁴ a mezőgép, csatoló, RTU, HMI, switch/router stb. tápellátását.

A tápellátás felügyeletének megfelelő mértékű kiépítettsége és ezáltal az összes többi ICS/SCADA komponens működőképességének biztosítása az alállomások működésének elengedhetetlen előfeltétele. Ez a megállapítás minden az alábbiakban bemutatásra kerülő esetre igaz.

1.2. Részben felújított alállomás

Gyakori eset, hogy egy alállomás egy része átépítésre kerül (pl. egy primer feszültség-szinthez tartozó rész rekonstrukciója, csatlakozó távvezetékek, transzformátorok számának növekedése) és az átépítéssel érintett részen az adott időben korszerűnek tekinthető védelem/automatika és irányítástechnikai adatgyűjtők, hálózatok kerülnek beépítésre.

²¹¹ OPGW: Optical Ground Wire (optikai kábelt tartalmazó távvezetési védővezető)

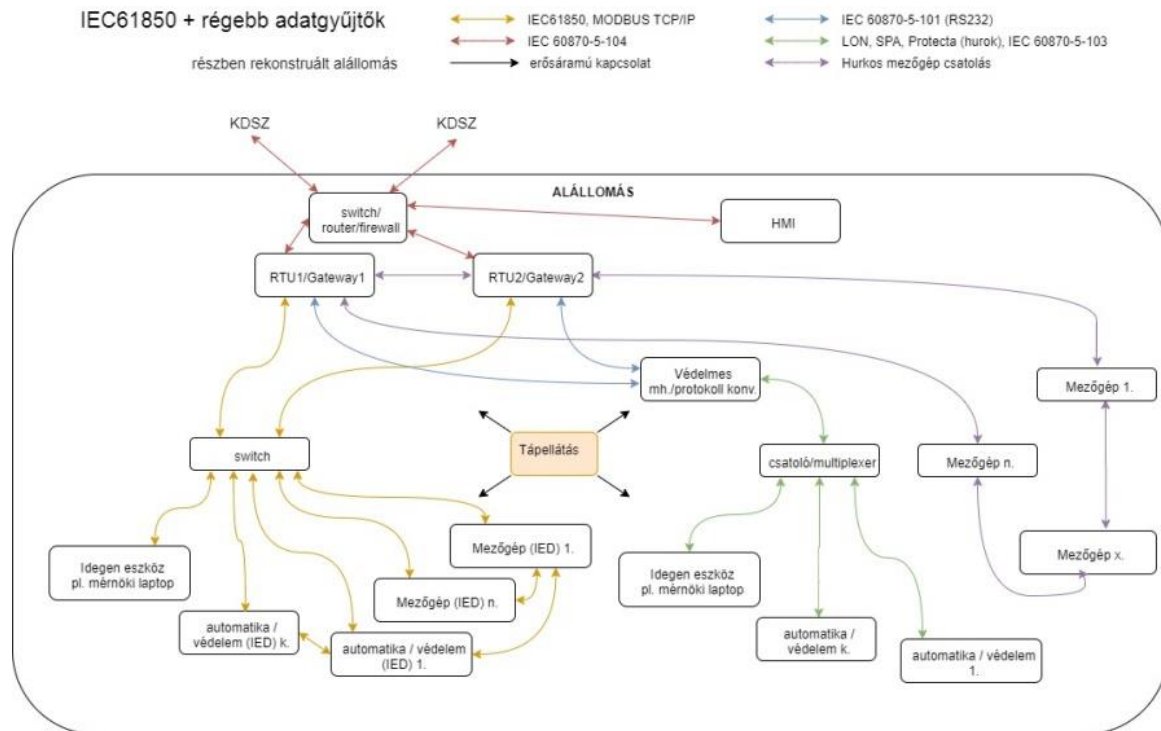
²¹² AC: Alternating Current (váltakozó áram)

²¹³ DC: Direct Current (egyenáram)

²¹⁴ Szekunder készülék/technológia: a primer készülékek vezérlését, diagnosztikáját, adatgyűjtését az információk feldolgozását és továbbítását végző berendezések



Így az alállomás szekunder része különböző korú és kialakítású készülékekből fog állni (ahogyan a 15.2. ábra mutatja). A régebbi rész gyakran 20 éves (vagy annál is régebbi) technológiát takar.



15.2. ábra: Részben felújított adatgyűjtő rendszer

A vegyes technológia alkalmazása azt a helyzetet okozza, hogy EoL és a jelenlegi kornak megfelelő technológiájú (a legtöbbször IEC 61850 szabványú) – TCP/IP alapú kommunikációt használó – adatgyűjtő készülékek is vannak az alállomáson. Ez megbontja a homogenitást és megnehezíti az üzemeltetést. Az EoL készülékek és csatolóik a legtöbb esetben egyáltalán nem – vagy csak erősen korlátozott módon – felügyelhetők (pl. csak 1 db erősáramos ÜKE²¹⁵ jelzés áll rendelkezésre és a távoli szoftveres elérés teljesen hiányzik).

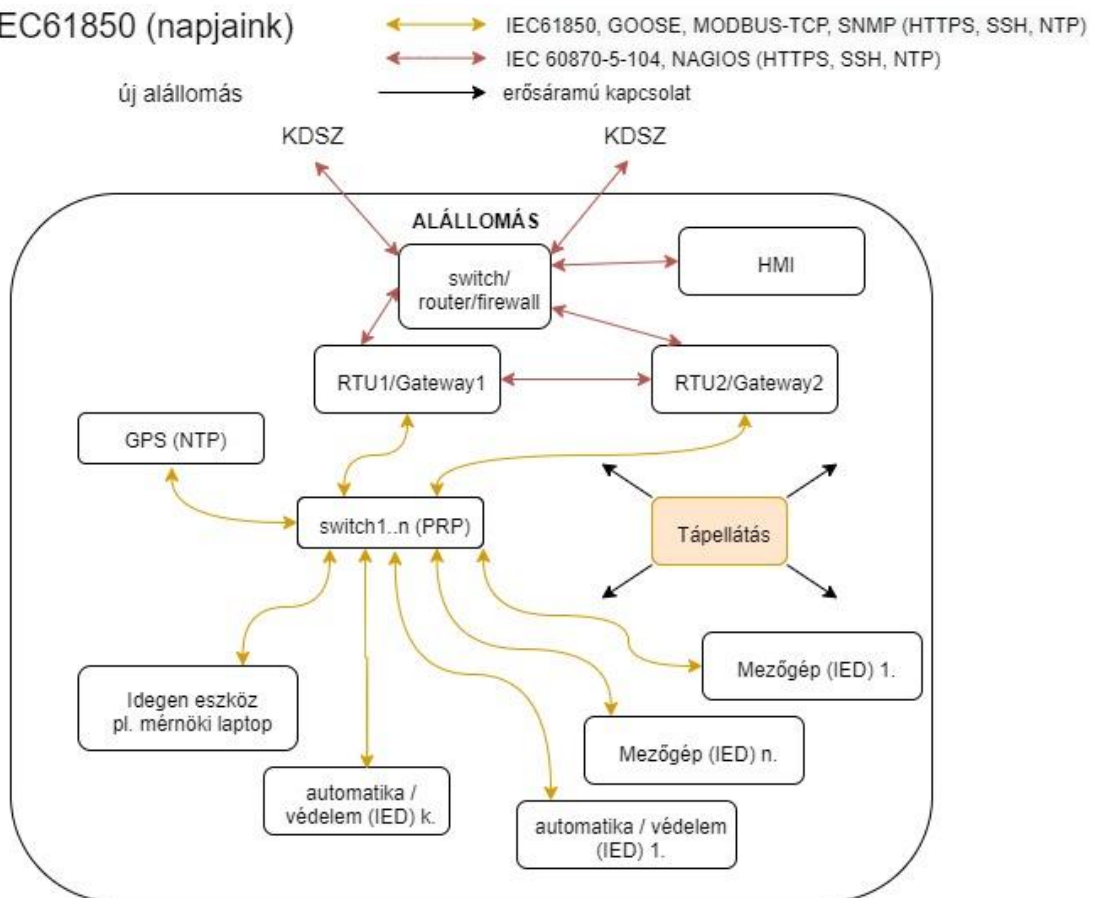
1.3. Jelenlegi technológiájú alállomás

Majdnem teljeskörűen IEC 61850 protokoll szerinti (ezen felül jellemzően Modbus-TCP, SNMP), de minden esetben TCP/IP alapú kommunikációt alkalmazó alállomás, amely zöldmezős beruházás vagy egy alállomás teljes körű szekunder rekonstrukciója során létesül. Elvi felépítését a 15.3. ábra mutatja.

²¹⁵ ÜKE jelzés: üzemkésztség jelzés



IEC61850 (napjaink)



15.3. ábra: Jelenlegi technológiai szintű adatgyűjtő rendszer

Az adatgyűjtést alállomási környezetben alkalmazható (megfelelő EMC védettségű) switchek végzik, az itt jellemző hálózati protokollok szerint (pl. PRP²¹⁶, HSR²¹⁷ egyre ritkábban RSTP²¹⁸). Minden esetben szükséges legalább egy NTP szerver, ami jellemzően az alállomáson van és GPS alapú, a másodlagos NTP szerver távoli, leggyakrabban a KDSZ/ODSZ²¹⁹-ben elhelyezve. Mivel a TCP/IP alapú kommunikáció nem idősorrendi működésű, ezért az időbélyegzés, a csomagvesztés elkerülése miatt pedig a biztos tápellátás kiemelt fontosságú.

1.4. Jövőbeli technológiájú alállomás

Az 1.3. pontban bemutatott technológia továbbfejlesztett változata, amelyben a mért értékek (feszültség/áram) – kellő felbontású A/D²²⁰ átalakítás után (lásd. 15.4. ábra mérőegység:

²¹⁶ PRP: Parallel Redundancy Protocol (Párhuzamos redundancia elvű adatgyűjtő protokoll)

²¹⁷ HSR: Highly-available Seamless Redundancy (Nagy megbízhatóságú, fűrtös elvű protokoll)

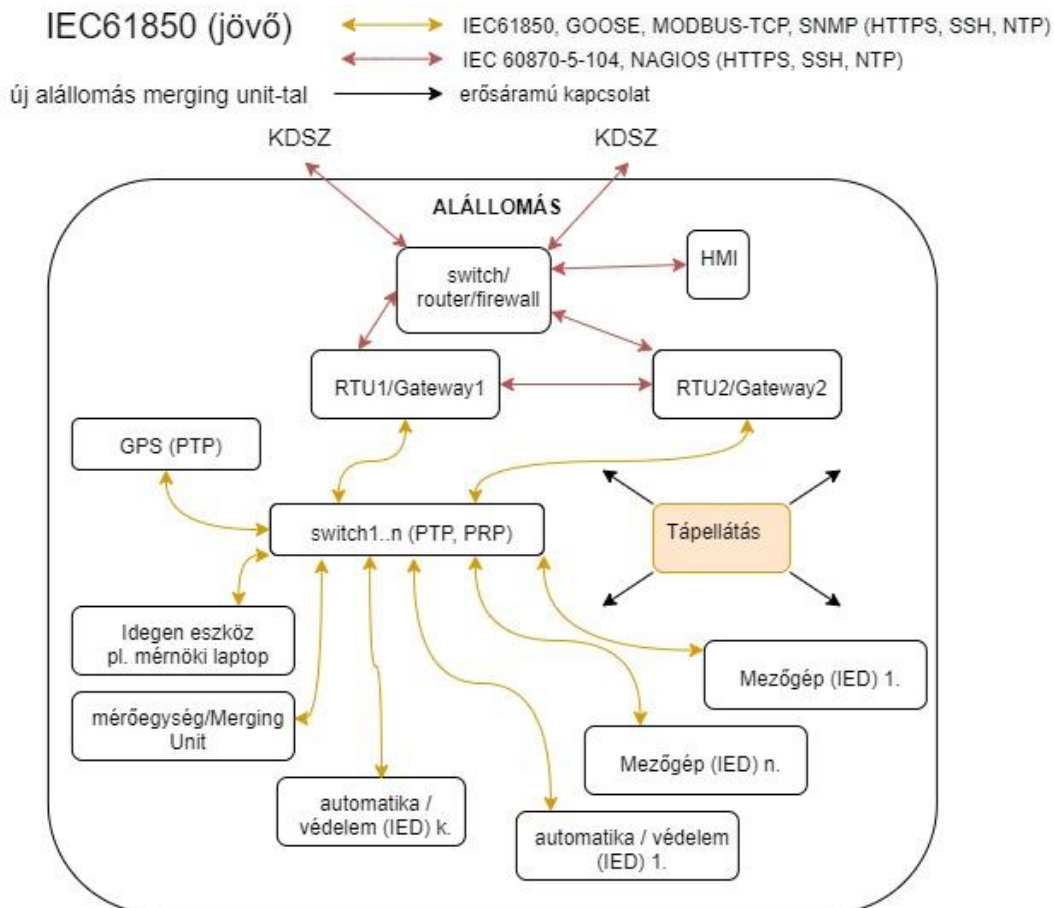
²¹⁸ RSTP: Rapid Spanning Tree Protocol (Gyors hasítófa elvű adatgyűjtő protokoll)

²¹⁹ ODSZ: Országos Diszpécser Szolgálat (a MAVIR üzemirányító központja)

²²⁰ A/D átalakítás: analóg/digitális átalakítás



Merging Unit²²¹) – is a TCP/IP hálózaton keresztül jutnak el a védelem/automatika és irányítástechnikai készülékekhez, azaz a készülékek nem mérik közvetlenül a mérőváltók analóg értékeit.



15.4. ábra: Jövőbeli technológia szintű adatgyűjtő rendszer

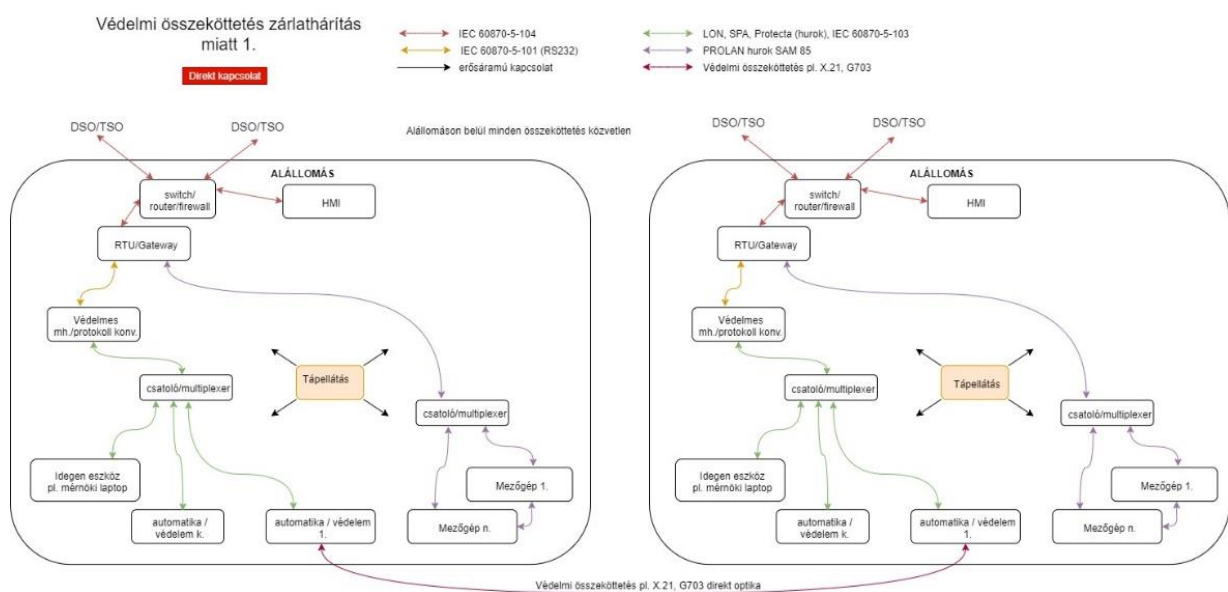
A védelem/automatika készülékek megfelelő reagálási idejű (~40 ms) és pontosságú működéséhez a mért értékeknek legalább 1 μ s felbontásúnak kell lennie időbélyeggel ellátva, amelyet a PTP szabványnak való megfelelés biztosít. Ezen technológia alkalmazásakor minden az analóg jelet digitálissá konvertáló (Merging Unit), továbbító (switch) és feldolgozó (védelem/automatika) elemnek PTP kompatibilisnek kell lennie.

²²¹ Merging Unit: analóg áram és feszültség értékből IEC 61850 szabványnak megfelelő értéket előállító mérő eszköz



2. Direkt alállomási összeköttetések

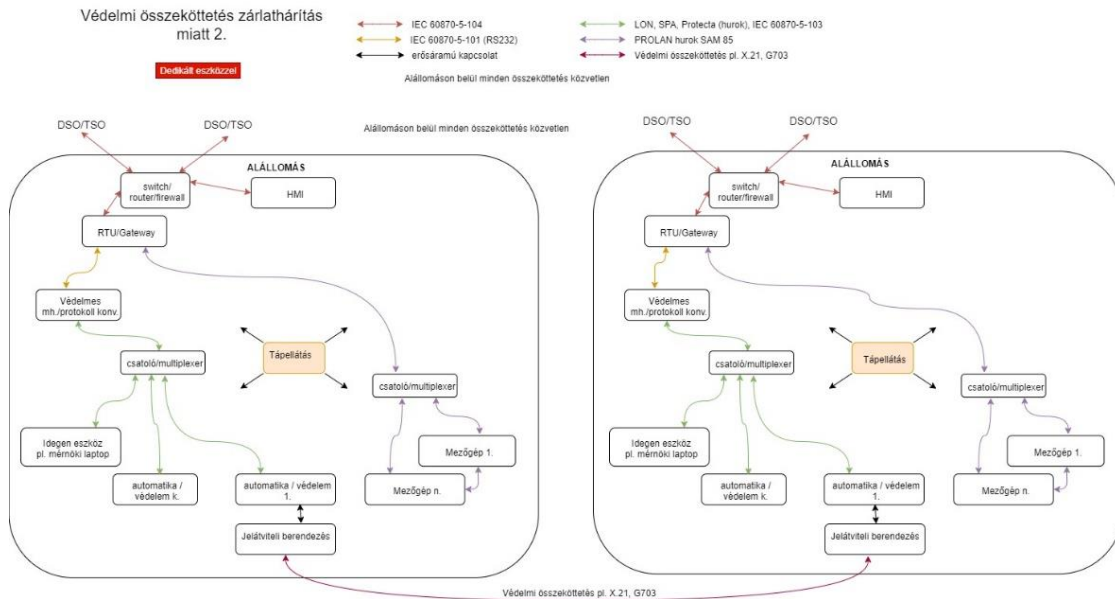
Abban az esetben, ha azonos távvezeték két végén helyezkednek el az alállomások, akkor összeköttetésben állhatnak egymással. Az összeköttetés célja ebben az esetben a minél gyorsabb zárathárítás. Az egyik alkalmazott megoldás, hogy a védelem/automatika készülék közvetlen – jelátviteli készülék nélküli – összeköttetésben van a távvezeték túlvégén lévő védelmi/automatika készülékkel (lásd 15.5. ábra) direkt (sötét) optikai szálon vagy valamilyen távközlési vonalon (pl. X21, G703) valósul meg. A távközlési vonal lehet saját tulajdonú vagy bérelt vonal.



15.5. ábra: Védelmi jelátvitel direkt optikai szálon

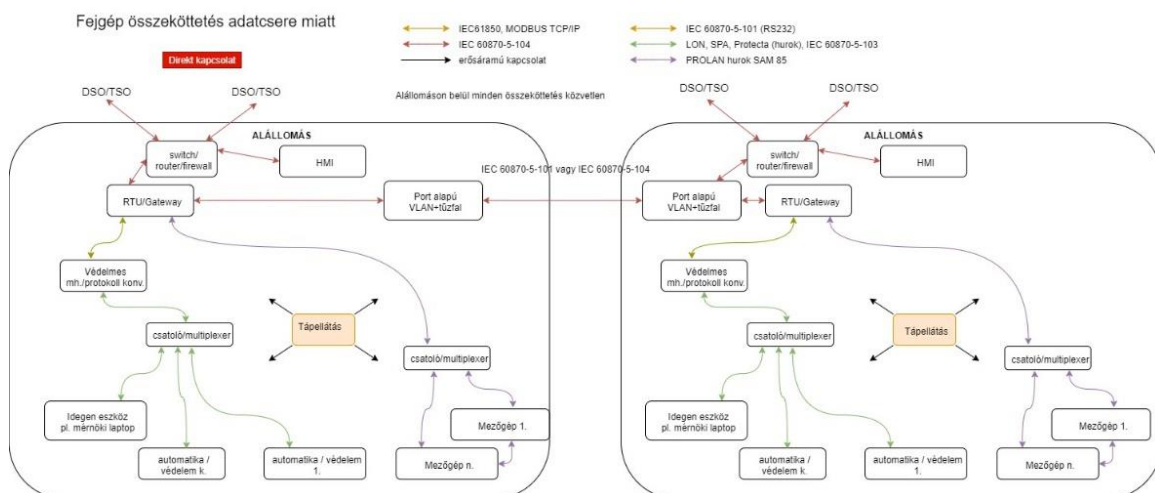
A másik megoldás, hogy a védelem/automatika készülék mellé külön jelátviteli berendezés van telepítve és ekkor a jelátviteli berendezés biztosítja a távvezeték túlvégén lévő párjával az összeköttetést (a 15.5. ábrán bemutatott felületeken). A jelátviteli és a védelem/automatika készülék között erősáramos összeköttetés van. A jelátviteli készülék saját kezelőfelülettel (készüléken lévő vagy távoli pl. böngésző) rendelkezik.





15.6. ábra: Védelmi jelátvitel külön jelátviteli berendezésen

Gyakran alkalmazott megoldás abban a felállásban, ha egy alállomáson belül több tulajdonos van (elhatárolt tulajdonrészsel (pl. ÁSZ – MÁV, MAVIR – Erőmű)) akkor az adatgyűjtés is külön hálózaton történik, illetve saját központja (RTU) van mindkét félnek. Az üzemeltetéshez nélkülözhetetlen információk cseréjére szolgál az RTU-k közötti jelátviteli összeköttetés, ahogyan a 15.7. ábra mutatja.



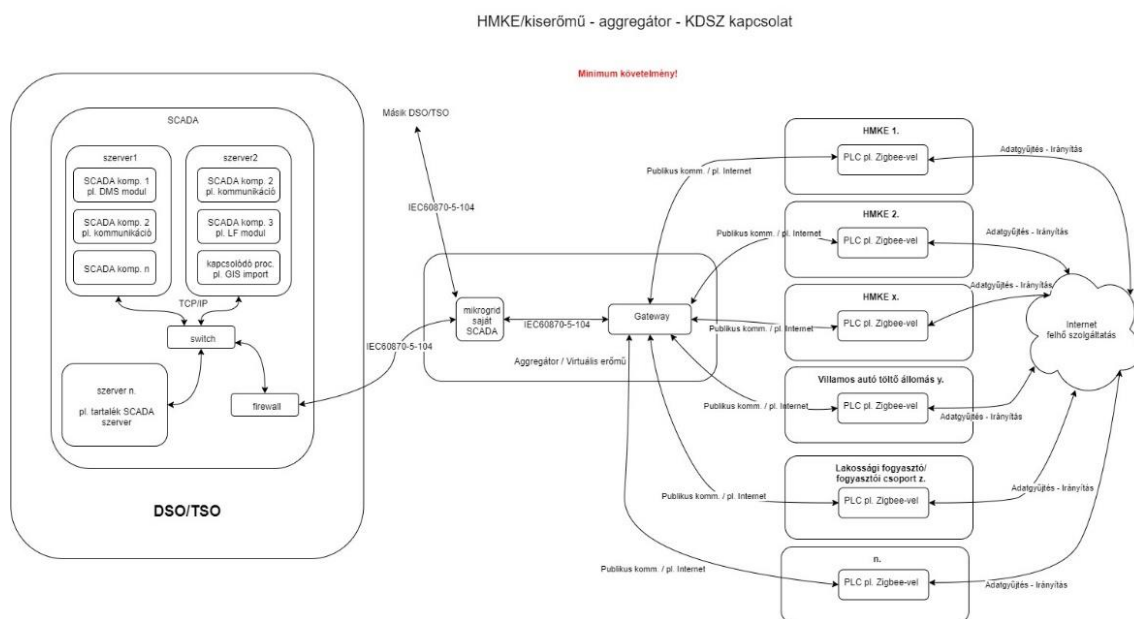
15.7. ábra: Alállomási RTU - alállomási RTU



Amennyiben az összeköttetés IEC 60870-5-104 szerinti, akkor Port alapú VLAN-t és tűzfalat kell alkalmazni.

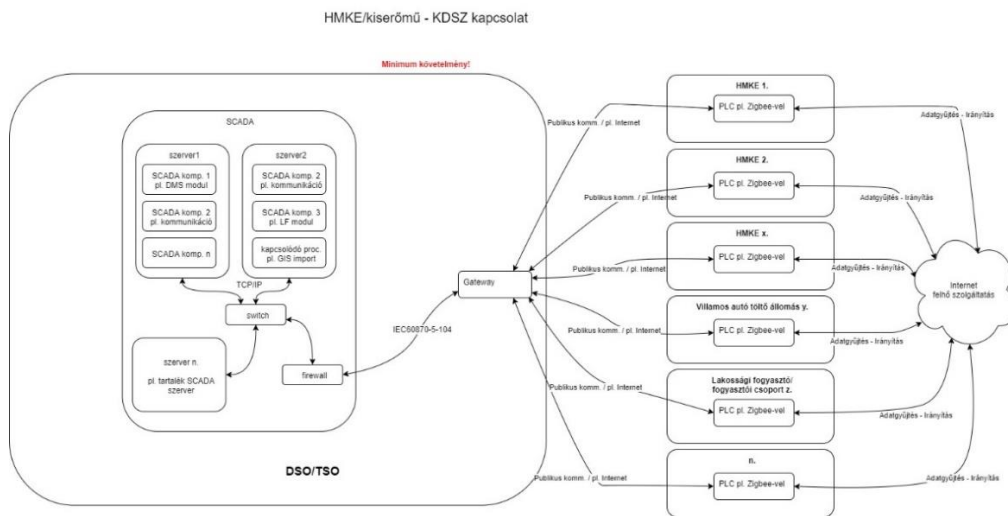
3. HMKE (Háztartási méretű kiserőművek)

A HMKE esetében a helyi adatgyűjtés szinte minden esetben valamilyen lokális (kis hatótávolságú pl. Zigbee) vezeték nélküli kapcsolattal működik. Mivel ezen termelők esetében a beépített eszközök megbízhatósága/származása/backdoor-mentessége nem garantálható, valamint gyakran csatlakoznak a szállítójuk által biztosított internetes felhőszolgáltatáshoz adatgyűjtési/irányítási céllal, valamint az adatgyűjtés is publikus kommunikáción keresztül történik ezért mind az aggregátoron keresztüli (pl. virtuális erőmű) mind a direkt KDSZ kapcsolat esetén is tűzfalas kapcsolatkiépítés szükséges (lásd 15.8. és 15.9. ábrák).



15.8. ábra: HMKE-SCADA direkt kapcsolat





15.9. ábra: HMKE-Aggregátor-SCADA kapcsolat

Mind a két esetben szükséges Gatewayt alkalmazni, amelynek a feladata a publikus kapcsolat átalakítása a feldolgozó rendszerek számára megfelelő protokollra.

4. Kiserőmű összeköttetések

A kiserőmű beépített teljesítmény/csatlakozási feszültség szinttől függően csatlakozhat KDSZ-hez vagy alállomáshoz. Előbbi esetben a kiserőműben az ÁSZ által letelepített PLC/TMOK²²² APN²²³-es GPRS²²⁴ vagy MDLC²²⁵-s URH²²⁶ kapcsolattal csatlakozik a KDSZ-ben lévő Gateway-hez, amely után egy tűzfalnak kell állnia (lásd. 15.10. ábra). Ritkán előfordulhat direkt optikai (pl. OPGW) kapcsolat is.

²²² TMOK: telemechanizált (távvezérelt és -felügyelt) oszlopkapcsoló

²²³ APN: Access Point Name (egyedi hálózat elérési azonosító)

²²⁴ GPRS: General Packet Radio Service (csomagkapcsolt, IP-alapú rádiós adatátviteli technológia)

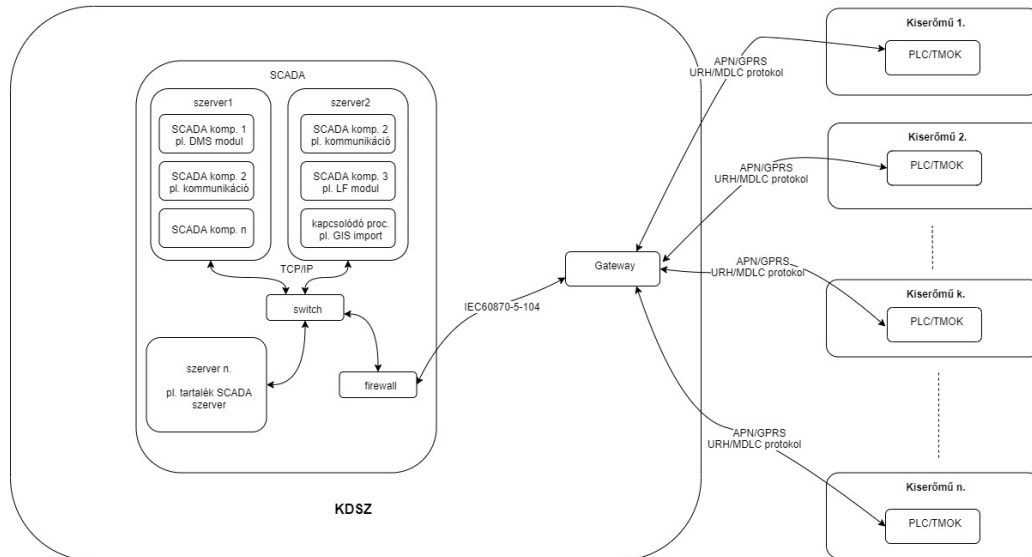
²²⁵ MDLC: Motorola Data Link Communication (Motorola fejlesztésű adatkommunikációs protokoll)

²²⁶ URH: ultrarövid hullám (nyílt rádiós jelátviteli technológia)



Kiserőművek - KDSZ kapcsolat

Minimum követelmény!



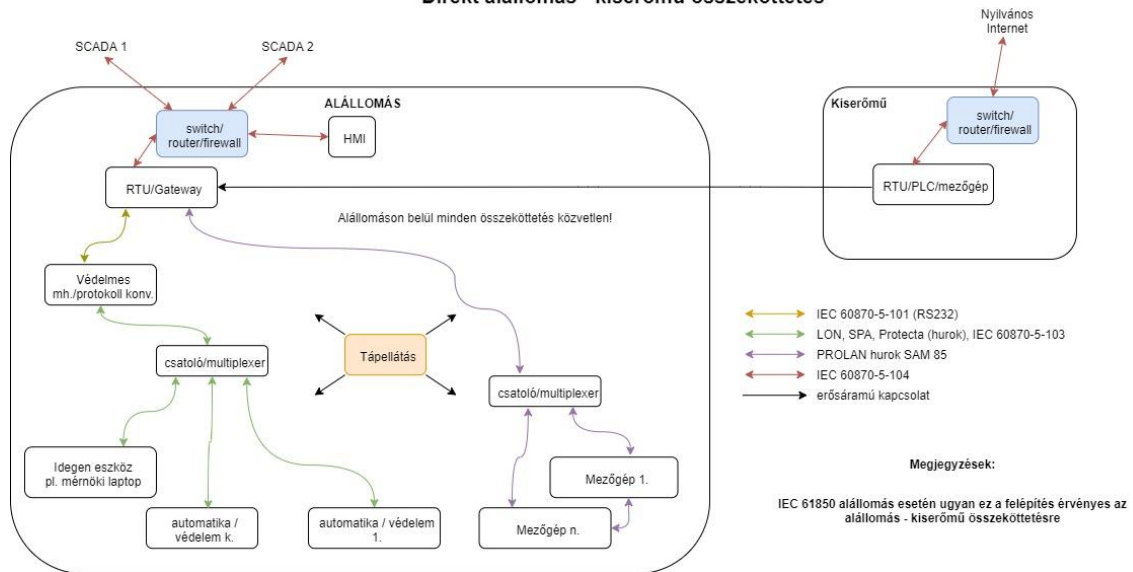
15.10. ábra: Kiserőmű-KDSZ

Amennyiben a kiserőműben elhelyezett PLC/RTU adatait a termelt villamosenergiát fogadó alállomás RTU-jához kell csatlakoztatni akkor két eset lehetséges:

Ha a kapcsolat erősáramos összeköttetéssel van kialakítva (pl. 4-20mA, I/O kártyák) akkor a kiserőmben megengedett az internet kapcsolat (pl. felhő alapú adatgyűjtés/irányítás) kiépítése (lásd 15.11. ábra).



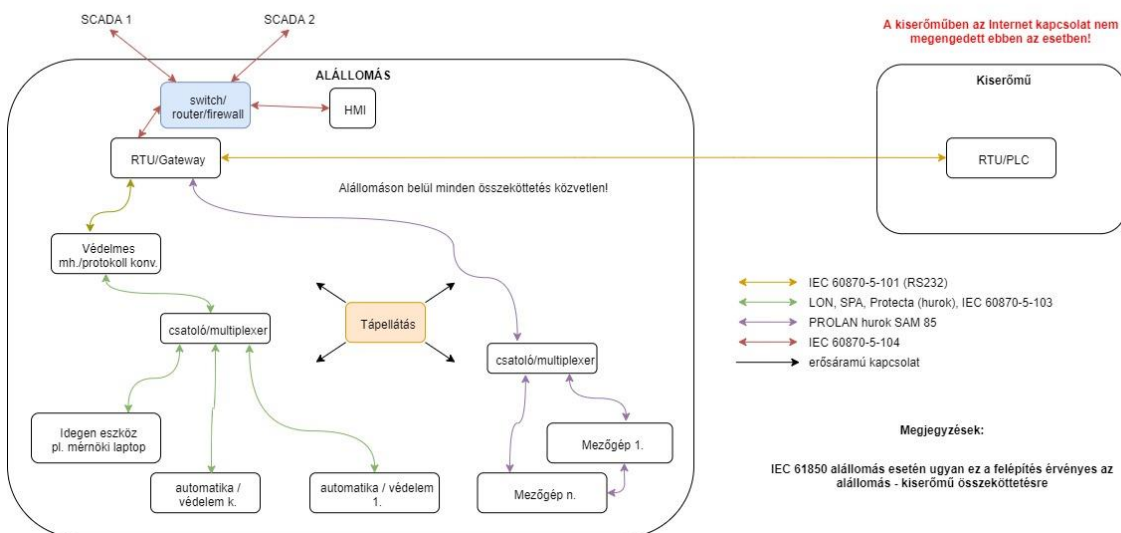
Direkt alállomás - kiserőmű összeköttetés



15.11. ábra: Kiserőmű-alállomás erősáramú kapcsolat

Ha a kapcsolat jelátvitteles (pl. IEC 60870-5-101, IEC 60870-5-104, Modbus stb.) akkor a kiserőműben NEM! megengedett az internet kapcsolat (pl. felhő alapú adatgyűjtés/irányítás) kiépítése (lásd 15.12. ábra).

Direkt alállomás - kiserőmű összeköttetés

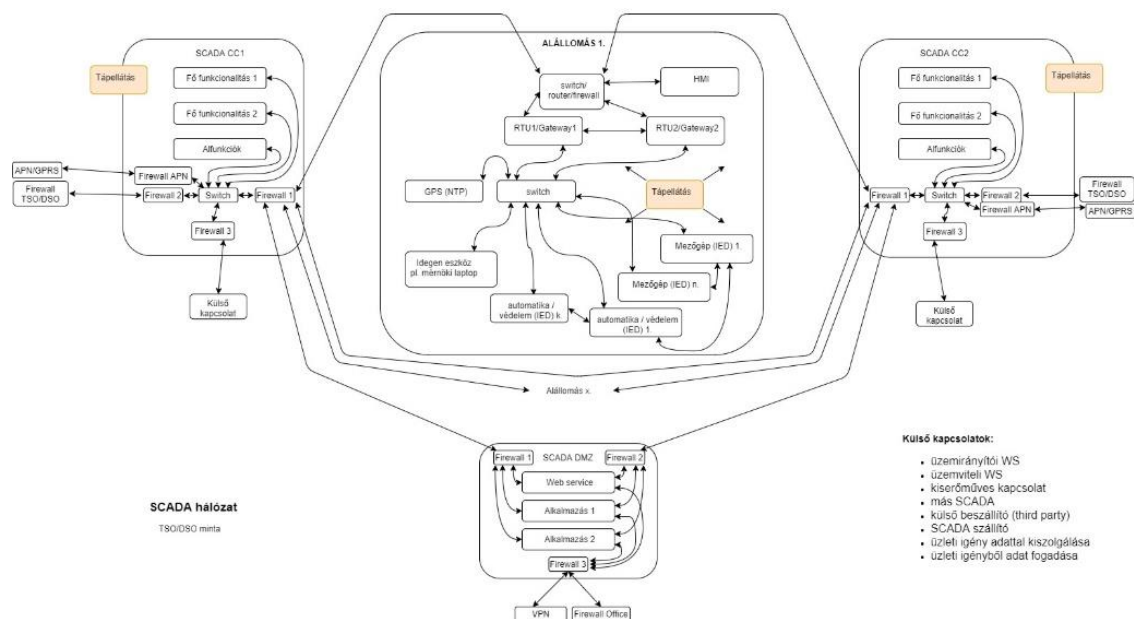


15.12. ábra: Kiserőmű-alállomás jelátvitteles kapcsolat



5. SCADA rendszer felépítése

Annak függvényében, hogy TSO-ban vagy DSO-ban fut egy SCADA rendszer számos azonos mellett más és más funkcióit alkalmazzák mivel eltérő a kiszolgálandó igény. Ennek függvényében a konkrét felépítés eltér(het) a jelen ajánlásban bemutatottól, de törekedni kell arra, hogy a struktúrája (elsősorban a CC/DMZ/külső kapcsolatok) legalább ilyen szinten szeparált és jól elkülöníthetők legyenek, megkerülő átjárások nélkül. A felépítést a 15.13. ábra mutatja.



15.13. ábra: SCADA felépítése

Főbb elemek:

- SCADA CC1...CC2: A megfelelően felépített SCADA rendszerben a core funkciókhoz nincs közvetlen elérés kintről (külső kapcsolatok) csak tűzfalon keresztül. A CC-n belül minden olyan dolog fut, ami közvetlenül az üzemirányításhoz tartozik és az egyéb üzleti folyamatok backend rendszerét tápláló modulok is itt vannak (például aktuális mérések közül a nemzetközi kooperációhoz szükségesek küldésre előkészítése). Megfelelően kialakított rendszerben csak a SCADA CC fér közvetlenül hozzá hálózati elemekhez (láthat nyers méréseket, állapotokat, adhat például kapcsolási utasítást).
- DMZ: a kintről (internetről) is elérhető részek, üzleti folyamatok backend komponensei futnak benne (pl. publikus adatok honlapokra, menetrend feltöltő entitás, külföldi TSO kapcsolat ki/be adatáramlással).



Optimális esetben a DMZ-ből a SCADA CC core funkcióit ellátó szerverek nem érhetők el közvetlenül, hanem a külső kapcsolatot is ellátó üzleti adatigényt feldolgozó szerveren keresztül kaphat adatot.

A SCADA-nak szükséges legalább egy éles és egy teszt/fejlesztői (sőt inkább külön teszt és külön fejlesztői, akár több is!) rendszerrel rendelkeznie. Ezek közül a fejlesztői rendszer egy része vagy egésze kerüljön a DMZ-be.



Irodalomjegyzék

- [1] Rinaldi, S.M. & Peerenboom, James & Kelly, T.K.. (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE. 21. 11 - 25. 10.1109/37.969131.
- [2] Kiss, Á. P. (2019). A hibrid hadviselés természetrajza. Honvédségi Szemle, 2019/4. 17-37.
- [3] Nai-Fovino, I., Neisse, R., Lazari, A. & Ruzzante, G. (2018). European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey. Luxembourg, Publications Office of the European Union, ISBN 978-92-79-92954-0, doi:10.2760/42369, JRC111211.
- [4] Európai Bizottság. „EU-finanszírozás a kutatás és az innováció területén (2021–2027)” https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-research-innovation_hu.pdf (Letöltve: 2020. 08. 26.)
- [5] J. Slowik. „The False Choice of IT Vs. OT.” Dragos. <https://www.dragos.com/blog/industry-news/the-false-choice-of-it-vs-ot/> (Letöltve: 2020. 08. 26.)
- [6] Turcsányi K., Minőségelmélet és -módszertan. Budapest: NKE, 2014.
- [7] L. Obregon. „Secure Architecture for Industrial Control Systems.” SANS Institute. <https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327> (Letöltve: 2020. 08. 26.)
- [8] D. Peterson. „Is The Purdue Model Dead?” <https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/> (Letöltve: 2020. augusztus 26.)
- [9] B. Johnson et. al. „Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure.” Fireye. <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html> (Letöltve: 2020. 08. 26.)
- [10] Dragos. „TRISIS Malware. Analysis of Safety System Targeted Malware.” <https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf> (Letöltve: 2020. 08. 26.)
- [11] D. Greenfield. „Is the Purdue Model Still Relevant?” AutomationWorld. <https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant> (Letöltve: 2020. 08. 26.)
- [12] Dragos. „Building security to achieve engineering and business requirements.” https://www.dragos.com/wp-content/uploads/SecIndSys_Purdue_GEDragos.pdf (Letöltve: 2020. 08. 26.)



- [13] R. Langner. „To Kill a Centrifuge.” The Langner Group. <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf> (Letöltve: 2020. 08. 26.)
- [14] Daavid. „Havex Hunts For ICS/SCADA Systems.” F-Secure. <https://archive.f-secure.com/weblog/archives/00002718.html> (Letöltve: 2020. 08. 26.)
- [15] Symantec. „Dragonfly: Western energy sector targeted by sophisticated attack group”. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks> (Letöltve: 2020. 08. 26.)
- [16] R. M. Lee, M. J. Assante, T. Conway. „Analysis of the Cyber Attack on the Ukrainian Power Grid.” E-ISAC. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (Letöltve: 2020. 08. 26.)
- [17] J. Slowik. „CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack.” Dragos. <https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf> (Letöltve: 2020. 08. 26.)
- [18] R. M. Lee, M. J. Assante, T. Conway. „Analysis of the Malware Reportedly Used in the December 2016 Ukrainian Power System Attack” E-ISAC. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf (Letöltve: 2020. 08. 28.)
- [19] A. Cherepanov, „Win32/Industroyer: a new threat for industrial control systems.” Eset. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf (Letöltve: 2020. 08. 28.)
- [20] Dragos. „CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations” https://www.dragos.com/wp-content/uploads/SecIndSys_Purdue_GEDragos.pdf (Letöltve: 2020. 08. 28.)
- [21] K. Zetter. „The Ukrainian Power Grid Was Hacked Again.” Vice. https://www.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report (Letöltve: 2020. 08. 28.)
- [22] A. Greenberg. „How an Entire Nation Became Russia's Test Lab for Cyberwar.” Wired. <https://www.wired.com/story/russian-hackers-attack-ukraine/> (Letöltve: 2020. 08. 28.)
- [23] M. Moyer. „Expert: A Virus Caused the Blackout of 2003. Will the Next One Be Intentional?” Scientific American. <https://blogs.scientificamerican.com/observations/expert-a-virus-caused-the-blackout-of-2003-will-the-next-one-be-intentional/> (Letöltve: 2020. 08. 28.)
- [24] G. Burke, J. Fahey. „AP Investigation: U.S. power grid vulnerable to foreign hacks.” Las Vegas Sun. <https://lasvegassun.com/news/2015/dec/21/ap-investigation-us-power-grid-vulnerable-to-forei/> (Letöltve: 2020. 08. 28.)



- [25] T. Staff. „Steinitz: Israel’s Electric Authority hit by ‘severe’ cyber-attack.” The Times of Israel. <https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/> (Letöltve: 2020. 08. 28.)
- [26] P. Paganini. „Malware based attack hit Japanese Monju Nuclear Power Plant.” Security Affairs. <http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html> (Letöltve: 2020. 08. 28.)
- [27] P. Paganini. „Nuclear plant in South Korea hacked.” Security Affairs. <http://securityaffairs.co/wordpress/31416/cyber-warfare-2/nuclear-plant-south-korea-hacked.html> (Letöltve: 2020. 08. 28.)
- [28] P. Paganini. „Virus discovered at the Gundremmingen nuclear plant in Germany” Security Affairs. <https://securityaffairs.co/wordpress/46708/security/virus-gundremmingen-nuclear-plant.html> (Letöltve: 2020. 08. 28.)
- [29] A. Shalal. „IAEA chief: Nuclear power plant was disrupted by cyber attack.” Reuters. <https://in.reuters.com/article/nuclear-cyber-idINKCN12A1P1> (Letöltve: 2020. 08. 28.)
- [30] C. McMahon. „Exclusive: EirGrid targeted by ‘state sponsored’ hackers leaving networks exposed to ‘devious attack’.” Independent.ie. <https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html> (Letöltve: 2020. 08. 28.)
- [31] B. Sobczak. „Report reveals play-by-play of first U.S. grid cyberattack.” E&E News. <https://www.eenews.net/stories/1061111289>. (Letöltve: 2020. 08. 28.)
- [32] World Energy Council. „Cyber challenges to the energy transition.” https://www.worldenergy.org/assets/downloads/Cyber_Challenges_to_the_Energy_Transition_WEC MMC 2019.pdf (Letöltve: 2020. 08. 28.)
- [33] D. R. Hayes, „Using Open Source Intelligence for Risk Assessment to the U.S. Power Grid” presented at the 15th International Conference e-Society 2017, Budapest, Hungary, Apr. 10–12, 2017.
- [34] D. E. Whitehead, K. Owens, D.s Gammel, J. Smith. „Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies.” presented at the Power and Energy Automation Conference, Spokane, WA, USA, March 21-23, 2017
- [35] The Recorded Future Team. „What Is Open Source Intelligence and How Is it Used?”. <https://www.recordedfuture.com/open-source-intelligence-definition/> (Letöltve: 2020. 08. 28.)



- [36] J. Elder. „Open Source Intelligence (OSINT) for OT: What adversaries can learn about your organisation and what you can do.” Applied Risk. <https://applied-risk.com/resources/osint> (Letöltve: 2020. 08. 28.)
- [37] Dragos. „Energy Organizations Continue to be Compromised Globally.” <https://www.dragos.com/blog/industry-news/energy-organizations-continue-to-be-compromised-globally/> (Letöltve: 2020. 08. 28.)
- [38] Danish Ministry of Defence. „New sectoral strategies to prepare society for cyber attacks.” <https://www.fmn.dk/eng/news/Pages/New-sectoral-strategie-stop-repare-society-for-cyberattacks.aspx> (Letöltve: 2020. 08. 28.)
- [39] White House. „Executive Order on Securing the United States Bulk-Power System.” <https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/> (Letöltve: 2020. 08. 28.)
- [40] S. Varghese. „US seized Chinese-built transformer – but nobody knows why.” IT Wire. <https://www.itwire.com/government-tech-policy/us-seized-chinese-built-transformer-%E2%80%93-but-nobody-knows-why.html> (Letöltve: 2020. 08. 30.)
- [41] J. Weiss. „ICS cyber security is the second coming of the Maginot Line – and the Chinese have breached it.” EnergyCentral. <https://energycentral.com/c/ics-cyber-security-second-coming-maginot-line-%E2%80%93-and-chinese-have-breached-it> (Letöltve: 2020. 08. 30.)
- [42] J. Weiss. „An Assessment of Presidential Executive Order 13920 – Securing the United States Bulk-Power System.” Control Global. <https://www.controlglobal.com/blogs/unfettered/an-assessment-of-presidential-executive-order-13920-securing-the-united-states-bulk-power-system/> (Letöltve: 2020. 08. 30.)
- [43] J. Weiss. „Emergency Executive Order 13920 – Response to a real nation-state cyberattack against the US grid.” Control Global. <https://www.controlglobal.com/blogs/unfettered/emergency-executive-order-13920-response-to-a-real-nation-state-cyberattack-against-the-us-grid/> (Letöltve: 2020. 08. 30.)
- [44] A. King. „Senate Passes King Bill Protecting Energy Grid from Cyber-Attacks.” U.S. Senate. <https://www.king.senate.gov/newsroom/press-releases/senate-passes-king-bill-protecting-energy-grid-from-cyber-attacks> (Letöltve: 2020. 08. 30.)
- [45] Energy Central Community. „FERC versus NERC.” Energy Central. <https://energycentral.com/c/ferc-versus-nerc> (Letöltve: 2020. 08. 30.)



Felelős kiadó:

Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet
Budapest

Szerkesztette:

Dr. Bonnyai Tünde
Görgey Péter
Dr. Krasznay Csaba

ISBN 978-615-00-9827-2





SeConSys

Security for Control Systems



NEMZETI
KIBERVÉDELMI INTÉZET