Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve 2022

NEMZETI KIBERVÉDELMI INTÉZET

Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve

2022

A 2019. decemberében kiadott, a 2021. évi történések alapján aktualizált kézikönyv aktualizálása a 2022. évi történesek alapján

(2023. január)

ISBN 978-615-82042-3-1

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), Bocsok Viktor (3. fejezet, 3., 8. melléklet), Bogáncs Tamás János (Fogalmak, rövidítések), Dr. Bonnyai Tünde (4., 5. fejezet, Fogalmak, rövidítések, 8., 9. melléklet), Dr. Buttyán Levente (5., 6. fejezet, 3. melléklet), Dr. Csatár János (6., 7. fejezet, 15., 16. melléklet), Dr. Danyek Miklós (6., 7. fejezet, 15. melléklet), Deák Veronika (5. fejezet), Faragó János (16. melléklet), Görgey Péter (1., 2., 4., 5., 7. fejezet, Fogalmak, rövidítések, 1., 2., 5., 7., 16. melléklet), Gyebnár Gergő (6. fejezet, 14. melléklet), Illés Gábor (6. fejezet), Kocsis Tamás (16. melléklet), Dr. Krasznay Csaba (1., 2., 5. fejezet, Fogalmak, rövidítések, Irodalomjegyzék), Molnár Ferenc (10., 13. melléklet), Ölvegyi Roland (4. fejezet, 9. melléklet), Pfeiffer Szilárd (7. fejezet, Fogalmak, rövidítések), Pongrácz Péter (3., 4., 7. fejezet, 1. melléklet), Winter Gábor, Sípos Róbert (Fogalmak, rövidítések), Szabó-Nyakas Zsolt Csaba (5. fejezet), Szádeczky Tamás (13. melléklet), Szent-Királyi Balázs (9. melléklet), Winter Gábor (Fogalmak, rövidítések), Zámbó Marcell (16. melléklet)

Munkacsoport vezetők:

Dr. Bonnyai Tünde, majd Baranya Zsolt, majd Arató György

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:

BM Országos Katasztrófavédelmi Főigazgatóság

BME-VET

E.ON Hungária Zrt.

Magyar Energetikai és Közmű-szabályozási Hivatal

MAVIR ZRt.

MVM Zrt.

Paks II. Zrt.

Prolan Irányítástechnikai Zrt.

Szakmai támogatók és pártoló tagok

ACPM IT Tanácsadó Kft.

Alverad Technology Focus Kft.

Black Cell Kft.

CCLab Kft.

Com-Forth Ipari Informatikai Kft.

CrySyS Lab

INFOWARE Vállalkozási és Kereskedelmi Zrt.

Prolan Innolab Ipari Informatikai Kft.

Prolan Power Zrt.

Protecta Elektronikai Kft.

Cyber Services 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 amértékben az informatikai rendszerekre támaszkodnak. A 2000-es évek elején lezajlott információtechnológiai fejlődés által azonban olyan szintre emelkedett az infokommunikáció biztosította 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 világhálóhoz.

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.

Különösen indokolt ez manapság, amikor a COVID, majd a háború, az energiaválság, az aszály megtépázta az ellátási láncokat, közte az energiahordozókét. A villamosenergia-rendszer rezilienciája csökkent, a teljes ökoszisztéma sérülékenyebbé vált, akár a kibertámadásokkal szemben is.

Mindez nemcsak Magyarországon, hanem egész Európában jelentős kihívások elé állítja a villamosenergia-szolgáltatókat. Elkerülhetetlen a szorosabb együttműködés.

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.

A kézikönyv immár második alkalommal frissül egy-egy újabb év történéseivel aktualizálva.

Örömömre szolgál, hogy a Nemzeti Kibervédelmi Intézet nem csak részese ennek az európai szinten is unikálisnak számító együttműködésnek, de immár harmadik alkalommal kiadója lehet a Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyvének.

Szabó Lajos
Nemzeti Kibervédelmi Intézet

A 2022. évi kiadás újdonságai

A Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyvének 1. kiadása 2020 decemberében jelent meg, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet ajánlásával. Az online kiadás előnyével élve már a publikálás időpontjában is az volt a szerzők határozott szándéka, hogy a könyv tartósan betölthesse szakmai kézikönyv funkcióját, azaz időről-időre frissítve megjelenhessenek benne az előző kiadás óta eltelt idő témába vágó fejleményei.

Ennek jegyében került sor kézikönyv aktualizálására a 2021. évi események alapján is.

A 2022. évi eseményeket is tükrözni hivatott jelenlegi kiadás lényeges új elemei a 2021. évihez képest:

- A fenyegetettségi térkép aktualizálása (3.2. pont, 3. melléklet)
- A Zero Trust biztonsági modell bemutatása (új 7.4. pont)
- Az incidenslista aktualizálása (1. melléklet),
- az IT, OT, ICS jellemzők, egyezések, specifikumok, bemutatása, fogalmi tisztázása (a 16. mellékletben),
- Javaslat a képzési rendszer fejlesztésére (16. melléklet)
- Fogalmi pontosítások (Energetikai, informatikai és kiberbiztonsági fogalmak, rövidítések jegyzéke)
- Jogszabály változás átvezetése

Az előző kiadáshoz képest lényegesen megváltozott, avagy újként bekerült szövegeket zöld szín jelöli.

A szerzők az info@seconsys.eu címen szívesen fogadják a kézikönyv további fejlesztésére vonatkozó javaslatokat.


351
639
419
ROMÁNIA
208
350
32
94
Rendszerterhelés : 5705 M
Termelés : 5067 M
Import-export szaldó
Terv : 603 M
Tény : 628 M
Eltérés pill : 31 M
Eltérés átlag : 4 M

Tartalom

Lezárva: 2022. január

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 (ICS[1]) esetében sem lehet abban bízni, hogy ezek speciális jellege érdemben akadályozhatná a támadót. Sőt a történtek 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[2]-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 (stakeholdereknek) 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 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 üzemzavarukkal a legnagyobb zavarokat, károkat okozó – elemeiben (erőműveiben, alállomásiban stb.) üzemelő ICS/SCADA-kra fókuszál.

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.

[1] ICS: Industrial Control System. A hazai gyakorlatban elterjedt megnevezésre tekintettel a továbbiakban ICS/SCADA néven említjük.
[2] SCADA: Supervisory Control and Data Acquisition (Felügyeleti irányítás és adatgyűjtés)

A kézikönyv jelenlegi változata a jelen állapot tükrében szakértői szinten optimálisnak tartott ajánlásokat tartalmazza. Ugyanakkor az új fejlemények, támadások ismeretében folyamatosan tovább zajlik a történtek szakértői értékelése és a kézikönyv elektronikusan elérhető változatának szükség szerinti finomítása. A kézikönyv elektronikusan 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 függőségek[3] [1] nyomán előbb-utóbb szükségképpen egyre súlyosabb zavart okoz például 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".[4]

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.

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, képviseltetik magukat, illetve fejezik ki egyetértésüket (2022. decemberi állapot).

[3] 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.

[4] A magyar szabályozások „létfontosságú rendszer", a nemzetközi szakmai terminológia „kritikus infrastruktúra" megnevezést használ, de a kettő szinonimája egymásnak.

1. ábra: A SeConSys együttműködés résztvevői (2022. decemberi 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 Közszolgálati 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 például a jelen kézikönyv – létrejöttét.

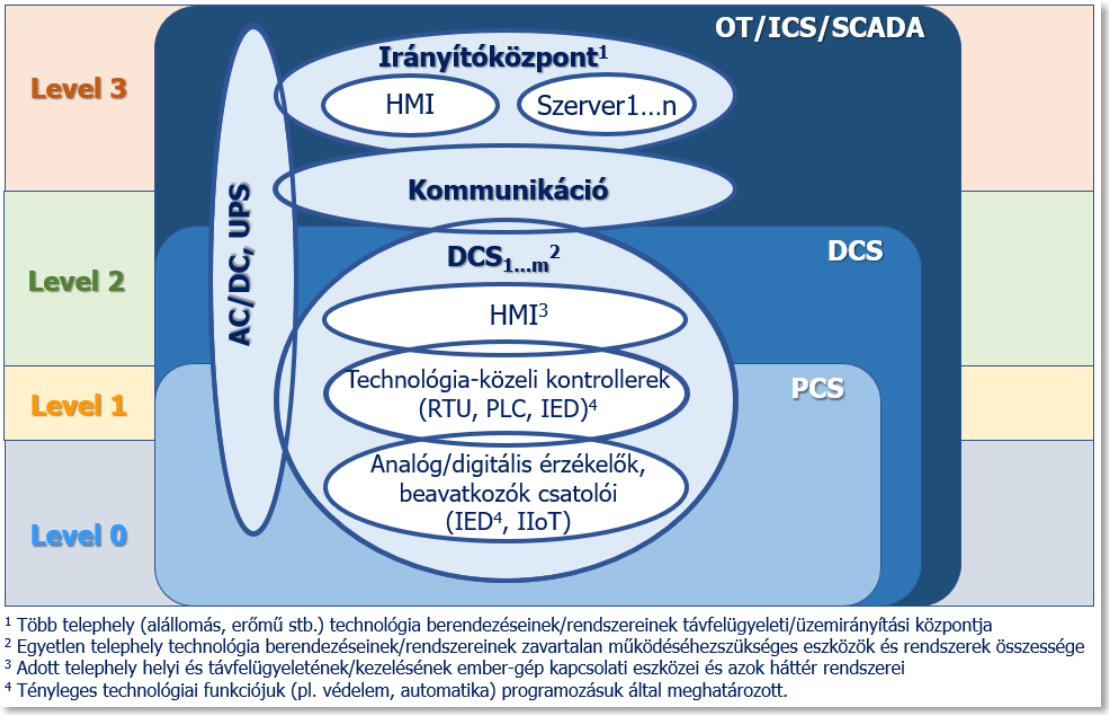
A SeConSys követendő jó gyakorlatnak tekinti az EE-ISAC céljait és működési kereteit.

Működési hangsúlyait és értékeit 2. ábra szerint fogalmazza meg.

2. ábra: A SeConSys működési hangsúlyai és értékei

2.4. Alkalmazott fogalmak

Az OT[5], ICS fogalomkörben gyakran eltérő fogalmak és fogalmi viszonyok jelennek meg. Az egyértelműség érdekében a 3. ábra mutatja be a kézikönyvben alkalmazott alapfogalmakat



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

[5] OT: Operational Technology (Operatív/üzemeltetési technológia)

Az ábrán alkalmazott fogalmak jelentése megtalálható a kézikönyv Energetikai, informatikai és kiberbiztonsági fogalmak, rövidítések jegyzékében.

Az ábra szerinti színes sávok a 7.1. pontban részleteiben tárgyalt Purdue modell szintjeit jelenítik meg.

A SeConSys fogalmi értelmezése egyetlen esetben tér el a nemzetközi gyakorlatban jellemzően alkalmazottól: az egyen- és váltakozóáramú, valamint a szünetmentes energiaellátás (rövid jelöléssel: AC/DC, UPS) tekintetében. A nemzetközi gyakorlat ezeket nem tekinti az OT/ICS szerves részének. Ugyanakkor a SeConsys megközelítése szerint e rendszerek:

- integritása kulcsfontosságú az összes többi rendszer működése szempontjából,
- sikeres támadása szélesebb körű, ezért súlyosabb hatású lehet, mint valamely OT/ICS komponens önmagában történő támadása,
- digitális rendszerek (pl. erre specifikusan felparaméterezett IED[6]-k, monitoring rendszerek) által felügyeltek (akár távolról is), vezéreltek[7], azaz potenciális támadásnak kitettek – hasonlóan az összes többi OT/ICS komponenshez.

Mivel a fentiek szerint az AC/DC, UPS komponensek sikeres kiejtése többnyire számos – ha nem az összes! – OT/ICS komponens kiesésével járhat (szemben az egyéb komponenseknek a többire gyakorolt, jórészt korlátozott működési hatásaival), ezért a SeConSys fogalmi értelmezése szerint az AC/DC, UPS komponenseket is indokolt az ICS/OT fogalomkör részének tekinteni.

[6] IED: Intelligent Electronic Device (Intelligens elektronikus eszköz)
[7] Mivel ezek távolról menedzselhető eszközök, ezért egy támadó ezeket távolról le is kapcsolhatja. Viszont a tápellátás támadói kiejtése előbb-utóbb az összes többi ICS komponens kiesését is okozza.

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, például 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. Bővebben lásd az 5.2.3. pontban.

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 megfelelve 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 kellene érvényesíteni a teljes villamosenergia-rendszerre. Ha ezt a kérdést onnan vizsgáljuk, hogy ugyanannak a biztonsági szintnek kell-e érvényesülnie egy háztartási méretű kiserőmű vagy egy hagyományos (fosszilis tüzelésű), több száz MW beépített teljesítményű alaperőmű esetében, egyértelmű a válasz: nem. Ezeknél 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 kiberfenyegetettségnek – való kitettségét. A következő időszak egyik – ha nem a – legfontosabb feladata a villamosenergia-szektorban ezeknek a kockázatoknak és kitettségnek csökkentése

3.2. Fenyegetettségi térkép

Jelen fejezet a villamosenergia alágazatot, annak rendszereire és rendszerelemeire 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 rendszerelemeinek sérülékenységei jelentős 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 protokollokban egyaránt előfordulhatnak. A *szervezet működési- és munkafolyamataiban* található sérülékenységek olyan eljárási hibák, amelyek kihasználása elősegítheti a fizikai és logikai támadások kivitelezését (pl. jogosultsági szintek indokolatlan engedélyezése, túlzott alvállalkozói függés stb.). A *humánerőforrás sérülékenysége* (pl. a biztonságtudatosság hiánya) ugyancsak megkönnyítheti a rendszer elleni fizikai és logikai támadások kivitelezését. A rendszerek és szervezetek felépítése egyre komplexebb, ami növeli a hibalehetőséget, a sérülékenységek létezésével folyamatosan számolni kell. A sérülékenységek jelenléte annak is köszönhető, hogy a rendszereket emberek tervezik és implementálják, általában szoros határidők és limitált költségvetés mellett. Valamennyi sérülékenység azonosítása és kijavítása lehetetlen, de folyamatosan törekedni kell az azonosításukra, az ismert sérülékenységekkel kapcsolatos kockázatok felmérésére, arányos csökkentésére. A sérülékenységek két fő osztályra, publikusan ismert és zero-day sérülékenységekre[8] bonthatók. A publikusan ismert sérülékenységekkel kapcsolatos információk a támadók számára is elérhetők.

Ha a javítás a gyártó érdekkörébe tartozik, az üzemeltető a javításig ki van téve a sérülékenység kihasználásából eredő veszélynek, ipari létesítmények esetében ugyanakkor

[8] zero-day sérülékenység: még nem javított és nem publikált sérülékenység

azzal is számolni kell, hogy az üzemeltető szándékosan nem javít egy hibát, mivel az 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, amelyeket (elsősorban célzott támadások során) nagy valószínűséggel sikeresen és többnyire észrevétlenül használhatnak ki.

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 resistant[9]), akkor a hozzáférés a tárolt adatok kiolvasásához, az eszközön futó programok módosításához vezethet. Emellett a 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 a rendszerkapcsolatokat 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 meglevő, a távoli hozzáférés lehetőségét biztosító funkciókat aktiváló kódot, majd ennek segítségével újabb és komplexebb modulokat (privilégium növelés, perzisztencia[10] 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, kliens programokba vagy az operációs rendszerbe is beépülhetnek. A távoli vezérléshez szükséges kommunikáció általában rejtjelezett és fedő forgalomba ágyazott, melyet a tűzfalak

[9] tamper resistant: jogosulatlan fizikai hozzáférés ellen védett eszköz
[10] perzisztencia: tartós fennmaradás, túlélés

átengednek. A kódnak önálló terjedést megvalósító funkciói is lehetnek, de gyakorta használt disztribúciós módszerek az e-mail, a drive-by-download[11] vagy watering hole[12], esetleg fertőzött adathordozó is. A kód által megvalósított funkciók és a kód minősége a támadó technikai tudásától és anyagi erőforrásaitól függ. Kártékony programokkal PLC-ket[13] és RTU-kat[14] 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 is számos kriptográfiai sérülékenység és támadás ismert, bár jellemzően egyszerűbb az algoritmust futtató számítógép, beágyazott eszköz kompromittálása, mint az algoritmus feltörése. Ugyanakkor mélyebb tudással rendelkező támadók esetében a lehetőséget sem lehet kizárni.[15]

Protokoll és API[16] 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 előállítása. 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.

---

[11] drive-by-download: letöltés általi támadás
[12] watering hole: gyakran látogatott weboldalak támadása
[13] PLC: Programmable Logic Controller (programozható logikai vezérlő)
[14] RTU: Remote Terminal Unit (telemechanikai alközpont)
[15] Számos gyenge kriptográfiai algoritmus használatos még az OT-n kívül is, míg az OT területén félő, hogy még nagyobb az arány a frissítések hiánya miatt.
- Algoritmusok esetén következők említhetőek: protokoll: SSL2, SSL3, TLS 1.0, TLS 1.1 protocol downgrade; symmetric cipher: RC2, RC4, DES; hash: MD5, SHA-1; key exchange: Diffie-Hellmann <1024 bit/unsafe prime, anonymous Diffie-Hellman; public key: RSA <=512 bit, DSA >= 512 bit
- Implementációk esetén a következők említhetőek: Heartbleed; ROBOT; POODLE attackok; DROWN; ...

[16] API: Application Programming Interface (alkalmazásprogramozási interfész/felület)

Social engineering[17]*, phishing, OSINT*[18]*:* a technikai jellegű támadások mellett a humán felhasználók ellen irányuló támadások is hatékonyak. Sokan a felhasználókra úgy tekintenek, mint az rendszerek biztonságának leggyengébb láncszemeire. Ez atekintetben 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-mailt 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 (bővebben lásd 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 információ-lopás, illetéktelen felhasználás és a 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 kiddie[19]:
- Belső munkatárs/beszállító, szerződéses partner
- Hacktivista csoportok
- Terrorszervezetek
- Kiberbűnözők
- Államilag támogatott támadó csoportok

A részletes fenyegetettségi térképet a 3. melléklet tartalmazza.

[17] social engineering: a pszichológiai befolyásolás, félrevezetés és megtévesztés módszere
[18] OSINT: Open Source Intelligence (nyílt forrású információszerzés)
[19] Script kiddie: komoly szaktudással nem rendelkező kezdő hacker

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 (COTS[20]), 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 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 azokat 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 azokat, 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).[21]

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

[20] COTS: Commercial off-the-shelf (kereskedelmi forgalomban kapható, ún. „dobozos" szoftverek és hardverek)
[21] https://www.youtube.com/watch?v=LM8kLaJ2NDU

folyamat megzavarása, tönkretétele volt. Amikor 2010 nyarán a világ tudomást szerzett a Stuxnetről, 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 weboldalairól letölthető telepítő fájlokat.

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 vesztették el a távfelügyelet lehetőségét. A 15:30 és 16:10 közötti időszakban a három üzemirányító központ HMI-jeiről[22] – kezelői beavatkozás nélkül – megszakító kikapcsolási parancsok kerültek kiadásra. Az ukrán hivatalos szervek és később az események elemzését végző szakértők által egyaránt orosz titkosszolgálatokhoz kapcsolható APT[23] 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,

[22] HMI: Human Machine Interfész (ember-gép kapcsolati felület)

[23] 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.)

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 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 fenyegetések[24] vagy támadások több összetevőből épülnek fel. Ilyenek például 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 helyzetet[25]. A folyamatos áramszolgáltatás kiesése esetén valamennyi további ágazat és alágazat szereplőjének folyamatos, elvárt szintű működése válik bizonytalanná. A hibrid fenyegetések alapvető célkitűzése a villamosenergia

[24] 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.

[25] 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.

elérhetetlenné tétele, amely által rombolják a társadalom államigazgatás iránti bizalmát, gyengítve ezzel az ellenálló képesség[26] mértékét.

A támadási faktorok számbavétele során – az előző fejezetben már említett ukrajnai 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 Blokád" – távvezetékoszlopok lerombolása), illetve humán és logikai faktorok sérülékenységeinek, valamint a meglévő eljárásrendek hiányosságainak kiaknázása is. Az ukrajnai 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).

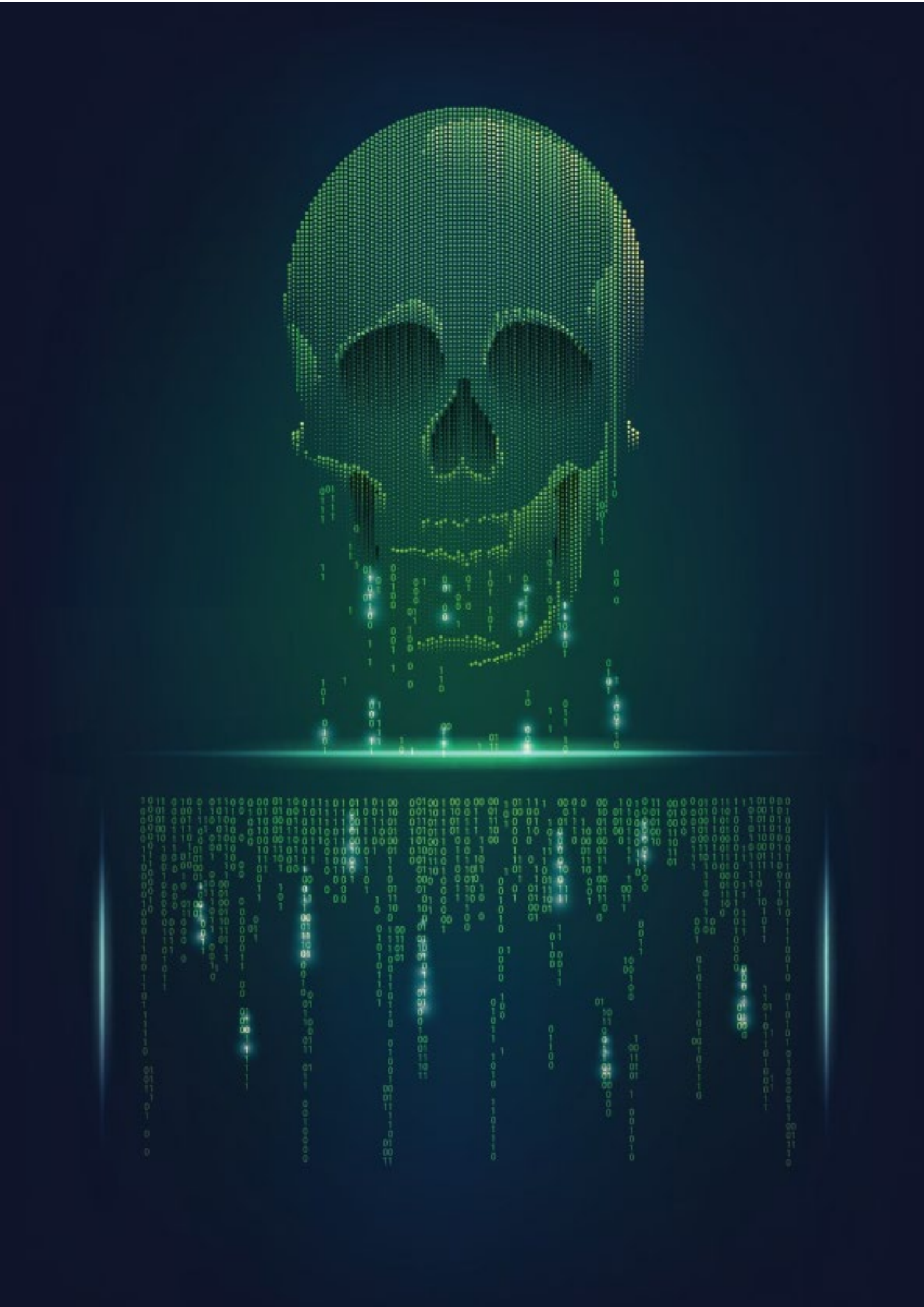
Éppen ezért a hibrid fenyegetésekre való felkészülés során fontos a komplex, átfogó megközelítés alkalmazása, amelyre jó alapul szolgálhat egy részletes kockázatelemzés kidolgozása, valamennyi kockázati tényező beemelésével, nagymértékben építve a már megtörtént támadások tanulságaira.

Érdemes megjegyezni, hogy a MAVIR Zrt., mint TSO által üzemeltetett átviteli hálózat összeköttetésben van más nemzetek rendszereivel. Az ENTSO-E[27] 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 – hangsúllyal villamosenergia alágazat – üzemeltetők közötti rendszeres, kölcsönös és érdemi információmegosztás.

[26] Angol terminológiával: resilience

[27] 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

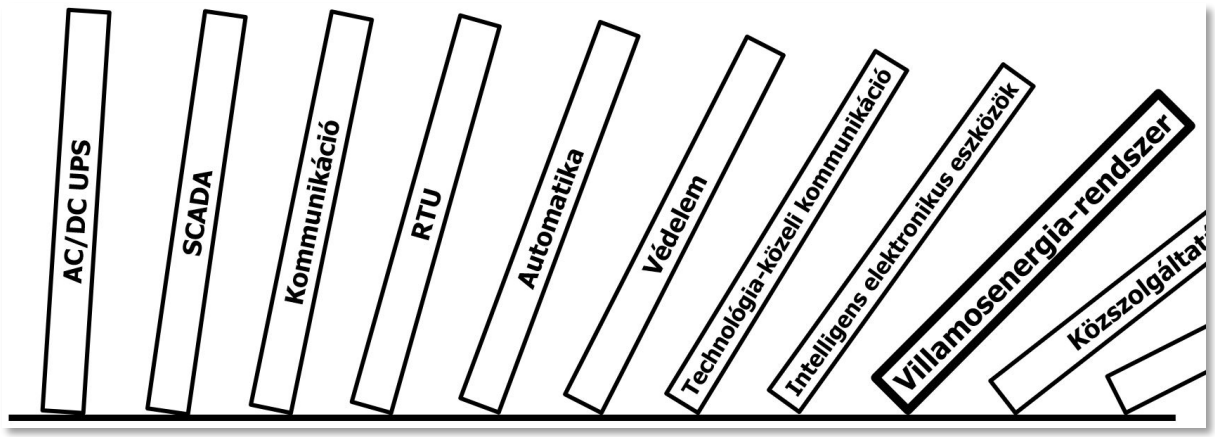
A folyamatos villamosenergia-ellátás egy egyensúlyi feladvány. Alapja, hogy a mindenkori villamosenergia-termelésének és -fogyasztásnak minden időpillanatban egyensúlyban kell lennie. A termelési, átviteli és elosztási folyamatokat, az azokat megvalósító, százezer-milliárd forintos nagyságrendű energetikai 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 (IED[28]) vannak közvetlen kapcsolatban. Ezek között, valamint a felsőbb szintekkel a technológia-közeli 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.

[28] IED: Intelligent Electronic Device (intelligens elektronikus eszköz)



4. ábra: Lehetséges dominó effektus a villamosenergia-rendszerben

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 patchelési rendszerének kidolgozására és működtetésére. Márpedig ennek tartós hiánya az ICS/SCADA-komponensek akár 10 évet is meghaladó élettartamára előre vetítheti azok ismert, de kijavítatlan 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 nagy kapacitású 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 gridek[29] tömegessé válása, annak fejlettebb változataként a microgridek 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.

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


ROMÁNIA
157
179
Fogyasztás : 5076 MW
Termelés : 4276 MW
Import terv : 821 MW
–"– tény : 793 MW
Eltérés pill. : –20 MW
–"– átlag : 9 MWh/h
416
133
411
132
ZERJ–1
116
70
ZERJ–2
120
77
414
135
132
0
0

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 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.

Vélhetően stratégiai hatása lesz az USA IT (de egyre növekvő számban OT) rendszereit (közte kritikus infrastrukturáit) érő, vagy érintő támadásoknak, azokon belül a zsarolóvírusos (pl. Colonial Pipeline), ill. ellátási láncon keresztüli (pl. SolarWinds/Orion) támadásoknak. Az elmúlt

néhány évben az USA-t ért és (villamos)energetikai szempontból releváns kiberfenyegetéseket. ill. -támadásokat 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 mindenkori célirányos szabályozási és finanszírozási környezetre vonatkozó elemzések végzését, döntés-előkészítő 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 döntés-előkészítők 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.

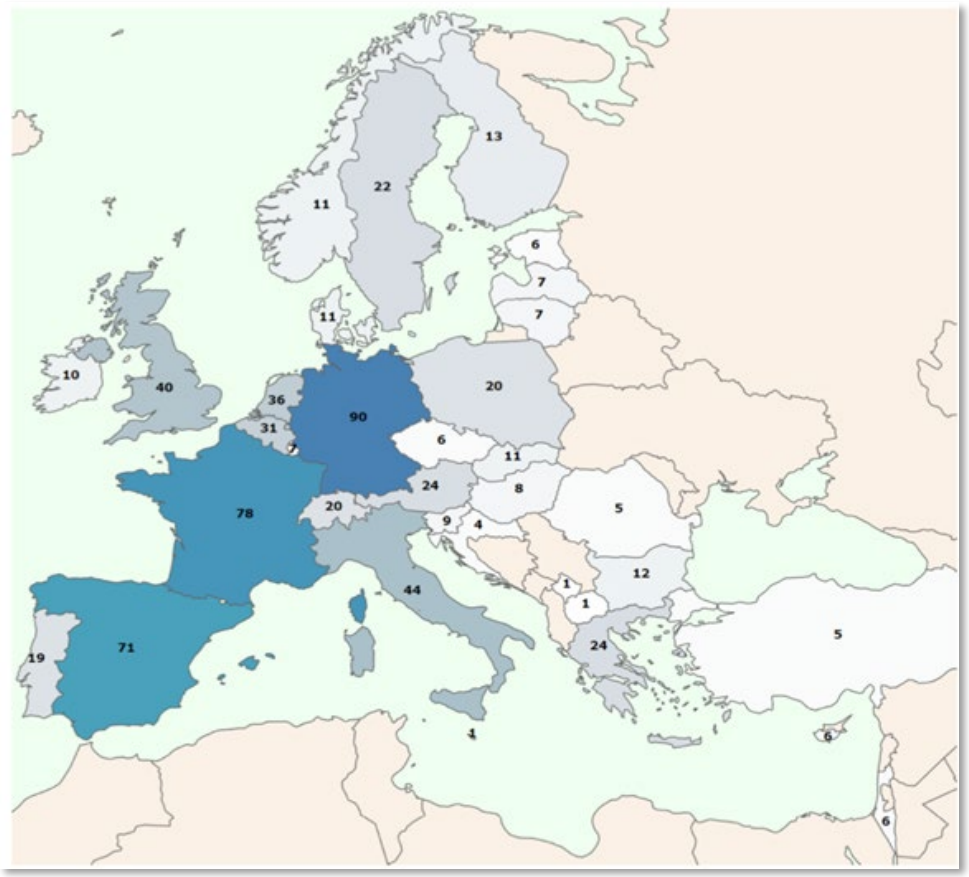
5.2.1. Kiberbiztonsági kutatás-fejlesztés

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 következésképpen 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

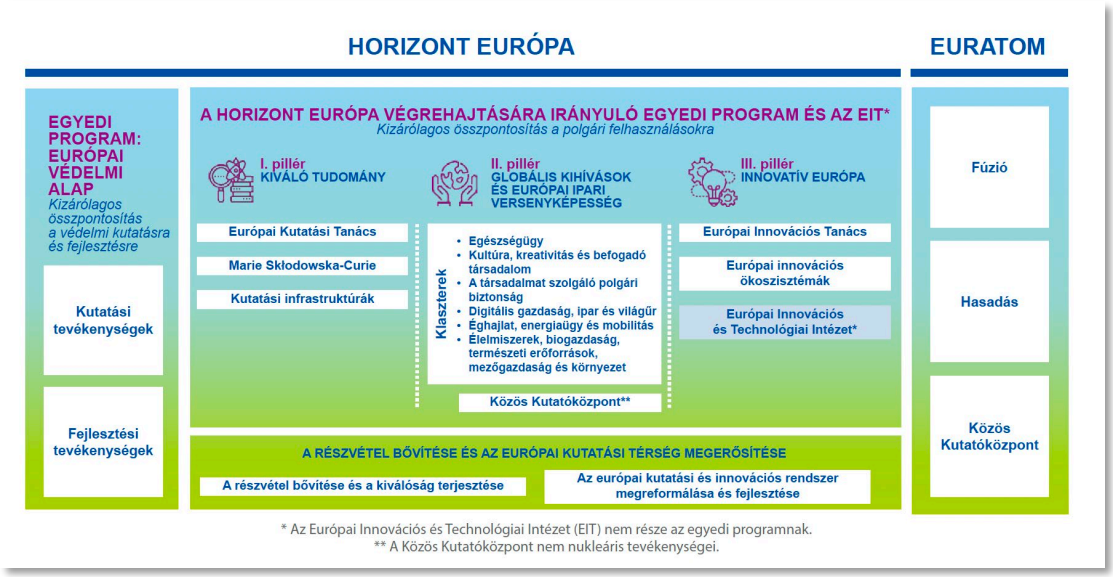
például Németországban, Franciaországban vagy éppen Spanyolországban meglehetősen sok olyan intézmény van, ahol kiberbiztonsági kutatás-fejlesztés-innovációval foglalkoznak, Kelet-Közép-Európában, így Magyarországon is ezen intézmények száma alacsony, ahogy az 5. ábrán is megjelenik. Ez azt is jelenti, 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.



5. ábra: Európai kiberbiztonsági kutatóközpontok

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. Érthető, hogy az európai digitális szuverenitás megteremtése az Európai Bizottság egyik legfontosabb programpontja.

Az Európai Bizottság döntése alapján mind a Horizon Europe, mind a Digital Europe kutatási programban kiemelt szerepet kap a kiberbiztonság. Előbbiben három pillérre épül a kutatás-fejlesztés-innováció támogatása, ebből az első pillér a tudományos kiválóságról, a második pillér a globális kihívásokról és az európai ipar versenyképességéről, míg a harmadik pillér az innovatív Európáról szól. Ezt ábrázolja az 6. 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 96,899 milliárd euró összeg áll majd rendelkezésre a kutatás-fejlesztés-innovációra, ezen belül a Globális kihívások és az európai ipar versenyképessége pillér 53,516 milliárd euróra számíthat. Tovább bontva, A társadalmat szolgáló polgári biztonság klaszterben szerepel a kiberbiztonság, amely 1,596 milliárd euróval fog részesülni ebből a hatalmas összegből.[30]



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

Magyarország természetesen aktívan követi az Európai Unió innovációs törekvéseit. Ezt támasztja alá az, hogy a 2021-ben kiadott K+F+I stratégiai dokumentumok is kivétel nélkül foglalkoznak ezzel a szakterülettel. A fő stratégiai dokumentum a Magyarország kutatási, fejlesztési és innovációs stratégiájának (2021-2030) elfogadásáról szóló 145/2021. (VII. 13.) Korm. határozat alapján létrehozott stratégia. A részleteket az 1428/2021. (VII. 2.) Korm. határozat a 2021–2027. évekre vonatkozó Nemzeti Intelligens Szakosodási Stratégia (S3) elfogadásáról alapján megalkotott S3 stratégia segít megérteni. Ebben a kiberbiztonsággal is foglalkozó Gazdaság digitalizációja prioritás céljait az alábbiak szerint fogalmazzák meg: „A

[30] Európai Bizottság 2018

XXI. századra fokozottan jellemző digitalizáció és robotizáció korában a kiber- és egyéb biztonsági kihívásokra tekintettel, az S3-hoz kapcsolódóan megvalósított fejlesztések során a hazai szellemi tulajdon védelmi, adatvédelmi és nemzetbiztonsági követelményeket, illetve a nemzeti ellenállóképesség és a (védelmi ipar esetén) a kettős hasznosíthatóság egységes szempontjait az érintetteknek maradéktalanul érvényre kell juttatni." A kiberbiztonság, mint fejlesztési terület egyébként 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 akadálya, 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 kiberbizonsági tudatosságával kapcsolatos kihívások indokolttá 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.

a) 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 széles körű alapszintű ismeretek elsajátítása a cél, amely a munkaerőpiacon hasznosítható szakmai ismereteket és megfelelő elméleti alapozást nyújt az adott szakterületen a tanulmányok mesterképzésben történő folytatásához.

Kiberbiztonsághoz kapcsolódó hazai alapképzések:

a) Nemzeti Közszolgálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány (NKE KNY)[31]

b) Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció (ÓE BM)[32]

4.6.2.1. Mesterképzési szakok

A mesterképzés, amelyen MA (Master of Arts), illetve MSc (Master of Sciences) fokozat és szakképzettség szerezhető. Mesterképzésre az jelentkezhet, aki legalább egy alapképzési diplomával vagy a korábbi képzési rendszer szerinti főiskolai/egyetemi diplomával rendelkezik,

[31] Felvi.hu szakleírások: Nemzeti Közszolgálati Egyetem - Bűnügyi alapképzési szak - Kiber nyomozó szakirány, https://www.felvi.hu/felveteli/egyetemek_foiskolak/!IntezmenyiOldalak/meghirdetes.php?meg_id=20905&elj=20a.

[32] Felvi.hu szakleírások: Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció, https://www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/36/szakleiras.

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 munkaerőpiacra, illetve jelentkezni lehet a képzési rendszer harmadik lépcsőfokát jelentő doktori képzésre, amely a tudományos fokozat megszerzésére készít fel.[33]

Kiberbiztonsághoz kapcsolódó hazai mesterképzések:

b) Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés (NKE KB)[34]

c) Nemzeti Közszolgálati Egyetem – Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány (NKE VIKR)[35]

d) Budapesti Műszaki és Gazdaságtudományi Egyetem – Mérnök-informatikus mesterképzés, IT biztonság mellékspecializáció

4.6.2.2. Szakirányú továbbképzések

Fontos megemlíteni a szakirányú továbbképzés szintjét is, amely a már korábban megszerzett alap- és mesterfokozatra, főiskolai vagy egyetemi szintű végzettségre épülő oklevelet 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.[36]

Kiberbiztonsághoz kapcsolódó hazai szakirányú képzések:

a) Nemzeti Közszolgálati Egyetem – Elektronikus információbiztonsági vezető szakirányú továbbképzés (NKE EIB)[37]

[33] 2011. évi CCIV törvény a nemzeti felsőoktatásról.
[34] Felvi.hu szakleírások: Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés, https://www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/20554/szakleiras.
[35] Nemzeti Közszolgálati Egyetem: Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány szakleírás, tematika, https://hhk.uni-nke.hu/oktatas/mesterkepzes/vedelmi-vezetestechnikai-rendszertervezo.
[36] 87/2015. (IV. 9.) Korm. rendelet a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról.
[37] Nemzeti Közszolgálati Egyetem: Elektronikus információbiztonsági vezető szakleírás, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok.

b) Eötvös Loránd Tudományegyetem – Adatbiztonsági és adatvédelmi szakjogász/szakember szakirányú továbbképzés (ELTE ASZ)[38]

c) Óbudai Egyetem – Kiberbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE KSZ)[39]

d) Óbudai Egyetem – Információbiztonsági szakmérnök/szakember szakirányú továbbképzés (39 EISZ)[40]

e) Gábor Dénes Főiskola – Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés (GDF AIM)[41]

Meg kell jegyezni, hogy a Nemzeti Közszolgálati 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 közszolgálat 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

[38] ELTE: Adatbiztonsági és adatvédelmi szakjogász szakleírás, https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406.

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

[40] Óbudai Egyetem: Információbiztonsági szakmérnök/szakember képzés tartalma, http://www.bgk.uni-obuda.hu/hu/kepzeseink/tovabbkepzesek/informaciobiztonsagi-szakmernokszakember.

[41] Gábor Dénes Főiskola: Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés tartalma, http://gdf.hu/szakiranyu-tovabbkepzesek/adatvedelmi-es-informaciobiztonsagi-menedzser/.

képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgálatban és a KII[42] 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.

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. Például:

- 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 foglaltak rendszeres gyakoroltatásával, a válságkommunikációs tervek előkészítésével stb.

[42] KII: kritikus információs infrastruktúra

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 megvédik az OT rendszereket.

Az eddigi „IT vs. OT" megközelítés helyébe a két terület szakemberei közötti olyan együttműködésének 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.[43] [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.[44] 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 működnie. Csak komplex szakmai megközelítés ad esélyt arra, hogy például 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.

Az IT-OT sajátosságok tételes összevetését, valamint a szükségszerű IT-OT konvergencia – más megközelítés szerint integráció – lehetőségeit a 16. melléklet mutatja be.

5.2.4. Kibertámadást észlelő képesség fejlesztése

[43] 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.)
[44] Pl. ICS/OT snapshot 2019 (Black Cell Magyarország Kft.)

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

A kritikus infrastuktúrákat – 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) (SOC[45]) 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 gyakorlattokkal 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 – például az incidensek kivizsgálásában – is különös jelentősége van a villamosenergetikai és a kiberbiztonsági oldal szakértői szoros együttműködésének. Ezzel

[45] SOC: Security Operations Center

összhangban a forensics[46] 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 hasonlatosan a kiberbiztonsági rendszer működtetésében is érvényesítendő a PDCA-ciklus[47] [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.

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

5.3. Jogszabályi 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 Protection[48];

[46] forensics: informatikai eszközön vagy rendszerben bekövetkezett események hiteles rekonstruálása

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

[48] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

  - 2005. Zöld könyv ennek végrehajtásáról, lehetőségeiről, tagállamok véleményének kikérése érdekében[49];
  - 2008. CIP irányelv (114/2008/EK irányelv)[50].
  - 2020. CIP irányelv újragondolása (lásd: 4.7.2).
  - 2020. NIS 2.0. (lásd: 4.7.3.)
- 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 felülírni, hanem harmonizálni szükséges azokkal).

5.3.2. Az Európai Parlament és Tanács kritikus szervezetek ellenállóképességéről szóló Irányelve[51]

Az Európai Bizottság 2020. december 16-án terjesztette elő, a kritikus szervezetek ellenállóképességéről szóló irányelv-javaslatát (a továbbiakban: CER irányelv). A CER irányelv szakít a rendszerelemek fizikai védelmére fókuszáló korábbi szemlélettel, helyette a működés folytonosságára, az esetlegesen bekövetkező zavarokból történő minél gyorsabb helyreállításra, azaz az ellenállóképességre (reziliencia) és annak tudatos fejlesztésére helyeződik át a hangsúly. Ennek érdekében a CER irányelv alapján a tagállami hatóság feladatai:

  - stratégia elfogadása a kritikus entitások ellenálló képességének megerősítésére;
  - nemzeti kockázatelemzés elkészítése;
  - kritikus entitások azonosítási kritériumainak meghatározása;

[49] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=en
[50] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN
[51] Az alfejezetben szereplő információk a 2021. december 31-i állapotot tükrözik, a CER irányelv tervezetét mutatják be.

- kritikus entitások azonosítása;
- az azonosított szolgáltatások listája, az ágazatonkénti azonosított szervezetek száma, valamint az azonosításhoz használt küszöbértékek összesített eredményeiről a Bizottság tájékoztatása;
- az azonosított kritikus entitások listájának frissítése;
- kritikus entitások (helyszíni) ellenőrzése, hatósági felügyelete, tájékoztatása, jó gyakorlatok összegyűjtése és megosztása, ellenállóképességi gyakorlatok szervezése, bírságolás lehetőségével való felszólítás;
- folyamatos kapcsolattartás a NIS 2 irányelvben (lásd: 4.7.3. pontban) meghatározott feladatokat ellátó hatósággal;
- alapvető szolgáltatások listájának összeállítása a mellékletben említett ágazatokban;
- illetékes hatóságon belül egyedüli kapcsolattartó pont kijelölése és Bizottság felé történő bejelentése;
- jelentés a beérkezett eseményekről a Kritikus Entitások Ellenállóképességi Csoport részére;
- információcsere eszközrendszer kiépítése.

A kritikus entitások feladatai a CER irányelv alapján:

- kockázatértékelés készítése;
- rezilienciafejlesztési tervvel vagy azzal egyenértékű dokumentummal kell rendelkezniük;
- megfelelő és arányos technikai és szervezési intézkedések bevezetése és alkalmazása a kockázatértékelés alapján;
- bizonyos munkakörök háttérellenőrzéshez kötésének lehetősége;
- kérelmek benyújtása az adott hatóságok felé a háttérellenőrzések lefolytatása érdekében;
- jelentős zavart okozó esemény hatóság részére történő bejelentése.

A CER irányelv hatálya a korábbi szabályozás szerinti két ágazat (energia, közlekedés) helyett immár kilenc ágazatra terjed ki (energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, közigazgatás, világűr, agrárgazdaság). Az irányelvtervezet összveszély megközelítést alkalmaz, azaz a természeti és ember okozta fenyegetésekre egyaránt kiterjed. A CER irányelv nem terjed ki azonban a NIS 2 irányelv (lásd: 4.7.3. pontban) által kezelt kiberbiztonsági kockázatokra.

A szabályozás célja egyértelműen a párhuzamosságok megszüntetése, ezért elvi éllel fekteti le az irányelv, hogy ahol a NIS 2 irányelv (lásd: 4.7.3. pontban) alkalmazandó, ott a CER irányelv alkalmazása kizárt úgy szabályozási, mint hatósági felügyeleti szinten. A párhuzamosságok elkerülését szolgálja az a rendelkezés is, mely kimondja, hogy amennyiben van más olyan releváns (ágazatspecifikus) EU-s jogi aktus, mely kockázatértékelési-, intézkedési-, vagy bejelentési kötelezettséget ír elő az entitásnak, valamint ezek a követelmények egyenértékűek az ezen irányelvben meghatározott megfelelő kötelezettségekkel, úgy az egyéb uniós jogi aktus rendelkezéseit kell alkalmazni. Ilyen – legalább egyenértékű – szabályokat a Banki- és Pénzpiaci infrastruktúrák tekintetében a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról szóló Európai Parlament és Tanács rendelete (a továbbiakban: DORA), valamint a digitális szolgáltatások vonatkozásában a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 Irányelvet felváltó irányelv (a továbbiakban: NIS 2 irányelv) fog meghatározni.

A CER irányelv 8. Cikke szerint a fenti 3 ágazat vonatkozásában 11. cikk és a III., IV. és VI. fejezet rendelkezései nem alkalmazandók, így a CER irányelv alapján a 3 ágazatban kijelölt kritikus fontosságú szervezeteknek nem kell:

- kockázatelemzést készíteni;
- ellenállóképesség fejlesztési intézkedéseket hozni;
- a kritikus munkakörök beosztások esetén nem kérhetnek ezen irányelv által biztosított háttérellenőrzést,
- incidens bejelentési kötelezettség nem terheli őket;
- nem lehetnek EU-i jelentőségű jogalanyok;
- nem vehetnek részt a CER irányelv által létrehozott munkacsoportokban,
- CER irányelv alapján átültetett szankcióval nem sújthatók.

Azonban a 3. cikk szerinti minimum harmonizáció lehetőséget biztosít a tagállamok számára, hogy nemzeti jogukban a kritikus entitások magasabb szintű rezilienciájának megvalósítására irányuló rendelkezéseket fogadjanak el vagy tartsanak fenn, feltéve, hogy az ilyen rendelkezések összhangban vannak az uniós jogban megállapított tagállami kötelezettségekkel.

5.3.3. A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 Irányelvet felváltó irányelv[52]

Az NIS irányelvként 2016-ban megjelent, 2018-ban hatályba lépett, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 Irányelvet felváltó irányelv (a továbbiakban: NIS 2 irányelv) mereven szétválasztja a fizikai biztonságot és az ellenállóképességet (CER irányelv hatálya), valamint a hálózat- és információs rendszerek sérülékenységei okozta fenyegetettségeket, átfedést nem enged a két terület között, gyakorlatilag a mai hatályos magyar rendszernek megfelelő felosztást alkalmazva. A NIS 2 irányelvet az Európai Parlament 2022. november 10-én fogadta el. Ezután az Európa Tanácsnak kell elfogadnia. Ezt követően az egyes tagállamoknak 21 hónapjuk lesz a NIS 2 irányelv rendelkezéseinek a nemzeti jogrendekbe történő beillesztésére. Így a NIS 2 irányelv tagállami átültetése várhatóan 2024 második felében várható.

A tagállamok több létező hatóságot vagy egy hatóságot is kijelölhetnek az alapvető szolgáltatást nyújtó szereplők (operator of essential services - OES), illetve fontos szereplők (operator of important services) hálózati és információs rendszereik felügyeletére, valamint az eseménykezelésre. A kijelölt hatóságon belül egyedüli kapcsolattartó pont-, valamint egy ettől elkülönülő, de a hatóságon belül működő eseménykezelő központ (CSIRT) felállítása szükséges. Az irányelv kimondja, hogy amennyiben létezik (vagy később hatályba lép) olyan ágazatspecifikus EU-s szintű norma, mely jelen irányelvnek megfelelő szintű védelmet nyújt, úgy az ágazatspecifikus norma rendelkezései alkalmazandók. Az irányelv – bizonyos kivételektől eltekintve – kiveszi a hatálya alól a KKV-kat. Az irányelv kihangsúlyozza, hogy a kritikus entitások ellenállóképességéért felelős hatósággal történő folyamatos együttműködés nélkülözhetetlen, ezt egyenesen kötelezettségként írja le. Figyelemmel a határokon átnyúló szolgáltatások rendszerére, az irányelv úgy határoz, hogy minden egyes tagállam, ahol szolgáltatást nyújt az OES, ott a hatóságnak azonosítania kell azt. Mivel egyes szereplőknek egy adott incidens esetén több hatóság irányába lenne bejelentési kötelezettsége (pl.: elektronikus információs rendszerről történő személyes adatokat is érintő adatszivárgás – NIS 2, GDPR, Elektronikus Hírközlő Hálózatok), úgy csak egy irányba kell bejelentenie az ügyfélnek, mely a NIS 2 hatóság. Az azonosított szereplők listáját az ENISA vezeti. A kijelölt hatóságot fel kell ruházni olyan jogosítványokkal, mint a rendszeres audit, helyszíni ellenőrzés lehetősége, iratok megismerésének lehetősége,

[52] Az alfejezetben szereplő információk a 2021. december 31-i állapotot tükrözik, a NIS 2 irányelv tervezetét mutatják be.

Érintett ágazatok (alapvető): Energia, Közlekedés, Bank, Pénzpiacok és infrastruktúrák, Egészségügy, Ivóvíz, Szennyvíz, Infokommunikációs technológiák, Közigazgatás, Világűr

Érintett ágazatok (fontos): Postai szolgáltatások, Szemétszállítás, Vegyi anyagok előállítása és elosztása, Élelmiszer előállítás és elosztás, Ipar, Digitális szolgáltatók.

A NIS 2 egyik legjelentősebb változtatása az alapvető, illetve fontos szolgáltatást nyújtó szereplők által kiszervezett tevékenységet végző, illetve számukra szolgáltatásokat nyújtó szereplők NIS 2 hatálya alá történő bevonása. Ennek hatása jelenleg még nem mérhető fel, de az már most is valószínűsíthető, hogy tovább fog fokozódni a jelenleg is súlyos információ- és IT/OT-biztonsági szakemberhiány.

További változás, hogy a NIS 2 a kötelezettségeken túl szankciókat is meghatároz. Az egyik legfontosabb változás a biztonsági incidensek 72 órán belül történő jelentési kötelezettségével kapcsolatos. A NIS 2 értelmében az éves bevételük 1,4-től 2%-ig terjedő bírságot lehet kiszabni azokra a szervezetekre, amelyek jelentési kötelezettségüket elmulasztják, avagy megtagadják az együttműködést a kijelölt hatósággal.

5.3.4. 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 hatály[53] szerint 10 ágazat van: energia, közlekedés, agrárgazdaság, egészségügy, társadalombiztosítás, pénzügy, víz, infokommunikációs technológiák, honvédelem, közbiztonság-védelem.

A definíciós háttér tekintetében a következő fogalmak irányadóak:

- *nemzeti rendszerelem:* az Lrtv. alapján kijelölt létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt elsősorban Magyarországon lenne jelentős hatással,
- *európai létfontosságú rendszerelem:* a törvény alapján nemzeti létfontosságú rendszerelemmé kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős

[53] 2021. július 1.

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 lehetséges létfontosságú rendszerelem megnevezését, elhelyezkedésének beazonosíthatóságát biztosító helyadatokat,
- a vizsgált rendszerelemre vonatkozó kockázatelemzést és annak eredményét,
- a kijelölésre irányuló javaslatot (vagy a kijelölés indokolatlanságát),
- az Lrtv. 2/A. § (2) bekezdésében meghatározott szempontrendszerre vonatkozó elemzést, ha megállapítható, hogy az Lrtv. 1. mellékletében meghatározott azon alágazatba tartozik, amely az Lrtv. vhr. 3. melléklet alapján megfeleltethető a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és tanácsi irányelv (NIS Irányelv) szerinti valamely ágazatnak vagy alágazatnak,
- a teljességére vonatkozó üzemeltetői nyilatkozatot, valamint
- az azonosítási vizsgálat kezdő- és zárónapját tartalmazza.

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 részcselekmény a horizontális kritériumok[54] teljesülésének vizsgálata. Ennek érdekében az ágazati kijelölő hatóság szakhatóságként bevonja a hivatásos katasztrófavédelmi szerv központi szervét, a BM Országos Katasztrófavédelmi Főigazgatóságot (a továbbiakban: BM OKF).

[54] 65/2013. (III. 8.) kormányrendelet 1. sz. mellékletében felsorolt kritériumok.

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.

5.3.5. 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 létesítményei[55];
- 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.

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:

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

- *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.

5.3.6. Információbiztonsági kötelezettségek

A kijelölt létfontosságú rendszerelemek – így az energia ágazat kijelölt kritikus infrastruktúrái – az Ibtv. hatálya alá tartoznak, ezáltal 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 jelenlegi keretét három jogi aktus adja:

- a CIP irányelv[56],

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

- az Európai Uniós Kiberbiztonsági Ügynökségről (ENISA) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelet[57], valamint
- a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv[58] (a továbbiakban: NIS irányelv).

Mindezek keretrendszert biztosítanak a kritikus infrastruktúrák kiberbiztonságának megteremtéséhez, beleértve a villamosenergia alágazatot is. A nemzetközi tapasztalatok megismeréséhez mintavételesen 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.

  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.

[57] 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 hatályon kívül helyezéséről (kiberbiztonsági jogszabály)

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

- 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 ellenálló képességük 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 KRITIS[59] szakterületi érintettek munkacsoportja és annak működése is. Lásd bővebben a 13. mellékletben.

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

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

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 elkezdték 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. Mindenképpen szükséges a nemzetközi jó gyakorlatok és ajánlások figyelembevétele, továbbá az Uniós 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 a 7. ábra mutatja be. Az ábra szerinti szabályozásokat a kézikönyv egyéb részei ismertetik.

A 7. ábra szerinti hivatkozások listája:

[1] ISO/IEC 27001 Information Security Management

[2] IEC 62443 Industrial Automation and Control System

[3] 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről [CIP irányelv]

[4] 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről [NIS irányelv]

[5] Security and Privacy Controls for Federal Information Systems and Organizations [SP 800-53r4]

[6] A biztonsági unióra vonatkozó uniós stratégia (2020)

[7] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[8] Az Európai Unió Kiberbiztonsági Stratégiája a digitális évtizedre (2020)

[9] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[10] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról

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

[12] 2007. évi LXXXVI. törvény a villamosenergiáról

[13] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról [Ibtv.]

[14] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről [Lrtv.]

[15] 1996. évi CXVI. törvény az atomenergiáról

[16] 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

[17] 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

[18] 65/2013 (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról [Lrtv. vhr.]

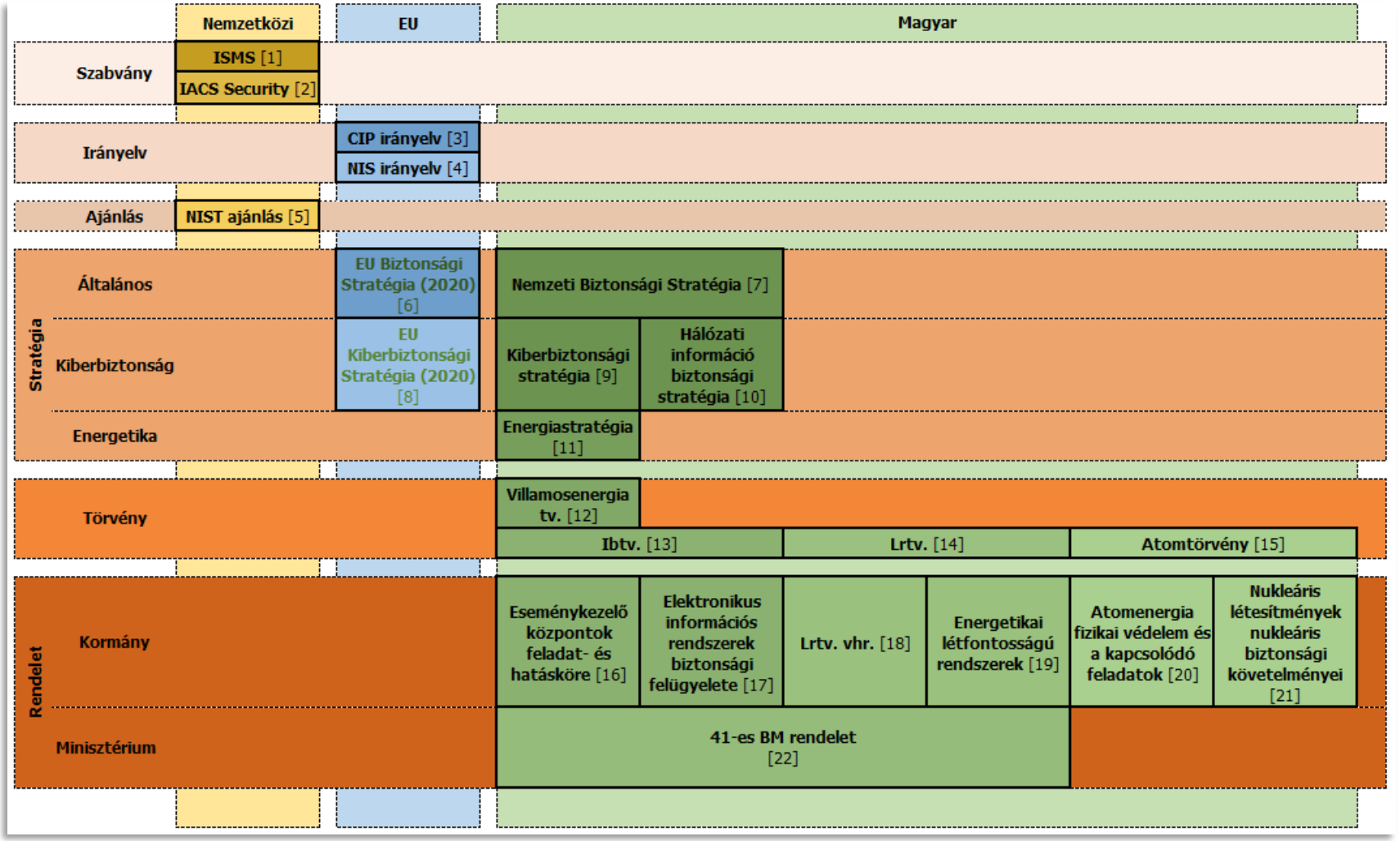
[19] 374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[20] 190/2011 (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről

[21] 118/2011 (VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről

[22] 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



7. 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 háttér információt 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/eseménysor 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 fenyegetettségek kategóriákba sorolása az alábbi szempontok (és megtörtént esetek) szerint:
  - Érdekelt ellenfelek (pl. Dragonfly[60])
  - Közvetlen ICS hatás (pl. MiniDuke[61])
  - Közvetett ICS-hatás (pl. Wannacry[62])
- A globális fenyegetés felderítési szcénában általánosan elfogadott különböző listák és szabályok használata, amelyek elősegítik a fenyegetettségek felismerését. Ilyen források többek között az IoC[63], Yara[64], Hash[65], URL, IP, DNS listák és szabálycsomagok. Ezek használata mind visszatekintő, mind előremutató 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 (CTI[66]) prioritása megvalósuljon a teljesség, a pontosság, a relevancia és az időszerűség szempontjából. Ennek során javasolt, hogy mind az emberileg olvasható (human readable), mind a gépek számára olvasható

[60] Dragonfly: villamosenergia-rendszer ellen támadást intéző rosszindulatú program
[61] 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 kémszoftver.
[62] Wannacry: 2017-ben elterjedt zsarolóvírus, melyet Észak-Koreának tulajdonítanak.
[63] IoC: Indicator of Compromise (kompromittálódásra utaló jel)
[64] Yara: rosszindulatú programok kutatásában és felismerésében használt eszköz
[65] Hash: lenyomat (előírás szerint képzett bitsorozat)
[66] 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”[67]-ok létrehozása, amelyek az ICS-specifikus protokollokat emulálják. Az emulálás során a szektorra jellemző protokollok (Modbus[68]; DNP3[69], OPC[70], IEC 104[71], IEC 61850[72], IEC 60870-5[73]) emulálása is kiemelten javasolt a generikus IP protokollok (HTTP, FTP, távoli elérések, Telnet stb.) mellett.
- A hatékony fenyegetés felderítés (TI[74]) megvalósításának elengedhetetlen részét képezi a képzés. Ennek ajánlott témái például a CTI használata a fenyegetés „vadászatban” (mind az automatikus észlelés és megelőzés, mind a kézi használat), az ICS ATT&CK[75] 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 CVE[76]-kre.

6.1.2. Kockázatértékelés

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 tartalmaznak kiberbiztonsági szempontokat. Fontos, hogy a jövőben az eddigi elemek mellett a kiberbiztonsági kockázatelemzés is a folyamat szerves részét képezze.

[67] honeypot farm: rosszindulatú kódok algoritmusok elfogására szolgáló csali számítógép „farm”
[68] Modbus: ipari környezetben alkalmazott adatkommunikációs protokoll
[69] DNP3: Distributed Network Protocol 3 (elosztott hálózati protokoll)
[70] OPC: Open Platform Communication, OLE for Process Control (Platformfüggetlen kommunikáció/Nyílt platformú kommunikáció. Az OLE ipari automatizálásra specializált alkalmazási rendszere.)
[71] IEC 104: Soros protokoll (RS232) TCP/IP implementációja
[72] IEC 61850: gyártófüggetlen energetikai adatkommunikációs szabvány
[73] IEC 60870-5: gyártófüggetlen energetikai adatkommunikációs szabvány
[74] TI: Threat Intelligence (fenyegetés felderítés)
[75] ICS ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge (támadói taktikák, technikák és közös tudásbázis)
[76] CVE: Common Vulnerabilities and Exposures (ismert sérülékenységek és kitettségek)

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

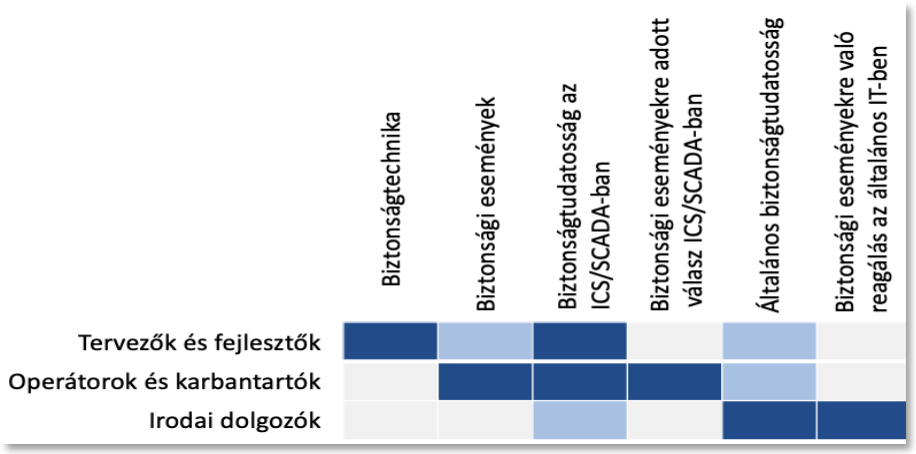
A biztonsági kiindulási irányelvek képezik a kiberbiztonsági kockázat kezelésének elősegítésére szolgáló politikák, eredmények, tevékenységek, gyakorlatok és ellenőrzések kiindulópontjait, alapeseteit (a baseline[77]-okat). Általában széles körű kockázatkezelési politikai célokat fednek le (pl. védelmet 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 8. ábra ajánlás a szakterületi képzések lehetséges rendszerére.



8. ábra: A kiberbiztonsági szakterületi képzések ajánlott rendszere

[77] 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) annak ismeretét, hogy az adott javítás a rendszer mely részeinek megfelelő,

b) a javítások megfelelő telepítésének biztosítását,

c) a rendszerek telepítés utáni tesztelését, valamint

d) 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 EoL[78] szoftver/hardver nyitott internetnek való kitettségéről szóló rendelet megalkotását, másrészt a kötelező készletleltár (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.

[78] 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 (IAM[79]) 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 ACL[80]-eket.
- Használjon VLAN-okat.
- Engedélyezze a port szintű biztonsági beállításokat (port security).
- Engedélyezze a MAC[81] cím kontrollt.
- Ne használjon ”háztartási” hardvereket (lásd VPNfilter).
- Használjon adat diódákat.
- Ne kizárólag a határvédelemre támaszkodjon.

[79] IAM: Identity and Access Management (azonosítás- és hozzáférés kezelés)
[80] ACL: Access Control List (hozzáférési lista)
[81] MAC: Media Access Control (közeghozzáférés-vezérlés, egyedi hálózati azonosító)

- Használjon mély csomag ellenőrzést (DPI[82]).
- 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-ERP[83]), 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 létrehozzuk 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 tűzfalakhoz:

- 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.

[82] DPI: Deep Packet Inspection (mély csomag ellenőrzés)
[83] ERP: Enterprise Resource Planning (vállalati erőforrás tervezés)

Minden olyan parancsot, amely nem szerepel az „engedélyezett” listán, minden olyan forgalmat blokkolni, naplózni és jelenteni (pl. syslog[84]) kell, amely

a) nem felel meg a Modbus szabványnak, vagy

b) bármilyen register vagy coil[85] 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 payloadba[86], vagy azt, hogy hogyan próbálta obfuszkálni[87] azt olyan technikákkal, mint a NOP slides[88]. 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 CRC[89] érték ellenőrzésekre.

A fentiken kívül javasolt olyan megoldást alkalmazni, amely rendelkezik:

- IEC 104 ellenőrzési lehetőségekkel,
- GOOSE ellenőrzési lehetőségekkel,

[84] syslog: system log (központi naplózás)
[85] 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.
[86] payload: csomagtartalom (adatcsomag üzenet része)
[87] 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.
[88] 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.
[89] CRC: Cyclic Redundancy Check (ellenőrző összeg)

- EtherNet/IP ellenőrzési lehetőségekkel,
- OPC ellenőrzési lehetőségekkel,
- biztonságos távoli konfigurációs lehetőségekkel,
- IEC 61850 mély csomag ellenőrzéssel (DPI).

6.2.5. Behatolás megelőzés

A behatolás észlelő és megelőző rendszer (IDPS[90]) 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 IPS[91] és IDS[92] 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

[90] IDPS: Intrusion Detection and Prevention System (behatolás észlelő és megelőző rendszer)
[91] IPS: Intrusion Prevention System (behatolást megelőző rendszer)
[92] IDS: Intrusion Detection System (behatolás észlelő rendszer)

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).

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 (TAP[93]) eszközön, vagy amennyiben ez nem áll rendelkezésre, akkor a forgalom kitükrözésével (SPAN[94] 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"[95] szakaszát követő automatizálási feladatokra is tökéletesen alkalmas.

A Suricata GPU[96] támogatásával számtalan egyéb előny is kiaknázható (pl.: DDoS[97], DoS[98] 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.

[93] TAP: Test Access Point, olyan hálózati hardvereszköz, mely a hálózati hozzáférést és monitorozást teszi lehetővé.
[94] SPAN: Switched Port Analyser (port forgalom figyelése, tükrözése, monitorozása)
[95] threat hunting: fenyegetettség elemzés
[96] GPU: Graphical Processing Unit (grafikus processzor)
[97] DDoS: Distributed Denial of Service (elosztott, szolgáltatásmegtagadással járó támadás)
[98] DoS: Denial of Service (szolgáltatásmegtagadással járó támadás)

Az IDPS rendszerek naplózása kiemelt fontosságú, mind megőrzés, mind a felhasználás tekintetében (pl. log elemzés, SIEM[99] rendszerek).

Az ipari hálózatokon ajánlott minden kommunikációt átterelni 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-vel[100] 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.[101] 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. TLS[102] és SSH[103] kapcsolat, a titkosítatlan FTP és TELNET helyett).
- Minimum elvárás: jelszavak ne legyenek nyílt szövegben tárolva és küldve.
- Minimum elvárás: a vezeték nélküli és a nyílt hálózaton keresztüli távoli elérések kriptográfiailag védetten történjenek.

6.3. Ajánlások: észlelés

[99] SIEM: Security Information and Event Management (biztonsági információ és esemény kezelés)
[100] SPI: Stateful Packet Inspection (állapotfüggő csomagfelügyelet)
[101] Ingyenes, nyílt forrású hálózati behatolás-érzékelő és -megelőző rendszer
[102] 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.)
[103] SSH: Secure Shell (Protokoll, amit egy helyi és egy távoli számítógép közötti biztonságos csatorna kiépítésére fejlesztettek ki.)

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.

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 architekturális 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"[104] 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 például a meggondolatlan – támadás esetén az ártó szándékú – kapcsolások, műveletek fizikai károkat is okozhatnak, sőt

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

emberéletet 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 meglátásaikat.

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 definiálandó 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 reagálás 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 egyrészről a behatolás megelőzéshez és észleléshez új származtatott információk jönnek létre, másrészről a jövőbeli eseménykezelési tréningekhez új szempontok merülhetnek fel, amivel javítható a legközelebbi hasonló eseményre adott reagálás 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 valósidejűség a villamosenergetikai ICS/SCADA komponensek – hangsúllyal a védelmek – esetében a kibervédelmükkel kapcsolatos többlet funkciók ellátása erős performancia-tartalék követelményeket támaszt, mivel például az adatok gyűjtése, a naplózás, 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

diszpécsert, vagy a szerverpark üzemeltetését végző rendszergazdát épp úgy, mint például a villamos védelmeket üzemeltető mérnököt.

- A legjobb gyakorlatok alapján reagálási eljárások, irányelvek készítendők az ICS/SCADA komponensek üzemeltetésében közvetlenül és közvetve illetékes valamennyi szervezet és személy számára, a szükséges együttműködéseket megjelölve.
- Ajánlott SOAR[105] rendszer használata.
- Ajánlott a leltár, a hálózati topológia, a függőségi gráf naprakész állapotban tartása.
- Mentések, visszaállási információk, megfelelő konfiguráció kezelés végzendő, illetve készítendő, 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 beépítendők 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.

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.

[105] 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)

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 tolakodóak. 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 funkcionalitást.

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 modellnek az ISA-99 bizottság által folyamatirányító rendszerekre alkalmazott hierarchia-modelljére hivatkozunk. Jelenleg a legismertebb verziója a SANS Reading Room ICS whitepaper publikációi között érhető el.[106] [7]

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

Ügyviteli zóna

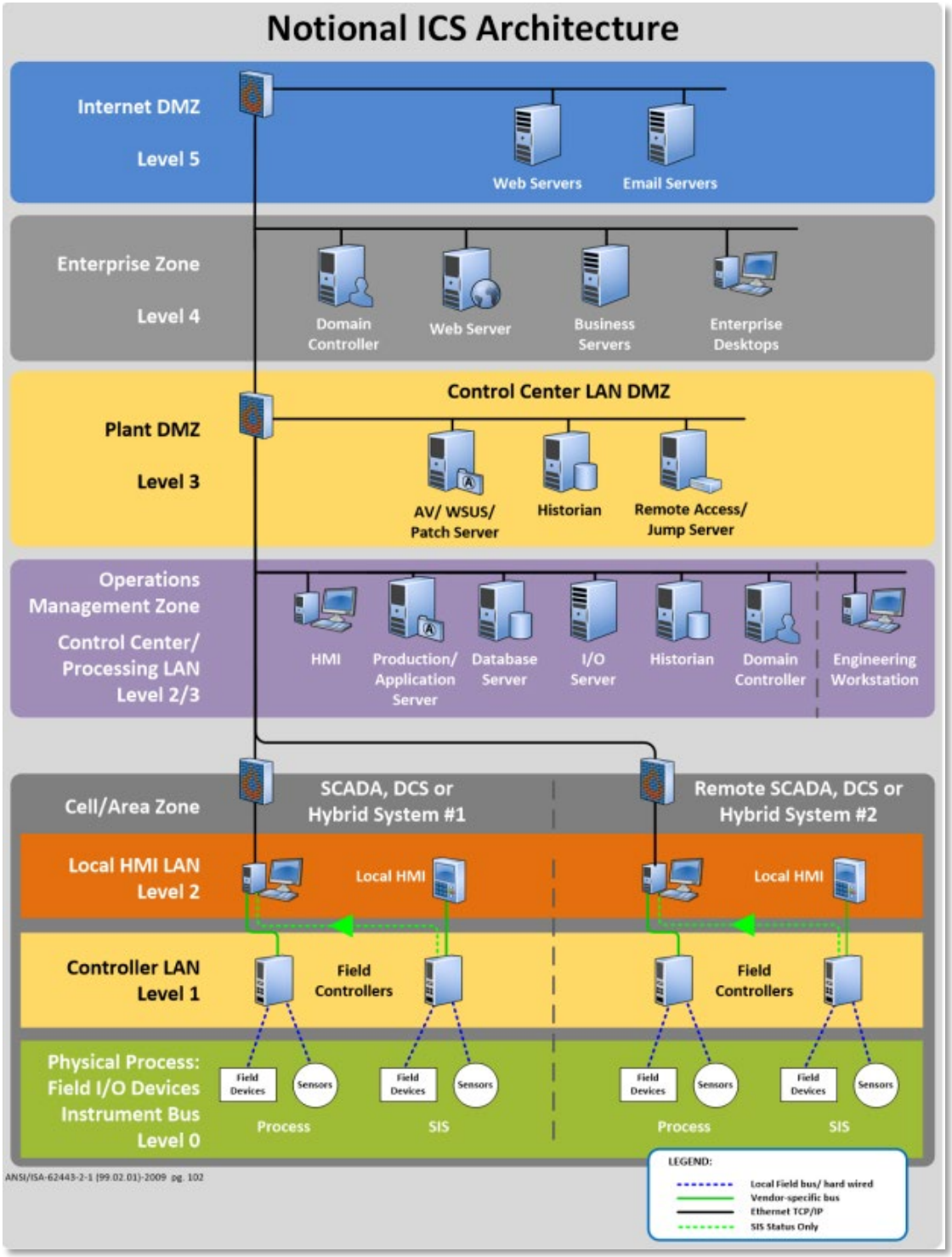
5. szint: Ügyviteli/vállalati rendszerek

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).

[106] 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.)


Notional ICS Architecture
Internet DMZ
Level 5
Web Servers
Email Servers
Enterprise Zone
Level 4
Domain Controller
Web Server
Business Servers
Enterprise Desktops
Control Center LAN DMZ
Plant DMZ
Level 3
AV/ WSUS/ Patch Server
Historian
Remote Access/ Jump Server
Operations Management Zone
Control Center/ Processing LAN
Level 2/3
HMI
Production/ Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation
Cell/Area Zone
SCADA, DCS or Hybrid System #1
Remote SCADA, DCS or Hybrid System #2
Local HMI LAN
Level 2
Local HMI
Local HMI
Controller LAN
Level 1
Field Controllers
Field Controllers
Physical Process:
Field I/O Devices
Instrument Bus
Level 0
Field Devices
Sensors
Process
SIS
LEGEND:
Local Field bus/ hard wired
Vendor-specific bus
Ethernet TCP/IP
SIS Status Only
ANSI/ISA-62443-2-1 (99.02.01)-2009 pg. 102

9. ábra: A Purdue modell az OSTI [107] ábrázolásában[108] [8]

Távfelügyeleti (üzemviteli) zóna[109]

3. szint: Üzemviteli 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 DNS[110], DHCP[111], NTP[112] 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 időszinkronizálás vagy DNS névfeloldás miatt erre szükség lehet).

Technológia-közeli (üzemeltetési) zóna[113]

2. szint: Ipari felügyelet és vezérlés

A 2. szinten működő rendszerek közé olyanok tartoznak, amelyek jellemzően az 1. szinten található rendszerekkel kell kommunikálniuk (ilyenek például a vezénylőtermi 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).

[107] OSTI: U.S. Department of Energy Office of Scientific and Technical Information
[108] M. C. Hurd, M. V. McCarty (2017) "A Survey of Security Tools for the Industrial Control System Environment" doi.org/10.2172/1376870
[109] A Purdue modellben a „Gyártási zóna" név szerepel. Mivel ez nem alkalmazható a villamosenergia-rendszerben, ezért az eredetitől eltérő, de helyénvaló megnevezést alkalmazunk.
[110] 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.
[111] 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).
[112] NTP: Network Time Protocol (hálózati idő protokoll. Az órák szinkronizálására szolgáló hálózati protokoll).
[113] Purdue modellben az „Ipari zóna" név szerepel. Mivel ez nem alkalmazható a villamosenergia-rendszerben, ezért az eredetitől eltérő, de helyénvaló megnevezést alkalmazunk.

1. szint: Alapvető vezérlés

Ezen a szinten olyan eszközök találhatóak, amelyek feladata a folyamatvezérlés biztosítása. Ezek az eszközök fogadják és dolgozzák fel a különböző szenzoroktól érkező adatokat. Ezek az eszközök (többnyire DCS[114]-ek, PLC-k, RTU-k) felelősek a folyamatos, szekvenciális, kötegelt és diszkrét vezérlésekért. Ezek az eszközök jellemzően gyártóspecifikus operációs rendszereket/firmware-eket 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 incidensnél[115] előfordult). [9][10]

2019 elején többen, több alkalommal (pl. az S4X19 konferencián[116], majd 2020 májusában David Greenfield cikkében is[117]) [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

[114] DCS: Distributed Control System (osztott intelligenciájú folyamatirányító rendszer)
[115] 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. 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.)
[116] D. Peterson. „Is The Purdue Model Dead?" https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/ (Letöltve: 2020. augusztus 26.)
[117] D. Greenfield. „Is the Purdue Model Still Relevant?" AutomationWord. https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant (Letöltve: 2020. augusztus 26.)

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, transzformátorok, mérőváltók stb. 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.

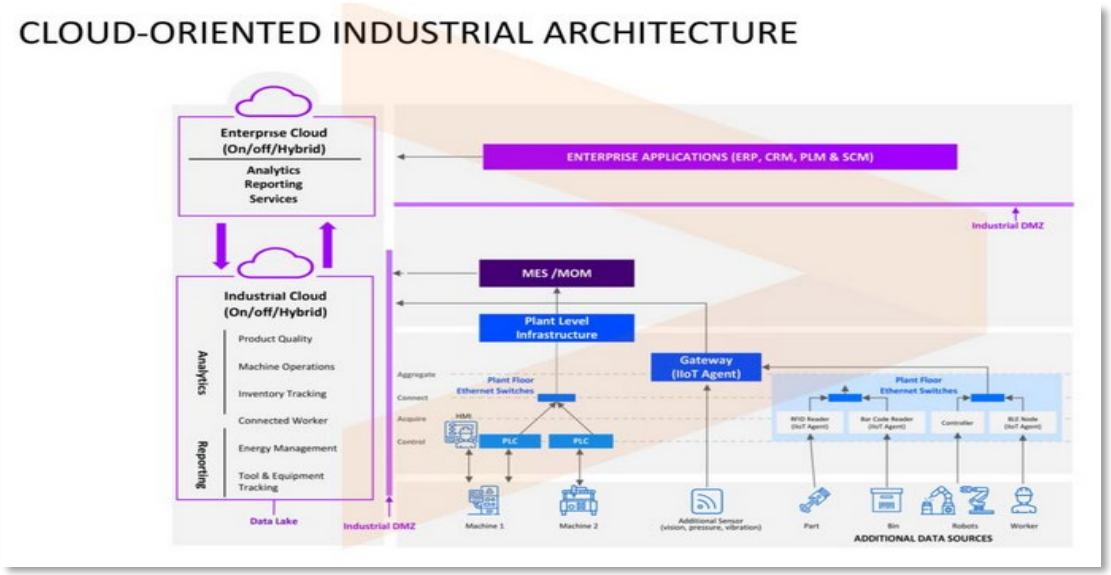
Ráadásul az ICS/SCADA hálózatokban egyre nagyobb arányban jelennek meg a különböző IT eszközök (switch-ek, szerverek és egyéb, korábban csak adatközpontokban használt megoldások), amikkel együtt jár a sávszélességek és a megbízhatósági (reliability) képességek megváltozása is, ami további számítási kapacitásokat 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 SDN[118] felé mozgatja a jövő ipari hálózatainak tervezőit is.

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-

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

alapú architektúra-modellje (10. ábra) vagy a General Electric és a Dragos whitepaper-sorozatának első részében megjelent Purdue modell változat[119]. [12]



10. ábra: Brad Hegrat felhő-orientált ipari architektúra-modellje[120]

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

A Purdue modell ugyan nem halott, de az általa nyújtott alapokon – vagy azt akár meg is haladva – új megközelítésre lesz szükségünk, a villamosenergia-szektor ICS/SCADA rendszereit illetően éppúgy, mint más iparágakban.

[119] Dragos. „Building security to achieve engineering and business requirements.” https://www.dragos.com/wp-content/uploads/SecIndSys_Purdue_GEDragos.pdf (Letöltve: 2020. augusztus 26.)
[120] D. Peterson. „Is The Purdue Model Dead?” https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/ (Letöltve: 2020. augusztus 26.)

> 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 jelenlegi adottságait figyelembe vevő, egyben a 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 üzemzavarukkal a legnagyobb zavarokat, károkat okozó – elemeiben (erőműveiben, alállomásiban stb.) üzemelő ICS/SCADA-kra fókuszál.

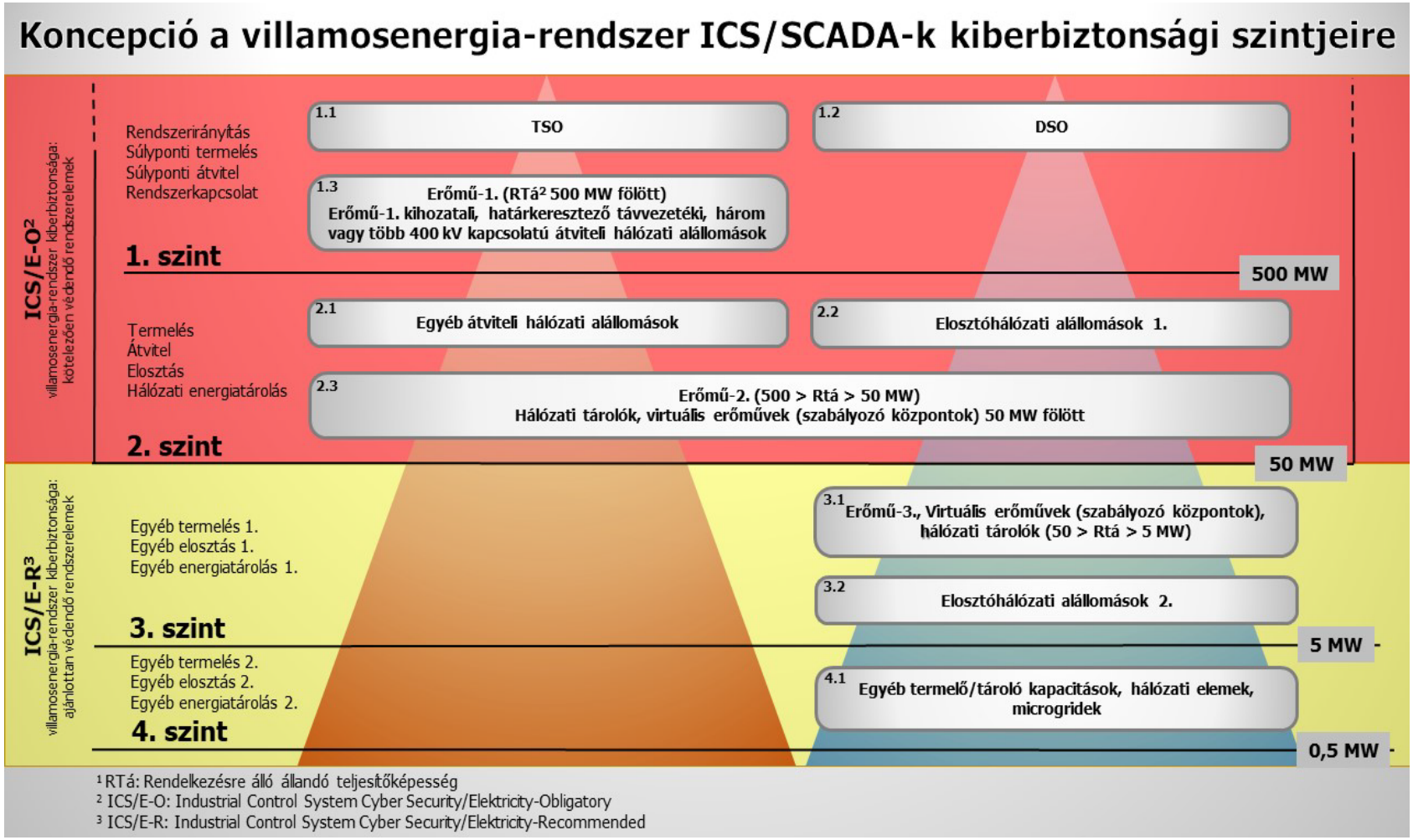
A kézikönyv készítése folyamatában konzultációk zajlottak a magyar villamosenergia-átviteli és -elosztó hálózat egyes mértékadó szakembereivel a villamosenergia-rendszer legnagyobb teljesítményű, legnagyobb energiaáramokat kezelő elemeinek azonosítására és esetleges kibertámadásuk miatti zavaraik miatti várható fogyasztói hatásaik – ezzel a velük kapcsolatban szükséges védelmi intézkedések – prioritásainak meghatározására[121]. Ezek eredményeként koncepció készülhetett a magyar villamosenergia-rendszer sajátosságaihoz illeszkedő ICS/SCADA kibervédelmi szintek rendszerére.

[121] 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 11. ábra szerinti négy – két kötelező és két ajánlott – védelmi szintbe célszerű szervezni.



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

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

- Kötelező, szabályozott, auditált módon védendők 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 védendők 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 Rtá = 50 MW alatti termelő kapacitások kiserőműnek, az akkora, vagy annál nagyobbak nagyerőműnek minősülnek.

Az Rtá[122] = 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 Rtá-k összegét kell alapul venni.

A 0,5 MW-nál kisebb teljesítőképességű termelők, tárolók, szabályozóközpontok, microgridek 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.

[122] 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. Mérni 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 távvezetéket 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. primer[123] készülékek közelében lévő mezőgépek[124] végzik.
- Az adatok összegyűjtését és kiértékelést a fejgép[125]/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) rendszerelemek. 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.

[123] 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

[124] 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.

[125] 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 μs nagyságrendű pontosságú kommunikáció is szükséges lesz egyes eszközök között a PTP[126] 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 másikhoz. A 15. melléklet 2-5. pontjai mutatják be a magyar villamosenergia-rendszerre jellemző megoldásokat, az ezekre elvárt minimum követelményeket is megfogalmazva.

7.4. A Zero Trust biztonsági modell

A Zero Trust biztonsági modell[127] tervezési és megvalósítási módszertanok összessége számítógép hálózatokra, tágabban értelmezve informatikai rendszerekre. Alapvetése, hogy sem a tervezés, sem a megvalósítás során nem élhetünk olyan módszerekkel, melyek a felhasználói eszközök – a hálózatban vett fizikai[128], vagy logikai[129] – elhelyezkedésére alapozva rendelnek jogosultságokat vagy jogosultsági szinteket felhasználókhoz (autorizáció). A jogosultságok hozzárendelése csakis a felhasználó kilétének hitelt érdemlő azonosítását (autentikáció) követően történhet meg, különös tekintettel arra, hogy mik a felhasználó által elvégezni rendelt feladatokhoz feltétlenül szükséges jogosultságok.

A Zero Trust biztonsági modell által megkövetelt szigorú autentikáció, illetve legkisebb jogosultság elve[130,131] semmiképp sem a bizalom hiánya – különösen nem a felhasználóval

[126] PTP: Precision Time Protocol (IEC 1588-2008 szabvány által definiált időfelbontás és szinkronizációs elv)
[127] Más néven zero trust architecture (ZTA), zero trust network architecture, vagy zero trust network access (ZTNA).
[128] Jelenthet egy adott munkahelyszínen (pl.: iroda, épület, telephely, …) való tartózkodást, vagy fizikai hozzáférést valamely eszközhöz.
[129] Például a belső hálózat (intranet), illetve a külső hálózat (internet) szétválasztása okán előálló logikai elválasztás.
[130] Az angol terminusban principle of least privilege (PoLP), principle of minimal privilege (PoMP), vagy principle of least authority (PoLA).
[131] Legkisebb jogosultság elve – Wikipédia (wikipedia.org)

szemben –, hanem a modell mottójának „sose bízz, mindig ellenőrizz”[132] következetes alkalmazása, mely feltételezi, hogy a támadók vagy már jelen vannak a rendszereinkben, vagy a közeli jövőben kerülhet sor a rendszereink kompromittálására. Amikor az incidens bekövetkezik, már csak a kármentesítésre, a jövőbeni esetek bekövetkezési valószínűségének minimalizálására van lehetőségünk. Ez utóbbit azonban már most megtehetjük azzal a gondolattal élve, hogy még ha egy támadás sikeres is, a károkozás lehetőségének mértéke legyen minimális, amely a kritikus infrastruktúrák – ezen belül is a villamosenergetikai ipari felügyeleti rendszerek – esetén alapvető hozzáállás.

A Zero Trust biztonsági modell tehát nem egy termék vagy szolgáltatás, sem nem ezek összessége, hanem egy gondolkodásmód, a hálózat biztonságának egy megközelítési módja, ahol természetesen az alapelvek gyakorlatba való átültetéséhez szükség lesz számos termékre, illetve szolgáltatásra. Maga a koncepció nem új, olyannyira nem, hogy a „zero trust” kifejezést megalkotója – Stephen Paul Marsh – már 1994-ben használta doktori disszertációjában, melyben a bizalom (trust) matematikai leírásával foglalkozik. Kijelentette egyebek mellett, hogy a bizalom fogalma meghaladja az erkölcs, az etika, a törvényesség, az igazságosság és az ítélkezés emberi fogalmait. 2003-ban a fogalom a kifejezetten a számítógép hálózati határvonalak leépítési trendjeivel foglalkozó Jericho Fórumon került elő a megvalósítás kihívásainak tárgyalása kapcsán. A 2000-es évek végére pedig már olyan neves cégek foglalkoztak a zero trust gyakorlati megvalósításával, mint a Forrester Research vagy a Google.

A Zero Trust biztonsági modell széles körben való ismertségre ugyanakkor csak a 2010-es évek végén tett szert, melyben elévülhetetlen szerepe volt az NIST[133,134] és az NCCoE[135,136] kutatóinak. Különösen kiemelendő az NIST Zero Trust Architectre[137,138] című kiadványa, mely számos a témával foglalkozó publikációnak – ahogy a jelen fejezetnek is – kiindulópontja. A gyakorlatba való átültetéshez igen komoly lökést adott a Joe Biden adminisztráció, mikor is elrendelte, hogy a *„Szövetségi Kormányzatnak át kell vennie a legjobb biztonsági gyakorlatokat; haladva a Zero Trust architektúra felé”*. Ebben kitüntetett szerepet játszanak az NIST már említett Zero Trust Architectre, valamint a CISA Zero Trust Maturity Model[139] című kiadványai. Előbbi elméleti és gyakorlati megfontolások sorát tartalmazza, míg az utóbbi

[132] Angol eredetiben „never trust, always verify”.
[133] Nemzeti Szabványügyi és Technológiai Intézet (Egyesült Államok), melynek angol elnevezése National Institute of Standards and Technology (NIST)
[134] National Institute of Standards and Technology – Wikipédia (wikipedia.org)
[135] Nemzeti Kiberbiztonsági Kiválósági Központ (Egyesült Államok), melynek angol elnevezése National Cybersecurity Center of Excellence (NCCoE)
[136] Zero Trust Architecture (nist.gov)
[137] SP 800-207 - Zero Trust Architecture
[138] Zero Trust Architecture (nist.gov)
[139] CISA Zero Trust Maturity Model

zsinórmértékül szolgál annak felmérésében, hogy a szervezet mely érettségi szinten áll jelenleg, illetve, hogy mik lehetnek, mik legyenek a szervezet következő lépései a Zero Trust tekintetében.

A Zero Trust biztonsági modell leszámol azzal a mai körülmények között[140] egyértelműen hamisnak tetsző előfeltételezéssel, miszerint az informatikai rendszereink rendelkeznek egy határvonallal[141], amelynek egyetlen belépési pontja létezik, és biztonságát pusztán határvédelmi eszközök révén képesek vagyunk megteremteni. A Zero Trust biztonsági modell lényege a határvonalak, illetve az általuk meghatározott szabályozási különbözőségek felszámolása, a támadási faktorok, a támadók állandó jelenlétének feltételezése. Ezzel kikényszeríti egy egyenszilárdságú rendszer létrehozását, ahol nincs különbség az alkalmazott védelmi eszközökben és módszerekben privát és publikus hálózatok esetén, mivel ezen fogalmak létjogosultságát nem ismeri el. Ehhez az alábbi alapelveket fekteti le és következetes betartásukat követeli meg.

1. Minden adat és szolgáltatás erőforrás.
2. Minden kommunikáció biztonságosan (titkosítva) történik, függetlenül a hálózati helytől.
3. A hozzáférés biztosítása az egyes vállalati erőforrásokhoz munkamenetenként történik.
4. Az erőforrásokhoz való hozzáférés dinamikus házirendek révén dől el.
5. A vállalat méri és nyomon követi a saját és a tárolt adatvagyon minden elemének biztonságát és integritását.
6. Minden erőforrás-hozzáférést következetesen érvényesített autentikácó és autorizáció előz meg.
7. A vállalat minden lehetséges információt gyűjt az adatvagyonra, a hálózati architektúrára, illetve kommunikációkra vonatkozóan, hogy növelhesse a biztonság szintjét.

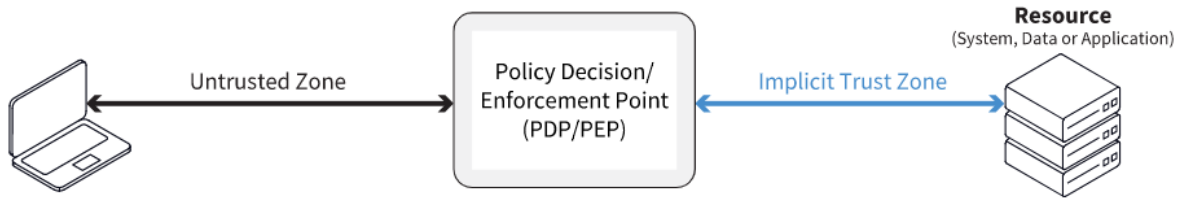
A fenti alapelvek – illetve általánosságban a Zero Trust biztonsági modell – alkalmazásának számos indoka sorolható fel a kritikus infrastruktúrák, és ezen belül a villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kapcsán, ugyanakkor nem feledkezhetünk meg azon sajátosságokról sem, melyek a bevezetés korlátait, de legalábbis sajátosságait jelentik majd. Ezen kézikönyvben talán nem szükséges hangsúlyozni, hogy milyen jelentőséggel bír a kritikus infrastruktúrák védelme, arra viszont mindenképpen érdemes kitérni, hogy mennyiben tűnik

[140] A bring your own device (BYOD), a Virtual Private Network (VPN) megoldások, a felhő alapú szoftvermegoldások széles körű elterjedése, a home office általános gyakorlattá válását követően.
[141] Az angol terminusban perimeter.

alkalmasnak a Zero Tust biztonsági modell, ugyanis az információs technológia (IT) területén elért eredmények az ipari rendszerek (OT) biztonsága esetén nem feltétlenül garantálják a sikert.

7.4.1. Minden adatforrás erőforrás

A Zero Trust biztonsági modell megköveteli, hogy kivétel nélkül minden adatforrást és szolgáltatást erőforrásnak tekintsünk még akkor is, ha a hálózat több eltérően klasszifikált biztonságú adatforrásból és szolgáltatásból áll. Gyakorlatilag ez azt jelenti, hogy a hálózatban lennie kell egy vagy több olyan pontnak, ahol minden hálózati forgalom áthalad, és ahol a házirend érvényesíthető (Policy Enforcement Point). A hálózat működésének fenntartásához elengedhetetlenül szükséges tehát, hogy tisztában legyünk azzal, hogy a hálózatunkban milyen adatforrások, illetve szolgáltatások vannak. Különösen fontos ez olyan környezetekben – mint amilyenek az OT rendszerek is –, ahol az adatforrások technológiailag heterogének[142] lehetnek, nehezítve ezzel az eszközök automatikus felderítését és számbavételét. Ugyanakkor meg kell jegyzeni, hogy ha nem is rendelkezünk egy minden adatforrást tartalmazó listával[143], úgy épp a Zero Trust elvek következetes alkalmazása vezethet el a szükséges információk teljes körének beszerzéséhez.



12. ábra: A Zero Trust hozzáférési modellje[144]

A Zero Trust biztonsági modell esetén nincs erőforrás-koncentráció, nincsenek határozott határvonalak, a hangsúly pedig a szolgáltatások elérésére, ezen belül is az adatforgalom útvonalaira tevődik a belépési pontok helyett. Mivel a számítógépes hálózatokban a forgalmi útvonalak teljeskörűen kontrollálhatók, a Zero Trust ezt tűzi ki elérendő célként az elmosódó hálózati határvonalak és az azokon megjelenő egyre több belépési pont ellenőrzése helyett. A megközelítés ugyanis, miszerint a belépési pontok védelme elégséges, és a megbízhatónak tekintett hálózatrészeken további ellenőrzésre nincs szükség, azzal a következménnyel jár,

[142] Egy adott OT hálózat – iparági, beszállítói, vagy épp történeti sajátosságok okán – egyidejűleg tartalmazhat meglehetősen eltérő kommunikációs technológiákat – soros vonali, Ethernet, vagy TCP/IP kommunikáció – alkalmazó eszközöket.
[143] Ennek egyik tipikus oka lehet az „árnyék IT" jelenléte, ami alatt hivatalosan nem létező szolgáltatások jelenlétét értjük hálózatunkban.
[144] Forrás: NIST Special Publication 800-207 – Zero Trust Architecture

hogy amennyiben a támadó a hálózat egy megbízhatónak tekintett részére képes bejutni[145], a hálózatban az oldalirányú mozgásának[146] a továbbiakban nincs korlátja. Ez különösen veszélyes OT területeken, ahol egyes hálózatrészek olyan eszközökből[147] állhatnak, melyek sem saját maguk, sem az általuk forgalmazott adatok védelméről nem képesek gondoskodni titkosítási és autentikációs képességek hiányában, és a korlátozottan rendelkezésre álló erőforrások mellett.

A megbízhatónak tekintett (belső) és a nem megbízhatónak tekintett (internet) hálózatrészek szegmentációja helyett a Zero Trust biztonsági modell elgondolása szerint a hálózatot a lehető legnagyobb mértékben szegmentálni kell, és ezeket a szegmenseket el kell választani egymástól. Ezen módszer a mikroszegmentáció, ami több mikrokörvonalat, vagy szegmenst hoz létre a hálózatban. Mivel a mikroszegmensek átlépése minden esetben valamilyen ellenőrzési ponton keresztül történik, itt hitelesítés és ehhez kapcsolódóan korlátozások vezethetők be. Az oldalirányú mozgás ezen környezetben tehát a továbbiakban nem kivitelezhető, mivel az már nem hierarchikus, nincsenek kiemelt jelentőségű erőforrások, minden erőforrást egyformán kezelnek, minden erőforráshoz való hozzáférést az erőforrás besorolásától függetlenül ellenőrzik. A szegmensek átjárhatósága, a korlátozatlan oldalirányú mozgás különösen aggályos, ha a belső hálózat – még ha elválasztás(ok)on keresztül is – de csatlakozik valamilyen kritikus rendszerhez. Ezen veszélyek enyhítését a további elvek betartása szintén szolgálja.

7.4.2. Minden kommunikáció titkosított

A biztonságos kommunikáció több szempontból is kiemelt fontosságú eleme a Zero Trust biztonsági modellnek. A titkosított kommunikáció egyszerre képes biztosítani a bizalmasságot, az integritást és a hitelességet.

- A *hitelesség* lehetővé teszi, hogy a kommunikáló felek egymást azonosítsák, ugyanakkor a központi döntéshozó eszköz (Policy Engine) számára is lehetővé válik a kommunikáció célpontjainak azonosítása. A Policy Engine ezután dönthet arról, hogy egy adott erőforráshoz adható-e hozzáférés a hitelesített kérelmező számára. Ezen döntés tényleges érvényesítése a Policy Enforcement Point eszközön történik meg.
- Az *integritás* biztosítja, hogy a kommunikációt a kommunikációs felek tudta nélkül megváltoztatni ne lehessen, ami lehetetlenné teszi az érzékeny adatok (pl.:

[145] Jelentheti ez bizonyos hálózatrészek (pl.: irodai, vagy terepen lévő hálózat) fizikai elérését, de logikai hálózatrészekbe (pl.: DMZ) való bejutást is.
[146] Az angol terminusban lateral movement.
[147] A programozható logikai vezérlők (PLC) szolgálhatnak erre pédául.

bankszámlaszám, kártyaszám, számlaösszeg) módosítását félrevezető információk hozzáadásával, vagy az eredeti tartalom egy részének törlésével, módosításával.

- A *bizalmasság* megakadályozza, hogy a passzív támadót abban, hogy a hálózat lehallgatása révén hitelesítési információkhoz, vagy más értékes, bizalmas adatokhoz jusson hozzá, amelyeket aztán egy aktív támadás során használhatna fel.

A bizalmasság, az integritás és a hitelesség következetes fenntartása nem csak a támadások elleni védekezésben, de azok utólagos vizsgálatában is komoly szerepet játszik, mivel a kompromittálódott eszközök könnyebben azonosíthatók hiteles adatok birtokában.

Az OT rendszerek esetén mind a bizalmasság, mind pedig az integritás kérdése kiemelt jelentőséggel bír. A bizalmasság kérdése nem csak az IT hálózatokban megszokott kockázatokat hordozza, miszerint a hitelesítéshez szükséges információk kompromittálódhatnak, de a passzív támadó hozzáférhet olyan vezérléssel összefüggő adatokhoz, amelyek önmagukban is kiemelten érzékeny adatok. Ilyenek lehetnek akár az irányított rendszerben mért értékek, azok időbeli lefolyása, a beavatkozási szintek értékei vagy a beavatkozások időpontjai és mértéke, melyekből a rendszer működésére, a folyamatokra vonatkozóan lehet értékes információkra szert tenni. Az integritás megőrzése szintén kulcsfontosságú, hiszen egy passzív megfigyelést követően aktív támadás hajtható végre a mért értek olyan módon történő meghamisításával, melyet integritás-ellenőrzés hiányában a megtámadott nem észlel. Elég csak a Stuxnet néven elhíresült biztonsági incidensre utalni, ahol az urándúsító centrifugák valós sebességét el kellett rejteni a monitorozó rendszer elől, amit az integritás kompromittálásával oldottak meg a támadók. Ugyanakkor természetesen a titkosítás implementációja során nem feledkezhetünk meg az általa okozott késleltetésről, különösen, ha mért értékek, vagy szabályozó utasítások továbbításáról van szó.

7.4.3. Munkamenet-alapú hozzáférés biztosítás

A Zero Trust alapelvei szerint az erőforrásokhoz való hozzáférés munkamenet-alapon történik. Mind a hitelesítés, mind az engedélyezés munkamenet-alapú, és a felhasználóknak ezt követően is csak a feladataik ellátásához feltétlenül szükséges hozzáférést biztosítja. A munkamenet-alapú megközelítés garantálja, hogy a jogosultságok megvonása a lehető legrövidebb időn belül érvényesül, mivel az erőforrásokhoz való hozzáférést adott esetben egy következő munkamenetben már nem, vagy nem ugyanazokkal a jogosultságokkal biztosítják, mint egy korábbiban. Ennek oka lehet egy incidens éppúgy, mint valamilyen szabályzat normál ügymenet szerinti módosulása, egy konkrét felhasználó jogosultságainak csökkentése, vagy akár a felhasználói fiók törlése munkaviszony megszűnésekor. Minden esetben fontos, hogy a jogosultságok megváltozása a lehető legrövidebb időn belül érvényre jusson, amelynek hatékony eszköze a munkamenet-alapú hozzáférés-biztosítás. Bár az IT rendszerek esetében sem lehet ennek az elvnek a fontosságát eléggé hangsúlyozni, a SCADA rendszereknél a lehető

legrövidebb határidőket kell tudnunk garantálni a jogosultságok helyes megállapításának tekintetében.

7.4.4. Szigorúan megkövetelt autentikáció és autorizáció

Ahogy erről a korábbiakban már szó esett, a Zero Trust biztonsági modell alapkoncepciója értelmében nem tehetünk megkülönböztetést azon az alapon, hogy egy erőforráshoz való hozzáférési kérelem a belső vagy a külső hálózatról érkezik-e. A hitelesítést és a jogosultságot mindig, minden hozzáférési kérelemnél ellenőrizni kell. Ugyanakkor felmerül a kérdés, hogy miként is azonosítható maga a felhasználó, hiszen a hitelesítési mechanizmusok csak valamilyen közvetett eszköz vagy módszer alkalmazásával vonnak le következtetéseket a felhasználó kilétére vonatkozóan. Az azonosításra szolgáló eszköz lehet például valami, amit a felhasználó tud[148], valami, ami a felhasználó birtokában van[149], vagy valami, ami a felhasználót jellemzi[150]. Ez persze feltételezi a tudás, a birtoklás vagy a jellemző kizárólagosságát is, vagyis azt, hogy az adott tudás, birtok vagy jellemző másnál nem lehet meg. Egyetlen tényező, például egy jelszó relatíve könnyen kompromittálódhat, de annak a valószínűsége már szignifikánsan kisebb, hogy több különböző típusú tényezőt egy támadó egyidejűleg sikeresen kompromittál. Ezen gondolatmenet mentén haladva pártolja a Zero Trust biztonsági modell a több faktoros hitelesítés minél szélesebb körű alkalmazását. Az OT rendszerek esetében azonban nem feledkezhetünk meg arról a tényezőről, hogy a kommunikáció jelentékeny része nem ember és gép, hanem gép és gép között zajlik. Ilyen esetekben az autentikáció során nem minden – az IT területeken a felhasználók azonosítása során megszokott és bevált – módszer alkalmazható, ugyanakkor számos más, a biztonsági követelményeknek maximálisan megfelelő, megoldás kínálkozik. A gép-gép kommunikáció további előnye, egyrészt, hogy kizárható az emberi tényező, másrészt, mivel a végpontok szabályozottak, alkalmazhatók a legmagasabb igényeket kielégítő módszerek és algoritmusok[151]. Megjegyzendő ugyanakkor, hogy az ember-gép kommunikáció viszonylatában is érdemes megkövetelni olyan kliensoldali szoftverek, illetve szoftververziók használatát, melyek támogatják a legmagasabb igényeket

[148] A tudásalapú felhasználói azonosítás legkézenfekvőbb példái a jelszavak, PIN-kódok, feloldó kódok, vagy minták.
[149] A birtokalapú felhasználói azonosítás történhet különböző technológiákat (NFC, Bluetooth, USB, smart card) alkalmazó token révén, amik önmagában is lehetnek tudás alapú (PIN kód),vagy biometrikus védelemmel ellátva.
[150] A biometrikus felhasználói azonosítás történhet a felhasználó számos tulajdonsága alapján, mint amilyen az ujjlenyomat, vagy az arc mintázata.
[151] Példaként lehet felhozni a forward secret, authenticated encryption, vagy éppen a post-quantum kriptográfiai eljárásokat.

kielégítő kriptográfiai eljárásokat. Ha ezeket szerver oldalon kötelezővé tesszük, rögtön kizárjuk azokat a támadásokat, melyeknél a támadó eszköz ezeket nem támogatja[152].

7.4.5. Hozzáférés dinamikus házirendek révén

A Zero Trust biztonsági modell esetében a felhasználó vagy az ügyfél azonosítása csak egy tényező a dinamikus irányelvekben. Az azonosítási folyamat a szervezet által a felhasználói fiókhoz rendelt egyéb kapcsolódó attribútumokat is magában foglalhatja. Ilyenek lehetnek a felhasználó által használt eszköz jellemzői, mint például a telepített szoftverek verziói, az operációs rendszer javítócsomagjainak telepítettsége, a felhasználó fizikai tartózkodási helye[153] vagy akár a kérés időpontja és dátuma. A viselkedési attribútumok[154] szintén mérhetők, és az eltérések összevethetők a megfigyelt használati mintákkal, mielőtt hozzáférést biztosítanánk egy vállalati erőforráshoz. Az erőforrás érzékenységének és besorolásának is változnia kell az erőforrás-hozzáférés feltételei szerint. Például bizonyos körülmények között csak olvasási hozzáférést adnak egy adott erőforráshoz, de további hitelesítés után – egy második vagy harmadik tényezővel –, írási és olvasási hozzáférés is biztosítható. Itt is ugyanazon elvek érvényesülnek, mint amiket a fizikai biztonság területén alkalmazunk, ahol a magasabb biztonsági besorolású helyszínre való belépés engedélyezését további vizsgálatok előzhetik meg. Így tehát mindezen attribútumok részét képezhetik a felhasználói személyazonosság ellenőrzésének, és részben vagy egészben meghatározhatják az alkalmazott házirendet is.

7.4.6. Erőforrások valósidejű nyomon követése

A Zero Trust biztonsági modell megköveteli a folyamatos diagnosztikai és kockázatmérséklő rendszer[155] (CDM) kiépítését és üzemeltetését. Mind a hálózat, mind pedig annak felhasználói kapcsán elengedhetetlen a biztonsággal összefüggő jellemzők aktuális állapotának ismerete, lévén akár a kliensek, akár a szerverek esetén korlátozásokra lehet szükség, amennyiben feltételezhető, hogy valamely biztonsági incidens során érintetté váltak. Például, ha egy eszköz olyan szolgáltatást futtat, ami távolról is kihasználható biztonsági hibával terhelt, és még nem érhető el hozzá javítás, akkor az érintett szolgáltatás hozzáférése kapcsán erőteljes korlátozások elrendelésére lehet szükség a kockázatok csökkentése érdekében mindaddig,

[152] Nem ritka, hogy a rosszindulatú szoftverek kriptográfiai képességei elmaradnak a kor elvárásaitól, és amennyiben csak és kizárólag a legújabb – egyúttal legbiztonságosabb – módszereket támogatjuk, a támadás már ezen a ponton meghiúsul.
[153] Fontos megjegyezni, hogy az ilyen típusú attribútumok felhasználása, akárcsak a biometrikus adatoké, fontos jogi kérdéseket vetnek fel, melyeket a bevezetés előtt át kell gondolni.
[154] Ilyen személyhez kötődő attribútum lehet a gépelés során a billentyűlenyomások késleltetése, illetve a késleltetés ingadozása, az egérmozgások mintázatai.
[155] Az angol terminusban Continuous Diagnostics and Mitigation (CDM).

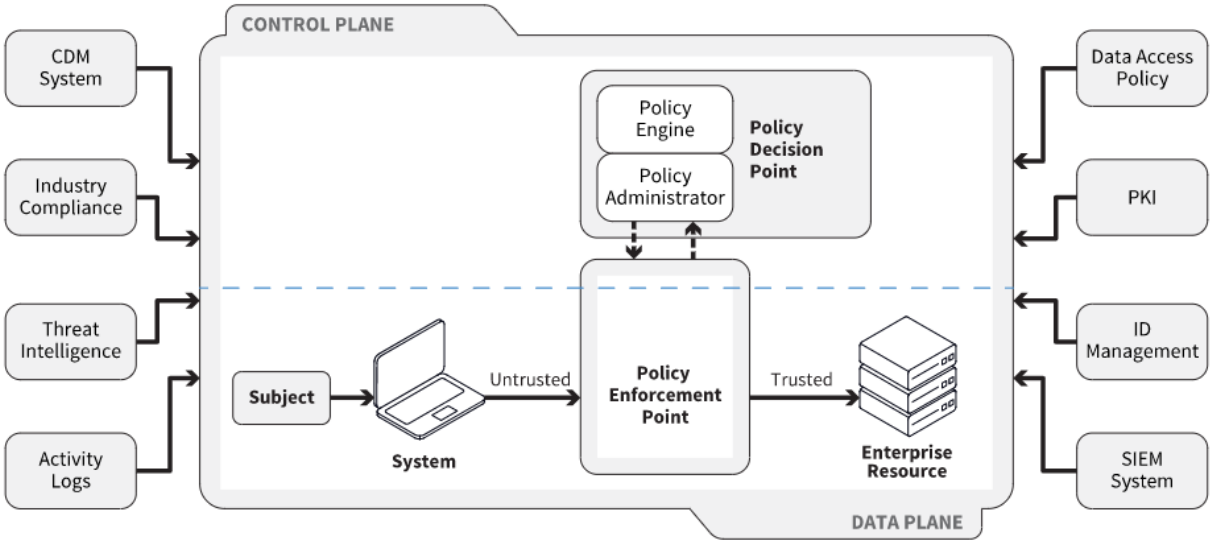
amíg a biztonsági hibában érintett szolgáltatást ki nem javítják. Természetesen ehhez elengedhetetlen, hogy a szervezet rendelkezzen azzal az információval, hogy érintettek valamilyen biztonsági problémában. Ezen érintettségi információk például CDM-rendszerekből származhatnak, és a biztonsági állapotok megváltozása a korábban említett dinamikus házirendek megváltoztatását vonhatja maga után.

Egy új eszköz megjelenése a hálózaton tipikusan olyan szituáció, ami jól rávilágít a monitorozás nélkülözhetetlenségére, hiszen a monitorozás teszi lehetővé, hogy egy, a privát hálózatunkban megjelenő eszközről tudomást szerezzünk. Ez kiemelt jelentőséggel bír azokban a környezetekben, ahol kritikus infrastruktúrák védelméről, vagy más kiemelt biztonságú hálózatról beszélünk, lévén itt egy új eszköz váratlan megjelenése és aktív kommunikációja nem életszerű, könnyen utalhat a hálózat illegitim használatára, de akár egy biztonsági incidensre is. A Zero Trust biztonsági modell maga is megköveteli, hogy ne bízzunk egy a hálózatra csatlakoztatott eszközben csupán azért, mert az a privát hálózatunkon belül van. Az újonnan megjelenő eszköz hálózati forgalmára mindenképp alkalmaznunk kell valamilyen szabály(oka)t, ami valószínűleg a teljes tiltást jelenti. Ugyanakkor az életszerű működés lehet, hogy bizonyos útvonalakat biztosítani kell egy újólag megjelenő eszköz számára. Például lehetővé kell tenni, hogy az eszközt a felhasználója regisztrálni tudja a hálózaton, különösen, ha valamilyen mobil, vagy saját tulajdonú eszközről van szó, amely a hálózatnak csak egy erősen korlátozott részét tudja elérni, azt is korlátozott jogosultságok mellett.

Még ha egy eszköz legitimnek is tekinthető a hálózaton, az általa generált hálózati forgalmat akkor is figyelni, szabályozni, elemezni és naplózni kell. Egy esetleges incidens kezelésének részeként ugyanis a vizsgálat során minden információra szükségünk lehet a felderítéshez. Már az incidens bekövetkezte előtt lehetnek ugyanis gyanúra okot adó jelek: ilyen lehet például az erőforrás-hozzáférésekben beálló változás, ami előre jelezheti magát az incidenst is. Ilyen változás lehet – egyebek mellett – a magasabb szintű jogosultság kérése egy erőforrás-hozzáférés során, írási engedély kérése olvasási engedély helyett, vagy éppen egy szokatlan helyről[156], szokatlan időpontban[157] érkező kérés, vagy egy olyan minta megjelenése, ami a hálózat felderítési kísérletére, ezen keresztül pedig rosszindulatú szoftverek jelenlétére utalhat. Ezen események mind bemenetéül szolgálhatnak egy CDM-rendszernek, melynek következménye lehet az eszköz átmeneti karanténba helyezése, megakadályozandó a rosszindulatú szoftver terjedését.

A Zero Trust biztonsági modell alapvető logikai komponensei a fentiek ismeretében a következőképp rajzolhatók fel.

[156] Például egy külföldi országból, amellyel a szervezetnek nincs kapcsolata.
[157] Például éjfélkor, ha az adott kolléga munkarendje szerint 9-től 5-ig dolgozik.



13. ábra: A Zero Trust modell alapvető logikai komponensei[158]

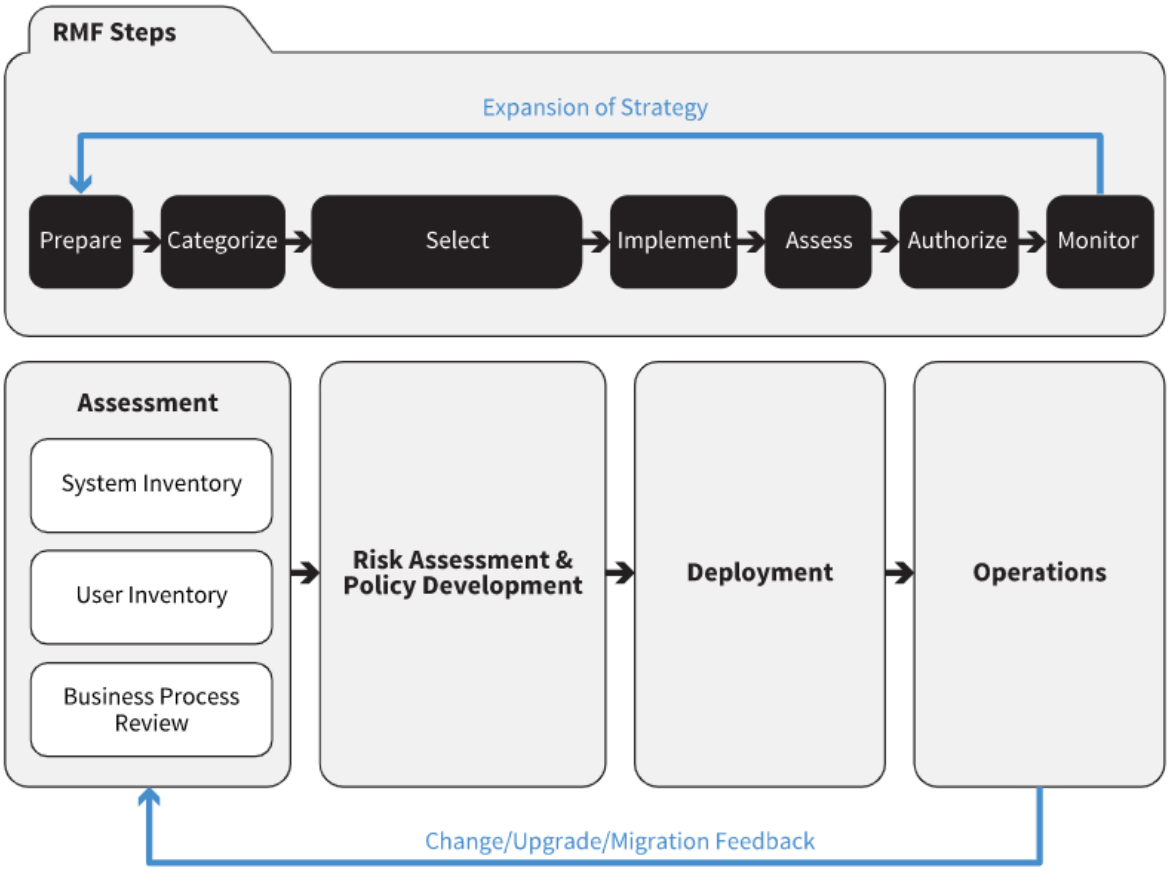
7.4.7. A modell bevezetése

Nem feledkezhetünk meg arról az igen komoly jelentőséggel bíró sajátosságról, hogy a fent ismertetett modell – mint bármely biztonsági modell – önmagában bármennyire működőképesnek tűnik is, egy adott szervezeten belül annyira tud működőképes lenni, amennyire azt a bevezetés előkészítése, maga a bevezetés, és később a folyamatos karbantartás hatékonysága lehetővé teszi. Ezekben a technikai megfontolásokon túl számos emberi tényező játszik szerepet, melyek adott esetben konfliktusos helyzetek feloldását kívánják meg. Példaként hozható fel a korábban említett „árnyék IT" jelenléte, mivel amikor elkezdjük betartatni a Zero Trust biztonsági modell alapelveit, ellehetetlenül az „árnyék IT" működése. Ennek oka, hogy a minden erőforrás alapelvének megfelelően minden szervezeti erőforrásról tudomással kell bírnunk, vagyis a továbbiakban nem lehetnek „árnyékban" egyes szolgáltatások. Igaz ez már csak azért is, mivel a minden erőforrás elvén túl a mikroszegmentáció, a legkisebb jogosultság, elveinek gyakorlatba való átültetése és a monitorozás is ellehetetleníti az „árnyékban" való működést.

A „árnyék" tevékenység felszámolása természetesen kívánatos biztonsági szempontból, egyúttal azonban azt is jelenti, hogy szembesülnünk kell a szervezetben jelen lévő hibákkal, hiányosságokkal. Adott esetben nem a tevékenység a problémás, mivel az maga a szervezet szempontjából hasznos és szükséges, hanem annak az „árnyék" mivolta. Tehát nem az öntevékeny embereket kell korlátozni, hanem a modell bevezetésének feltételeit kell megteremteni, ami viszont jelentékeny – előre nehezen felmérhető – költségekkel járhat mind az emberi, mind pedig a technikai erőforrások tekintetében. Ez már akkor is könnyen

158 NIST Special Publication 800-207 – Zero Trust Architecture

belátható, ha csak az első, de talán legfontosabb lépésre, az erőforrások, az adatvagyon és a felhasználók számbavételére és klasszifikációjára, a folyamatok megismerésére gondolunk.



14. ábra: A Zero Trust modell folyamatos fejlesztési ciklusa[159]

A Zero Trust érettségi modell[160] számol ezzel a tényezővel, és hatékony iránymutatást nyújt mindazoknak, akik a bevezetését komolyan fontolóra vették, illetve abba már bele is kezdtek. Az érettségi modell öt pillért,

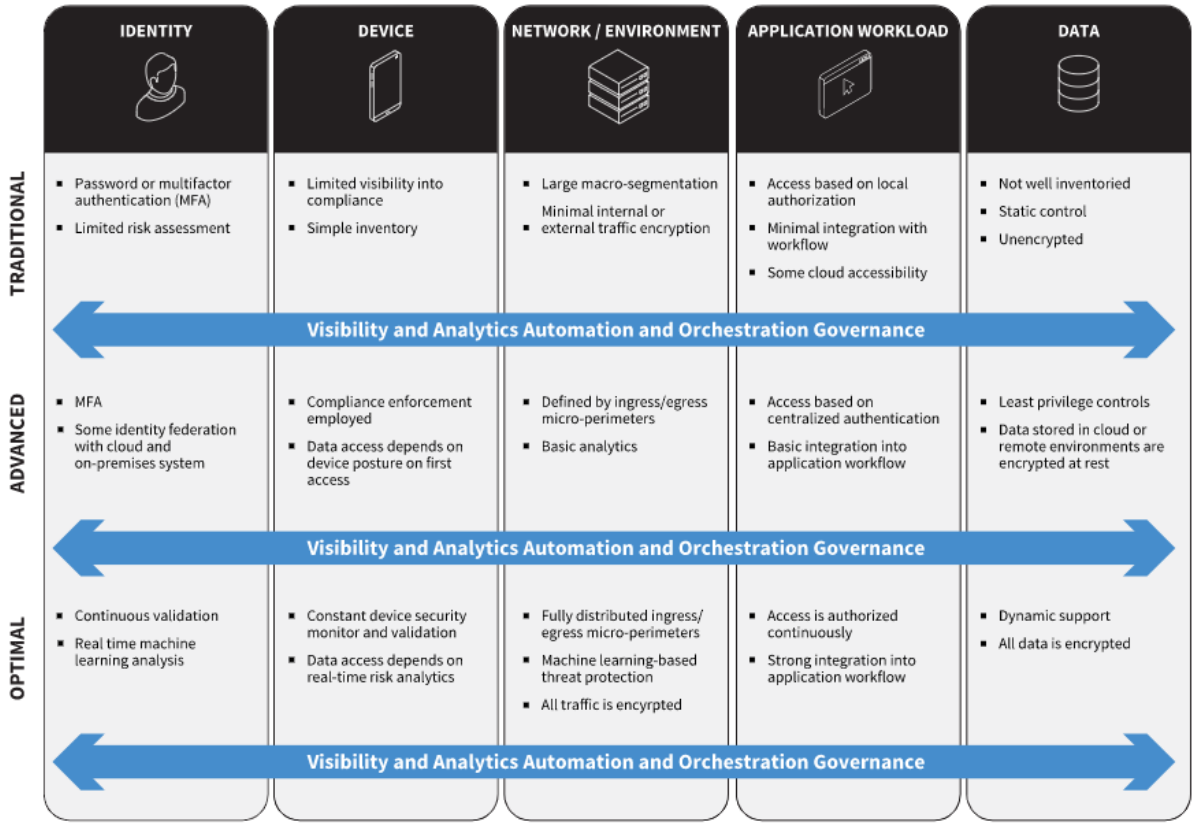
1. identitás (identity)
2. eszköz (device)
3. házlózat (network)
4. alkalmazások (application workload)
5. adat (data)

159 NIST Special Publication 800-207 – Zero Trust Architecture
160 CISA Zero Trust Maturity Model

illetve három érettségi szintet határoz meg,

1. tradicionális (traditional) – alapvetően manuális konfigurációt, statikus biztonsági házirendet, illetve manuális incidenskezelést jelent
2. haladó (advanced) – pillérek között megjelenő koordinációt, központosított hozzáférés- és jogosultságkezelést, az előre meghatározott kockázatcsökkentési módszerek alkalmazását, a legkisebb jogosultság elvének megjelenését jelent
3. optimális (optimal) – a pillérek közötti együttműködést, az ezek alapján magvalósuló dinamikus házirendeket, a legkisebb jogosultság elvének küszöbértékekkel meghatározott megvalósulását jelenti.

Ezek kapcsán magas szintű elvárásokat fogalmaz meg. A legelső lépéseknek – a már említett állapotfelmérésen túl – a különböző területeken meglévő kockázatok felmérése tekintendő. Az azonnali cselekvési tervek kidolgozása során a vezérlő elv a legnagyobb kockázatok mielőbbi csökkentése, a legégetőbb elmaradások felszámolása, az egyen-szilárdság megteremtése, a különböző területeken elérni kívánatos érettségi szint meghatározása lehet.



15. ábra: A Zero Trust érettségi modell magas-szintű koncepciója[161]

[161] Forrás: Zero Trust Maturity Model

Látható, hogy az optimális érettségi szint elérése komoly erőfeszítéseket kíván a legtöbb szervezettől, egyetlen lépésben szinte biztosan nem érhető el. De ha még elérhető is lenne, a Zero Trust biztonsági modell folyamatos felügyeletet és fejlesztést kíván meg. Mind a bevezetés, mind pedig a folyamatos fejlesztés során érdemes szem előtt tartani, hogy a Zero Trust nem a felhasználóval szembeni zéró bizalmat, hanem a feltételezésekkel szembeni zéró toleranciát jelenti. A Zero Trust nem a legitim szolgéltatás elérések ellehetetlenítésére, hanem a hozzáférések legitim mivoltának garantálására szolág és mint nem bizalomhiányt, hanem tényekre alapozott döntéshozatalt jelen, nem a felhasználó ellen, hanem azzal együttműködve kell történjen.

7.4.8. A Zero Trust modell OT relevanciája

A Zero Trust biztonsági modell kapcsán fontos hangsúlyozni – ahogy azt korábban is megtettük –, hogy nem egy teljességgel új metodológiáról, vagy épp egy divathullámról beszélünk, hanem olyan alapelvekről, melyek az IT területeken – még ha nem is ezen a néven – már évtizedek óta léteznek és bizonyítottak és melyek koherens egésszé való összesítése, de még inkább ezen névvel nevezett és dokumentál egész népszerűvé válása történik az elmúlt években. Maguk az elvek egyáltalában nem kizárólagosak az IT területekre, az OT területeken, vagy akár a fizikai biztonság területén ugyanúgy megállják a helyüket, természetesen az értelmezhetőség korlátai mellett. Mivel

1. maga az OT területeken alkalmazott szoftverrendszerek – értve ezalatt az irányítási és menedzsment szoftverrendszereit – gyakorlatilag IT rendszereknek tekinthetőek,
2. az OT-ben alkalmazott hardveres és hálózati megoldások egyre nagyobb arányban az IT világában alkalmazottak közül származnak[162], vagy ahhoz hasonlók,
3. az IT és az OT rendszerek határvonalai – mint általánosságban is a hálózati határvonalak – egyre inkább elmosódnak,

ezért a különbségek egyre kisebbé válnak az elvi megfontolások és koncepciók szintjén mindenképpen. Már csak ennek okán is elmondható, hogy az IT alapkoncepciók megállják a helyüket az OT területeken, még ha a megvalósítás szintjén számottevő különbségek állnak is fent.

Az IT és az OT világ nem csak a technikai megvalósításban közeledik egymáshoz, hanem a velük szemben megfogalmazott felhasználói és vezetői igények szintjén is. Az olyan – az OT területeken korábban kevésbé mindennapos igények –, mint az adatokhoz való távoli hozzáférésnek, vagy a rendszerek távolról való menedzselésének, frissítésének az igénye az

[162] Példaként hozható azt OT területeken a védelmi és mérő eszközök sorában egyaránt egyre nagyobb számban megjelenő PC alapú megoldások, vagy korábban alig alkalmazott TCP/IP alapú kommunikáció térhódítása.

IT területeken teljesen köznapinak számítanak, és azok kihívásaira megszülettek a megfelelő válaszok. Az OT területek a fenti igények megjelenésével olyan változásokon mennek keresztül, melyek nem csak az IT területek eszközeinek – és remélhetőleg kényelmének – egyre nagyobb arányú megjelenését hozzák magukkal, de azon kockázatokat is, amikkel az IT már évtizedes tapasztalatot szerzett. Az OT területek a biztonsági technológiák területén esetlegesen meglévő hátrányukat úgy fordíthatják előnyükre, hogy alkalmazzák az IT területeken számos kudarc révén megszerzett tapasztalatot. Erre kiválóan alkalmas lehet a Zero Trust biztonsági modell.

Energetikai, informatikai és kiberbiztonsági fogalmak, rövidítések jegyzéke

Fogalom, rövidítés	Kifejtés	Magyar megnevezés
2FA	Two Factor Authentication	Két faktoros azonosítás
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
ARP	Address Resolution Protocol	Címfeloldási protokoll
ARP spoofing/poisoning	-	ARP táblában található MAC-címek módosításán alapuló támadási forma
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
BCP	Business Continuity Plan	Üzletmenetfolytonossági terv
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, távvezérelt eszközök hálózata
BYOD	Bring Your Own Device	„Hozd be a saját eszközöd” – saját tulajdonú IT eszközök munkavégzés céljából történő használata
CC	Common Criteria	Informatikai eszközök és rendszerek biztonsági értékelését - közös szempontok alapján - szabályozó szabvány.
CCF	Common Cause Failure	Közös hibaok miatti meghibásodás
Censys	-	Internetre csatlakoztatott – egyebek mellett ipari – rendszerek és eszközök keresőfelülete (lásd még: Shodan)
CER	Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities	Az Európai Parlament és a Tanács irányelve a kritikus fontosságú szervezetek rezilienciájáról (TERVEZET!)
CERT	Computer Emergency Response Team. Computer Emergency Readiness Team (US)	Eseménykezelő Központ
CIA	Confidentiality, Integrity, Availability	Bizalmasság, sértetlenség, Rendelkezésre állás (OT rendszerek esetében jellemzően fordított fontossági sorrendben)
CIP	Critical Infrastructure Protection	Kritikus infrastruktúravédelem
CISA	Cybersecurity and Infrastructure Security Agency	Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség
CISO	Chief Information Security Officer	Információbiztonsági vezető
CMF	Common Mode Failure	Közös hibamódú meghibásodás
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.

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.
CSIRT	Computer Security Incident Response Team (EU)	Számítógép-biztonsági incidenskezelő csoport
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 kitettségek
DC	Direct Current	Egyenáram
DCS	Distributed Control System	Osztott intelligenciájú folyamatirányító rendszer
DDoS	Distributed Denial-of-Service	Elosztott, szolgáltatásmegtagadással járó támadás
DiD	Defense in depth	Mélységi védelem / mélységben tagolt védelem
Defacing támadás	-	Webtartalom engedély nélküli módosítása
DHCP	Dynamic Host Configuration Protocol	Dinamikus állomáskonfiguráló protokoll
DLP	Data Loss Prevention	Adatszivárgás-megelőzés (elleni védelem)
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
DRP	Disaster Recovery Plan	Katasztrófa utáni helyreállítási terv
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, authentikációs szerverek és logmenedzsment megoldások)
EDR	Endpoint Detection and Response	Végpontvédelmi- és elhárítási technológia
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 Uniós 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 rekonstruálása
GPRS	General Packet Radio Service	Csomagkapcsolt, IP-alapú rádiós adatátviteli technológia
GPU	Graphical Processing Unit	Grafikus processzor
Graded approach	-	Fokozatosság elve
Hash	-	Lenyomat (előírás szerint képzett bitsorozat)
HIDS	Host Based Intrusion Detection System	Host alapú behatolás észlelő rendszer
HMI	Human Machine Interface	Ember-gép kapcsolati felület
Honeypot	-	Támadók megtévesztésére, elemzésére szolgáló csali (mézesbödön) informatikai környezet

Honeypot farm	-	Rosszindulatú kódok algoritmusok elfogására szolgáló csali számítógép „farm”
HSR	Highly-available Seamless Redundancy	Nagy megbízhatóságú, fürtös elvű protokoll
I&C	Instrumentation and Control	Irányítástechnika
IBIR	-	Információbiztonsági irányítási rendszer
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
ISMS	Information Security Management System	Információbiztonsági irányítási rendszer
IT	Information Technology	Információs technológia
JTAG	Joint Test Action Group	Áramkörvizsgálati módszerekkel foglalkozó szakmai szervezet, illetve az IEEE-1149.1 szabvány által meghatározott módszer az integrált áramköri lapok/rendszerek gyors és automatikus tesztelésére
KDSZ	-	Körzeti 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 kiberteret 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
Least Privilige	-	Legkisebb jogosultság elve: Törekedni kell arra, hogy minden felhasználó, program, alkalmazás csak a funkciója ellátásához feltétlenül szükséges (ilyen értelemben tehát minimális) hozzáférési jogosultsággal rendelkezzen
Legacy eszköz/rendszer	-	Legacy eszközök, rendszerek azok, melyek cseréje/korszerűsítése nem megvalósítható és ennél fogva képtelenek a folyamatosan változó/fejlődő/aktuális biztonsági elvárásoknak

		megfelelni és ezen képességbeli hiányuk biztonsági kockázatot eredményez.
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 TAXXI.
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 értékből IEC 61850 szabványnak megfelelő értéket előállító mérő eszköz
MFA	Multi-factor Authentication	Több faktoros azonosítás
MISP	Malware Information Sharing Platform	Rosszindulatú alkalmazásokkal kapcsolatos információmegosztó felület
MiniDuke	-	Adobe Reader sérülékenységet kihasználó rosszindulatú alkalmazás vagy kód
MitM	Man-in-the-Middle	Közbeékelődéses támadás
MITRE ATT&CK™ Framework	MITTRE Adversarial Tactics, Techniques, and Common Knowledge Framework	Fenyegetettségek azonosításához és a védelmi hiányosságok feltárásához használható, támadói taktikákat, technikákat és folyamatokat bemutató keretrendszer
Modbus	-	Ipari környezetben alkalmazott adatkommunikációs protokoll
Need to know	-	Szükséges ismeret elve: Törekedni kell arra, hogy a felhasználók csak a szerepkörük és feladataik ellátásához szükséges és elégséges ismeretekkel rendelkezzenek.
NES	-	Nemzeti Energiastratégia
NIDS	Network Based Intrusion Detection System	Hálózat alapú behatolás észlelő rendszer
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
NIS 2	Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148	Javaslat Az Európai Parlament és a Tanács Irányelve az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről
NIST	National Institute of Standards and Technology	Nemzeti Szabványügyi és Technológiai Intézet (USA)
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 távvezetéki 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
OT	Operational Technology	Operatív/üzemeltetési technológia
OWASP	Open Web Application Security Project	Webes alkalmazások és az alkalmazásfejlesztés biztonságával foglalkozó szakmai szervezet, közösség.
Patch/patch-elés	-	Javítócsomag/szoftverfrissítés
Payload	-	Csomagtartalom (adatcsomag üzenet része)
PCA	Protected Cyber Asset	Eszköz, ami routolható protokollon keresztül kapcsolódik a rendszerhez
PCS	Process Control System	Folyamat irányító rendszer
Pentest	Penetration testing	Sérülékenységvizsgálat
Perzisztencia	-	Hozzáférés tartós fenntartása
PDCA	Plan, Do, Check, Act	Termékek és folyamatok kontrolljára és folyamatos fejlesztésére használt ciklus. Lépései: Tervezd meg, csináld meg, ellenőrizd, avatkozz be!
Phishing	-	Adathalászat
PKI	Public Key Infrastructure	Nyilvános kulcsú infrastruktúra
PLC	Programmable Logic Controller	programozható logikai vezérlő
PreDeCo	Preventív, Detektív, Korrektív	Megelőző, detektáló és javító kontrollokra épülő védelemtervezési elv
Privilege escalation	-	Jogosultsági szint emelés
PRP	Parallel Redundacy Protocol	Párhuzamos redundancia elvű adatgyűjtő protokoll
PTP	Precision Time Protocol	IEC 1588-2008 szabvány által definiált időfelbontás és szinkronizációs elv
Ransomware	-	Zsarolóvírus
RAT	Remote Access Tool	Távoli hozzáférést biztosító program/kód
RBAC	Role-Based Access Control	szerepkör alapú hozzáférés-kezelés
Resilience	-	Ellenálló képesség
RKR	-	Rotációs Kikapcsolási Rend
Root	-	Gyökér könyvtár. Korlátlan jogosultságú rendszerfelhasználó.
Rootkit	-	Saját és más programok jelentését elrejteni képes, rosszindulatú kód
RSTP	Rapid Spanning Tree Protocol	Gyors hasítófa protokoll a hálózati hurok és redundáns útvonalak kezelésére
RTá	-	Rendelkezésre álló állandó teljesítőképesség
RTU	Remote Terminal Unit	Telemechanikai alközpont
Sandbox	-	„Homokozó”, ellenőrizetlen forrásból származó állományok vizsgálatára szolgáló, elszeparált IT környezet
SCADA	Supervisory Control and Data Acquisition	Felügyeleti irányítás és adatgyűjtés
SeConSys	Security of Control Systems	Ipari Irányítástechnikai Rendszerek Biztonsága
Secure by design	-	Védettségre való tervezés elve: Már a tervezés során törekedni kell arra, hogy a választott technológia, az alkalmazott eszközök és megoldások minden eleme a védelem legmagasabb szintjének elérése irányába hasson.
SDN	Software Defined Networking	Szoftveresen meghatározott hálózatok

Shell	-	Parancssori felület, parancsértelmező
Script kiddie	-	Komoly szaktudással nem rendelkező kezdő hacker
Side-channel	-	Az infokommunikációs rendszer nem tervezett működéséből fakadó – fizikai-, vagy logikai síkon információ szivárgáshoz vezető – implementációs hiba
Shodan	-	Internetre csatlakoztatott – egyebek mellett ipari – rendszerek és eszközök keresőfelülete (lásd még: Censys)
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
Sniffing	-	Hálózati lehallgatás
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	-	Az emberi tényezőket kihasználó, a pszichológiai befolyásolás, félrevezetés és megtévesztés módszerein alapuló támadások gyűjtőfogalma
SPAN	Switched Port Analyser	Port forgalom figyelése, tükrözése, monitorozása
Spear-phishing	-	Célzott adathalászat, konkrét személy/szervezet ellen
SPI	Stateful Packet Inspection	Állapotfüggő csomagfelügyelet
SQLi	SQL injection	SQL kód befecskendezéssel végrehajtott támadás
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 volt hivatott védelmet biztosítani. Ma már a gyakorlatban nem használatos, a helyét a TLS protokol vette át.
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
Threat landscape	-	Fenyegetettség térkép
TI	Threat Intelliegence	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
TTP	Tactics, Techniques and Procedures	Taktikák, technikák és eljárások

Tűzfal	Firewall	Hálózati forgalom engedélyezésére vagy blokkolására szolgáló eszköz az informatikai hálózatokban.
XSS	Cross-site Scripting	Weboldalak, webalalmazások sebezhetőségét rosszindulatú kód befecskendezédével kihasználó támadási forma
Yara	-	Rosszindulatú programok kutatásában és felismerésében használt eszköz
UBA	User Behavior Analytics	Felhasználói viselkedés elemzés
UP KRITIS	Public-Private cooperation in Critical Infrastructure Protection	Köz- és magánszféra együttműködése a kritikus infrastruktúrák védelme terén
UPS	Uninterruptible Power Supply	Szünetmentes áramelletás
URH	-	Ultrarövid hullám (nyílt rádiós jelátviteli technológia)
ÜKE jelzés	-	Üzemkészség jelzés
VPN	Virtual Private Network	Virtuális magánhálózat
WAF	Web Application Firewall	Webalkalmazás-szintű tűzfal
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
ZTA	Zero Trust Architecture	A nulla megbízhatóságon alapuló architektúra

Ábrajegyzék

Mellékletek ábrái:

Táblázatjegyzék

Mellékletek

1. melléklet: Incidens katalógus (2022. decemberi állapot)

Jelmagyarázat: *Korábi, újként bekerült incidens* | *Pontosítás* | *Legutóbbi incidensek*

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
1	Sellafield Nuclear Plant	UK	1991	Számítógépes hiba miatt a reaktortér egyik kamrájának árnyékoló ajtajai nyitva maradtak, miközben súlyosan radióaktív anyagok voltak a kamrában	Nem ismert	Pontosan nem ismert	A létesítmény működését leállították az incidens kivizsgálásának idejére. Személyi sérülést a sugárzás nem okozott.	https://www.risidata.com/Database/Detail/computer-error-at-sellafield-nuclear-plant-in-uk
2	Ignalina Power Reactor Station	Litvánia	1992	Oleg Savchuk, az litván Ignalina Power Reactor Station programozója számítógépes vírust töltött fel a reaktor egyik számítógépébe, ezzel próbálva szabotálni az atomerőmű működését.	Belső támadó szándékos szabotázsa	Reaktorvezérlő számítógép	Az érintett reaktor leállításra került (jelentések szerint nema vírus miatt) Oleg Savchuk-ot szabotázsért letartóztatták.	https://www.risidata.com/Database/Detail/computer_sabotage_at_nuclear_power_plant
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
4	Auckland, NZ áramszünet	Auckland, Új-Zéland	1998	1998 február-márciusában 5 hétig voltak üzemzavarok az Új-zélandi Auckland áramszolgáltatásában. Egyes források (UK GCHQ) szerint az incidens hátterében a magát "Anti-Christ Doom Squad"-nak nevező csoport kibertámadásai állnak.	Részleteiben nem ismert	DSO SCADA rendszer	5 héten át voltak kiterjedt áramszünetek Auckland egyes részein	https://www.risidata.com/Database/Detail/hackers-attack-nz-aust-for-joining-gulf-taskforce
5	Dr. Chaos szabotázs	Wisconsin, USA	1999	Joseph D. Konopka ("Dr. Chaos"), egy korábbi rendszergazda illegális hozzáférésekkel okozott áramszüneteket és egyéb szolgáltatás-kimaradásokat Wisconsin államban	Nem ismert	Nem ismert	28 áramkimaradás és 20 egyéb szolgáltatás-kimaradás, amik összesen kb. 800.000 USD kárt okoztak Wisconsin állam 13 megyéjében	https://www.risidata.com/Database/Detail/power_outages_and_other_service_interruptions
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 g0eneráltak, ami zavart okozott a San Diego megyei vízmű és a San Diego-i gáz- és elektromos művek ICS rendszereiben használt távkezelt 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

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
7	Y2K teszt nukleáris reaktorban	USA	1999	A reaktor szabályozó rúdjainak vezérléséért felelős számítógépen végzett Y2K tesztek során a vezénylő egyes számítógépeink monitorjai elsötétültek. A helyreállítás szakaszosan történt, emiatt az incidens-elhárítás 7 órán át tartott.	Nem szándékos emberi hiba	Reaktorvezérlő számítógép	Loss of control, loss of view	https://www.risidata.com/Database/Detail/y2k-test-crashes-reactor-computer
3	CA ISO	USA, Califiornia	2001	2001-ben a kaliforniai független villamosenergia-ipari rendszerirányító IT rendszereit érte támadás. A támadók két, nem megfelelően tűzfalazott és Internetről elérhető webszerver kompromittálásán keresztül fértek hozzá a rendszerirányító belső hálózatához. Az incidens kiváltó okaként alapvetően a nem kellően biztonságtudatos tervezést és kivitelezést tartják, illetve az időkritikus üzleti folyamatok biztonságos működés fölé emelt prioritását	Nem megfelelően szegmentált hálózat, gyenge biztonsági intézkedések Internetről elérhető webszerverek 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
9	Utility SCADA System	USA	2001	Egy meg nem nevezett amerikai villamosenergia-ipari cég engedélyezte egy szerződéses partnerének, hogy VPN-kapcsolatot építsen ki a SCADA rendszerükkel. A VPN-kapcsolat a tervezettnél sokkal nagyobb mértékű kitettséget teremtett az Internet irányából, amit egy támadó ki is használt, ezzel jelentős anyagi veszteséget okozva a vállalatnak, bár a villamosenergia-ellátás biztonságára az incidens nem volt hatással. Az incidens okozta károk helyreállításához 4 emberhónapnyi munkára volt szükség. A cég nem jelentette az incidenst a felügyeleti szerveknek - nem volt ilyen kötelezettségük, mivel az incidens nem érintette a villamosenergia-ellátást.	Rosszul konfigurált VPN-hozzáférés a SCADA rendszerhez	SCADA rendszer	Pénzügyi veszteség, a villamosenergia-ellátásra nem volt hatása az incidensnek	https://www.risidata.com/Database/Detail/utility-scada-system-attacked
10	Slammer-féreg a vezénylői SQL szerveren	USA	2003	Egy meg nem nevezett amerikai villamosenergia-ipari cég vezénylői hálózatában futó SQL szerverre a hiányzó patch-ek miatt bejutott a Slammer-féreg egy példánya, ami végül egy belső VPN-csatornán keresztül utat talált a SCADA rendszer hálózatába is és blokkolni tudta a SCADA rendszer kommunikációját.	Nem patchelt vezénylői SQL szerver	SCADA	A Slammer-féreg blokkolta a SCADA rendszer kommunikációját, további részletek nem ismertek.	https://www.risidata.com/Database/Detail/power-industry-slammer-1

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
11	Slammer-féreg egy frame relay hálózaton	USA	2003	Egy meg nem nevezett amerikai villamosenergia-ipari cég SCADA rendszer egy frame-relay hálózatot használt kommunikációra, ami egyéb rendszerek kommunikációját is biztosította Asynchronous Transfer Mode (ATM) használatával. A Slammer-féreg támadása miatt az ATM sávszélessége elégtelennek bizonyult a SCADA rendszer megbízható működése szempontjából.	Nem megfelelően tervezett hálózati szolgáltatások a SCADA rendszer számára	SCADA	SCADA kommunikáció elvesztése	https://www.risidata.com/Database/Detail/power-industry-slammer-2
12	Slammer-féreg az Ohio-i atomerőműben	USA	2003	2003.01.25-én az Ohio állambeli Davis-Besse atomerőmű egyik MS-SQL 2000 szerverét fertőzte meg a Slammer-féreg. A fertőzés hatására a hálózati kommunikáció ellehetetlenült.	Nem megfelelő tűzfalszabály-beállítások	Folyamatirányító és safety rendszerek	A számítógépes feldolgozási sebesség lassulása miatt 16:50-re a Safety Parameter Display System elérhetetlenné vált összesen 4 óra 50 perc időtartamra 17:13-ra az üzem folyamatvezérlő számítógépe is elérhetetlenné vált, összesen 6 óra 9 perc időtartamra. Az elveszített rendszerek ugyanakkor a folyamatirányítási és védelmi funkciókban nem okoztak jelentős degradációt.	https://www.risidata.com/Database/Detail/slammer-impact-on-ohio-nuclear-plant
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	Nem ismert	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
14	Iráni kibertámadások az izraeli villamosenergia-rendszer ellen	Izrael	2003	Feltételezések szerint iráni támadók (egyes források szerint iráni egyetemisták részvételével) vírus- és DoS-támadásokat intéztek az Israel Electric Corporation rendszerei ellen.	Vírusos állományok és túlterheléses (DoS) támadások	Nem ismert	A rendelkezésre álló információk szerint a támadások nem okoztak fennakadásokat.	https://www.risidata.com/Database/Detail/iranian-hackers-attempt-to-disrupt-israel-power-system
15	Vírustámadás európai elosztóhálózati rendszerek ellen	Európa	2003	Egy közelebbről meg nem nevezett európai áramszolgáltató elosztóhálózati SCADA rendszerét érte vírustámadás, aminek következtében a vezénylői operátorok 3 napra elvesztették a felügyeleti képességeiket számos alállomásukon. Az áramszolgáltató munkatársainak 40 emberhétnyi munkába került helyreállítaniuk az érintett rendszerek működését (egy 4 naptári hetet felölelő időszakban).	Vírusos állomány jutott be az áramszolgáltató SCADA rendszerébe.	Elosztóhálózati SCADA rendszer	Loss of view (3 nap)	https://www.risidata.com/Database/Detail/virus-attacks-a-european-utility
16	Vírustámadás operátori munkaállomások ellen	USA	2004	W32/Korgo vírustámadás érte egy meg nem nevezett amerikai szervezet SCADA rendszerének operátori munkaállomásait és egy, a vállalati hálózaton található terminálját.	Hiányzó patch-ek és antivírus szoftver	SCADA rendszer	SCADA operátori munkaállomások elvesztése 1 óra 45 percre.	https://www.risidata.com/Database/Detail/scada-workstation-infected-by-w32-korgo-worm
17	Optikai kábelvágás Arkansasban	USA	2005	Az Arkansas Nuclear One egyes rendszerei (ERCS, END, Health Physics Network) átmenetileg nem működtek, miután Russelville-től keletre több optikai kábelt vágtak át véletlenül.	Nem szándékos emberi hiba	ERCS, END, Health Physics Network	Az érintett rendszerek átmenetileg működésképtelenné váltak.	https://www.risidata.com/Database/Detail/offsite-fiber-cable-cut-causes-loss-of-communications

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
17	Optikai kábelvágás Arkansasban	USA	2005	Az Arkansas Nuclear One egyes rendszerei (ERCS, END, Health Physics Network) átmenetileg nem működtek, miután Russelville-től keletre több optikai kábelt vágtak át véletlenül.	Nem szándékos emberi hiba	ERCS, END, Health Physics Network	Az érintett rendszerek átmenetileg működésképtelenné váltak.	https://www.risidata.com/Database/Detail/japanese_nuclear_company_virus_attack
18	Atomerőművi adatok nyilvánosságra kerülése vírustámadás során	Japán	2005	A Mitsubishi Plant Engineering Corp. Egyik munkatársának privát számítógépére telepített fájlcserélő alkalmazáson keresztül egy vírusfertőzés után 11 japán villamosenergia-ipari céggel (köztük több atomerőművel) kapcsolatos fájlok (összesen 44 MB-nyi) kerültek nyilvánosságra.	Vírustámadás és fájlcserélő alkalmazás	Nem ismert	Az incidens nem érintett nukleáris eszközöket. Az incidens 2005-től márciustól júniusi felfedezéséig tartott.	https://www.risidata.com/Database/Detail/japanese_nuclear_company_virus_attack
19	E-Tag incidens	USA	2005	Az USA egy meg nem nevezett villamosenergia-ipari szektorában a kereskedelmi (Purchasing-Selling Entity, PSE) cég rendszerében egy illetéktelen személy által szerzett illegális hozzáférésen keresztül több, nagy mennyiségű villamosenergiára vonatkozó megrendelést tartalmazó E-Tag-et adott fel.	Megosztott felhasználói fiókok használata.	Nem volt közvetlen ICS érintettség.	A PSE információ biztonsági felelőse visszavonta az érintett felhasználói fiók tanúsítványát.	https://www.risidata.com/Database/Detail/e-tag-incident
20	A Taum Sauk víztározó gátjának meghibásodása	USA	2005	2005.12.14-én a Taum Sauk felső víztározó gátja meghibásodott és ennek következtében közel 5 millió m3 vizet engedett ki a Black River keleti ágába. A kiáradó víz jelentős károkat okozott a Johnson's Shut-Ins állami parkban és bár halálos áldozatokat az incidens nem követelt, sérültek voltak.	Helytelenül telepített és karbantartott monitoring berendezések miatt túltöltött volt a víztározó. A vészhelyzeti tartalék szenzorok nem megfelelő helyre voltak telepítve, ezért nem működtek hatékonyan.	A víztározó gátrendszerének monitoring rendszerei	Jelentős anyagi kár és több sérült személy.	https://www.risidata.com/Database/Detail/taum_sauk_water_storage_dam_failure

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
21	Erőművi biztonsági információk kiszivárgása	Japán	2006	Egy hőerőmű bizalmas, fizikai biztonsági információi kerültek illetéktelen kezekbe egy vírusfertőzött számítógépre telepített fájlmegosztó szoftveren keresztül.	Fájlmegosztó szoftver, amit az erőmű biztonságáért felelős cég egyik munkatársának számítógépére telepítettek	Nem ismert	Fizikai biztonsági eljárásokat és személyes adatokat tartalmazó fájlok kerültek nyilvánosságra.	https://www.risidata.com/Database/Detail/power_plant_security_information_leaked_onto_internet
22	"Kama Sutra" vírustámadás az indiai villamosenergia-rendszer ellen	India	2006	Az indiai villamosenergia-rendszert kiszolgáló számítógépes hálózatba egy "Kama Sutra" nevű malware jutott be.	Nem ismert	Nem ismert	Nem ismert	https://www.risidata.com/Database/Detail/power_network_survives_virus_attack
23	Browns Ferry atomerőmű leállása	USA	2006	A Browns Ferry atomerőmű 3A és 3B reaktoraiban használt keringető szivattyúk kiesése után az operátorok manuálisan leállították a két reaktort. Az incidenst az erőművi ICS hálózaton tapasztalt kiemelkedően nagy hálózati forgalom következtében a Siemens Perfect Harmony VFD vezérlők hibája okozta.	VFD vezérlők hibája túlzottan nagy hálózati forgalom miatt	Keringető szivattyúkat vezérlő Siemens Perfect Harmony VFD vezérlők	Nukleáris reaktorok manuális leállítása	https://www.risidata.com/Database/Detail/browns_ferry_nuclear_plant_scrammed_shut_down
24	Adathalász támadás villamosenergia cég ellen	Ismeretlen	2006	Adathalász e-maileket felhasználva a támadók kompromittálták egy villamosenergia cég egyes felhasználóinak számítógépeit és olyan szintű jogosultságokat szereztek, amikkel az üzleti folyamatokat tudtak módosítani és vezérelni	Adathalász e-mail	SCADA rendszer	A villamosenergia cég teljes hálózatához hozzáfértek a támadók.	https://www.risidata.com/Database/Detail/energy_company_exposed_to_hackers_by_a_phishing_attack

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
25	Számítógépes hiba okozta áramkimaradás	USA	2007	Egy számítógépes hiba miatt kiterjedt áramkimaradások voltak Phoenix városa körül, 80.000-100.000 fogyasztót érintve. Az áramkimaradás 20-30 percig tartott.	Számítógépes hiba	Tehermentesítő rendszer	Áramkimaradás, 80.000-100.000 ellátatlan fogyasztó 20-30 percen át.	https://www.risidata.com/Database/Detail/computer_glitch_causes_major_power_outage
26	Áramkimaradás Floridában	USA	2008	Egy karbantartást végző mérnök engedély nélkül kikapcsolt elsődleges és tartalék védelmeket, majd amikor egy kapcsolót működésbe hoztak, nagyobb rövidzárlat jött létre.	Emberi hiba	Védelmek	Több millió ellátatlan fogyasztó. Több villamosenergia-szolgáltató hálózatában voltak üzemzavarok és még a Turkey Point atomerőművet is érintette az incidens.	https://www.risidata.com/Database/Detail/blackout_in_florida
27	Georgia-i atomerőmű leállása	USA	2008	A Hatch atomerőművet 48 órára kellett leállítani, miután egy külső vállalkozó frissített egy, az üzleti hálózaton működő szervert, ami vegyületek és diagnosztikai adatok szinkronizálását végezte az atomerőmű elsődleges vezérlőrendszerével. A frissített szerver újraindulásakor a szinkronizált adatokat resetelte, ami miatt a vezérlőrendszer úgy érzékelte, hogy az erőmű hűtéséhez használt víztározóban a vízszint lecsökkent és emiatt a SIS megkezdte az erőmű leállítását.	Nem ismert kapcsolat az üzleti hálózat és az elsődleges folyamatirányító rendszer között	Erőművi folyamatirányító rendszer	48 órás leállás az atomerőműben	https://www.risidata.com/Database/Detail/georgia_nuclear_power_plant_shutdown
28	Limerick atomerőmű 1-es reaktorának leállása	USA	2008	A Limerick atomerőmű 1-es blokkjában leállás történt a turbinavezérlő rendszerrel kapcsolatos, részletesebben nem ismert probléma miatt. Az incidens a 2-es blokkot nem érintette.	Nem ismert	Nem ismert	Egy 1134 MW beépített teljesítményű nukleáris reaktorblokk átmeneti kiesése.	https://www.risidata.com/Database/Detail/limerick_nuclear_reactor_1_shut_down

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
29	Hibás szenzor okozta safety incidens	UK	2008	Szenzorhiba miatt egy jegesedő szélerőmű leállítása nem történt meg, ami miatt a szélturbina lapátjain keletkezett jég nagy darabokra törve zuhant a közeli lakóházakra.	Nem ismert	Szenzorok és szélturbina-vezérlő rendszer	A szélturbina lapátjairól lezuhanó nagyméretű jégdarabok károkat okoztak több lakóházban (safety incidens). Személyi sérülésről nincs információ.	https://www.risidata.com/Database/Detail/failed_sensor_on_wind_turbine_caused_shower_of_ice_shards
30	Texas-i villamosenergia cég elleni kibertámadás	USA	2009	Don Chul Shin, az Energy Future Holdings-tól (egy számos erőművet, köztük a Comanche Peak atomerőművet üzemeltető cég) 2009. március 3-án elbocsátott alkalmazott 2009. május 28-án a számára kiadott és hibásan vissza nem vont VPN-hozzáférésen keresztül adatokat lopott és módosított az EFH rendszereiben. A szabotázs észlelése után az EFH jelentette az incidenst és Don Chul Shin-t letartóztatták.	Hibásan le nem tiltott, korábban legitim VPN-hozzáférés	Nem ismert	Az incidens tisztán pénzügyi hatásokkal (kb. 26.000 USD veszteség) járt.	https://www.risidata.com/Database/Detail/texas_power_company_hack
31	Hibás jelzés miatt leállított hűtőrendszer	USA	2009	A Duke Energy által az ügyfeleinek adott, légkondícionálókra kapcsolt fogyasztás-optimalizáló berendezések hibás jelzések kiküldése miatt 3 órára teljes mértékben leálltak ahelyett, hogy ciklikusan leálltak és újra elindultak volna.	Hibás jelzés kiküldése (feltételezhetően hibából eredően és nem szándékos károkozási céllal)	Fogyasztás-optimalizáló készülékek	3 órára leállított légkondícionáló berendezések	https://www.risidata.com/Database/Detail/wrong_signal_shuts_down_cooling_systems
32	Vírustámadás villamosenergia cég rendszerei ellen	Ausztrália	2009	Az Integral Energy rendszerei elleni vírustámadás mintegy 1000 munkaállomást érintett. A vírustámadás nem érintette a villamosenergia-rendszer Integral Energy által menedzselt részét.	Nem frissített végpontvédelmi megoldás egyes munkaállomásokon, amelyek így védtelenek voltak a W32.Virut.CF nevű malware ellen.	Nem érintett ICS rendszereket	Az Integral Energy összes, 1000 db munkaállomását újra kellett telepíteni.	https://www.risidata.com/Database/Detail/energy_company_virus_attack

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
33	Kibertámadás Texas-i áramszolgáltató ellen	USA	2010	Meg nem erősített információk szerint egy kínai IP címről közel 5000 alkalommal próbáltak meg bejelentkezni a Texas-i Lower Colorado River Authority rendszereibe. Az Electricity Reliability Council of Texas nevű szervezettől származó információk szerint az authentikációs próbálkozások mindegyike sikertelen volt. Az LCRA illetékesei "sem cáfolni, sem megerősíteni" nem kívánták az incidenssel kapcsolatos információkat.	Nem ismert	Nem ismert	Nem ismert	https://www.risidata.com/Database/Detail/cyber_attack_on_texas_electricity_provider
34	Szoftver-inkompatibilitás miatt kiesett SCADA alarm-funkció	USA	2010	A PCAnywhere nevű szoftver 12.5-ös verziójának telepítése után furcsa kompatibilitási problémákat tapasztaltak Windows 2000-es operációs rendszert futtató számítógépeken egy meg nem nevezett amerikai villamosenergia-ipari vállalatnál, ami miatt bizonoys távoli hozzáférési módok esetén a SCADAlarm nevű megoldás átmenetileg elérhetetlenné vált.	Szoftver-inkompatibilitás	SCADAlaram nevű SCADA alarm funkció	Nem ismert	https://www.risidata.com/Database/Detail/scadalalarm_pcanywhere_compatibility
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
36	Watts Bar atomerőmű leállása	USA	2011	Az amerikai Watts Bar atomerőmű egyik, turbinavezérléshez használt számítógépében történt nyomtatott áramköri kártya-meghibásodás miatt az érintett számítógép használhatatlanná vált, emiatt pedig (a turbinavezérlés kiesése miatt) a reaktort 3 napra le kellett állítani. Az incidens kivizsgálásának eredményéről nincs információ.	Nyomtatott áramköri meghibásodás	Turbinavezérlő szervere	3 napos reaktor-leállás	https://www.risidata.com/Database/Detail/circuit_card_shuts_down_nuclear_plant
37	Amerikai erőmű vírusfertőzése	USA	2012	Egy külsős technikus által használt USB adathordozón keresztül Mariposa malware jutott be egy amerikai erőmű folyamvezérlő rendszereinek hálózatába és a turbinavezérlő szerverek közül kb. 10 hostot fertőzött meg. Az incidens következtében az érintett rendszereket le kellett állítani és az üzem újraindítását 3 héttel el kellett halasztani.	Malware-fertőzött USB adathordozó	Turbinavezérlő rendszer szerverei	Jelentős kiesés az üzemi rendszerekben	https://www.risidata.com/Database/Detail/u._s._electric_utility_virus_infection

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
38	Vírusfertőzés erőművi rendszerekben	USA	2012	Egy amerikai erőműben 3 malware-t fedeztek fel az egyik alkalmazott folyamatvezérlő rendszerek konfigurációinak mentésére használt USB adathordozóján. A háromból két malware ismert és gyakran előforduló malware volt, a harmadik azonban egy kifinomult és ritkán látható példány, ez utóbbit két mérnöki munkaállomáson is megtalálták a későbbi vizsgálatok során.	Nem ismert	Mérnöki munkaállomások	Nem ismert	https://www.risidata.com/Database/Detail/u._s._power_plant_infected_with_malware
39	Számítógépes hiba okozta nukleáris reaktor-leállás	USA	2012	A Susquehanna Atomerőmű két reaktorából az egyiket számítógépes hiba miatt manuálisan le kellett állítani. A hiba a reaktor vízszintjét vezérlő egyik folyamatirányító rendszerében jelentkezett, aminek okát vizsgálták, de a vizsgálat ereményéről nincs információ.	Nem ismert	A reaktor hűtővíz-vezérlő rendszere.	Manuális reaktor-leállítás	https://www.risidata.com/Database/Detail/computer_glitch_leads_to_shutdown_of_nuclear_reactor
40	Brute-force támadás közmű-szolgáltató rendszerei ellen	USA	2014	Egy nem azonosított amerikai közműszolgáltató rendszerei ellen hajtottak végre támadást, amit a gyenge jelszavakra építettek a támadók. A támadás idején a mechanikus rendszereket karbantartás miatt lecsatlakoztatták a számítógépes vezérlőrendszerekről, így az incidens nem tudott károkat okozni a fizikai folyamatvezérlésben.	Gyenge jelszavakon keresztül szerzett illegális hozzáférések	Nem ismert	Nem ismert	https://www.risidata.com/Database/Detail/public-utility-compromised-after-brute-force-hack-attack-says-homeland-secu
6	Havex/ Dragonfly	Európa, USA	2014	ICS rendszerek és ICS fejlesztő/felhasználó európai és Észak-amerikai vállalatok ellen indított, elsődlegesen információszerzésre specializált támadás-sorozat, ami kifejezetten kritikus infrastruktúrákat (elsődlegesen az energia-szektort) 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 információszerzés 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 villamos-energia 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-attack-hit-japanese-monju-nuclear-power-plant.html

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
9	Ukrán áram-szolgáltatók	Nyugat-Ukrajna	2015	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 tettek 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	Nincs	Nem ismert	https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/
11	Malware-támadás német atomerőmű ellen	Német-ország	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	Nem ismert	Az incidensnek nem volt közvetlen hatása az erőmű alap funkcióira.	https://securityaffairs.co/wordpress/46708/security/virus-gundremmingen-nuclear-plant.html
12	Industroyer/CrashOverride	Ukrajna, kijevi körzet	2016	Az Ukrenergo 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 Ukrenergo 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 esetén.	Industroyer/CrashOverride ICS malware	ICS/SCADARTU Digitális védelem	200 MW teljesítmény kiesése a villamosenergia-rendszerből (az érintett felhasználók száma ismeretlen)	https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
13	NotPetya	Ukrajna, Csernobil	2017. június	Az EternalBlue sérülékenységet kihasználó NotPetya ransomware (más források szerint cryptowiper malware) támadása miatt a Csernobili atomerőmű környezetében használt sugárzásmérő 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-irországi leányvállalata, a SONI ellen intéztek támadást ismeretlenek, a becslések szerint 2 hónapig lehallgatva a két villamosipari rendszerirányító hálózati forgalmát.	A két érintett szervezet Interneten elérhető hálózati eszközeiről a támadók GRE tunnel alkalmazásával kitükrözték a hálózati forgalmat és kb. két hónapon keresztül hallgatták le a két rendszerirányító Internetes kommunikációját.	Nem ismert	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
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 infrastuktúrákat gyakran azok beszállítóin (nem csak fejlesztő, hanem gyakran szolgáltatást biztosító vállalatokon) keresztül, a beszállító rendszereit és gyakran termékeit kompromittálva támadták. Érdemes megfigyelni a hasonlóságot a 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

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
16	Ransomware-támadás a johannesburgi áram-solgáltató ellen	Dél-Afrikai Köztár-ság	2019. július	Ransomware-támadás érte a johannesburgi áramszolgáltató rendszereit, aminek következtében – bár az áramszolgáltató ICS rendszereit állításaik szerint nem érintette az incidens – mégis egyes ügyfeleknél, (akik, (hasonlóan a magyar feltöltő kártyás mobil telefont konstrukciót használókhoz hasonlóanhasonló módon) előre fizettek a villamosáramért), hosszabb áramkimaradások voltak.	Ransomware-támadás, ami az áramszolgáltató adatbázisait és más rendszereit tette használhatatlanná	Nem ismert	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 alállomás 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 alállomások távfelügyeletét.	Az internetre csatlakoztatott tűzfal webes adminisztrátori felületének egy ismert, de nem javított hibáját kihasználva folyamatos újraindításokat idéztek elő a támadók	SCADA és alállomási rendszerek közötti kommunikáció	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/1061111289
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 hátterű Lazarus csoporthoz köthető malware-ként azonosították.	A rendelkezésre álló információk szerint a malware a KKNPP ügyviteli hálózatait fertőzte meg, feltehetősen 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/
19	Kibertámadás az ENTSO-E ellen	Belgium	2020. március	Támadás érte az ENTSO-E (European Network of Transmission System Operators for Electricity) 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/

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
20	EDP ransomware-támadás	Portugália	2020. április	Nagyszabású ranswomware-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/
22	SNAKE/ENAKS-támadás az ENEL csoport ellen	Argentína, Európa	2020. június	SNAKE/ENAKS ransomware-támadás érte az ENEL csoport argentin és európai cégeit.	Egyes források szerint Internetről RDP-n (Remote Desktop Protocol) elérhető hostokon keresztül jutottak be a támadók az ENEL cégek hálózataiba	Nincs	Nem ismert, de az ENEL szerint villamosenergia-termelésért és elosztásért felelős rendszereiket nem érintette az incidens.	https://www.utilitydive.com/news/enel-ransomware-attack-highlights-the-value-of-a-top-down-security-culture/581179/
23	K-Electric ransomware-támadás	Karacsi, Pakisztán	2020. szeptember	Pakisztán legnagyobb, Karacsi városa és környékének villamosenergia-ellátásáért felelős vállalatának rendszereit érte ransomware-támadás. A NetWalker ransomware egyes, Interneten elérhető szolgáltatásokat tett használhatatlanná az áramszolgáltató ügyfelei számára. Az elérhető információk alapján a K-Electric üzemirányító rendszereit az incidens nem érintette.	Nem ismert	Nincs	A K-Electric egyes online szolgáltatásai (pl. számlákhoz történő ügyfél-hozzáférések) átmenetileg leálltak.	https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/
24	Netwalker-támadás az ENEL ellen	Európa	2020. október	Netwalker ransomware-támadás érte az ENEL rendszereit	Nem ismert	Nem ismert	Nem megerősített információk szerint a támadók a zsarolóvírussal nem csak titkosították az ENEL egyes adatait, de 5 TB-nyi adatot el is loptak a cégtől.	https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
25	APT-támadások indiai kritikus infrastruktúrák ellen	India	2021. március	A Recorded Future threat intelligence riportja alapján legalább 10 különböző, indiai villamosenergia-ipari céget ért kibertámadás, köztük négyet az öt indiai TSO-ból is és több erőmű rendszereit is. A villamosenergia-szektor mellett más indiai kritikus infrastruktúrákat is hasonló támadások értek ebben az időszakban.	A támadók a ShadowPad malware-t használták a célba vett szervezetek hálózatai elleni támadásokhoz	Nem ismert	Nem ismert.	https://go.recordedfuture.com/redecho-insikt-group-report
26	Ransomware-támadás a WEC rendszerei ellen	Alabama, USA	2021. július	Ransomware-támadás történt egy alabamai áramszolgáltató, a Wiregrass Electric Cooperative hálózatában. A támadás következtében az ügyfelek felhasználói fiókjai és a feltöltőkártyás szolgáltatások átmenetileg elérhetetlenné váltak.	Nem ismert	Nincs	A Wiregrass Electric Cooperative ügyfeleinek felhasználói fiókjait és a feltöltőkártyás áramvásárlási lehetőség feltöltő rendszerét elővigyázatosságból átmenetileg lekapcsolták.	https://dothaneagle.com/news/no-data-compromised-in-weekend-wec-ransomware-attack/
63	Kibertámadás német szélerőművek műholdas kommunikációja ellen	Európa	2022. február 24.	Feltételezések szerint nem függetlenül a február 24-én hajnalban megindult, ukrajnai orosz katonai inváziótól, kibertámadás érte a KA-SAT nevű cég műholdas kommunikációs rendszereit. A kommunikáció elvesztése nyomán 5800 szélerőművi turbina állt le az Enercon nevű német, szélerőműveket üzemeltető cég telephelyein.	Célzott DoS-támadás a KA-SAT ukrán ügyfeleinél telepített SurfBeam2 and SurfBeam 2+ modemei ellen.	Szélerőművi SCADA rendszerek kommunikációja	5800 szélturbina leállása.	https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview
64	Kibertámadás az orosz Egyesült Nukleáris Kutatóközpont rendszerei ellen	Oroszország	2022. március	Egy Telegram bejegyzés szerint illetéktelenek hatoltak be Oroszország Egyesült Nukleáris Kutatóközpontjának (Joint Institute for Nuclear Research, JNRI) rendszereibe.	Nem ismert	Nem ismert	Nem ismert	Telegram (pontos Telegram csatorna nem ismert, CT.R Facebook csoportban megosztva)

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
65	Kibertámadás érte a Rjazan-i közvilágítási rendszert	Oroszország	2022. március 23.	Az AnonGhost nevű hackercsoport állítása szerint kompromittálta Rjazan város közvilágításának vezérlőrendszerét és lekapcsolta az orosz város közterületi lámpáit.	Nem ismert	Nem ismert	Szolgáltatáskiesés a város közvilágításában	AnonGhost Twitter-csatorna
66	Industroyer2	Ukrajna	2022. április	Az Ukrajna ellen indított orosz invázióhoz kapcsolódva fedezte fel a CERT-UA az általuk és az ESET elemzői által Industroyer2-nek nevezett malware-t, amit a feltételezések szerint az orosz katonai titkosszolgálat által támogatott/irányított APT-csoport (akiket neveznek Sandworm-nek is) fejlesztett. A nyilvánosságra került információk szerint az Industroyer2 a 2016-os, eredeti Industroyer-hez hasonlóan az ukrán villamosenergia-rendszerben okozott komoly károk elérésére volt tervezve, de még az aktiválása előtt sikerült felfedezni és ártalmatlanítani.	Nem ismert	Nem ismert	Az elérhető információk szerint a malware-t az aktiválása előtt sikerült felfedezni és ártalmatlanítani, így károkat nem okozott.	https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
67	Pipedream	Nem ismert	2022. első negyedév	"A Pipedream nevű ICS malware-ről az első információkat a Dragos publikálta 2022. áprilisában. Állításuk szerint a malware-t, ami egy 5 modulból álló, moduláris támadó framework, az általános tevékenységük során fedezték fel és nagy valószínűséggel állították, hogy az áprilisi publikációig a Pipedream nem került éles, fizikai károkozási céllal történő bevetésre. A Pipedream képes többek között CODESYS, Modbus és OPC UA technológiák ellen támadásokra, a támadások során az ismert támadói technikák 38%-át és az ismert támadói taktikák 83-át tudják alkalmazni.	67	Pipedream	Nem ismert	https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/ https://www.dragos.com/blog/analyzing-pipedream-results-from-runtime-testing/
68	Gysinoozerskaya vízerőmű-incidens	Oroszország	2022. július	A GhostSec nevű ukránpárti hackercsoport felelősséget vállalt a Gysinoozerskaya orosz vízerőmű ICS rendszerei elleni kibertámadásért, amely robbanást okozott az erőműben.	Nem ismer	Nem ismert	Robbanással járó üzemzavar	https://www.thetechoutlook.com/news/technology/security/exclusive-ghostsec-has-taken-the-responsibility-for-the-recent-russian-ics-attack-with-zero-causality/?fbclid=IwAR21Nb9m9taI8ppMdJPJEGfEhp2UJHKQejJLyY8f5lUnyTyXmr2RYizCsRE

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
69	Rosseti Lenenergo elleni kibertámadás	Oroszország	2022. augusztus	A OneFist ukránbarát hackercsoport kompromittálta a Rosseti Lenenergo 110 kV-os PS-249 "Dymi" alállomásán használt SCADA rendszerét a SCADA rendszerhez tartozó UPS rendszer sérülékenységét kihasználva. A támadás során a OneFist tagjai tönkretették az UPS rendszert, túlmelegedésre kényszerítve az akkumulátorokat és felgyújtva a berendezést (safety incidens!).	Sérülékeny UPS rendszer a SCADA rendszerhez csatlakoztatva	SCADA és kapcsolódó UPS rendszerek illetve a SCADA rendszer szenzorai	Jelentős károk a SCADA rendszer és érzékelői, valamint a kapcsolódó UPS rendszerben, feltételezések szerint üzemzavarok a leningrádi régió/SPB áramellátásában.	https://www.cyberthreat.report/ukranbarat-hackercsoport-azt-allitja-hogy-feltortek-a-rosseti-lenenergo-scada-rendszeret/?fbclid=IwAR28BSb3pOMIfrq13AQKkGxjXHm0WFsc2c7w1O19pCaQwUKpOthZjjHD7uU
70	Kibertámadás jekatyerinburgi bevásárló-központ SCADA rendszere ellen	Oroszország	2022. szeptember	Egy magát Thraxman-nek nevező, ukránpárti hacker állítása szerint hozzáférést szerzett egy jekatyerinburgi bevásárlóközpont villamosenergia-rendszerét vezérlő SCADA rendszeréhez és a SCADA által vezérelt SNR-ERD-4, Moxa NPort 5130 és Incotec Mercury 225 típusú vezérlőkhöz (többek között a liftek vezérlőrendszeréhez is), összesen 266 db PLC-hez és 256 db mérőberendezéshez.	Nem ismert	SCADA, PLC-k	A támadó állítása szerint használhatatlanná tette a SCADA rendszert.	https://www.cyberthreat.report/scada-power-control-system-of-a-russian-shopping-center-was-hacked/?fbclid=IwAR3k18Op8iiqVZ6pGHTPatJorRd7xhHCdIE3vFNxiNdrpqON-F6BJH1RufM
	Szentpétervári eset Pongi							

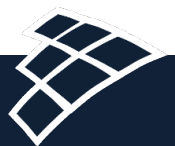
Az alábbiakban a megtörtént incidensek különösen fontos elemeit és azok tanulságait emeljük ki.

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 (RBAC[163]), titkosított és hitelesített kommunikáció, hálózatbiztonsági eszközök és jó gyakorlatok alkalmazása és sok más, a 2000-es évek közepére más, üzleti területeken tevékenykedő szervezetek (pl. pénzintézetek) 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;

[163] 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 tesztsorozatban 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 teszt[164] néven vált ismertté az ICS kiberbiztonsággal foglalkozó szakemberek között) végül a használt transzformátor leégésével és a téma fontosságával érvelők igazának maradéktalan bizonyításával ért véget.[165] 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.

[164] https://www.youtube.com/watch?v=LM8kLaJ2NDU
[165] A teszt részleteit a 7. melléklet 3.3.1. pontja mutatja be.

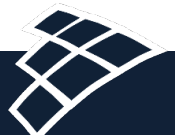
2. Stuxnet

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”[166] [13] című munkája alapján készült.

A történtek utólagos rekonstrukciója alapján a Stuxnet fejlesztése valamikor 2004/2005-ben kezdődhetett, míg a bevetésére valamikor 2007/2008 során kerülhetett sor. A történteket rekonstruálva az derült ki, hogy a támadó elsőként USB-s adathordozókon bejuttatta a Stuxnetet 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 szabotálásához. 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 –

[166] 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 százasával 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 RAT[167] 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 (emiatt is van az esetnek egynél több neve, az F-Secure Havex-ként[168] [14], a Symantec Dragonfly-ként[169] [15] hivatkozik nagyjából ugyanarra a támadói csoportra és támadásokra). Az elemzések alapján a biztonsági kutatók arra a következtetésre jutottak, hogy a támadás

[167] RAT: Remote Access Tool (Távoli hozzáférést biztosító program/kód)
[168] Daavid. „Havex Hunts For ICS/SCADA Systems.” F-Secure. https://archive.f-secure.com/weblog/archives/00002718.html (Letöltve: 2020. augusztus 26.)
[169] 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 hátterű 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 diszpécserek azt vették észre, 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.[170] 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.

[170] 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 megtéveszteni 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 valódinak 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 (csoportházirendekkel) 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 mellékszálnak 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 például , hanfolyamatosan, 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.[171] [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 2016-os egyetlen alállomással szemben) nem volt összehasonlítható az egy évvel

[171] 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.)

korábbiincidenssel, 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 készített[172] [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 Ukrenergo 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 sérülékenység, 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 Ukrenergo 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.

[172] 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.)

«

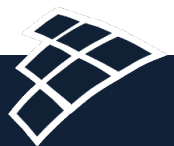
Az ICS-CERT 2015. július 21-én ICS biztonsági javaslatot hozott nyilvánosságra a Siemens SIPROTEC 4 és SIPROTEC Compact védelmeinek, valamint EN100 Ethernet kártyáinak sérülékenysége kapcsán azt követően, hogy egy orosz szakember felfedezte, majd bejelentette azt a Siemensnek, amely ennek nyomán firmware 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 DA[173] protokollokat ismerte, de a támadásról és a malware-ről megjelent, kifejezetten színvonalas elemzések[174] [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 hoztak 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 előadásban[175] [21] és cikkben[176] [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.

---

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

[174] 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.)

[175] 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. augusztus 28.)

[176] 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.)

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.[177] [23]

2015. december 21-én (két nappal az ukrán áramszolgáltatók elleni támadás előtt) jelent meg a Las Vegas Sun cikke[178] [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 cikket[179] [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 publikált[180] [26] információk[181] [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 források[182] [28][29] szerint a gundremmingeni) atomerőműben történt kiberbiztonsági incidensről.

[177] 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.)

[178] 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.)

[179] 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.)

[180] 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.)

[181] 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.)

[182] 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.)

2017 júliusában a Cisco-n belül működő Talos biztonsági labor publikált részleteket több ún. template injection[183] 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.

2017. augusztus 6-án jelent meg az ír Independent-ben egy cikk[184] [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-sorozatot tartott az USA kritikus infrastruktúrája elleni orosz kibertámadásokról[185]. Ebben az egyik újdonság az volt, hogy a támadók a különböző célba vett kritikus infrastuktúrákat gyakran azok beszállítóin (nem csak fejlesztő, hanem gyakran szolgáltatást biztosító vállalatokon) keresztül, a beszállító rendszereit – és gyakran termékeit – kompromittálva támadták. Érdemes megfigyelni a hasonlóságot a 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.

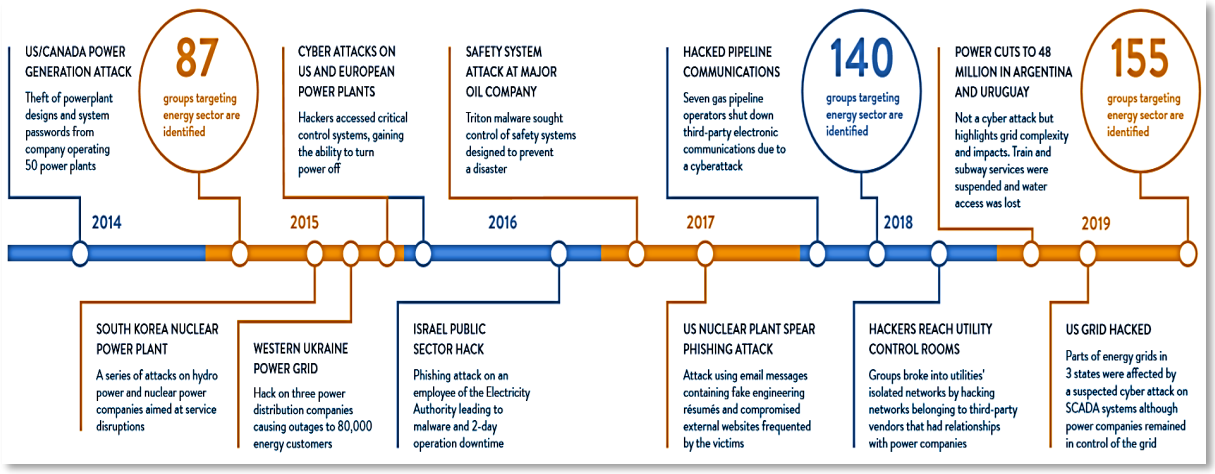
2019. szeptember közepén ismét az USA villamosenergia-rendszerének egyik szervezete elleni támadásról jelentek meg részletek.[186] [31]

[183] Bővebben ld. https://portswigger.net/web-security/server-side-template-injection és https://portswigger.net/kb/issues/00200308_client-side-template-injection

[184] 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.)

[185] Az előadás prezentációja a US-CERT weboldalán érhető el: https://www.us-cert.gov/sites/default/files/c3vp/Russian_Activity_Webinar_Slides.pdf

[186] 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.)



1.1. ábra: Hatásukban és számukban is növekvő incidensek[187] [32]

> 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.

187 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.)

2. melléklet: A villamosenergia-rendszer kiberbiztonsága és az OSINT[188]

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. »

[188] Köszönet Droppa Béla és Kocsis Tamás értékes tanácsaiért.

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.

A villamosenergetikában is alkalmazható néhány OSINT technika (a teljesség igénye nélkül):[189] [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 például 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 hasonlító adatkérő csalilevelek küldése nyomán szerezte meg.[190] [34]

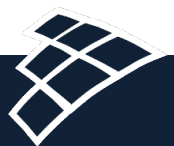
Lehetőségek a célszemélyek azonosítására:

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 közzé tételének, azaz akár a munkavállaló személyiségi jogainak szükséges mértékű korlátozására[191], a közzé nem tehető adatok körének meghatározására. A munkaviszonyra vonatkozó adatok szabályellenes közzététele fegyelmi vizsgálatot alapozhat meg.

[189] 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.
[190] 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
[191] A Munka Törvénykönyvéről szóló 2012. évi I. törvény



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.

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 például 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.

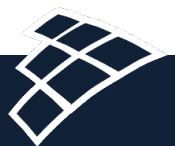
a. Karrier információk

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.

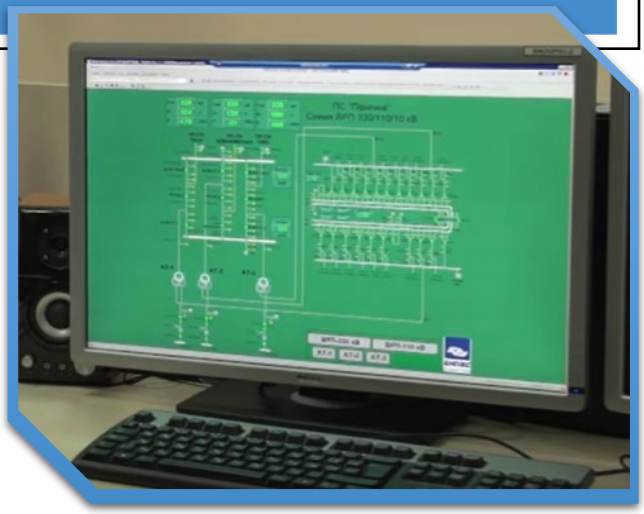
Az állashirdetéseknek nincsen jogszabályban meghatározott kötelező minimum vagy maximum tartalmi eleme, azaz az abban megjeleníthető információk körét szintén a szervezet vezetője jogosult korlátozni.

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 érzékenységű információhoz juttathat egy támadót.



A 2016. december 17-ei ukrajnai kibertámadás kapcsán még évekkel később is érdemes rákeresni 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:



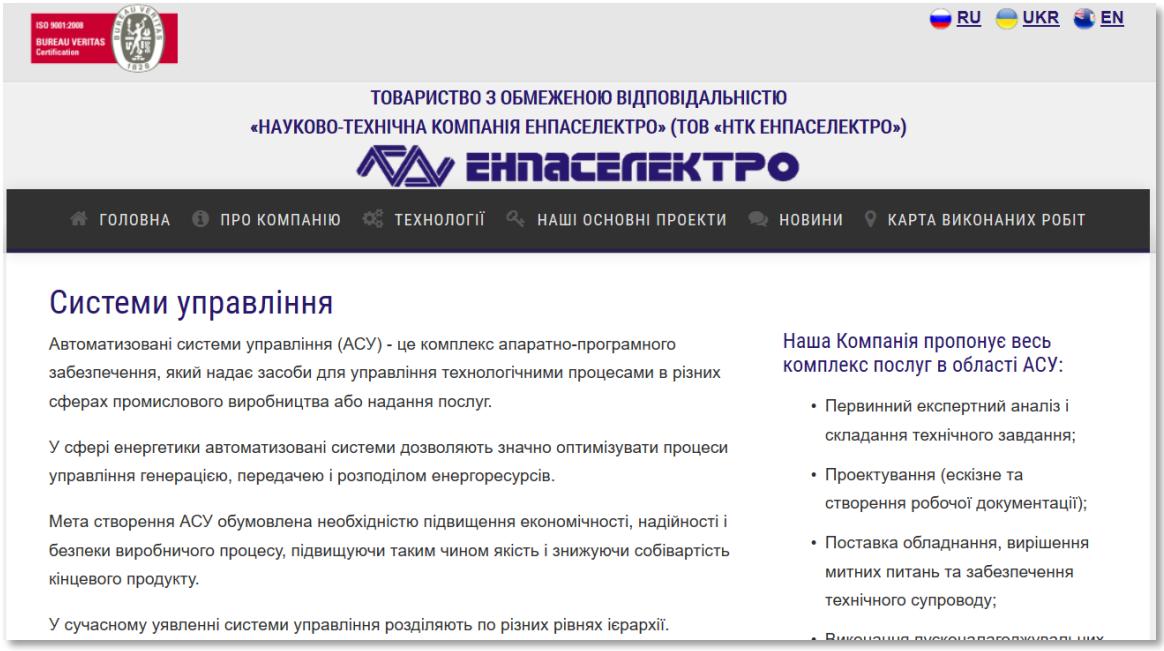
2.1. ábra: Az alállomási kapcsolási séma a Pivnichna-i vezénylő monitorán

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

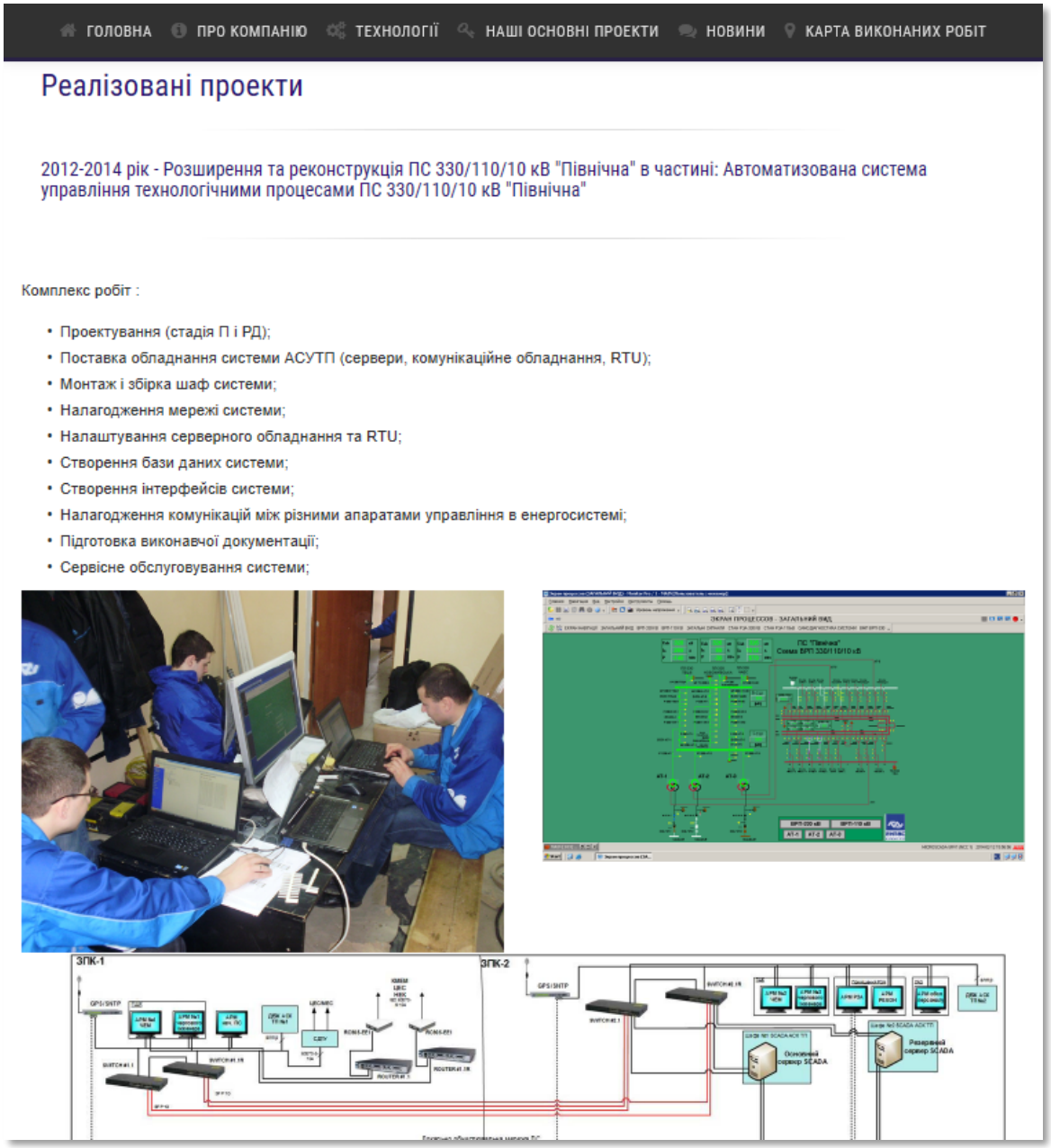
Ukrán nyelvet beállítva a Google-n és rákeresve a „Північна 330/110/10 підстанції схема” kifejezésre egyebek mellett elérhető a 2.3. ábra szerinti tervező cég honlapja:



2.3. ábra: Az Enpaszelektro honlapja[192]

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

192 https://enpaselectro.com/ua/tehnologii/sistemy-upravleniya.html



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.

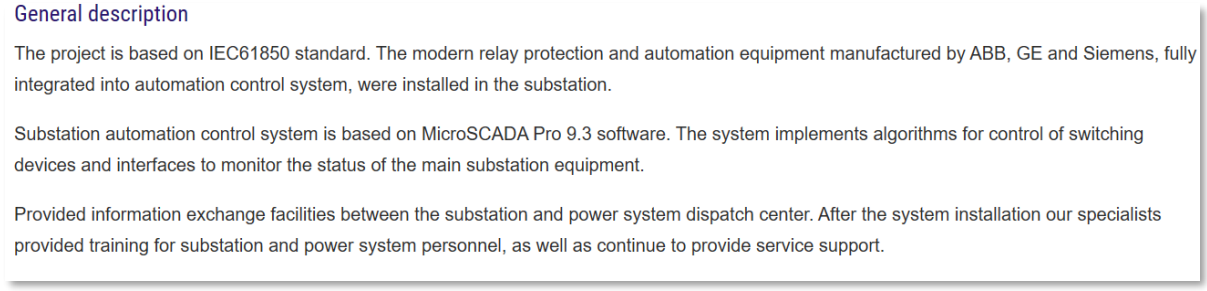
Hazai viszonyok között a kritikus infrastruktúra üzemeltetője az általa kötelezően készítendő ún. üzemeltetői biztonsági tervben rögzítendő eljárásrend szerint a beszállítóval kötött beszállítói szerződésben (illetve felektől függően egyéb megnevezésű, de ilyen tartalmú

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 például 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 megtörténtéig 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. [193] [194] [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 töröltetése.[195] [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.

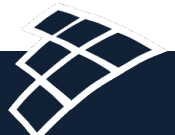
A támadók rendszerirányítók, illetve egyéb kapcsolódó szervezetek iránti növekvő érdeklődése is figyelmet érdemel.

---

[193] 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.)

[194] https://github.com/jivoi/awesome-osint

[195] 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.[196] [37]

[196] 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 értékelendőek.

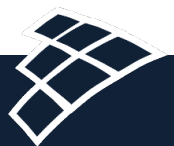
A fenyegetettség-térkép első fejezete a domain szempontjából releváns támadási vektorokat, biztonsági problémákat, kihívásokat áttekintő jelleggel tárgyalja. A második fejezet a domain szempontjából releváns támadó profilokat/modelleket, azaz a szóba jöhető aktorokat mutatja be. A komplex, átfogó fenyegetettség-térkép 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 zárak, 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 telepített és futtatott szoftverkomponensekben. Egy alkalmazásban található programozói hiba szoftvert érintő implementációs szintű sérülékenységnek tekinthető, míg egy kriptográfiai protokoll man-in-the-middle[197] támadást lehetővé tevő hibája tervezési szintű sérülékenység.

A szervezet *eljárásrendjeiben, működési- és munkafolyamataiban található sérülékenységek* olyan eljárási hibák, amelyek kihasználása nagymértékben segítheti a rendszer elleni fizikai és logikai támadások kivitelezését. Ilyen hiba lehet például, 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 hozzáférést, stb.

A *humánerőforrást érintő hibák* kihasználása ugyancsak segítheti a rendszer elleni fizikai és logikai támadásokat. Ilyen típusú hiba például a személyzet anyagi megbecsülésének alacsony szintje, vagy egyéb, a személyzet elégedetlenségét növelő hiányosság, amely csökkenti a szervezet iránti lojalitást, megvesztegethetővé 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

[197] MitM: man-in-the-middle (Közbeékelődéses támadás)

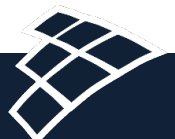
ismert sérülékenységekkel kapcsolatos kockázatok felmérésére és a kockázatarányos ellenintézkedések megtételére, ami a sérülékenység teljes megszüntetését, áthidaló megoldások bevezetését, vagy adott esetben a sérülékenység változatlanul hagyását és a kockázat elviselését, esetleg nem technikai eszközökkel 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, míg 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 (exploitability[198]), valamint referenciákat a sérülékenység javítását biztosító megoldásokra és eszközökre.

Az ipari rendszerek szempontjából releváns a Shodan kereső rendszer[199], 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. alapértelmezett jelszó beállítás), a rendszerekre és eszközökre vonatkozó publikusan ismert sérülékenységekről és az alkalmazható exploitok-ról. 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

[198] exploitability: kihasználhatóság
[199] https://www.shodan.io



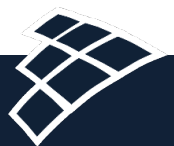
szervezet formális jóváhagyása vagy engedélye nélkül nem lehet végrehajtani. Amikor egy sérülékenység nem szüntethető meg azonnal, olyan áthidaló (work-around) megoldásokat kell alkalmazni, amelyek a rendszer szolgáltatásait nem befolyásolják, de a sérülékenység potenciálisan káros hatásait minimalizálják, kihasználási lehetőségét szűkítik.

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 a gyártók és az üzemeltetők által nem ismert, 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 exploitokat jobbára 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 válik. 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 például 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 JTAG[200] interfésszel, amely 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-channel[201] 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.

[200] JTAG: Joint Test Action Group (áramkörvizsgálati módszerekkel foglalkozó szakmai szervezet, illetve az IEEE-1149.1 szabvány által meghatározott módszer az integrált áramköri lapok/rendszerek gyors és automatikus tesztelésére)
[201] side-channel: kerülő út

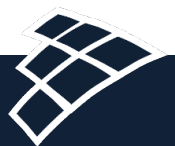
A hálózati behatolás tipikus példája, mikor a támadó egy kívülről elérhető hálózati szolgáltatásban fedez fel kihasználható hibát, és megfelelő inputok segítségével távolról átveszi egy belső rendszerkomponens felett az irányítást. Általában már az is támadásnak minősül, ha a támadó nem tudja átvenni az irányítást, de az általa kívülről bejuttatott inputok hatására a rendszer hibás szolgáltatást nyújt, vagy nem tudja biztosítani az elvárt szolgáltatásminőséget, rendelkezésre állása sérül. 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 végigpróbálgathatja 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 megzavarhatja, 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, például rávehet egy legitim felhasználót arra, hogy mondja el neki a jelszavát.

A hálózati behatolások ellen 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

Privilégium-szint emelés (privilege escalation[202]): miután a támadó sikeresen bejutott a rendszerbe, általában további lépéseket kell tegyen 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 privilégium szint emelést hajt

[202] privilege escalation: jogosultsági szint emelés



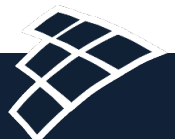
végre és rendszergazda (root[203], superuser[204], administrator[205]) jogosultságot szerez. A privilégium szint emelés a kompromittált rendszerelem operációs rendszerében található további sérülékenységek kihasználásával érhető el.

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 backdoorok[206] 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 mindemellett olyan rosszindulatú programokat (rootkiteket[207]) telepíthet, és konfigurációs beállításokat végezhet, mellyel elrejtheti jelenlétét.

Oldalirányú mozgás (lateral movement[208]): 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 végezhetők. Az oldalirányú mozgás során a támadó olyan belső protokollokat is támadhat vagy kihasználhatja azok hibáit, amelyek a rendszeren kívülről nem láthatóak.

[203] root: gyökér könyvtár; korlátlan jogosultságú rendszerfelhasználó.
[204] superuser: magas hozzáférési jogosultsággal bíró felhasználói fiók
[205] administrator: rendszergazda
[206] backdoor: hátsóajtó
[207] rootkit: saját és más programok jelentését elrejteni képes, rosszindulatú kód
[208] 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.

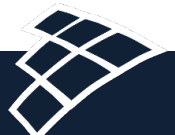
Ez tipikusan minimális méretű kód, ami a rendszerben eleve meglevő funkciókat aktivál (pl. elindít egy shell-t[209] és létrehoz egy hálózati kapcsolatot). Ennek segítségével a támadó aztán újabb és komplexebb kártékony modulokat tud a rendszerbe juttatni, amelyek célja lehet a privilégium szint növelés, 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-k[210] 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 programrészletek, 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 népszerű weboldalon keresztül). A jellemzően használt disztribúciós módszerek a következők:

- e-mail: a kártékony program e-mail csatolmányként érkezik vagy az e-mailben 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-phishing[211] levél, amely kifejezetten az áldozatra szabott, akár személyes információkat is tartalmazhat, ezért megvan a valószínűsége, hogy a megcélzott személy megnyitja majd a csatolmányt.

[209] shell: parancssori felület, parancsértelmező
[210] malware: rosszindulatú, kártékony alkalmazás vagy kód
[211] spear-phishing: célzott adathalászat, konkrét személy/szervezet ellen.



- drive-by-download: a malware egy weboldalról töltődik le 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 sérülékenységét 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 népszerű web site, vagy kifejezetten erre a célra létrehozott áloldal.
- 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 antivírus szoftverek ne ismerjék fel. Egy ilyen malware-t adott esetben egy hagyományos antivírus szoftvernél fejlettebb védelmi eszköz képes lehet detektálni. Az államilag 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 fejlettebnek mondható eszközök sem ismerik fel, sőt egyre több malware detektálja azt, ha védelmi eszközök próbálják vizsgálni, megfigyelni működésüket (ez esetben jellemzően passzívak maradnak). A PLC-ket és RTU-kat ugyanúgy meg lehet fertőzni kártékony programokkal, mint asztali PC-ket, laptopokat, vagy tableteket. Sőt, a beágyazott eszközök még nagyobb veszélynek vannak kitéve, mert a tervezés során 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 kernel[212] szintjén futnak, hanem a számítógépen vagy beágyazott eszközön futó firmware-t módosítják. PC-k esetében például malware támadás

[212] kernel: rendszermag

célpontja lehet a BIOS[213], mert az ebben található programkód az, amit a hardver boot-oláskor először lefuttat. A BIOS-ban elhelyezett kártékony kód, az ún. bootkit[214], általában tetszőleges módosítást tud végrehajtani a boot-olási folyamat során később betöltésre kerülő szoftvereken, például 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-mozgatás bevett szokás ezen a területen is.

Kártékony funkció, például back door, nemcsak utólag kerülhet egy rendszerbe. Elméletileg, a rendszer vagy a rendszer egyes komponenseinek tervezője vagy megépítője – nem is feltétlen károkozási céllal, hanem például a rendszertámogatás megkönnyítése érdekében – 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 praktikusan 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 programkönyvtárat vagy egyéb modult tartalmaznak. Ezek intenzív használatának praktikus okai vannak, ha a licenc 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. 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.

[213] BIOS: Basic Input/Output System (alapvető bemeneti/kimeneti rendszer)
[214] bootkit: a számítógép indulásakor betöltődő rosszindulatú kód

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 részeivé 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 államilag 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.

A kriptográfia algoritmusok ellen egyre gyakoribbak azok a támadások, melyen nem a bizalmasság, vagy az integritás megsértését célozzák, hanem a szolgáltatás elérhetősége ellen irányulnak. A szolgáltatásmegtagadással járó támadásoknak az ipari rendszerek azon komponensei, ahol kis teljesítményű hardver eszközök nyújtanak valamilyen hálózati szolgáltatást komolyabban is kitettek lehetnek, különösen akkor, ha az eszköz által nyújtott szolgáltatás időkritikus, vagy az eszköz önmagában érzékeny olyan fizikai tényezőkre (pl.: hőmérséklet), melyre a támadás kifejezett hatással lehet.[215]

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

[215] Az olyan támadások esetén, mint a DHEat, vagy a Slowloris attack, a minimális befektetés mellett lehet az áldozat erőforását (CPU, memória) jelentékeny mértékben túlterhelni.

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 a rendszer egészét tekintve.

Egy széles körben használt protokoll például a TLS – vagy korábbi – mára elavult – változata az SSL[216] – 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, például az SSH, az OpenVPN, az IPsec[217], vagy a WPA2[218] stb. Ezek különböző hálózati rétegekben működnek, vagy valamilyen speciális feladatot látnak el. Ezen protokollokat intenzíven használják a modern számítógépes rendszerek. A legtöbb széles körben 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-résztvevő 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 előállítása. A támadóról általában azt feltételezzük, hogy tetszőlegesen be tud avatkozni a felek közötti kommunikációba, ami általában MitM támadót jelent, aki fizikailag

[216] SSL: Secure Socket Layer (titkosítási protokoll, amely az interneten keresztüli kommunikációhoz biztosít védelmet. Az SSL a TLS elődje.)
[217] IPsec: Internet Protocol Security (IP biztonsági protokoll, Az IP protokollon működő, minden IP-csomagot titkosító és a jogosultságát ellenőrző protokoll.)
[218] WPA2: Wi-Fi Protected Access 2 (A vezeték nélküli hálózati rendszerek biztonsági protokollja, amely tartalmazza az IEEE 802.11i szabvány főbb szabályait.)

vagy logikailag ékelődik be a protokoll-résztvevők 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.

A protokollokhoz hasonlóan biztonsági API-kkal is számos környezetben találkozhatunk. Ezekben a széles körben 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 tokent[219], 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 szoftvermodulban).

2.8. Social engineering, phishing

A technikai jellegű támadások mellett nagyon hatékonyak a humán felhasználók ellen irányuló támadások. Sokan a 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 paraméterek bizalmas és biztonságos kezelésére. Egy képernyőre ragasztott cetlire vagy táblára felírt, vagy egyszerű, könnyen kitalálható jelszó például 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 alcsoportját alkotják a phishing[220] támadások, amelyekben a támadó a felhasználók számára hamis információt tartalmazó e-mailt küld vagy weboldalt jelenít meg, ezzel megtévesztve és rávéve őket valamilyen kompromittáláshoz vezető lépésre. Tipikus példa, mikor a támadó olyan e-mailt 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 a tényleges rendszerre mutató linket tartalmaz, hanem egy támadó által birtokolt, az eredetihez mindenben hasonlító weboldalra, felületre mutat. Ha a gyanútlan támadó ezen keresztül kísérli meg a belépést, akkor közvetlenül a támadónak küldi el a valódi rendszerhez történő hozzáféréshez szükséges azonosítót és jelszót.

[219] token: jogosultsági és biztonsági kódgeneráló eszköz
[220] phishing: adathalászat

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

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 rendelkezésre állás 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 ismerheti a szervezet biztonsági szabályzatait és eljárásrendjeit, illetve azok gyengeségeit, valamint személyes kapcsolatai 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 hosszabb 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 beszállítói lánchoz tartozó bármely beszállító felől érkezhet támadás az együttműködés 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 kiskapukat (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 adott beszállító, annak alvállalkozója 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 (és hajlandóak) 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 tartalom 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.

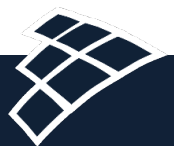
- *A technikai tudás mélysége:* a technikai tudás egyrészt az információszerzés mélységének növelése szempontjából lehet fontos, másrészt ez a jellemző az, amelynek segítségével a publikusan elérhető és a rendszerről megszerzett belső információk sikeres támadássá alakíthatók. Ipari folyamatirányítási 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., megvesztegetéssel, 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 exploitok 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 (információszerzési lehetőséggel) és anyagi erőforrásokkal, de általában határtalan lelkesedéssel és motivációval 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 és sokszor tart a potenciális következményektől is. A létesítmények tipikusan elavult technológiája,



az elérhető támadó eszköztár folyamatos bővülése, valamint a rendszerek 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 rendszer általános 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.

  Az elégedetlen munkatárs mellett a szándékolatlan belső támadó is megemlítendő. Egy nem megfelelően képzett, ám privilegizált jogosultsággal bíró munkavállaló szintén komoly károkat tud okozni. Ezért is kiemelten fontos a megfelelő oktatás, illetve a privilegizált jogosultságok megfelelő kezelése.

- *Hacktivista csoportok:* a hacktivista csoportok általában laza szerveződésű, eltérő szintű technikai tudással rendelkező, amatőr hackerekből állnak (ugyanakkor olykor nagyobb tudású hackerek is csatlakozhatnak a szerveződéshez). 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 opportunista elemeket is tartalmaz (néha könnyen kompromittálható rendszereket támadnak meg, amelyet utólag a támadást társadalmi vagy politikai küzdelmük érdekében végrehajtott, előre eltervezett akciónak állítják be). Ha a célpont kiválasztását és a stratégiai cél kijelölését a csoportok eredeti

motivációja határozza meg, akkor az gyakran valamilyen, a motivációval összefüggésbe hozható aktuális társadalmi vagy politikai eseményre reflektál, 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 képessége és ezáltal potenciális veszélyessége széles skálán mozog. Jellemzően van néhány magas technikai tudással rendelkező tagjuk, ám a csoport nagy része alacsony, script kiddie-hez hasonló szintű technikai tudással rendelkezik.

A hacktivista csoportok egyes tagjai kapcsolatban állhatnak kiberbűnözői csoportokkal vagy maguk is tagjai lehetnek kiberbűnözői szervezeteknek, amelyek segítségét és magasabb szintű technikai tudását alkalmanként igénybe vehetik. A hacktivista csoportok anyagi erőforrásai jellemzően korlátozottak, egyrészt a laza szerveződés nem teszi lehetővé, hogy a csoportok strukturált módon erőforrásokat halmozzanak fel, másrészt általában nem rendelkeznek külső szponzorral. A hacktivista csoportok korlátozott információszerző képessége és technikai tudása valószínűleg nem elegendő rendkívüli következményekkel járó kibertámadások végrehajtásához, valószínűbb, hogy politikai vagy társadalmi üzeneteiket weboldalak megbénításával és módosításával (de-face) próbálják elérni (ld. Anonymous). Ugyanakkor nem hagyható figyelmen kívül, hogy kis komplexitású támadásoknak is lehetnek előre nem tervezett negatív mellékhatásai.

- *Terrorszervezetek:* 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 médiafigyelemre és a civil lakosság megfélemlítésére és elbizonytalanítására, trigger-hatás kiváltására 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 jelentős lehet, de határozottan mélyülő tendenciát mutat. A terrorista szervezetek sok esetben modern eszközrendszerrel rendelkeznek és intenzíven használják az internetet online tudásbázis készítésére és tagjaik kiképzésére is. Aggasztó tendencia továbbá a terrorista szervezetek és a hagyományos bűnszervezetek kooperációja. A

villamosenergiai-ipari létesítmények ellátási láncban betöltött szerepük miatt akár közvetlen célpontjai is lehetnek terrorista támadásoknak. A terrorista szervezetek jelentős kockázatot, komoly fenyegetést jelentő támadók.

- *Kiberbűnözők:* elsődleges motivációjuk a pénzügyi 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 online szolgáltatók számítógépes rendszereiből is, ezért ezen rendszerek is a kiberbűnöző szerveződések célpontjai. A megszerzett információk közvetlenül felhasználhatók haszonszerzésre, vagy akár értékesíthetők is. A támadások másik tipikus célja az irányítás átvétele nagy mennyiségű számítógép felett, és a kompromittált számítógépek ún. botnetbe 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 céljuk lehet hozzáférhetetlenné tenni az áldozat számára annak adatait, 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, például 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 és kisebb jogkövetkezmény veszélyével (a létfontosságú rendszerelemek elleni támadások számos jogrendben súlyoabban minősülő bűncselekmények pl. terrorcselekmény vagy közérdekű üzem működésének megzavarása) képes hasznot termelni.

- *Államilag 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), kiber-fizikai rendszerek esetében fizikai kár okozása, illetve egy fizikai támadás támogatása, hatékonyságának és hatásának növelése, elterelés. Az államilag támogatott, nem egyszer reguláris hadseregek, speciális szolgálatok egységeként, hivatásos állományú tagokkal működő 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 tárgyalt 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.

  Az államilag támogatott támadói csoportok sajátos ágát képezik az ún. „kiber-szabadcsapatok”, melyeket az államok támadói vagy védelmi célokra, egyfajta irreguláris hadseregként szerveznek – akár nemzetközi – önkéntesekből. Ezen szabadcsapatok motivációi sokszor nemzeti érzületre, vagy az agresszióval szembeni ellenállásra épülnek. Tudásuk sokszor jelentős, tagjaik közt kevésbé valószínű script

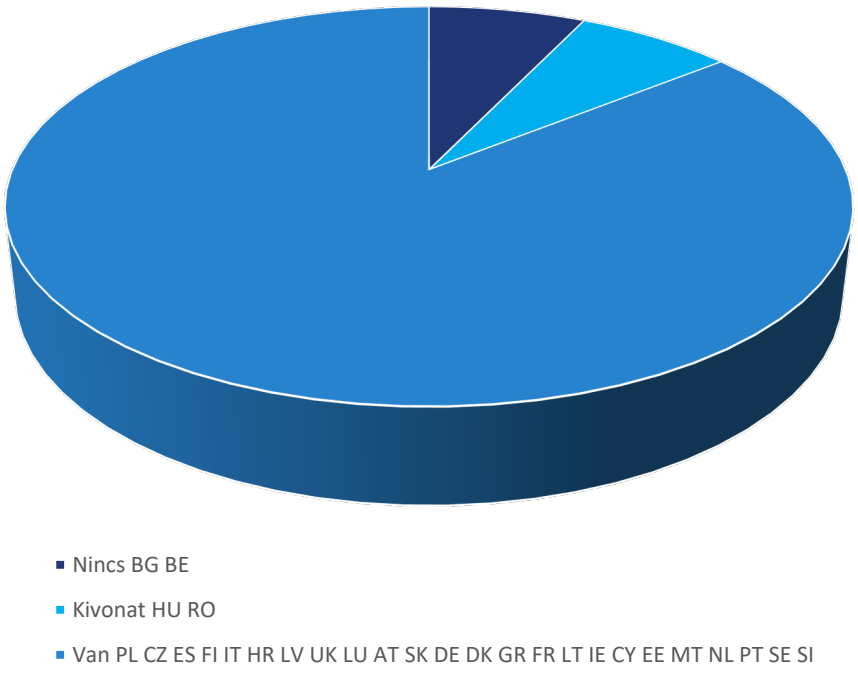
kiddiek megjelenése. Tagságuk jellemzően nem állandó, adott esetben ad-hoc jelleggel egy-egy akcióra is szerveződhetnek. Veszélyességük megegyezhet – de legalábbis jelentősen megközelítheti – az államilag támogatott támadó csoportok veszélyességével. Jellemzően valamilyen aktuális konfliktus, háború hívja életre ezen csoportokat. Kifejezett céljuk lehet támogató célú információszerzés, de akár katonai célpontok, létfontosságú rendszerelemek (így kifejezetten a villamosenergia-rendszer elemeinek) támadása, kiiktatása, az ellátás akadályozása, korlátozása.

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 említenek 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

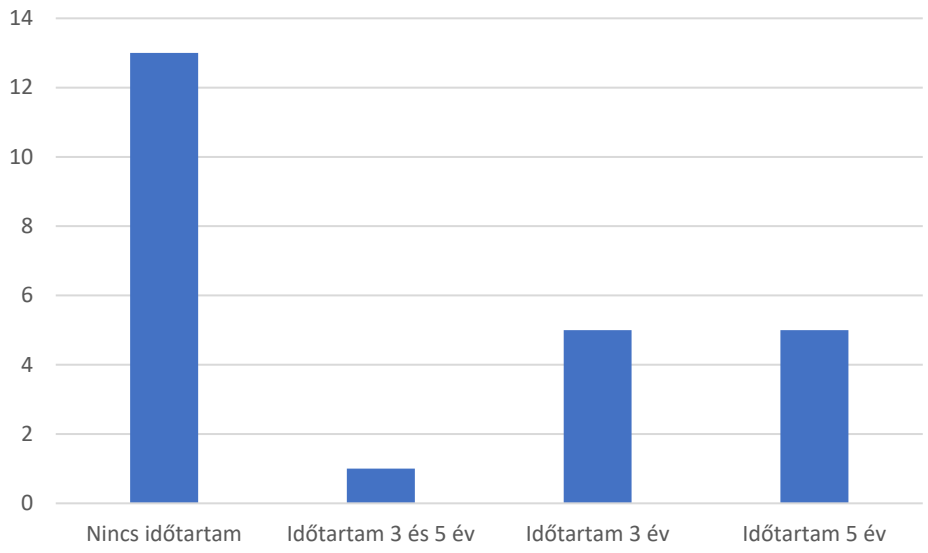
A magyar stratégia egy „kivonat”, amely mellett Románia is egy ilyen hasonló kivonatot tett közzé az ENISA honlapján (a vizsgálat során előzőekre tekintettel a belga, a bolgár, a román és a magyar stratégia nem került bele a vizsgálati adatokba). A magyar kivonat nem tesz

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 stratégia[221] [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.

[221] 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 eszközrendszerét. 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 visszamérhetők 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.[222]

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 Stratégia[223] (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.

[222] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[223] 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

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).
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.[224]
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 teljes körűen kezeltek, ezáltal nem lehet azt mondani, hogy a magyarországiak teljes körűen 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

[224] 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.

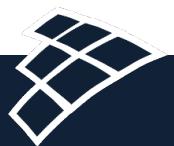
duplikáció és egyéb (pl. azonosítási) problémák merültek fel. A párbeszéd megindult, az eredménye feltételezhetően a CER irányelvben és a NIS 2 irányelvben fog megjelenni.

Meg kell jegyezni, hogy az Ibtv. és a végrehajtására kiadott 41/2015. BM rendelet nem kezelik 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 – is például víz, egészségügy stb. – is érintő probléma.

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 supervisori 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 kellenek 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 teljes körű 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.[225] 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 feltételeként 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.

[225] 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 szerintiek 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 hazánknak, amelyet fenntartani és erősíteni szükséges.

A nemzeti létfontosságú infrastruktúra védelmét a stratégia megfelelően megoldottnak tekinti. A hibrid támadásokkal szembeni ellenálló képességről 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 energiaimport 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 energiaimportban 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: Villamosenergetikai szempontból is releváns kiber-fenyegetések ill. -támadások az USA-ban

1. Az USA villamosenergia-rendszere

Az USA rendkívül összetett villamosenergia-rendszerében ~3300 szolgáltató (melyből ~180 nagybefektetői tulajdonban van, 2000+ közüzemi jellegű, míg 800+ vidéki villamos szövetkezetek kezében van) ~55 000 alállomását összekötő ~200 000 mérföldnyi átviteli hálózati és ~5,5 millió mérföldnyi elosztóhálózati távvezetéken szolgáltat villamosenergiát. A szolgáltatók nem képeznek egységes villamosenergia-rendszert, így még a NERC[226] kritikus infrastruktúrák védelmét szabályozó, több mint egy évtizede kidolgozott, előírásai (CIP[227]) is csak az észak-amerikai közművek alig felére vonatkoznak kötelező jelleggel.[228,229] [39] 2017-ben a NERC konkrétumok említése nélkül, általánosságban hívta fel a figyelmet az ellátási lánc elégtelen védelméből fakadható kibertámadás lehetőségére, egyebek mellett az átviteli hálózat ellen.[230] [40] 2018-ben a GAO[231] adott ki ajánlást az USA szövetségi kormányzata felé arról, hogy az ügynökségek vegyék komolyabban az ellátási láncot fenyegető veszélyt.[232] [41]

Az elvégzett vizsgálatok szerint kibertámadással a hálózat mérete és bonyolultsága ellenére is komoly áramszünetek okozhatók. Az egyik forgatókönyv szerint az USA keleti országrészének hálózatát támadva 15 államban akár mintegy 92 millió fogyasztót érintő áramszünet lenne előidézhető. A vizsgálat szerint az erőművi generátorok alig 10%-ának kiejtése is kiterjedt áramszünetet okozna. Míg a ténylegesen megtörtént 2003. évi 4 napos északkeleti áramszünet mintegy ötvenmillió embert érintett és „csak" 4-10 milliárd $ közötti gazdasági

[226] NERC: North America Electric Reliability Council (Észak-Amerikai Villamos Megbízhatósági Tanács)
[227] CIP: Critical Infrastructure Protection
[228] R. K. Knake. „A Cyberattack on the U.S.s Power Grid, Center for Preventive Action" https://www.cfr.org/report/cyberattack-us-power-grid (Letöltve: 2022.01.14.)
[229] https://ics-community.sans.org/media/download/q5lgya/2020-07-23_Christopher-Conway-Miller-DOE-RFI.pdf
[230] K. D. Bose. "NERC Cyber Security Supply Chain Risks: Staff Report and Recommended Actions Docket No. RM17-13-000" North American Electric Reliability Corporation https://www.eenews.net/assets/2019/05/29/document_ew_02.pdf (Letöltve: 2022.01.14.)
[231] GAO: Government Accountability Office (Kormányzati Elszámoltatási Hivatal)
[232] GAO. "Information Security: Supply Chain Risks Affecting Federal Agencies". U.S. Government Accountability Office https://www.gao.gov/products/gao-18-667t (Letöltve: 2022.01.14.)

veszteséget okozott, addig a modellezett áramszünet kárértéke mintegy 243 milliárd $ lenne.[233]

Kína és Oroszország 2010-2012 óta támadja az USA ICS ellátási láncát. Az oroszok 2014 óta „vannak jelen" az USA villamosenergia-rendszerében.[234] [42]

2. Előzmény

SolarWinds/Orion támadás, amely az ellátási lánc sérülékenységét használta ki. A Colonial Pipeline támadás pedig azt bizonyította, hogy még IT rendszert érő zsarolóvírus támadással is lehetséges egy kritikus infrastruktúra működését alapvetően megzavarni, akár leállítani. Ezek az incidensek drámai módon azzal szembesítették az USA vezetését, hogy a kiberbiztonságban illetékes ügynökségeik képtelenek voltak megelőzni az utóbbi idők legnagyobb hatású kibertámadásait.

Történt ez annak ellenére, hogy az USA szövetségi kormányzata az elmúlt évek során több milliárd $-t fektetett egy olyan – Einstein nevű – rendszerbe, amelyet a digitális behatolások szövetségi szintű felderítésére terveztek. De mivel pl. a SolarWinds/Orion incidensben a támadó a bejutáshoz nem a már ismert kártékony szoftverek valamelyikét használta, hanem a kódsorokat egy megbízhatónak tartott szoftverbe rejtette, így az Einstein képtelen volt annak felderítésére. A támadást végül nem is az USA illetékes szervei, hanem egy magáncég fedte fel.

3. Kiemelkedő incidensek

A 2010-es évek végétől egyrészt mennyiségükben, másrészt minőségükben (újszerűség, súlyosság) súlyosabbá váltak az USA-t érő kibertámadások. Az alábbiak a villamosenergetikai szempontból legsúlyosabbakat emelik ki. Ez korántsem jelenti azt, hogy történtek volna további tanulságos támadások (pl. Oldsmar-i vízműben történt incidens, ahol a támadó hozzá tudott férni az ivóvízhez adagolt vegyszerek mennyiségét szabályozó rendszerhez).[235] [43]

[233] R. K. Knake. „A Cyberattack on the U.S.s Power Grid, Center for Preventive Action" https://www.cfr.org/report/cyberattack-us-power-grid (Letöltve: 2022.01.14.)

[234] 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: 2022.01.14.)

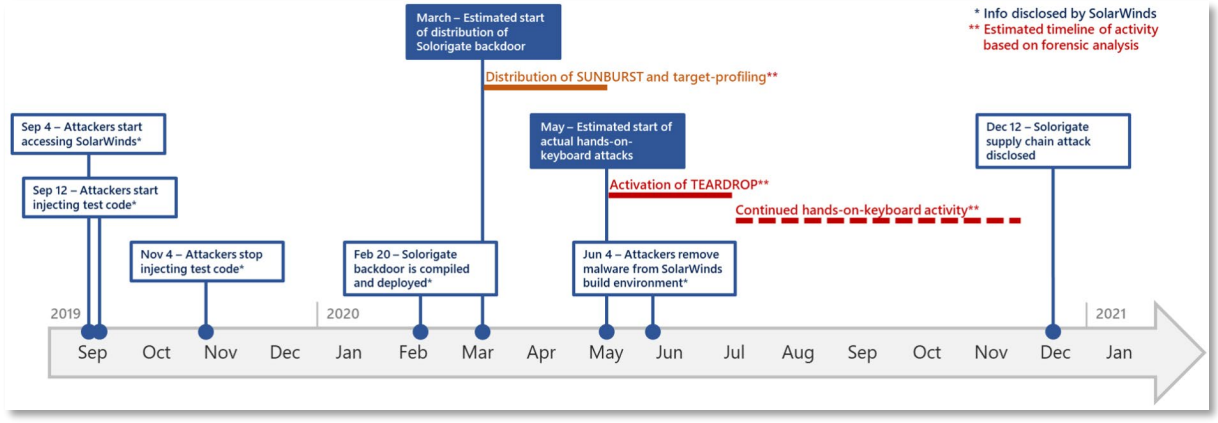
[235] K. Backman. "When Intrusions Don't Align: A New Water Watering Hole and Oldsmar." Dragos https://www.dragos.com/blog/industry-news/a-new-water-watering-hole/ (Letöltve: 2022.01.14.)

3.1. SolarWinds/Orion

2020. december 9-én a FireEye a rendszerébe történt betörést jelzett: a SolarWinds általa is használt termékében, az Orion IT hálózatmenedzsment szoftverben fedezett fel backdoort. A Orion backdoorolt verziója a szoftver rutinszerű frissítésével került a FireEye rendszerébe.

Az incidens a SolarWinds ~18.000 ügyfelét (ennek mintegy 20%-a kormányzati, pl. DHS, DOE), köztük az USA villamos művek ~25%-át érintette.[236] [44] Bár az eset jellegét tekintve inkább adatgyűjtő, felderítő, hírszerzési művelet, mintsem „hagyományos" kibertámadás, ennek ellenére az egyszerűség érdekében a továbbiakban támadásként említjük.

A támadás időbeli lefolyását, fontosabb lépéseit a 7.1. ábra mutatja be.



7.1. ábra: A SolarWinds/Orion támadás lépései[237] *[45]*

A Microsoft elemzése szerint a támadó a Solorigate DLL hátsó ajtót és a Cobalt Strike downloadert alkalmazta. Az első lépés a SolarWinds-nek az Orion következő verzióját tartalmazó szerverébe való behatolás, majd a kártékony kódsoroknak a letöltésre váró új Orion-verzióba való beültetése volt. 2020 tavaszán a biztonsági azonosítóval is ellátott új verziót az ügyfelek kétely nélkül letöltötték, melynek következtében rendszereikben backdoorok nyíltak a támadó számára.

A támadók 2020 júniusában eltávolították a Solorigate backdoor kódot a SolarWinds Orion szerveréről. Ez arra utalhat, hogy ekkorra a támadók a gyanútlan ügyfelek által letöltött

[236] I. Jibilian, K. Canales. "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal." Business Insider https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 (Letöltve: 2022.01.14.)

[237] P. Paganini: "SolarWinds Attack: Microsoft sheds lights into Solorigate second-stage activation." Security Affairs https://securityaffairs.co/wordpress/113681/apt/microsoft-solorigate.html/ (Letöltve: 2022.01.14.)

frissítések révén már a SolarWinds elegendő számú ügyfelének szervereit érték el. A támadó a backdoor telepítések és aktiválások után a Cobalt Strike hands-on-keyboard funkció használatával áttért az áldozatok hálózatainak óvatos felderítésére.

A támadók mindent megtettek nyomaik eltüntetésére. Pl. nagyon óvatosan mozogtak. „Csak" „szétnéztek", teljes adatállományok helyett csak célzottan vittek el anyagokat. A támadó a backdoorolt Orion-frissítés révén „elért" ügyfelek rendszereit, adatállományait a gyengébb védelműekkel kezdve haladt az erősebbek felé. Végül a FireEye egyik alkalmazottja kezdett gyanakodni akkor, amikor riasztást kapott arról, hogy a VPN hitelesítő adatait egy új eszközről használták. A FireEye-nál a történteknek utánajárva szembesültek a támadás jellegével és roppant súlyával.[238] [46]

A támadó a hatékony álcázásnak köszönhetően a FireEye általi decemberi leleplezésig hosszú ideig – mintegy 6-10 hónapig! – észrevétlenül mozoghatott a kompromittált rendszerekben. A nyomok professzionális eltüntetésével a támadó egyszerre nehezítette a behatolások detektálását és a forensics tevékenységet.[239]

A támadó sikerét a SolarWinds elégtelen biztonsági intézkedései is elősegíthették. Pl. az Orion frissítés kompromittált szerverének "solarwinds123" volt a jelszava.[240] [47] Az elégtelen biztonságról a támadást megelőzően a SolarWinds management belsős figyelmeztetést is kapott, de figyelmen kívül hagyta azt.

A támadás mögött – annak erőforrás- és időigényét, szofisztikáltságát látva – minden bizonnyal állami hátterű, APT támadót kell feltételezni. Az ukrajnai, Pivnichnai alállomás elleni 2016. évi támadáshoz hasonlóan a SolarWinds/Orion incidensre sem túlzás azt mondani, hogy a támadás mélységét, hatásait nem is annyira a támadó lehetőségei, hanem inkább szándékai korlátozták.

A történtek hazai tanulsága lehet, hogy különösen a kritikus infrastruktúráknak ajánlott – hangsúlyozottan csak a sok szükséges teendő egyikeként[241] – sürgősséggel elvégezni

[238] "What You Need to Know About the Massive Solarwinds Hack." ExcalTech https://www.excaltech.com/what-you-need-to-know-about-the-massive-solarwinds-hack/?nowprocket=1/ (Letöltve: 2022.01.14.)
[239] P. Paganini: "SolarWinds Attack: Microsoft sheds lights into Solorigate second-stage activation." Security Affairs https://securityaffairs.co/wordpress/113681/apt/microsoft-solorigate.html/ (Letöltve: 2022.01.14.)
[240] B. Barett. "Security News This Week: Russia's SolarWinds Hack Is a Historic Mess" https://www.wired.com/story/russia-solarwinds-hack-roundup/ (Letöltve: 2022.01.14.)
[241] A szervezeti szintű kockázatelemzésbe célszerű bevonni a beszállítókat és még inkább a kiszervezett tevékenységeket szolgáltató cégeket is. További hangsúlyos teendők (a teljesség igénye nélkül: biztonsági fókuszú rendszer- és hálózat-tervezés; a ZTA fokozatos bevezetése; folyamatos hálózatbiztonsági monitoring; netflow-elemzések stb.

beszállítói kockázataik felmérését és elemzését. Ehhez jó kiindulási alap lehet a NIST témába vágó publikációja.[242] [243] [48]

3.2. Colonial Pipeline

2021. május 6-án masszív ransomware támadás érte a Colonial Pipeline (USA) IT rendszerét. A támadók ~100 gigabájtnyi adatot loptak el, majd zárolták az IT rendszert.

A Colonial Pipeline az USA keleti országrészében, Texastól New Jersey-ig 14 államot érintő, kiemelt fogyasztókat – köztük hét repülőteret is – kiszolgáló, mintegy 5500 mérföldnyi csővezeték-rendszert üzemeltet, melyen napi mintegy 100 millió gallon üzemanyag mozog.

Bár a támadás „csak" az IT rendszert érintette, de ezen olyan, a működés szempontjából kritikus alkalmazások futottak, mint pl. a számlázás. Ezek elérhetetlenségére tekintettel a Colonial Pipeline vezetése az üzemanyagszállítások leállítása mellett döntött. Ennek nyomán az USA keleti keleti országrészében általános üzemanyaghiány lépett fel. A pánikszerű vásárlások miatt 1000+ benzinkúton fogyott el az üzemanyag.

A támadók mindezt a DarkSide zsarolóprogram alkalmazásával érték el.

A vizsgálat szerint a támadást egyetlen, hanyagul kezelt/megválasztott jelszó kiszivárgása okozhatta. A jelszó a ma már általánosnak (?) tekintendő két- vagy többfaktoros autentikáció helyett kizárólag egy „felhasználónév + jelszó" alapú VPN hozzáférés (kompromittált) jelszava volt. A kérdéses VPN-felhasználó ráadásul már nem is volt aktív, a hozzáférése mégis élt. A Colonial Pipeline tehát maga is segítette a támadó sikerét, mivel egyes alapvető megelőző intézkedések megtételét vétkes módon elmulasztotta.[244] [49]

Ennek ellenére az üzemanyagellátás szövetségi szinten is kiterjedt zavarára tekintettel a súlyos helyzet kezelésében a CISA, az FBI és az NSA révén a kormányzat is segítséget nyújtott.

A Colonial Pipeline végül ~4,4 millió $ váltságdíjat kifizetett.

[242] Information Technology Laboratory: Cybersecurity Supply Chain Risk Management https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management (Letöltve: 2022.01.14.)
[243] icscybersec. "A SolarWinds incidens tanulságai Magyarországon". ICS Cyber Security Blog https://icscybersec.blog.hu/2021/01/30/solarwinds-tanulsagok-magyarorszagon (Letöltve: 2022.01.14.)

[244] W. Turton, K. Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." Bloomberg https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (Letöltve: 2022.01.14.)

Az üzemanyagszállítások fokozatosan, először mellékvezetéken, kézi (!) vezérléssel indultak újra[245] [50]. Ez is felveti a vészhelyzeti, kézi üzemmódban történő működésre vonatkozó tervek kidolgozásának, valamint az azok szerinti működés rendszeres oktatásának, gyakoroltatásának szükségességét.

3.3. Kiber-fizikai támadások

A kiber-fizikai rendszerek „a kibertérben megjelenő utasítás vagy vezérlés hatására a fizikai térben, például egy aktuátor vagy manipulátor segítségével valamilyen fizikai változást (például mozgást) tudnak előidézni."[246][51] A paradigmaváltó villamosenergia-rendszer komponensei egyre inkább kiber-fizikai rendszereknek, ill. az ilyen rendszerek rendszerének tekintendők (különösen a digitális alállomások megjelenésével).

A kibertámadások sorában a Stuxnettel megjelentek, majd további támadásokkal – pl. Pivnichna (2016, SIEMENS SIPROTEC), Saudi Aramco (2017, Schneider Electric Triconex) – szaporodtak a kiber-fizikai rendszerek elleni támadások.

A villamosenergetikai berendezések elleni – fizikai kárt is okozó – kiber-fizikai támadás gyakorlati kivitelezhetőségét az ún. Aurora teszt igazolta.

3.3.1. Aurora teszt (2007)

Az USA Idaho National Laboratory-ban 2007-ben végrehajtott ún. Aurora teszt csak egy meglehetősen szűk szakmai kör előtt ismert, holott az ICS-ek elleni támadás, de főleg az ICS által felügyelt technológia tönkre tétele gyakorlati lehetőségének igazolása tekintetében – némi túlzása ellenére is – mérföldkőnek tekintendő.

A teszt egy 2,25 MW-os diesel-generátor gépegységen zajlott. A teszt erősáramú oldalról kifejezetten egyszerű: vajon a szinkronellenőrző relé szinkronhelyzet helyett oppozícióra történő átprogramozása után végzett hálózatra kapcsolások néhány kísérlet után a gépegység tönkremenetelét okozzák-e? Kiberbiztonsági oldalról a teszt azt volt hivatott vizsgálni, hogy a szinkronellenőrző relét távolról lehetséges-e elérni és úgy átprogramozni, hogy ez a jelzett állapotot hozza létre? A teszt lefolyását, a gépegység rázkódásait, a megjelenő füstöt, a szétrepülő alkatrészeket egy széles körben ismert videó[247] mutatja be.

A tesztet némi misztikum is övezi. Ez abból fakadhat, hogy bár a teszt dokumentumait nem titkosították, de 2014. júliusáig azokat mégis csak korlátozottan lehetett elérni. Az akkor

[245] J. Panettieri. "Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details." MSSPAlert https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/ (Letöltve: 2022.01.14.)
[246] Kovács László: A kibertér védelme, Hadtudomány, Ludovika Kiadó 2018.

[247] (38) Aurora Test Footage - YouTube

nyilvánossá vált több száz oldalnyi dokumentum itt[248] érhető el. De a misztikumot talán a teszt időpontja is növelhette. A 2000-es évek közepén nem volt triviális az, hogy a technológiai rendszerek kiberbiztonságát érintő problémákat csak a kiberbiztonsági **és** a technológiai szakterületek szakértőinek szoros együttműködésében lehet eredményesen, összefüggéseiben megérteni és kezelni. Ennek hiányában talán mindkét fél túlbecsülhette az Aurora teszt szofisztikáltságát. Míg erősáramú oldalról abban az időszakban nem lehetett kihívás a teszt eredményének megjóslása, addig a kiberbiztonsági oldal (akkor még) valóban nem lehetett teljesen biztos abban, hogy a gyakorlatban is kivitelezhető-e egy olyan kiber-fizikai támadás, azaz távolról elvégezhető-e egy olyan programmódosítás, amely akár a gépegység tönkremenetelét is előidézheti.

Ugyanakkor túlzásai ellenére is a teszt mérföldkőnek tekinthető annak felismerésében, hogy a kibertér felől olyan támadások indítása is lehetséges, amelyek anyagi javakat, vagy akár emberi életeket is veszélyeztethetnek. További adalék, hogy akár safety funkciójú – azaz éppen a javak és/vagy élet védelmét (!) (is) szolgáló – eszköz immár bizonyítottan ellentétes funkcióba (!) váltható át.

Az Aurora teszt igazi jelentősége annak gyakorlati bizonyítása, hogy technológiai berendezéseket fizikailag lehet károsítani akár a védelmükre, felügyeletükre hivatott berendezések manipulálásával is. Súlyos hiba lenne úgy tekinteni a tesztre, hogy a kibertérből kizárólag generátor károsodását okozó támadást lehetne kivitelezni. Valójában elvileg bármely technológiai berendezést (pl. transzformátort, segédüzemi tápellátást, villamos védelmet) is érhet ilyen jellegű támadás (mint azt a 2015. és 2016. évi, Ukrajna elleni támadások már a gyakorlatban is igazolták).

A tesztnek kiterjedt – esetenként felületes – irodalma van, így érdemes a szakmailag megalapozott, kiegyensúlyozott forrásokat keresni.[249] [52]

A teszt talán fontos gyakorlati megerősítés is lehetett a 2000-es évek végén lezajlott – az uráncentrifugák fizikai károsítását célzó – Stuxnet, avagy a SIEMENS védelmeket is megcélzó 2016. decemberi ukrajnai támadás tervezőinek is.

[248] 14f00304-documents.pdf (documentcloud.org)

[249] M. Zeller. (2011) Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator? Schweitzer Engineering Laboratories, Inc., IEEE 10.1109/CPRE.2011.6035612

A 2014. júliusától elérhető dokumentumokból kiolvashatóan az Aurora jellegű „sérülékenység" kihasználását új támadási vektorként felismerve a DHS kiterjedt vizsgálatot indított az USA saját kritikus infrastruktúráinak Aurora-jellegű sérülékenysége tekintetében.[250] [53]

3.3.2. JSHP transzformátor (201?-202?)

A szaksajtóban intenzíven tárgyalt SolarWinds/Orion incidens mellett jóval kevésbé kapott figyelmet a kínai JiangSu HuaPeng Transformer (JSHP)[251] által gyártott 2 db transzformátor esete.

A Pivnichna-i alállomás (2016) és a szaúdi finomító (2017) elleni támadások után is vannak arra utaló jelek, hogy a potenciális támadók nem adták fel a kifejezetten villamosenergetikai berendezésekben történő károkozás szándékát, hangsúllyal az USA kárára. A téma érzékeny, nemzetbiztonsági vonatkozásaira tekintettel nehéz megbízható információkhoz jutni, de a töredékekből az alábbi kép rakható össze.

A Colorado állam Ault alaphálózati alállomására a kínai JSHP transzformátorgyártól a 2010-es évek végén megrendelt 2 db 345/230 kV-os transzformátor közül az elsőnek 2019. augusztusi leszállítását követő átvizsgálásakor abban az átvevők „oda nem való elektronikát" találtak[252].

A második transzformátor 2020. tavaszán érkezett meg a Houston-i kikötőbe. Itt az USA szövetségi hatóságai lefoglalták és Sandia National Laboratories-be (SNL) szállíttatták. Önmagában a célállomás is elgondolkodtató. Az SNL hangsúlyos nemzetbiztonsági – pl. (atom)fegyverkezési – profillal rendelkezik. Az SNL a JSHP transzformátor odaszállításáig kevésbé volt villamos nagykészülék vizsgáló laboratóriumként nyilvántartva.

A „manipulált kínai trafó" teóriát erősíti, hogy a 2020. tavaszi lefoglalás után nem sokkal, május 1-én elnöki rendelet került kiadásra, amely egyebek mellett a külföldi eredetű transzformátorok beszerzésével és üzemeltetésével kapcsolatban is kemény megszorításokat írt elő. Ezt vélhetően az is motiválta, hogy az USA átviteli hálózatában ~2000 db, U_p>345 kV transzformátor üzemel úgy, hogy az elmúlt ~10 év alatt ~200 kínai gyártású transzformátor került be a hálózatba.

[250] Swearingen, M., Weiss, J., Huber, D. **„**What You Need to Know (and Don't) About the AURORA Vulnerability.": https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/ (Letöltve: 2022.01.14.)

[251] JSHP: A világ elsőszámú főtranszformátor gyártója. A 110 kV-500 kV feszültségtartományban éves kapacitása 500+ db transzformátor gyártása.

[252] 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: 2022.01.14.)

A transzformátorban valószínűsített backdoor a támadónak arra adhat lehetőséget, hogy pl. meghamísítsa az érzékelők jeleit. Pl. a hűtést indító hőmérsékleti érték meghamisításával elérheti, hogy pl. túlmelegedő tekercselés miatt felmelegedő szigetelőolaj esetén se induljon be a hűtés. A támadó ezzel a transzformátorban lévő tekercsek villamos szigeteléseinek olyan katasztrofális meghibásodását idézheti elő, amely enyhébb esetben a transzformátor üzemképtelenné válását, súlyosabb esetben kigyulladását okozhatja.

Fontos kiemelni, hogy az érzékelő jelének meghamisítására a támadó már 10 évvel korábban, a Stuxnet támadás keretében is képes volt, hiszen az üzemeltető semmit sem érzékelt az uráncentrifugák – végül tömeges tönkremenetelüket okozó – fordulatszám változtatásairól.

A transzformátorok igen drágák, emiatt nagy számban történő tartalékolásuk nem gazdaságos. Gyártási, pótlási idejük is hosszú. Ráadásul hatalmas súlyuk és méretük miatt mozgatásuk, szállításuk speciális nehézjármű-szerelvényt és hosszas előkészületeket kíván.

Amerikai szakmai berkekben vita bontakozott ki a transzformátorok Purdue modell szerinti 0. és 1. szintű elemeit veszélyeztethető új típusú fenyegetésről, amely az ezekbe (pl. transzformátorok szenzorjaiba, avagy felügyeleti elektronikáiba) még a gyártó által beépített backdoorok formájában jelenik meg.[253] [54]

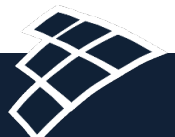
Van olyan szakértői vélemény, amely szerint a 0. és 1. szintű eszközök esetleges sérülékenysége komoly veszélyt jelenthet, mivel az IT és OT rendszerek elterjedten alkalmazott kibervédelmi megoldásai csak a magasabb szintű eszközöket és azok hálózatait védik, szükségtelennek tartva a legalsó szint(ek)hez tartozó eszközök védelmét.

Elvi lehetőségek a transzformátor backdooron keresztül elvégezhető műveletekre pl.:

- jel/adathamisítás, azaz a valóságos állapotot leképzőktől eltérő jelzések, ill. mérési értékek küldése a védelmek, automatikák, monitoring rendszerek és/vagy a SCADA felé, ezzel téves működés és/vagy fizikai károsodás és/vagy téves üzemirányítói döntés kiváltása,
- az ún. szabályozó transzformátorok fokozatkapcsolóinak biztonságostól eltérő működtetése.

Mint a 7.2. ábra mutatja, a korszerű transzformátorokba épített számos szenzor és működtető elem, továbbá a különféle automatikák és monitoring berendezések akár további lehetőségeket is kínálhatnak backdooron keresztüli – jogosulatlan, emberre és/vagy berendezésre veszélyes – műveletek végrehajtására.

[253] J. Weiss. "ICS cyber security is the second coming of the Maginot Line – and the Chinese have breached it." Energy Central https://energycentral.com/c/iu/ics-cyber-security-second-coming-maginot-line-%E2%80%93-and-chinese-have-breached-it (Letöltve: 2022.01.14.)



7.2. ábra: Nagytranszformátor Purdue 0. és 1. szintű eszközei, berendezései[254]

A backdooron keresztüli jel/adathamisítás erősödő veszélye felerősíti az ún. hihetőségvizsgálati alkalmazások szükségességét. Ezek szerepe, hogy hiányos, vagy nem egyértelmű adatállomány esetén is legyen lehetőség egy-egy paraméter valós értékének megbecslésére (pl. a fuzzy logikán alapuló alkalmazások esetében adathiányos környezetben, valószínűségi alapon).

A lefoglalt transzformátor a jelen 2. kiadás lezárásáig nem érkezett meg tervezett beépítési helyére, az Ault-i alállomásra. De az SNL a transzformátor vizsgálat eredményéről sem adott ki semmilyen hivatalos információt. Viszont nem hivatalos információ szerint a gyanú megalapozott volt, a transzformátorban potenciálisan kihasználható backdoort találtak.[255] [55] Azonban továbbra sincs olyan hivatalos (!) információ, amely bizonyított backdoora, de főleg azon keresztül megvalósított sikeres behatolásra utalna.[256] Így az sem tudható, hogy az elmúlt évek transzformátor meghibásodásai közül melyek lehettek esetleg backdooron keresztüli behatolás következményei. Az USA-ban indokolt lehet az elmúlt évek transzformátor meghibásodásainak vizsgálati anyagait ebből a szempontból ismételten átvizsgálni.[257] [56]

Bonyolítja a helyzetet, hogy Kínán kívüli transzformátor gyártók is egyre nagyobb mértékben szereznek be Kínában gyártott alkatrészeket, részegységeket. Így a nem kifejezetten kínai

[254] *https://www.ruggedmonitoring.com/advanced-energy/transformer*

[255] *J. Weiss. "Do the Chinese "own" our electric grids and other infrastructures?" Control Global https://www.controlglobal.com/blogs/unfettered/do-the-chinese-own-our-electric-grids-and-other-infrastructures/ (Letöltve: 2022.01.14.)*

[256] https://www.eenews.net/stories/1060216451/

[257] J. Weiss. "Large electric transformers are subject to cyber attacks which can cause outages of months to years." ControlGlobal https://www.controlglobal.com/blogs/unfettered/large-electric-transformers-are-subject-to-cyber-attacks-which-can-cause-outages-of-months-to-years/ (Letöltve: 2022.01.14.)

gyártmányú transzformátorokban is előfordulhatnak kínai gyártású – esetleg backdoorolt – komponensek. Ráadásul olyan globális – egyebek mellett óriástranszformátorokat is gyártó – villamosipari konglomerátumok, mint az ABB és a SIEMENS is befektettek Kínában, azaz a gyártmányaikban ugyancsak megjelenhetnek ezek a komponensek.[258]

Az SNL-vizsgálat részletes eredménye a kézikönyv 2. kiadás lezárásig nem került nyilvánosságra. Ugyanakkor figyelemre méltó az USA Nemzeti Hírszerzési Tanácsa által közzétett Nemzeti Hírszerzési becslés 2021. őszi megállapítása, amely szerint *„Kína a világ ultranagyfeszültségű rendszerei fejlett hálózati elemeinek – például* ***transzformátoroknak****, megszakítóknak és invertereknek – vezető beszállítója, ami megítélésünk szerint* ***kiberbiztonsági kockázatot jelent****.”*[259] [57]

Ki kell emelni, hogy a backdooron keresztüli behatolással a transzformátoron kívül további energetikai (fő)berendezések (pl. turbinák, generátorok, keringtető szivattyúk, segédüzemi berendezések) is célponttá válhatnak. Ez felveti a lehetséges célpont-berendezések, avagy általánosságban a villamosenergia-rendszer egésze ellenálló képessége (reziliencia) erősítésének szükségességére.

[258] https://www.eenews.net/stories/1060216451/

[259] National Intelligence Estimate. "Climate Change and International Responses Increasing Challenges to US National Security Through 2040." National Intelligence Council https://www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf (Letöltve: 2022.01.14.) Kiemelések a szerkesztőtől.

4. Kormányzati intézkedések az USA-ban

A Trump adminisztráció elkezdte, de a hivatalba lépő Biden-kormányzat – nyilván a SolarWinds, majd Colonial Pipeline támadásokkal még inkább ösztökélve – felpörgette a kormányzati szintű intézkedések sorát.

A főbb intézkedések, történések idősorosan:

- **Ault alállomás, első JSHP transzformátor telepítése** (2019 augusztus) Information Technology (controlglobal.com)[260]
  - *A transzformátor helyszíni vizsgálata során „oda nem való elektronikát, hardver backdoort" találtak.*
- Második JSHP transzformátor lefoglalása (2020 június) STG-Coalition-Letter-DOE-OMB.pdf (securethegrid.com)[261] [58]
  - *A Houston-i kikötőbe érkező második JSHP transzformátort szövetségi ügynökök lefoglalták és a Sandia National Laboratories-be (SNL) szállíttatták.*
- **Elnöki rendelet kiadása az Egyesült Államok átviteli hálózata biztonságának megerősítéséről** (EO 13920) (20.05.01.) Federal Register :: Securing the United States Bulk-Power System[262] [59]
  - *Az USA villamosenergia-rendszerét fenyegető veszélyek miatt országos vészhelyzetet kihirdetése.*
  - *Az EO 13920 hatálya alá tartozó berendezések: 69 kV, vagy annál nagyobb névleges feszültségű villamos hálózati és erőművi berendezések, valamint azok felügyeleti rendszerei.*
  - *A külföldi tervezésű, fejlesztésű, gyártású villamos hálózati berendezések eddigi beszerzési és alkalmazási gyakorlata, valamint az ilyen berendezések és rendszerek külföldiek általi tulajdonlása, irányítása nemzetbiztonsági kockázatot jelent.*
  - *Azonosítani kell a korábban külföldi tervezésben, fejlesztésben, gyártásban létrejött villamos hálózati rendszerelemeket. Ajánlásokat kell kidolgozni az ilyen elemek mielőbbi elkülönítésére, megfigyelésére vagy cseréjére. Kritériumokat kell meghatározni a kockázatot hordozó villamosenergetikai berendezéseknek és azok beszállítóinak meghatározására.*
- **A DOE információkérése az EO 13920 végrehajtási rendeletek**

[260] J. Weiss. "Emergency Executive Order 13920 – Response to a real nation-state cyberattack against the US grid." ControlGlobal https://www.controlglobal.com/blogs/unfettered/emergency-executive-order-13920-response-to-a-real-nation-state-cyberattack-against-the-us-grid/ (Letöltve: 2022.01.14.)
[261] Secure the Grid Coalition. "Improving Executive Branch Policies to Secure the United States Electric Grid." https://securethegrid.com/wp-content/uploads/2021/02/STG-Coalition-Letter-DOE-OMB.pdf (Letöltve: 2022.01.14.)
[262] 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.)

megalapozásához (RFI[263]) (20.07.08.)
Federal Register :: Securing the United States Bulk-Power System[264]

- *Az EO 13920-hoz kapcsolódó végrehajtási rendeletek előkészítése folyamatában a DOE az érdekelt felek számára lehetőséget biztosít észrevételeik, javaslataik megtételére.*
- *A DOE véleményeket kér az ellátási lánc fenyegetésekkel és sebezhetőségekkel szembeni védelemről, valamint az EO 13920 várható gazdasági hatásairól is.*

- **A DOE villamossági tanácsadó testülete megalapította hálózati ellenállóképességi és nemzetbiztonsági albizottságát** (20.11.30.)
  Department of Energy's Electricity Advisory Committee Establishes the Grid Resilience for National Security Subcommittee | Department of Energy[265] [60]
  - *Az EO 13920-szal összhangban magas szintű intézményi keret létrehozása a villamosenergia-rendszer elleni – a nemzetbiztonságot érintő (hangsúllyal ellátási lánc) – támadások elleni ellenállóképesség erősítéséhez.*
- **SolarWinds/Orion incidens kirobbanása** (20.12.13.)
  Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | Mandiant[266] [61]
  - *A felfedezett támadás méretének (globális jellegének) és módjának (SolarWinds Orion szoftver frissítésekor bejuttatott trójai) felismerése.*
  - *A támadás mögött APT áll.*
- **Tiltó rendelet kiadása a kritikus védelmi létesítmények biztonsága érdekében** (20.12.17.)
  BPS EO Prohibition Order Securing Critical Defense Facilities 12.17.20 - SIGNED.pdf (energy.gov)[267] [62]

[263] RFI: Request for information (RFI)

[264] 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.)
[265] Office of Electricity. "Department of Energy's Electricity Advisory Committee Establishes the Grid Resilience for National Security Subcommittee". https://www.energy.gov/oe/articles/department-energy-s-electricity-advisory-committee-establishes-grid-resilience-national/ (Letöltve: 2022.01.14.)
[266] FireEye "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor" https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor (Letöltve: 2022.01.14.)
[267] Department of energy. "Prohibition Order Securing Critical Defense Facilities" https://www.energy.gov/sites/prod/files/2020/12/f81/BPS%20EO%20Prohibition%20Order

  - *Vélhetően az EO 13920-hoz kapcsolódó végrehajtási rendeletek kiadásának késedelme miatt egyedi szigorítások kihirdetése a védelmi kritikus infrastruktúrák villamosenergia-ellátásának biztonsága érdekében.*
  - *Beszerzési, behozatali, átruházási, telepítési tilalom életbe léptetése a védelmi kritikus infrastruktúrákat ellátó villamos művekben meghatározott transzformátorokra és azok védelmi, felügyeleti rendszereire; megszakítókra; kondenzátor és fojtó telepekre; a mindezek felügyeletéhez, védelméhez kapcsolódó bármely szoftverre és firmware-re, amennyiben ez meghatározott ellenséges országokból – egyedüli nevesítettként Kínából – származnak.*

- **Elnöki rendelet az EO 13920 felfüggesztéséről (21.01.20.)**
  Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis | The White House[268] [63]
  - *A Trump után hivatalba lépő Biden elnök első intézkedései között 90 napra felfüggesztette az EO 13920 végrehajtását.*
- **Elnöki rendelet kiadása az USA ellátási láncok védelmének megerősítéséről** (21.03.01.)
  EO 14017 America's Supply Chains - Federal Register[269] [64]
  - *100 napos programok indítása az ellátási láncok védelmének erősítése céljából.*
  - *Vizsgálandó területek: pl. félvezető és nagy kapacitású akkumulátor gyártás, ritka földfém beszerezhetőség, közbeszerzési szabályozás.*
  - *A kritikus ellátási láncok reziliencijának erősítése.*
- **DOE: 8 millió $-os támogatás kiberbiztonsági kutatás-fejlesztésre** (21.04.06.)
  DOE Announces $8M to Build Robust and Cyber-Resilient Energy Delivery Systems | Department of Energy[270] [65]
  - *A DOE 8 millió $-os támogatási keretet hoz létre a villamosenergia-rendszer kiberbiztonságát és ellenállóképességét erősítő kutatások és fejlesztések finanszírozására*
- **DOE: intézkedések a villamosenergia-ipari műveleteket egyre gyakrabban**

%20Securing%20Critical%20Defense%20Facilities%2012.17.20%20-%20SIGNED.pdf (Letöltve: 2022.01.14.)

[268] The White House. " Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis" https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-protecting-public-health-and-environment-and-restoring-science-to-tackle-climate-crisis/ (Letöltve: 2022.01.14.)
[269] Executive Office of the President. "America's Supply Chains", Executive Order 14017 https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains (Letöltve: 2022.01.14.)
[270] Office of Cybersecurity, Energy Security, And Emergency Response. "DOE Announces $8M to Build Robust and Cyber-Resilient Energy Delivery Systems" https://www.energy.gov/ceser/articles/doe-announces-8m-build-robust-and-cyber-resilient-energy-delivery-systems/ (Letöltve: 2022.01.14.)

érő kiberfenyegetésekkel szembeni védelem erősítésére (21.04.20.)
Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats | Department of Energy[271] [66]

- *A DOE a villamosenergia szektorra fókuszálva 100 napos tervet indít az érdekelt felek véleményének megismerésére és a kiberbiztonsági kockázatok kezelésére.*
- *A tulajdonosoknak és üzemeltetőknek 100 nap alatt tervet kell készíteniük a közel valós idejű helyzetfelismerést és reagálási képességeket biztosító technológiák és rendszerek azonosítására és telepítésére az OT és ICS hálózatokban.*
- *Újabb RFI kiadása az USA energiarendszerek ellátási láncai biztonságára vonatkozó ajánlások megalapozásához.*
- *A 90 napra felfüggesztett EO 13920 ismét hatályba helyezése.*

- **A decemberi tiltó rendelet visszavonása** (21.04.22.)
  Federal Register :: Revocation of Prohibition Order Securing Critical Defense Facilities[272] [67]
  - *A tiltó rendelet visszavonása annak érdekében, hogy stabil politikai környezet jöjjön létre a 04.20-án kiadott RFI eredményes lebonyolítása érdekében, figyelembe véve az EO 13920 érvényességének 21.05.01-jei lejáratát is.*
- **Elnöki rendelet a nemzet kiberbiztonságának fejlesztéséről** (EO 14028) (21.05.12.)
  Executive Order on Improving the Nation's Cybersecurity | The White House[273] [68]
  - *Az USA aktuális kibervédelmi pillérjeinek meghatározása, közöttük negyedikként a szoftver ellátási lánc biztonságának erősítése.*
  - *Beszállítói megfelelőségi krit*
  - *ériumok dolgozandók ki, valamint kidolgozandó ezek ellenőrzési rendszere.*
  - *Kidolgozandó a forráskódok integritásvédelmének, tesztelésének rendszere.*
  - *Kidolgozandó a harmadik féltől származó szoftverkomponensek kezelésének rendszere.*
  - *Zero Trust Architecture bevezetése a szövetségi kormányzat intézményeiben.*
- **A Fehér Ház ajánlást ad ki a magánszektornak** (21.06.03.)

[271] Department of Energy "Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats" https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0 (Letöltve: 2022.01.14.)

[272] Energy Department. "Revocation of Prohibition Order Securing Critical Defense Facilities" https://www.federalregister.gov/documents/2021/04/22/2021-08483/revocation-of-prohibition-order-securing-critical-defense-facilities (Letöltve: 2022.01.14)

[273] The White House. "Executive Order on Improving the Nation's Cybersecurity" https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (Letöltve: 2022.01.14.)

White House sends out memo to private sector on cyberattack protections - thehill.com[274] [69]

- *Aktualitása: a Colonial Pipeline és a SolarWinds/Orion támadások.*
- *Ajánlások: pl. többfaktoros hitelesítés bevezetése, biztonsági mentések rendszeres tesztelése, IRP-k tesztelése.*

- **Nemzetbiztonsági memorandum a kritikus infrastruktúrák felügyeleti rendszerei kiberbiztonságának javításáról** (21.07.28.)
  National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems | The White House[275] [70]
  - *Szabályozási paradigmaváltás: kritikus infrastruktúra ágazatonkénti szabályozás helyett először egységes, majd ennek lebontásával ágazati szabályozások kidolgozása.*
  - *Kiberbiztonsági teljesítménycélok dolgozandók ki.*
  - *Ipari Felügyeleti Rendszerek Kiberbiztonsági Kezdeményezése: a kollaboráció szükségessége, azaz a kormány és kritikus infrastruktúrák közösségének önkéntes, közös erőfeszítésére vonatkozó kezdeményezés.*
- **CISA kezdeményezés** (21.08.09.)
  CISA sets up latest cyber defense initiative to defend critical infrastructure - Industrial Cyber[276] [71]
  - *Célja a köz- és magánszektor együttműködésének támogatása a kritikus infrastruktúrák kibervédelmének erősítése érdekében.*
  - *Annak felismerése, hogy az egyre súlyosabb kiberfenyegetéseket önmagában sem a szövetségi kormányzat, sem a magánszektor nem képes kezelni. Szoros együttműködésük elkerülhetetlen.*
  - *Ennek első lépése a kölcsönös információ megosztás rendszerének kidolgozása.*
- **Előrehaladási jelentés a 100 napos program végrehajtásáról** (21.08.16.)
  Progress Report: 100 Days of the Biden Administration's Industrial Control Systems (ICS) Cybersecurity Initiative and Electricity Subsector Action Plan | Department of

[274] T Axelrod. "White House sends out memo to private sector on cyberattack protections" The Hill https://thehill.com/policy/cybersecurity/556625-white-house-sends-out-recommendations-to-private-sector-on-protections (Letöltve: 2022.01.14.)

[275] The White House. "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems" https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (Letöltve: 2022.01.14.)

[276] IndustrialCyber. "CISA sets up latest cyber defense initiative to defend critical infrastructure" https://industrialcyber.co/article/cisa-sets-up-latest-cyber-defense-initiative-to-defend-critical-infrastructure/ (Letöltve: 2022.01.14.)

Energy[277] [72]

- *A DOE hitet tesz a kollektív felkészültség és a kollektív reagálás mellett.*
- *A DOE technikai és elemzési támogatást nyújt kisebb közüzemi szolgáltatóknak, önkormányzati és vidéki szövetkezeti áramszolgáltatóknak.*
- *A DOE frissítette a Kiberbiztonsági Képességek Érettségi Modelljét (C2M2).*

- **Biden elnök Fehér házi találkozója a nagy technológiai cégek vezetőivel** (21.08.25.)
  FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity | The White House[278] [73]
  - *A nagy technológiai vállalatok vezetői ígéretet tettek arra, hogy erősítik ellátási láncaik biztonságát, továbbá konkrét intézkedések felvállalásával több milliárd dollárt fektetnek be a zéró bizalmi programok kiterjesztésébe, a nyílt forráskódú biztonság javításába és más intézkedésekbe.*
  - *A NIST és a további érdekelt felek együttműködésében kezdődjön meg a technológiai ellátási lánc új biztonsági keretrendszerének kidolgozására.*
- **Paradigmaváltás lehetőségének felvetése a NERC szabályozási gyakorlatában** (21.09.30.)
  'Maybe it's not the right approach anymore' — FERC Chair Glick mulls new security paradigm for power sector | Utility Dive[279] [74]
  - *Éves megbízhatósági technikai konferenciáján a FERC[280] bejelentette, hogy a fejlemények (SolarWinds/Orion és Colonial Pipeline támadások, a villamosenergia-rendszer paradigmaváltása, az elosztott energiatermelés térnyerésére, az IT-OT konvergencia, az ellátási láncok sérülékenysége) nyomán a FERC hajlamos újra gondolni az energiaágazat kiberbiztonsági szabályozását.*
  - *Az eddigi gyakorlat (a biztonsági követelmények szintjét a létesítmény mérete határozza meg) megváltozhat a kockázatértékelésen és hatásvizsgálaton alapuló besorolásra.*
- **Kritikus infrastruktúrák felügyeleti rendszerei kiberbiztonsági teljesítménycéljai és célkitűzései** (21.09.21.)

[277] Department of Energy. "Progress Report: 100 Days of the Biden Administration's Industrial Control Systems (ICS) Cybersecurity Initiative and Electricity Subsector Action Plan." https://www.energy.gov/articles/progress-report-100-days-biden-administrations-industrial-control-systems-ics (Letöltve: 2022.01.14.)

[278] The White House. "FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity" https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/ (Letöltve: 2022.01.14.)

[279] R. Walton. " 'Maybe it's not the right approach anymore' — FERC Chair Glick mulls new security paradigm for power sector" https://www.utilitydive.com/news/maybe-its-not-the-right-approach-anymore-ferc-chair-glick-mulls-new-se/607594/ (Letöltve: 2022.01.14.)

[280] FERC: Federal Energy Regulatory Commission (Szövetségi Energia Szabályozási Bizottság)

Control Systems Goals and Objectives | CISA[281] [75]

- *A CISA a létező szabályozásokból kiindulva ajánlott gyakorlatokat, előzetes teljesítménycélokat dolgozott ki.*
- *A munka az érdekelt felek lehető legszélesebb körének részvételével folytatódik.*

A fejleményeket összegezve látható, hogy az EO 13920 tételes és azonnali tiltásai helyébe hosszabb távú és kollaboratív építkezés lép. A kereteknek az érdekelt felek bevonásával történő kidolgozását követően alapvető kérdés lesz a várhatóan hatalmas költségek fedezetének megteremtése. A költségek mértékének megítélése nem lehet független attól a vagyoni, társadalmi kártól, amely a kiadások révén megelőzhető vagy csökkenthető.

[281] Cybersecurity & Infrastructure Security Agency. "CRITICAL INFRASTRUCTURE CONTROL SYSTEMS CYBERSECURITY PERFORMANCE GOALS AND OBJECTIVES" https://www.cisa.gov/control-systems-goals-and-objectives (Letöltve: 2022.01.14.)

5. Hazai vonatkozások

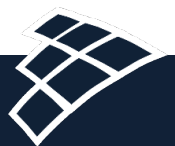
A publikus információk alapján hazánk jelenleg nem célpont. Ugyanakkor ennek jövőbeni lehetősége nyilván nem is zárható ki teljes bizonyossággal. Így a köteles gondosság jegyében folyamatosan figyelnünk és értékelnünk kell a globális fejleményeket.

Az USA az utóbbi néhány évben történtek alapján mind a beszállítók, mind a tulajdonosok, üzemeltetők felé új, szigorúbb követelményeket kezd támasztani. A tervezők, gyártók nem fognak külön-külön USA-specifikus és nem-specifikus rendszereket készíteni. Hazánk a globalizált világ része. Ebből következően az USA-ban érvénybe lépő szigorúbb szabályozások hatásai szükségképpen globálisan – így előbb-utóbb hazánkban is – megjelennek.

Ez a helyzet egyben esély is az élvonalbeli hazai kutató-fejlesztő helyek számára. Nálunk is helye van olyan aktuális témák kutatásának, mint pl. a gyári eredetiség garantálásának, tanúsításának, a hamisított berendezések, alkatrészek, manipulált szoftverek kiszűrésének.

Egyre inkább elkerülhetetlen lesz, hogy a (köz)beszerzések szabályozásában és gyakorlatában az eddigi „árközpontúság" helyébe „ár **ÉS** biztonság központúság" lépjen. Értelemszerűen ehhez (is) kormányzati szintű intézkedések (szabályozási, szervezeti stb.) és ezek részeként a finanszírozás biztosítása lesz szükséges. Végül alapvető szemléleti váltásra is szükség van. Az eddigi részleges, csak egy-egy szakterület szempontjait érvényesítő szemlélet helyébe átfogó, ténylegesen holisztikus megközelítésnek kell lépnie. Ennek jegyében érdemes akár a 2015. és 2016. évi ukrajnai támadásokról fellelhető forrásokat ismét áttekinteni és a korábbinál is átfogóbban átvizsgálni. „A leggyengébb láncszem az ember!" elv alapján az érintett vezetők és munkavállalók érzékenyítése is szükséges a fentiek szerinti erősödő fenyegetési típusokra.

A ténylegesen holisztikus megközelítés az egyik előfeltétele annak, hogy csökkenthető legyen a magyar villamosenergia-rendszert érő, akár berendezés meghibásodásával is járható kiber-fizikai támadás esélye.



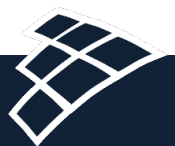
8. melléklet: A hatályos hazai szabályozási környezet bemutatása

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
  - 1/2022. (IV. 29.) OAH 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.)

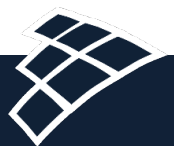
személyi/szervezeti hatály	• 2. § (1) bekezdésében felsorolt állami- és önkormányzati szervek, intézmények • a 2. § (1) bek. szerinti szervek számára adatkezelést végzők • a jogszabály alapján a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói • az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek (*a továbbiakban együttesen: létfontosságú infrastruktúrák*) • az alapvető szolgáltatást nyújtó szereplőként azonosított szervezetek • az elektronikus információs rendszert működtető, a központi államigazgatási és kormányzati tevékenység szempontjából fontos, nemzetbiztonsági védelem alá eső szervek
szabályozási kör	a jogszabály hatálya alá tartozó szervezetek elektronikus információs rendszerei (*hálózatok, eszközök/eszközcsoportok és digitális adatok; a továbbiakban: EIR*)
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; intézkedési*) 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	Incidenskezelés, 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*); • taxatíve 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 rendszerelemek (*az ágazatok valamelyikébe tartozó szolgáltatás, eszköz,*

	létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna) üzemeltetői
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

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)

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 összehangban)*
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 zártsági feltételei (*jogosulatlan hozzáférés kizárása, adatmódosítás elleni védelem – a számlázási rendszernek meg kell felelnie az általános információbiztonsági zártsági követelményeknek is, ennek érdekében adminisztratív, fizikai és logikai intézkedésekkel*

	kell biztosítani az általános információbiztonsági zártsági 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.)

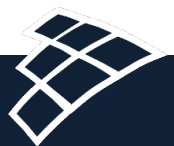
személyi/szervezeti hatály	• nukleáris létesítmény és radioaktívhulladék-tároló engedélyesek; • atomenergia alkalmazók
szabályozási kör	az atomenergia békés célú alkalmazása, a kapcsolódó jogosultságok és kötelezettségek
releváns főbb rendelkezések	• a fizikai védelem szabályai (tervezési alapfenyegetettség, mélységében tagolt védelem)
releváns kapcsolódások	• 190/2011. Korm. rendelet • 1/2022. OAH 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 radioaktívhulladék-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 bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer sértetlenségének és rendelkezésre állásásnak 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 bizalmasságára, 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.
- 1/2022. OAH rendelet
- OAH FV-18. sz. útmutató

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

1.11. 1/2022. (IV. 29.) OAH 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 rendszerelemei, 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 managemen*

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 egyenszilárdságú 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*) teljes körű, 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 alágazaton) 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 összehangban 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 metódusára és fogalomhasználatára épülő, egyedi, de teljes körű szabályozás bevezetése jelentene előrelépést. »

9. melléklet: Útmutató a létfontosságú rendszerelemmé kijelölt, valamint az alapvető szolgáltatást nyújtó villamosenergia alágazati szereplők jogszabályi megfelelőségéhez

1. Kötelezettségek

Kiindulási alap létfontosságú rendszerek esetében: 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 kötelezettségek*et 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 alágazatonként, villamosenergia alágazat tekintetében a *Magyar Energetikai és Közmű-szabályozási Hivatal*: Energia vhr. 3. § a);
- európai és nemzeti létfontosságú rendszerelemek ágazati kritériumainak meghatározása, villamosenergia alágazatban: Energia vhr. 4. § a) és 5. §;
- *jelentős zavar értelmezése a villamos energia alágazatban*: Energia vhr. 9. §;
- *alapvető szolgáltatásokhoz tartozó küszöbértékek a villamos energia alágazatban*: Energia vhr. 13. §;
- *biztonsági összekötő személy képesítési követelményei*: Energia vhr. 17. §.

Kiindulási alap alapvető szolgáltatást nyújtó szereplők esetében: az Lrtv. 2020 júliusában hatályba léptetett módosítása alapján a NIS irányelv szerinti alapvető szolgáltatást nyújtó szereplők nem csak a létfontosságúvá kijelölt rendszerelemek közül kerülhetnek ki, hanem a 2/A. § értelmében külön is azonosíthatóak.

Információbiztonsági vetület:

Az energia ágazat kijelölt kritikus infrastruktúrái, valamint az önmagukban alapvető szolgáltatást nyújtó villamosenergia alágazati szereplők 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 egyenszilárdságú 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 hatóság meghatározása: Hatósági vhr. 2. §;
- *a honvédelmi célú elektronikus információs rendszerek kivételével valamennyi az Ibtv. hatálya alá tartozó szerv 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 létfontosságú rendszerelemeknél

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 létfontosságú rendszerelemeknél

A kijelölő hatóság a szervezetre vonatkozó kijelölő határozatban felhívja az üzemeltető figyelmét az Lrtv. által meghatározott, biztonsági összekötő személy alkalmazására vonatkozó kötelezettségére. Ennek teljesítésére az Lrtv. vhr. 6. § (8) bekezdés alapján a kijelölő határozat véglegesség válásától számított 60 napja van, amelynek elmulasztása esetén a nyilvántartó hatóság közigazgatási szankciót alkalmazhat.

A biztonsági összekötő személy megbízásáról, a biztonsági összekötő személy bejelentésére szolgáló elektronikus űrlap kitöltésével, 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 képesítési követelményei az energia ágazatban kijelölt létfontosságú rendszerelemeknél

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 képesítéseket, 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 szakképesítés, 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 létfontosságú rendszerelemeknél

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)],

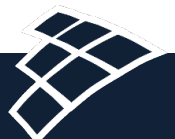
– kijelölés visszavonásának alátámasztásaként [Lrtv. vhr. 2. §. (2) a.]

- *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 létfontosságú rendszerelemeknél

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) akkumulálja 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 széles körűek, 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 üzemeltető az üzemeltetői biztonsági tervét és az annak alapjául szolgáló kockázatelemzést a BM OKF által meghatározott (honlapján közzétett[282]) elektronikus (géppel olvasható) formában és módon írásban készíti el – 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.

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

[282] BM Országos Katasztrófavédelmi Főigazgatóság (katasztrofavedelem.hu)

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. Fentieken 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 feltüntetésével.

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 – például 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 légterének, 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.

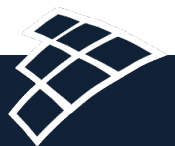
A normál működés ismertetését követően a minimálisan elvárt működés folyamata, erőforrásai is kerüljenek bemutatásra a fenti keretrendszer mentén.

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 fentieken 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:

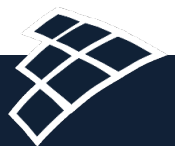
A létfontosságú rendszerelem tevékenységének ismertetése során törekedni kell a részletes, kapacitásadatokkal kiegészített, teljes körű leíró bemutatásra.

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).

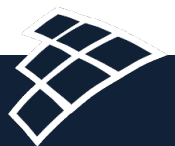
A következő lépésben meg kell határozni a kockázatok valószínűsíthető okait, a bekövetkezéskor prognosztizálható negatív hatásait, az okozott kárértéket.

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(eke)t. A kockázatcsökkentő (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 döntés-előkészítéshez 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.

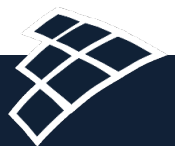
3. A kijelölt létfontosságú rendszerelemek, illetve az alapvető szolgáltatást nyújtó szereplők elektronikus információs rendszereikkel kapcsolatos kötelezettségei:

a. A létfontosságú rendszerelemnek és az alapvető szolgáltatást nyújtó szereplőnek a hatóság kijelölő/azonosításról szóló határozatának véglegessé válásától számított 60 napon belül be kell jelentkeznie elektronikus úton a hálózati és információs rendszerei biztonságának felügyeletét ellátó hatóságnál, amely során:

- *megadja a szervezet azonosításához szükséges alábbi adatokat:*
  - 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 nemzeti CSIRT 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: Létfontosságú rendszerelemnek és alapvető szolgáltatást nyújtó szereplőnek a hatóság kijelölő/azonosításról szóló határozatának véglegessé válásától számított egy éven belül vizsgálatot kell folytatnia az Ibtv. rendelkezései alapján, a következők szerint:

- *Ibtv. 2. § (2) c)* pont alapján a *kijelölt létfontosságú rendszerelemekre,*
- Ibtv. 2. § (2) d) pont alapján az *alapvető szolgáltatást nyújtó szereplőkre 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 követelmények[283]

- Ibtv. 7-8. § alapján az *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 az érintettek 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 bekövetkezhető 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 foganatosítani az adott kockázat csökkentésére. Végül fel kell tárni a *maradványkockázatokat* is, amelyek további értékelésre szorulnak.

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*

[283] Forrás: Saját szerkesztés

elsődlegesen[284] 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 *irányadó* (jogszabály 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 9.2. ábrákon szereplő 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. Jogszabályi 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 jogszabályokban előírtaknak, vagyis adott időn belül el kell érni az irányadó biztonsági osztályt.

9.3. ábra: Az Ibtv. szerinti biztonsági osztályba sorolás módszertana

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:

[284] BM rendelet, 1. melléklet 1.1.2. alapján.

- *adminisztratív* védelmi intézkedések: például a szabályzatok, a biztonságért felelős személyek kinevezése, nyilvántartások, kockázatelemzés, dokumentációk, eljárásrendek megléte, üzletmenet-folytonosság tervezése, oktatás, képzés stb.
- *fizikai* védelmi intézkedések: például a rendszerhez és az eszközökhöz történő hozzáférés szabályozása, ellenőrzése, felügyelete, az áramellátás biztosítása, tűz-, víz-, egyéb károk elleni védelem, karbantartás stb.
- *logikai* védelmi intézkedések: például a biztonsági elemzések, tesztelések, konfigurációkezelés, frissítések, naplózások, az adathordozók védelme, azonosítás, hitelesítés, vagy a kommunikáció védelme.

Amennyiben a vizsgálat eredményeként az adott rendszer vonatkozásában megállapított *irányadó biztonsági osztály magasabb, mint az aktuális, akkor cselekvési tervet kell készíteni* az Ibtv. 8. § (5) bekezdésnek megfelelően. A következő biztonsági osztályba lépést az Ibtv. 8. § (3) bekezdése alapján két év alatt kell biztosítani, vagyis az elektronikus információs rendszerre vonatkozó védelem elvárt erősségének eléréséhez a szervezetnek *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.[285]

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 funkciójukat, szerepüket, illetve meghibásodásuk, kiesésük következményeit mutatja be.

[285] https://nki.gov.hu/hatosag/tartalom/urlapok/

Biztonsági szint meghatározása

Az elektronikus információs rendszerek 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 teljes körű védelmet.

Az elektronikus információs rendszer szintbe sorolását az NBSZ NKI által közzétett ún. *SZVI tábla segíti*, amely – kitöltési útmutatóval együtt – letölthető.[286]

[286] 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.

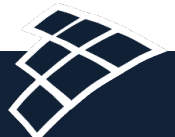
Az 1999. évi alkotmány szerint a kantonokat (tartományokat) mindazok a hatáskörök megilletik, amelyeket nem utaltak tételesen a szövetség hatáskörébe. A kétkamarás svájci parlament – a Szövetségi Gyűlés – a legfőbb államhatalmi szerv. Az egyik kamara az Államtanács 46 tagját (minden kantonból 2 tag, 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 több száz szolgáltató osztozik. Két szervezet fogja össze a piaci szereplők jelentős részét. A több mint 400 tagot számláló svájci villamosenergia társaságok szövetsége (VSE[287]) a villamosenergia előállításában, szállításában, elosztásában és kereskedelmében érintett vállalatokat, míg a svájci smart grid iparági szövetség (SWISSMIG[288]) a gyártókat, megoldásszállítókat tömöríti.

Szabályozási oldalról a svájci Szövetségi Energia Hivatal[289] (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.

[287] https://www.strom.ch/de
[288] https://www.swissmig.ch/
[289] 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 törvény[290] (Stromversorgungsgesetz vagy röviden StromVG). Célja a biztonságos villamosenergia-ellátás és a versenyképes villamosenergia-piac feltételeinek megteremtése. A törvényt az alkotmány 91. cikke[291] 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.[292] 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 rendelet[293] (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

[290] https://www.admin.ch/opc/de/classified-compilation/20042411/index.html
[291] https://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a91
[292] https://www.bfe.admin.ch/bfe/de/home/politik/energiestrategie-2050.html
[293] https://www.admin.ch/opc/de/classified-compilation/20071266/index.html

kormány és az SFOE energiakutatási tervei támogatták az elektromos hálózatok intelligens hálózatok felé történő fejlesztését.

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 Intézetet[294] (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.[295]

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 metodológia[296] alapján. Az újonnan beszerzett okosmérők esetén a kötelező tanúsítás alkalmazásának hatályát elhalasztották 2020. január 1-jére.

5. Prüfmethodologie - 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 Prüfmethodologie megalkotásakor az ESMIG (The European Smart Energy Solution Providers[297]) által készített, akkor még nem publikált Protection Profile-ból (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,

294 https://www.metas.ch/metas/de/home/dl/datensicherheitspruefungen.html
295 https://www.strom.ch/de/media/6404/download
296 https://www.swissmig.ch/wp-content/uploads/2019/07/PruefMethodologie-V21.pdf
297 https://esmig.eu/news/first-harmonised-european-approach

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.

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.

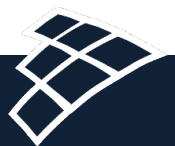
7. Tapasztalatok

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 megfelelőséget 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 ENCS[298] 2019. júliusában tette közzé az intelligens mérőrendszerek beszerzésekor érvényesítendő információbiztonsági követelményrendszerét.[299]

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

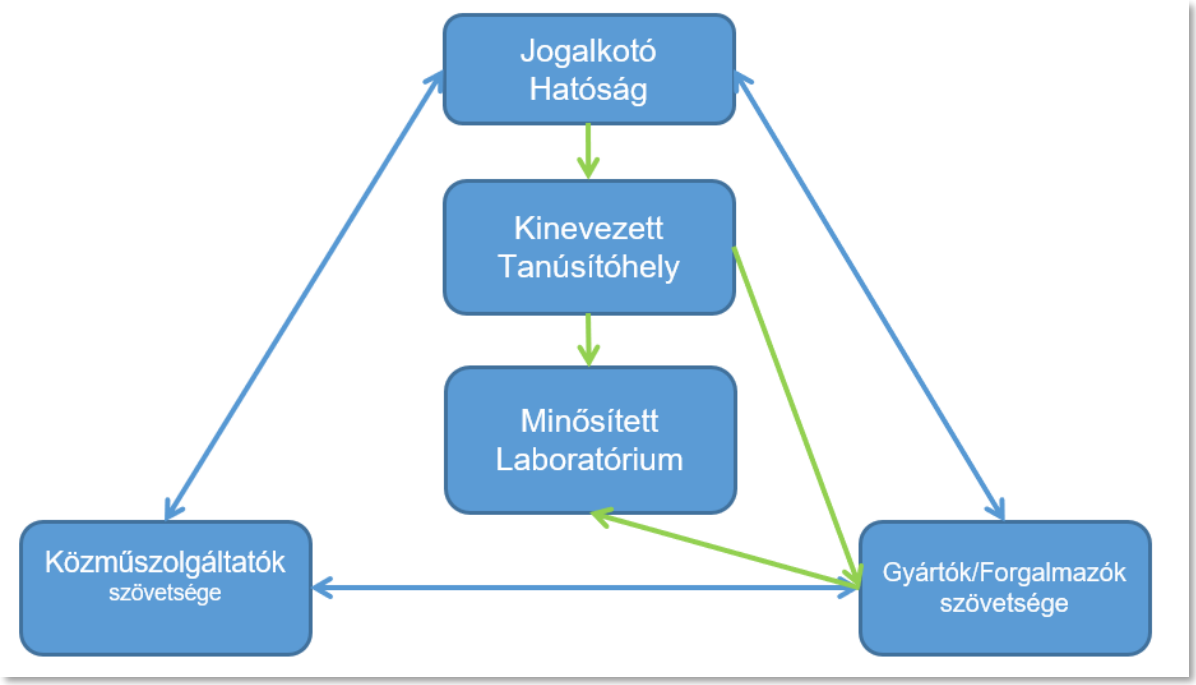
[298] ENCS: European Network for Cyber Security (Európai Hálózat a Kiberbiztonságért)
[299] https://encs.eu/encs-document/smart-meter-security-requirements/

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.
- Kidolgozott, évtizedesen bizonyított módszertanok, és szakemberek állnak mögötte (tanácsadók, értékelők, tanúsítók).
- Bevezetése 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 megfelelve 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 Cybersecurity[300]-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.

[300] 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 beszúrt 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 legsúlyosabb 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, széles körű 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 kötöttségek 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, például a 300 MW-nál nagyobb fogyasztás korlátozást végző automatikus terhelésledobási 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.[301] [76]

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 kiterjeszteni[302] [77], 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.

[301] 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.)

[302] 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 ellenálló képességük 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 kötöttségek 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 szerveket 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 ellenálló képességének 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.[303]

[303] 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 kétévente 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.

Például 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 kiszolgálását 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. Például az 2. Ivóvízellátás / 2.2. Ivóvízfeldolgozás / 2.2.1. Ivóvízfeldolgozó vízmű esetén évi 22 millió m^3 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 kétévente 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

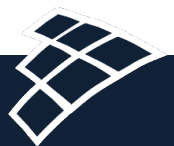
A BSIG 8.a. szakasz 2. bekezdés szerint az iparági szereplők ágazatspecifikus "state-of-the-art" biztonsági szabványokat határozhatnak meg. Ezek összefoglaló neve B3S (Branchenspezifische Sicherheitsstandards). A BSI kérés esetén eldönti, hogy ezek a szabványok megfelelnek-e a jogszabályi előírásoknak, 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.



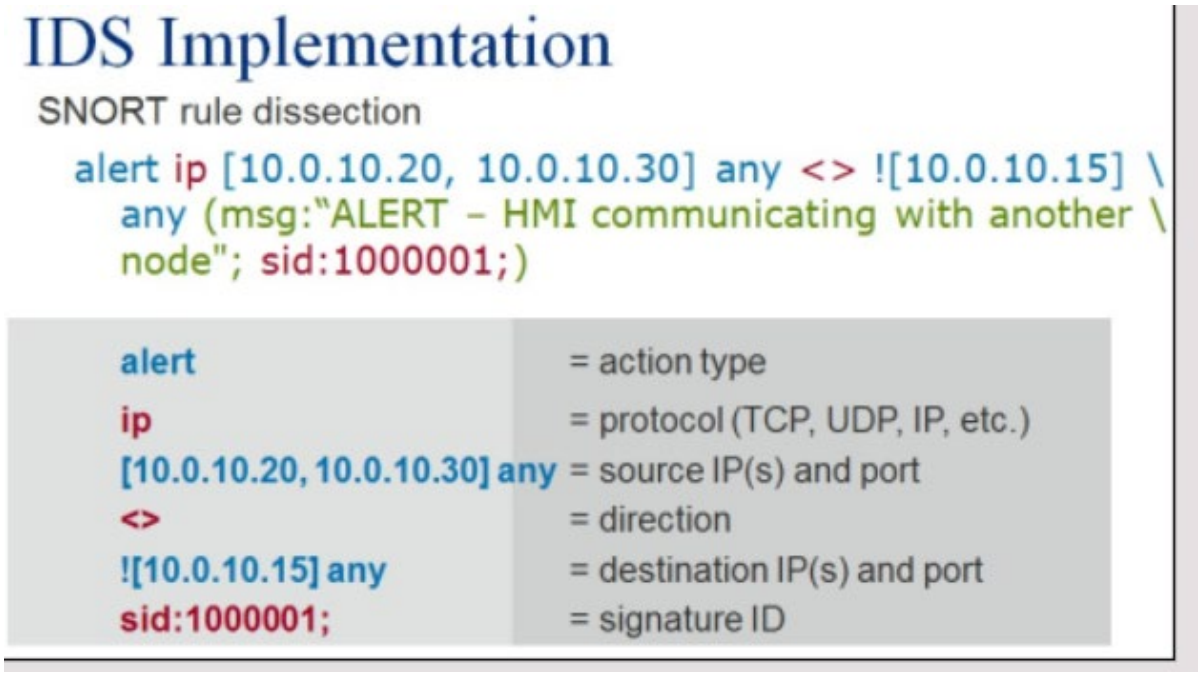
A KRITIS rendszer azon alapállásból készült, hogy a világ legbiztonságosabb rendszerét hozza létre a kritikus infrastruktúrák védelmére. Ehhez sikerült széles körű szakmai együttműködést kialakítani, és kevés átfedéssel a meglévő ágazati szabályozásokkal összhangban megalkotni és bevezetni a szabályozást. Ugyanakkor sikerült elkerülni a túlszabályozást és kezelhető rendszert kialakítani, észszerű 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. példa[304]

SNORT-szabály, ami szerint, ha a HMI a vezérlőtől eltérő bármely eszközzel kommunikál, akkor az IDS a zöld üzenetben megadott riasztást küldi:



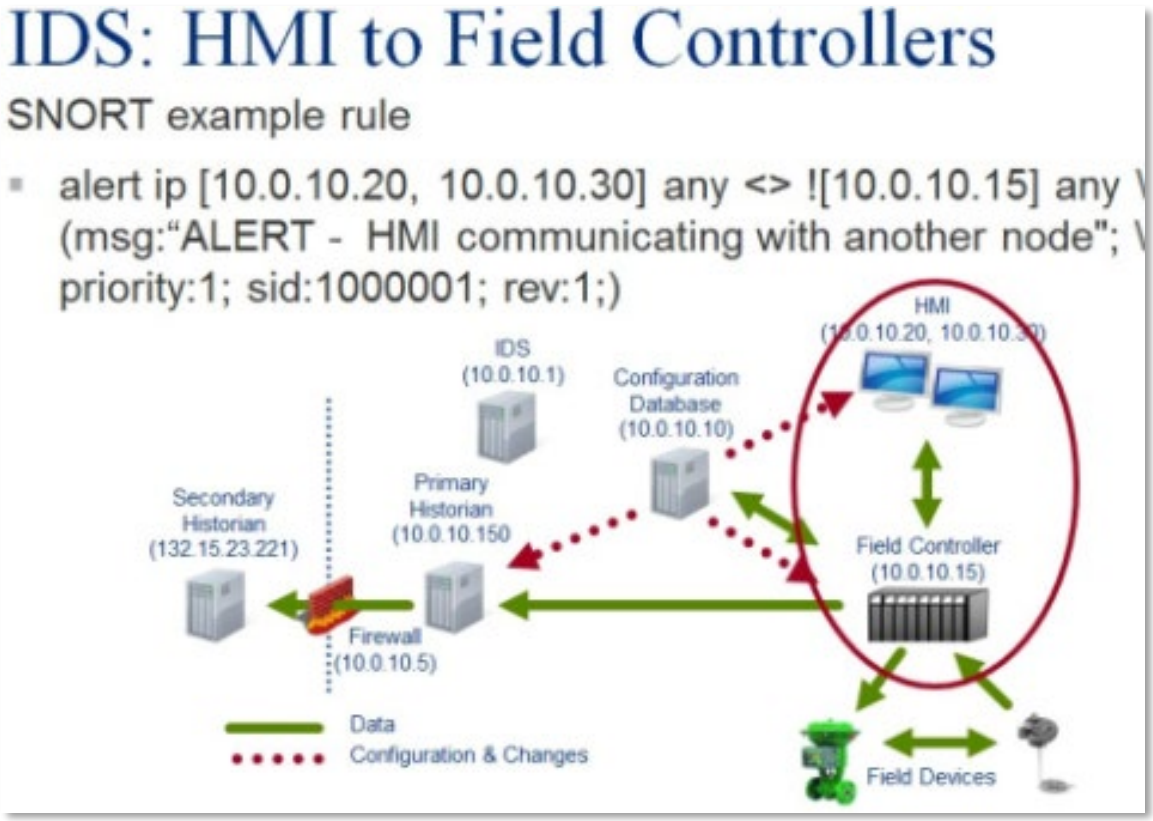
14.1. ábra: Alkalmazási példa 1.

- 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 „triggert".
- 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).

[304] ICS CERT oktatási anyag

2. példa

Kommunikáció "terepi" vezérlők és HMI között:



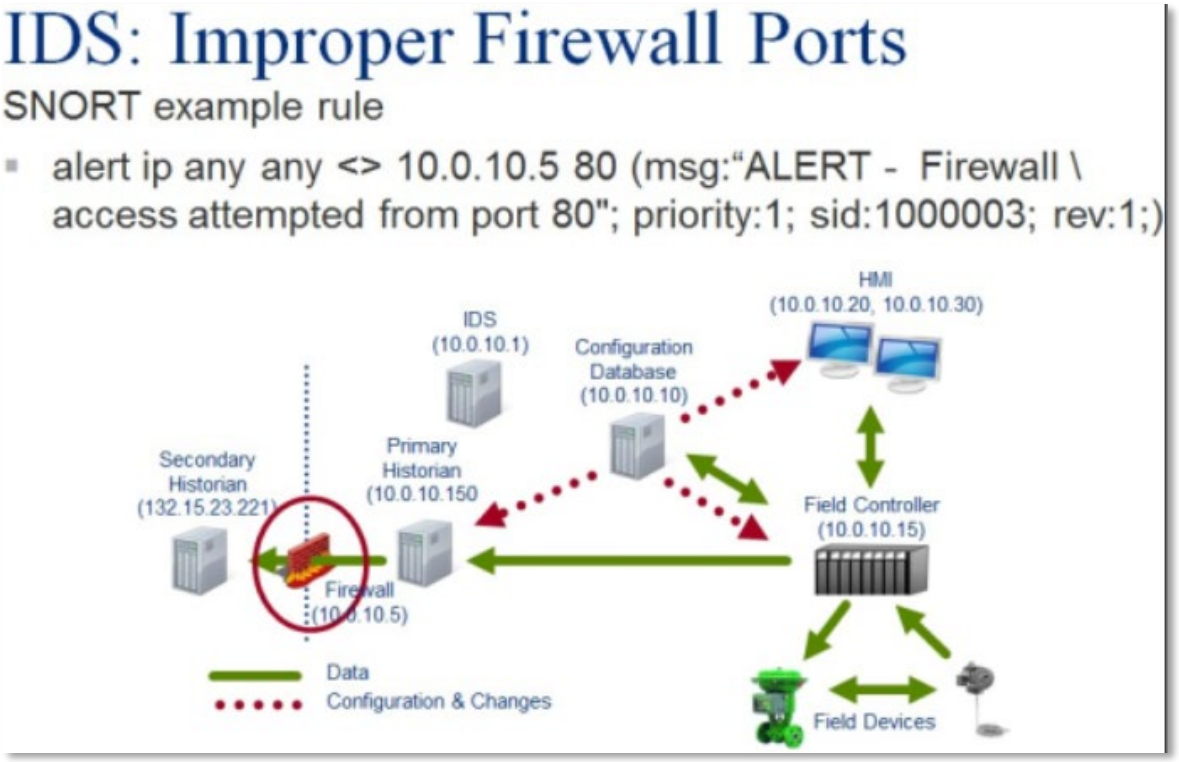
14.2. ábra: Alkalmazási példa 2.

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:



14.3. ábra: Alkalmazási példa 3.

A tűzfal figyelésére is kidolgozhatunk szabályokat. Ez a szabály például 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.

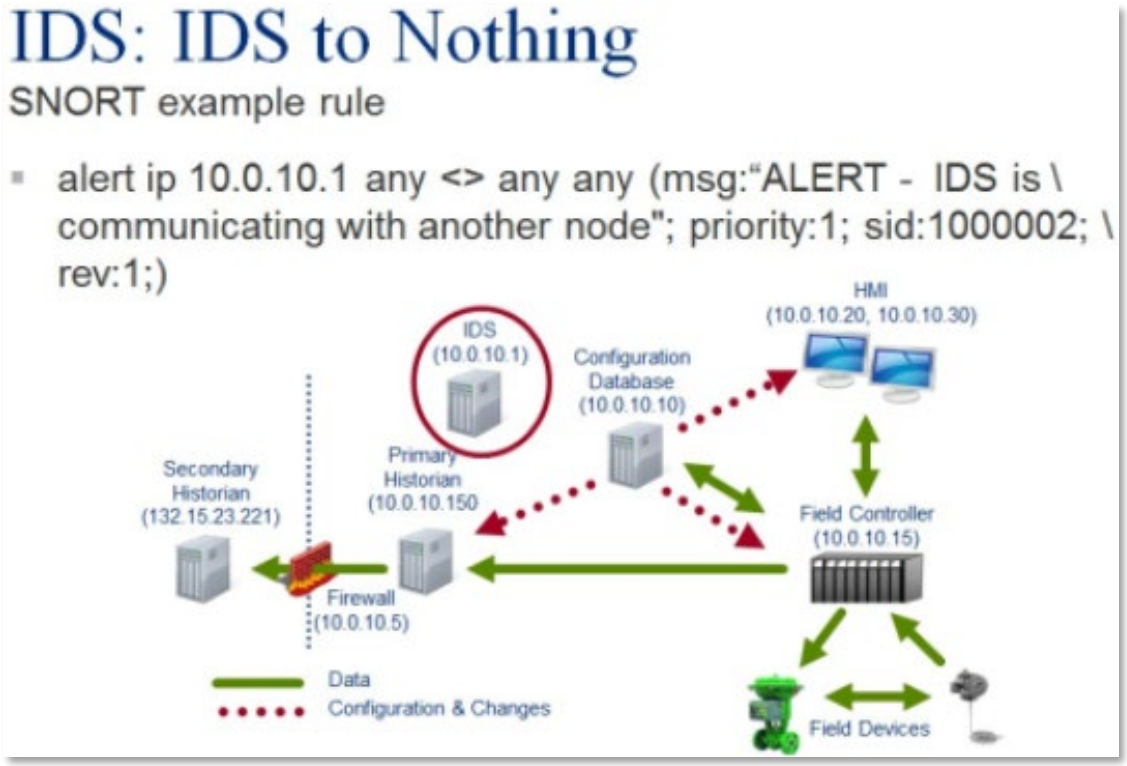
4. példa

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 például:

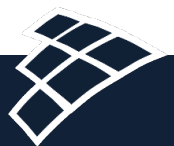
- Honeytoken-ek,
- DNS honeypotok,
- Honeyapp-ek,
- ICS Honeypotok,
- Teljes honeynet-ek,
- Fake persona-k,
- Purdue Decoy rendszerek.

Az alábbi példa egy igen általános esetet mutat be:



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 honeypotként működik.



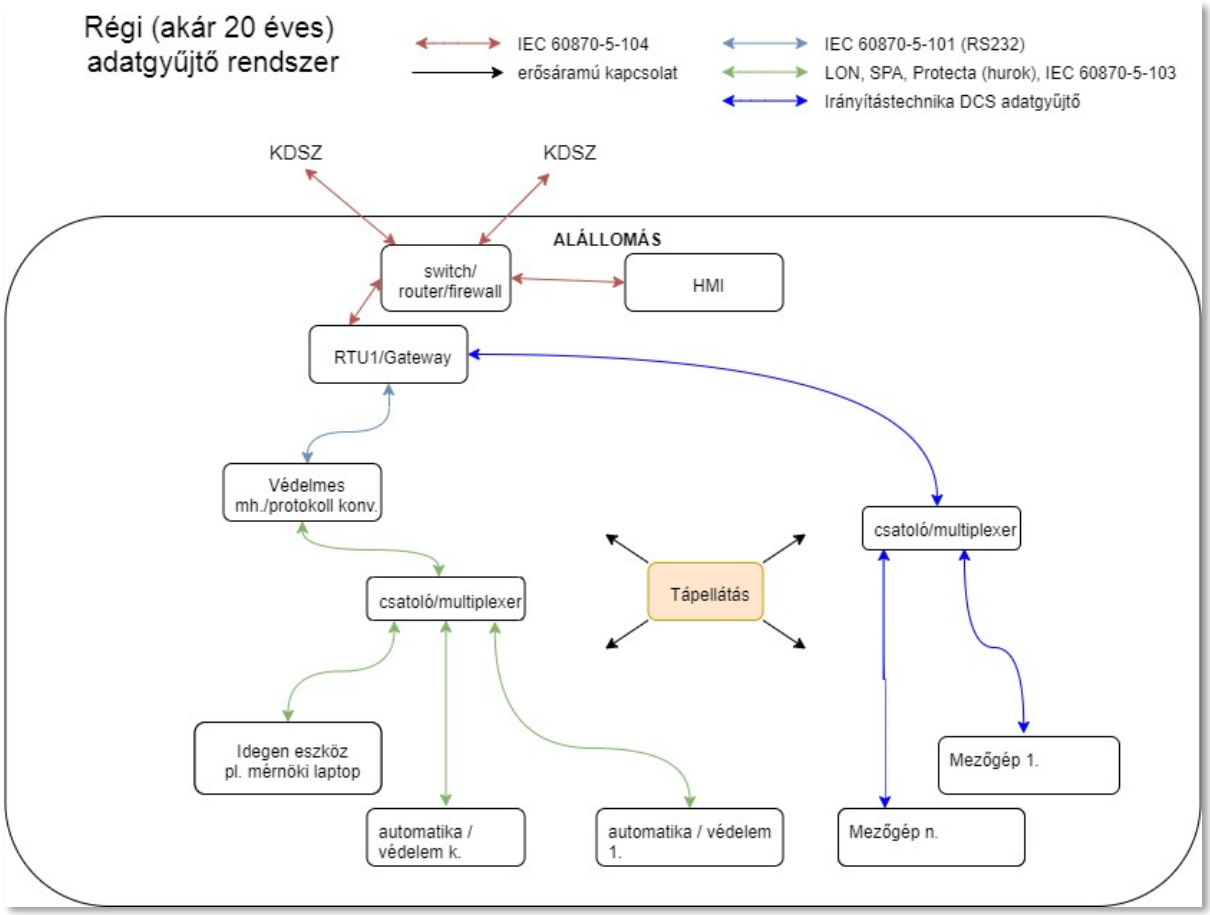
15. melléklet: Villamosenergetikai ICS/SCADA-k felépítése

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 üvegszálas 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/firewallhoz csatlakozik az alállomást teljes körűen felügyelő helyi megjelenítő (HMI). A KDSZ két – a legtöbb esetben – független útvonalon (lehetőleg más fizikai felületen például OPGW[305], 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 (AC[306], DC[307] 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:

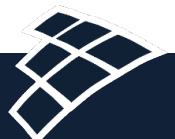
- primer készülék/technológia esetében a működtetéshez szükséges tápellátást és az adatgyűjtéshez szükséges segédüzemi feszültséget,
- szekunder készüléknél/technológiánál[308] a mezőgép, csatoló, RTU, HMI, switch/router stb. tápellátását.

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

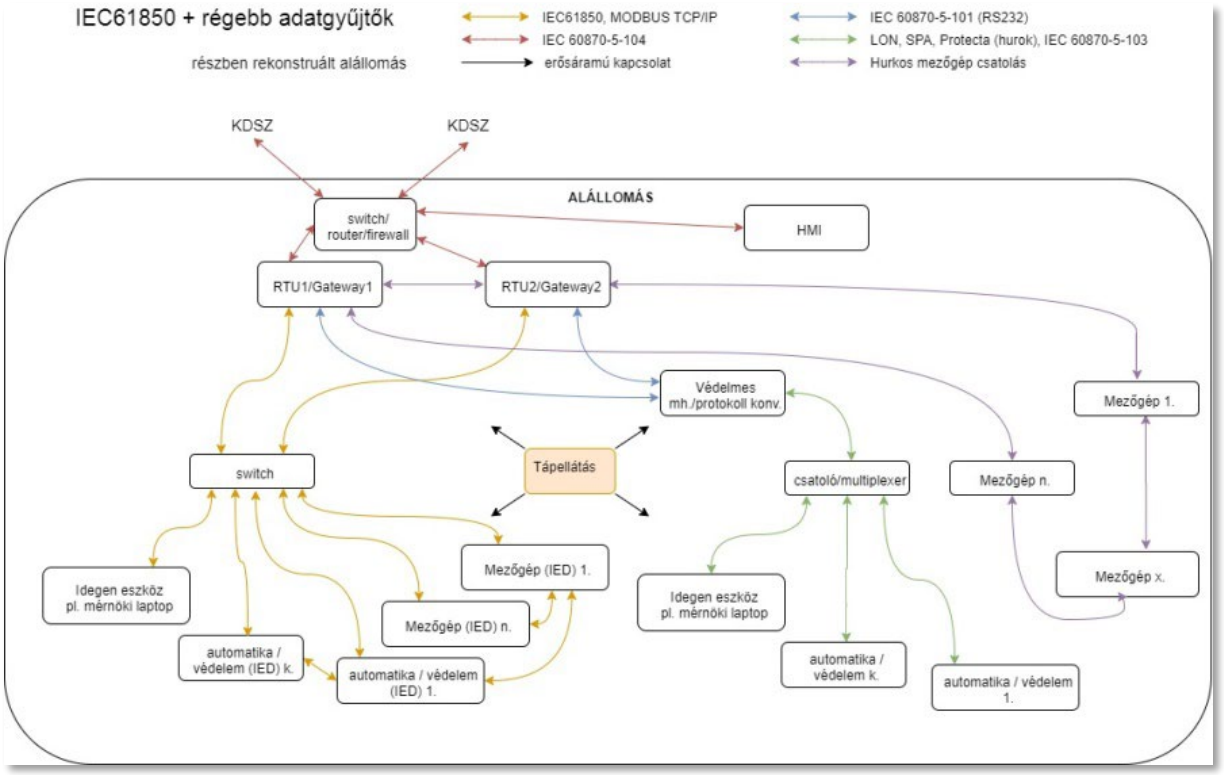
Gyakori eset, hogy egy alállomás egy része átépítésre kerül (pl. egy primer feszültségszinthez tartozó rész rekonstrukciója, csatlakozó távvezetékek, transzformátorok számának növekedése) és az átépítéssel érintett részen az adott időben korszerűnek tekinthető

[305] OPGW: Optical Ground Wire (optikai kábelt tartalmazó távvezetéki védővezető)
[306] AC: Alternating Current (váltakozó áram)
[307] DC: Direct Current (egyenáram)
[308] Szekunder készülék/technológia: a primer készülékek vezérlését, diagnosztikáját, adatgyűjtését az információk feldolgozását és továbbítását végző berendezések



védelem/automatika és irányítástechnikai adatgyűjtők, hálózatok kerülnek beépítésre.

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

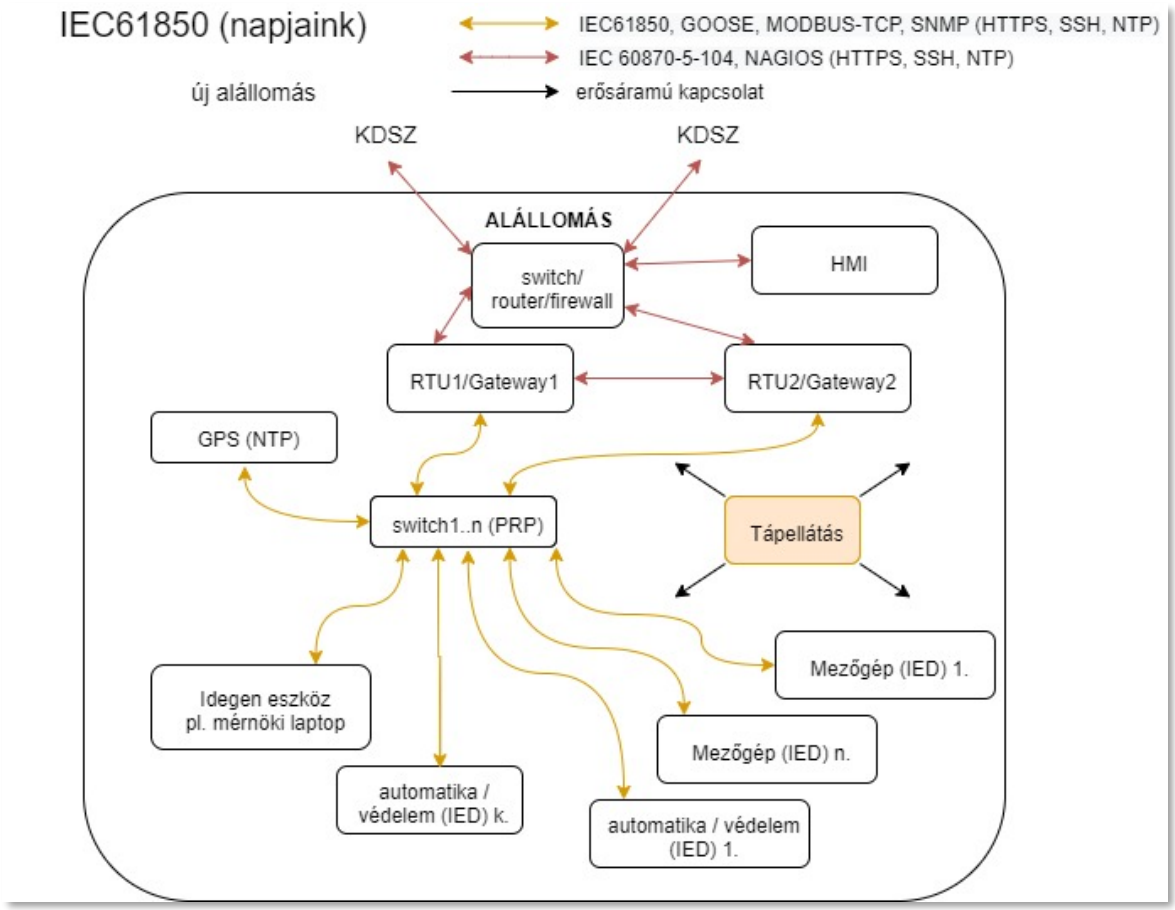
A vegyes technológia alkalmazása azt a helyzetet okozza, hogy EoL és a jelenlegi kornak megfelelő technológiájú (a legtöbbször IEC 61850 szabványú) – TCP/IP alapú kommunikációt használó – adatgyűjtő készülékek is vannak az alállomáson. Ez megbontja a homogenitást és megnehezíti az üzemeltetést. Az EoL készülékek és csatolóik a legtöbb esetben egyáltalán nem – vagy csak erősen korlátos módon – felügyelhetők (pl. csak 1 db erősáramos ÜKE[309] jelzés áll rendelkezésre és a távoli szoftveres elérés teljesen hiányzik).

1.3. Jelenlegi technológiájú alállomás

Majdnem teljes körűen IEC 61850 protokoll szerinti (ezen felül jellemzően Modbus-TCP, SNMP), de minden esetben TCP/IP alapú kommunikációt alkalmazó alállomás, amely

[309] ÜKE jelzés: üzemkészség jelzés

zöldmezős beruházás vagy egy alállomás teljes körű szekunder rekonstrukciója során létesül. Elvi felépítését a 15.3. ábra mutatja.



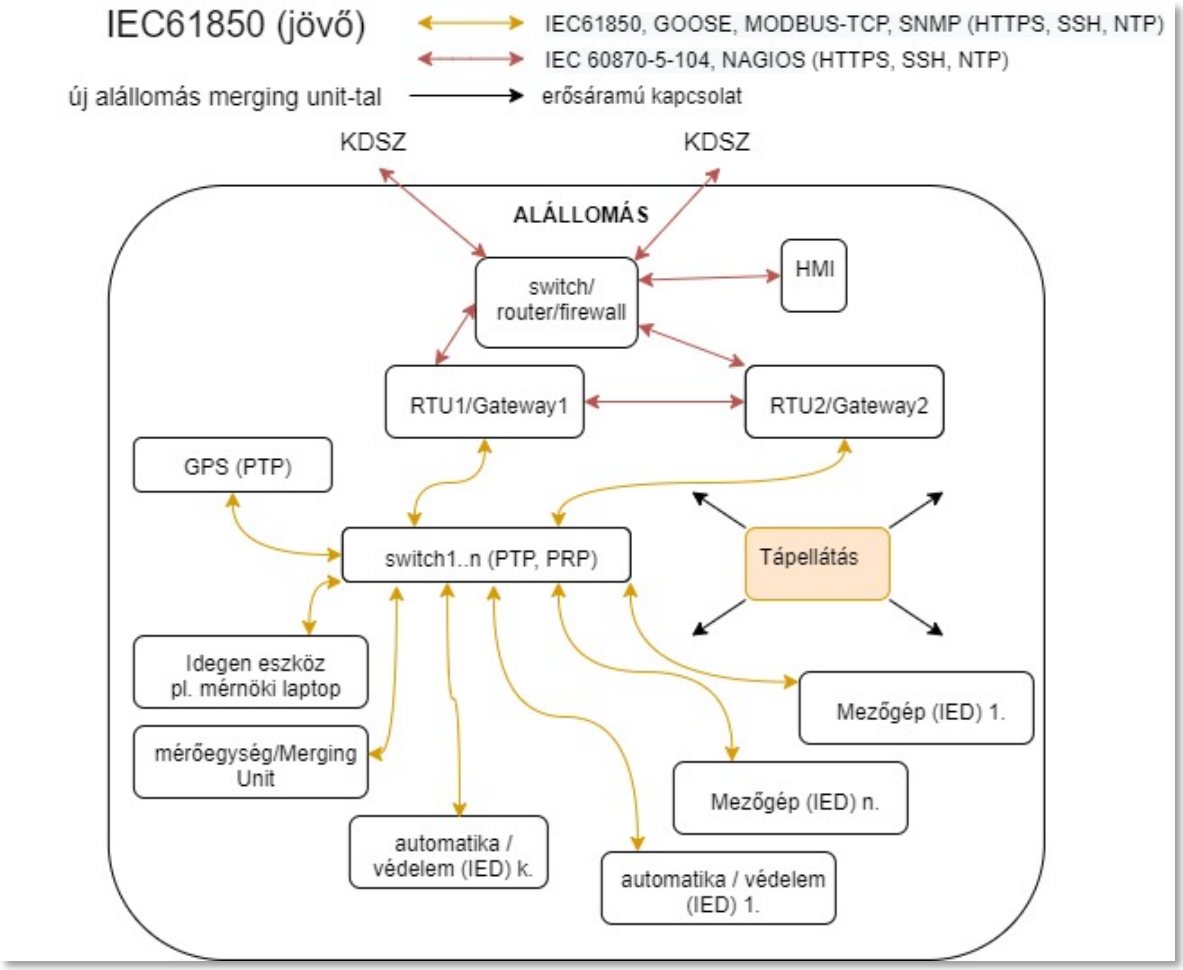
15.3. ábra: Jelenlegi technológiai szintű adatgyűjtő rendszer

Az adatgyűjtést alállomási környezetben alkalmazható (megfelelő EMC védettségű) switchek végzik, az itt jellemző hálózati protokollok szerint (pl. PRP[310], HSR[311] egyre ritkábban RSTP[312]). Minden esetben szükséges legalább egy NTP szerver, ami jellemzően az alállomáson van és GPS alapú, a másodlagos NTP szerver távoli, leggyakrabban a KDSZ/ODSZ[313]-ben elhelyezve. Mivel a TCP/IP alapú kommunikáció nem idősorrendi működésű, ezért az időbélyegzés, a csomagvesztés elkerülése miatt pedig a biztos tápellátás kiemelt fontosságú.

[310] PRP: Parallel Redundacy Protocol (Párhuzamos redundancia elvű adatgyűjtő protokoll)
[311] HSR: Highly-available Seamless Redundancy (Nagy megbízhatóságú, fürtös elvű protokoll)
[312] RSTP: Rapid Spanning Trea e Protocol (Gyors hasítófa elvű adatgyűjtő protokoll)
[313] ODSZ: Országos Diszpécser Szolgálat (a MAVIR üzemirányító központja)

1.4. Jövőbeli technológiájú alállomás

Az 1.3. pontban bemutatott technológia továbbfejlesztett változata, amelyben a mért értékek (feszültség/áram) – kellő felbontású A/D[314] átalakítás után (lásd. 15.4. ábra mérőegység: Merging Unit[315]) – is a TCP/IP hálózaton keresztül jutnak el a védelem/automatika és irányítástechnikai készülékekhez, azaz a készülékek nem mérik közvetlenül a mérőváltók analóg értékeit.



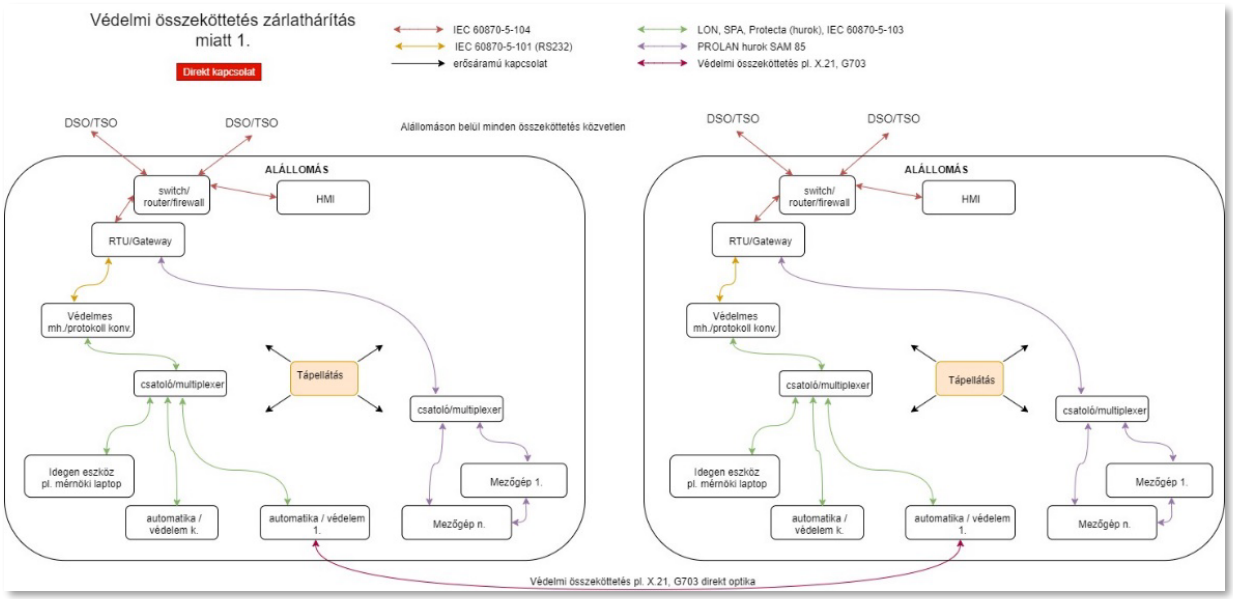
15.4. ábra: Jövőbeli technológia szintű adatgyűjtő rendszer

[314] A/D átalakítás: analóg/digitális átalakítás
[315] Merging Unit: analóg áram és feszültség értékből IEC 61850 szabványnak megfelelő értéket előállító mérő eszköz

A védelem/automatika készülékek megfelelő reagálási idejű (~40 ms) és pontosságú működéséhez a mért értékeknek legalább 1 μs felbontásúnak kell lennie időbélyeggel ellátva, amelyet a PTP szabványnak való megfelelőség biztosít. Ezen technológia alkalmazásakor minden az analóg jelet digitálissá konvertáló (Merging Unit), továbbító (switch) és feldolgozó (védelem/automatika) elemnek PTP kompatibilisnek kell lennie.

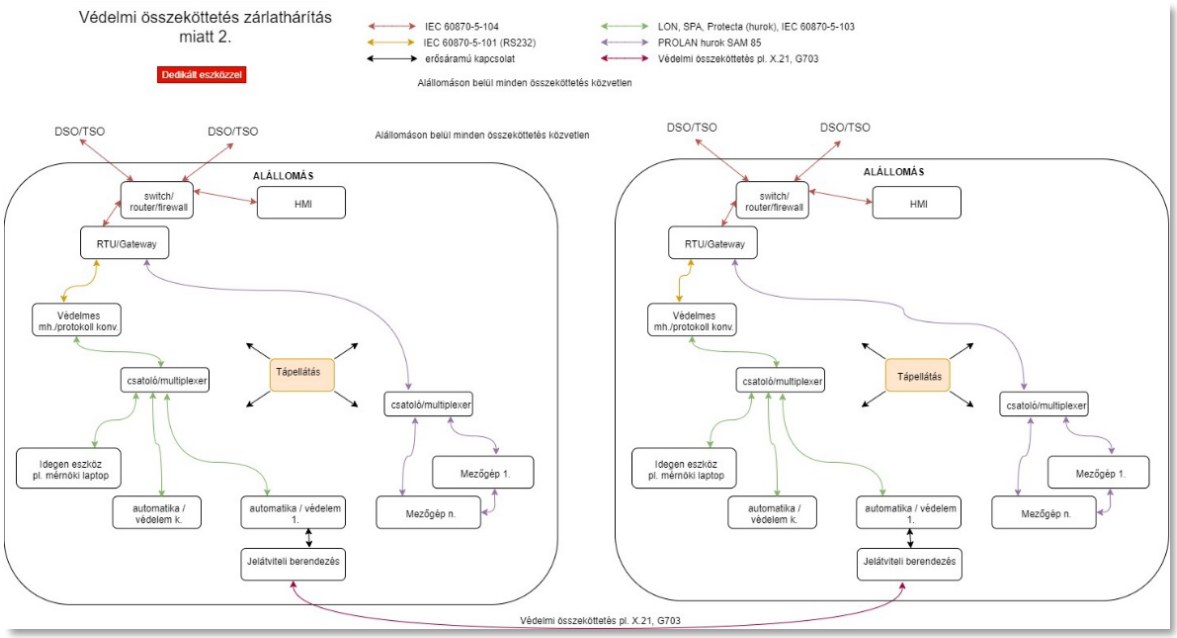
2. Direkt alállomási összeköttetések

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 zárlathárítás. 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.



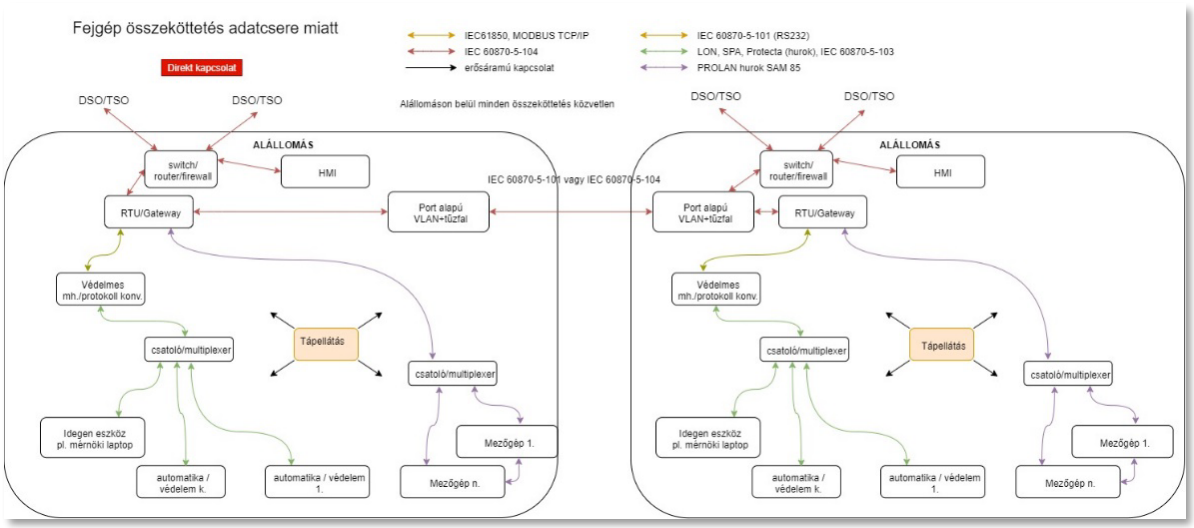
15.5. ábra: Védelmi jelátvitel direkt optikai szálon

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 például böngésző) rendelkezik.



15.6. ábra: Védelmi jelátvitel külön jelátviteli berendezésen

Gyakran alkalmazott megoldás abban a felállásban, ha egy alállomáson belül több tulajdonos van (elhatárolt tulajdonrésszel (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 jelátviteles összeköttetés, ahogyan a 15.7. ábra mutatja.

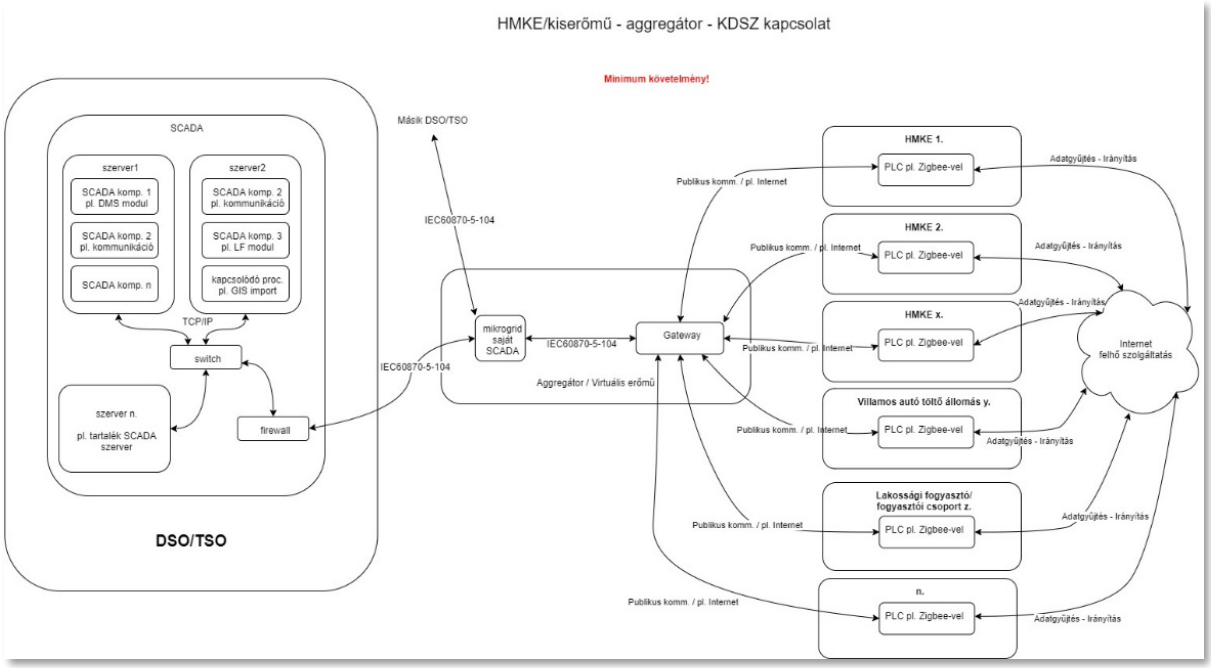


15.7. ábra: Alállomási RTU - alállomási RTU

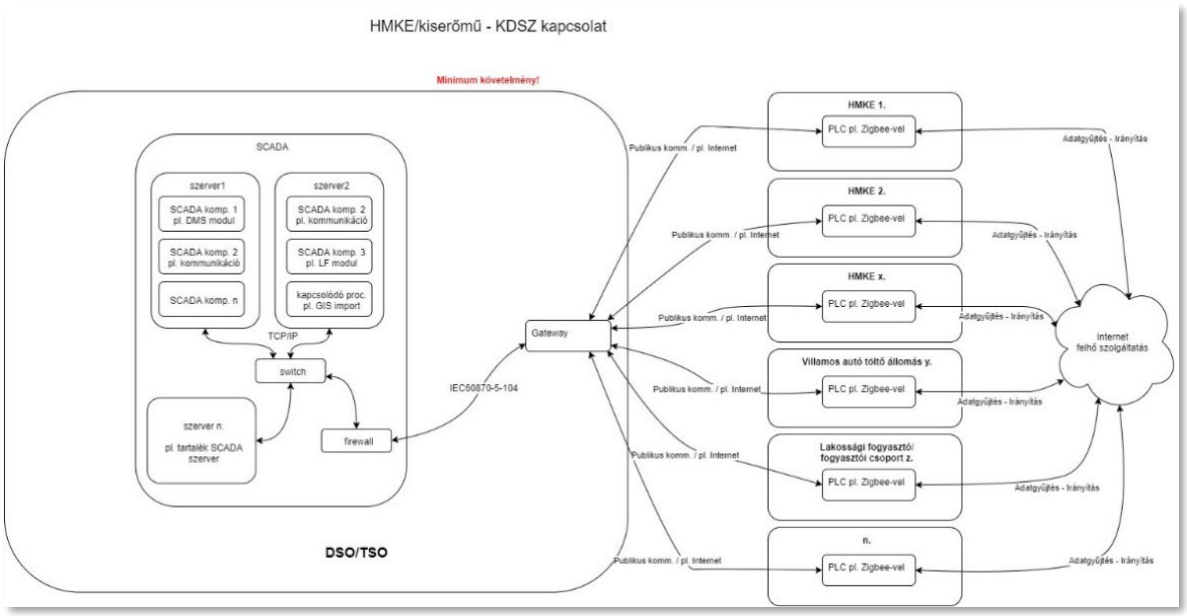
Amennyiben az összeköttetés IEC 60870-5-104 szerinti, akkor Port alapú VLAN-t és tűzfalat kell alkalmazni.

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/backdoormentessége 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



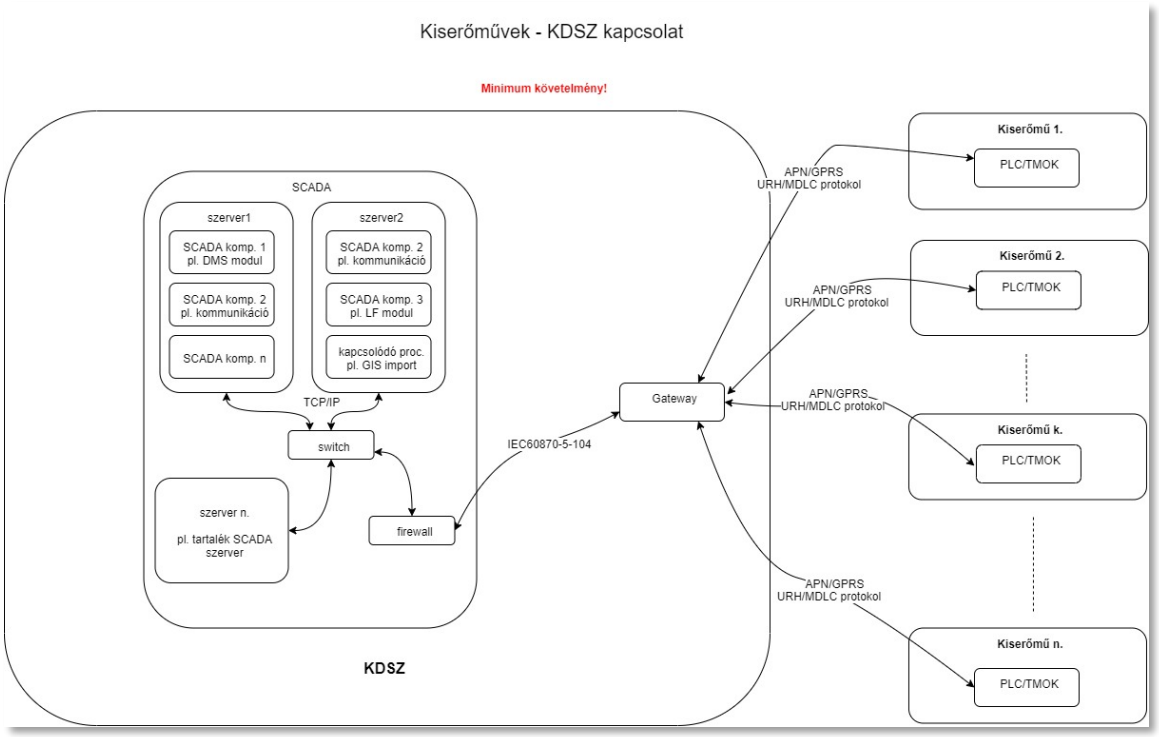
15.9. ábra: HMKE-Aggregátor-SCADA kapcsolat

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/TMOK[316] APN[317]-es GPRS[318] vagy MDLC[319]-s URH[320] 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.

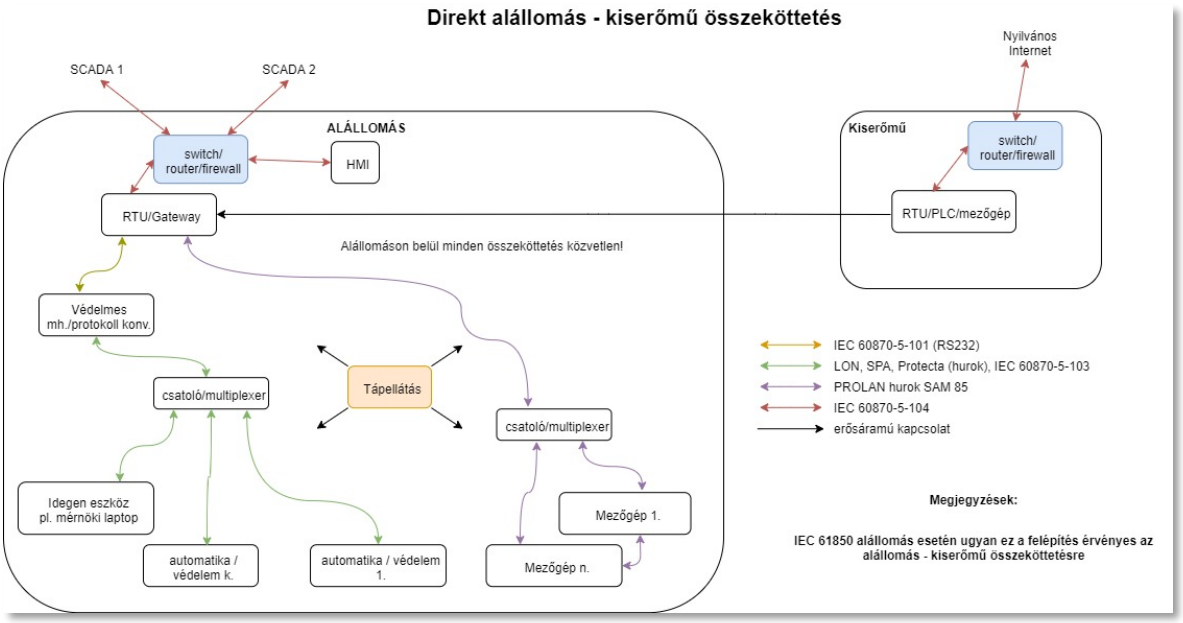
[316] TMOK: telemechanizált (távvezérelt és -felügyelt) oszlopkapcsoló
[317] APN: Access Point Name (egyedi hálózat elérési azonosító)
[318] GPRS: General Packet Radio Service (csomagkapcsolt, IP-alapú rádiós adatátviteli technológia
[319] MDLC: Motorola Data Link Communication (Motorola fejlesztésű adatkommunikációs protokoll)
[320] URH: ultrarövid hullám (nyílt rádiós jelátviteli technológia)



15.10. ábra: Kiserőmű-KDSZ

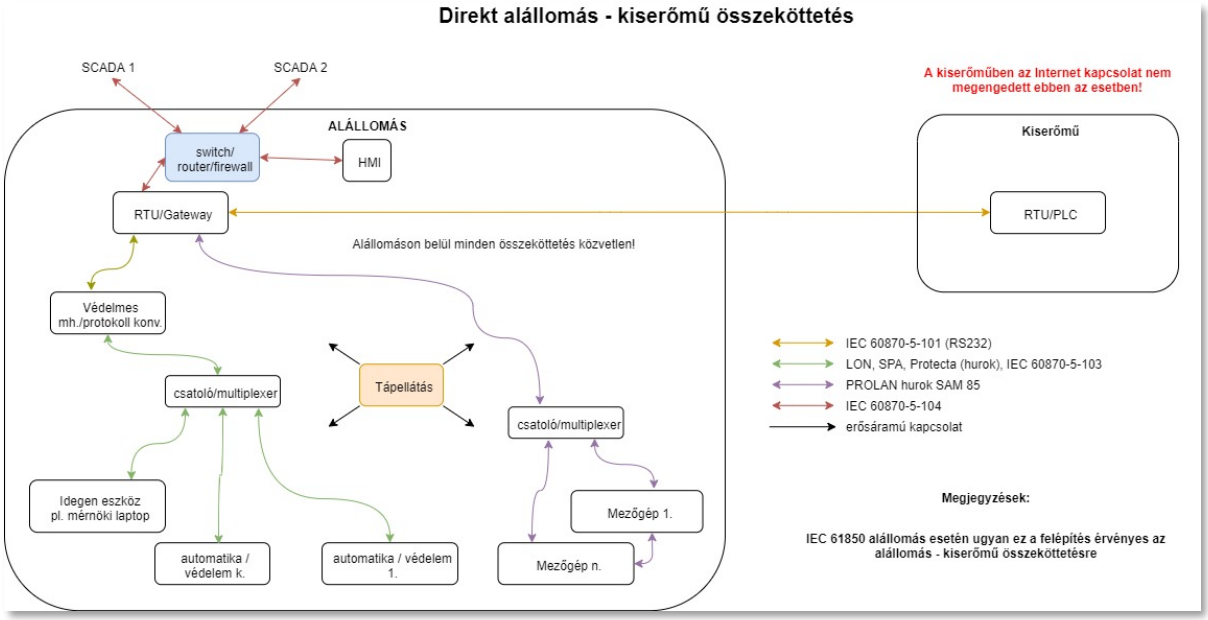
Amennyiben a kiserőműben elhelyezett PLC/RTU adatait a termelt villamosenergiát fogadó alállomás RTU-jához kell csatlakoztatni akkor két eset lehetséges:

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).



15.11. ábra: Kiserőmű-alállomás erősáramú kapcsolat

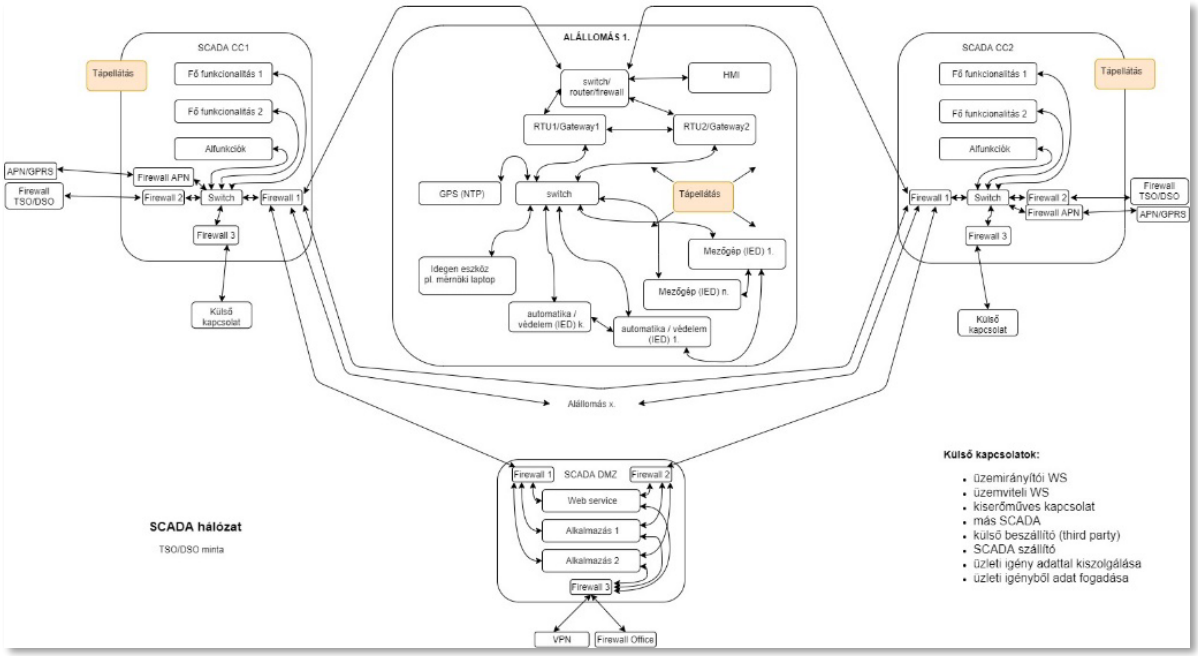
Ha a kapcsolat jelátviteles (pl. IEC 60870-5-101, IEC 60870-5-104, Modbus stb.) akkor a kiserőműben NEM! megengedett az internet kapcsolat (pl. felhő alapú adatgyűjtés/irányítás) kiépítése (lásd 15.12. ábra).



15.12. ábra: Kiserőmű-alállomás jelátviteles 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.



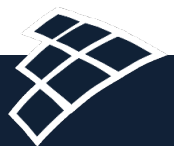
15.13. ábra: SCADA felépítése

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.



16. melléklet: IT-OT konvergencia

Számos publikáció tesz kísérletet mind az IT, mind az OT sajátoságainak megfogalmazására. Magas szintű, tömör definícióként a SeConSys az alábbiakat ajánlja:

- IT: Adat vagy információ tárolása, keresése, átvitele és feldolgozása.
- OT: Érzékelés és működés kiváltása a fizikai eszközök, folyamatok és események közvetlen megfigyelése és felügyelete révén.

  Vagy bővebben:

  OT: Olyan hardver, szoftver, hálózati eszközök/rendszerek, amelyek az ipari berendezések, eszközök, folyamatok és események közvetlen megfigyelése és/vagy felügyelete révén változást észlelnek vagy okoznak azokban.

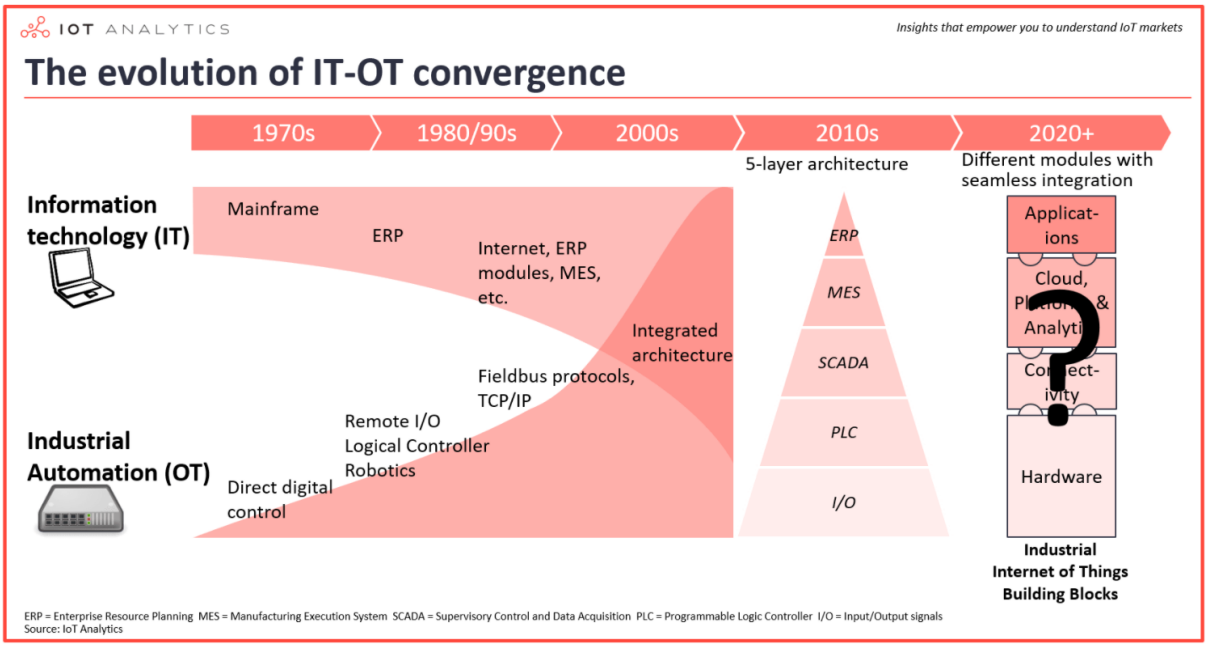
Tekintettel

- a korábban csak az ügyviteli rendszerekben alkalmazott hardverek és szoftverek OT-oldali egyre nagyobb mértékű megjelenésére (lásd pld. a digitális alállomások kialakítására),
- továbbá az OT rendszereket rohamosan növekvő számban érő fenyegetésekre

indokolt áttekinteni az IT és OT rendszerek sajátosságait, különbségeiket, fejlődéstörténetüket továbbá a konvergencia lehetséges/szükséges területeit.

1. Fejlődéstörténet

A számítástechnikai fejlődés korai szakaszában az IT és OT minden tekintetben élesen elkülönült egymástól. Pl. a protokollok, mint a fontos jellemzők tekintetében már az IT fejlődés korai szakaszában is (kvázi)szabványok kezdtek kialakulni, addig az OT esetében ez a folyamat csak jóval később indult meg. Ez utóbbi hosszú ideig fenn is állt, azt a (hamis) reményt keltve, hogy az egyedi kialakítású OT rendszereket éppen az egyediségük óvja meg az illetéktelen behatolásoktól.



16.1. ábra: Az IT-OT konvergencia fejlődéstörténete[321] *[78]*

A felhő technológia és az IIoT megjelenése pedig manapság feszegeti a Purdue modell kereteit. Ennek egyik látványos megnyilvánulása a digitális alállomások megjelenése, amely megindította a 0. szintű technológiai elemek és az 1. szintű IED-k, PLC-ék egyre szorosabb kapcsolatának kiépülését.

A fentieket részleteiben a 16.1. ábra mutatja be.

2. Sajátosságok

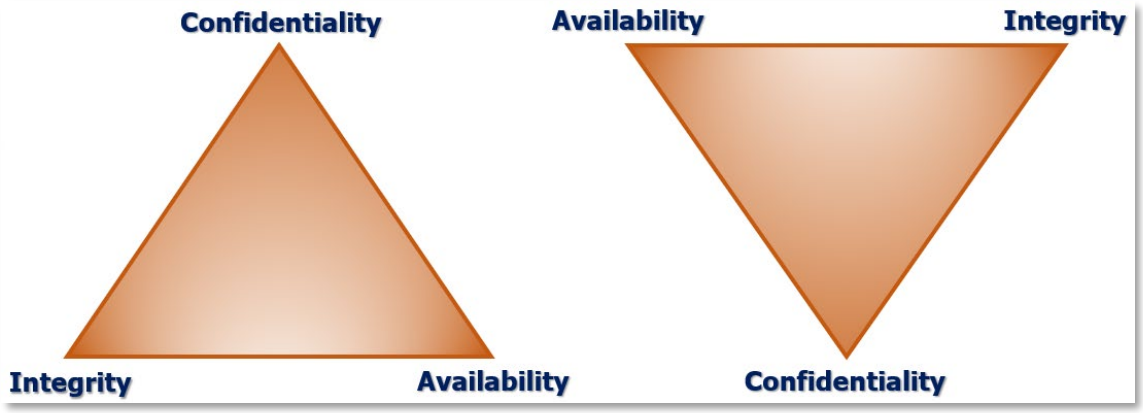
2.1. Magas szintű sajátosságok

Az IT és OT rendszerektől elvárt legfontosabb jellemzők:

- IT: bizalmasság, sértetlenség (integritás), rendelkezésre állás (angol terminológiában: **C**onfidentiality, **I**ntegrity, **A**vailability, azaz CIA)
- OT: rendelkezésre állás, sértetlenség (integritás), bizalmasság (angol terminológiában: **A**vailability, **I**ntegrity, **C**onfidentiality, azaz AIC)

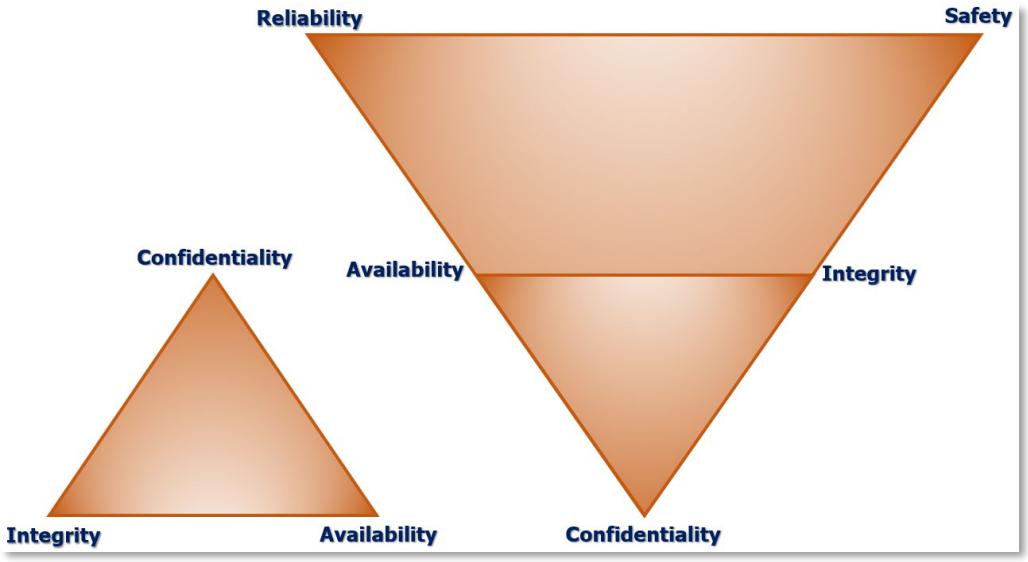
[321] M. Wopata "5 Industrial connectivity trends driving the IT-OT convergence." IoT. Analytics https://iot-analytics.com/5-industrial-connectivity-trends-driving-the-it-ot-convergence/ (Letöltve: 2022.01.14.)

A CIA és az AIC követelményrendszerei az IT és OT rendszerekkel szembeni elvárások, prioritások alapvető eltérését mutatja (16.2. ábra).



16.2. ábra: CIA vs. AIC [322] [79]

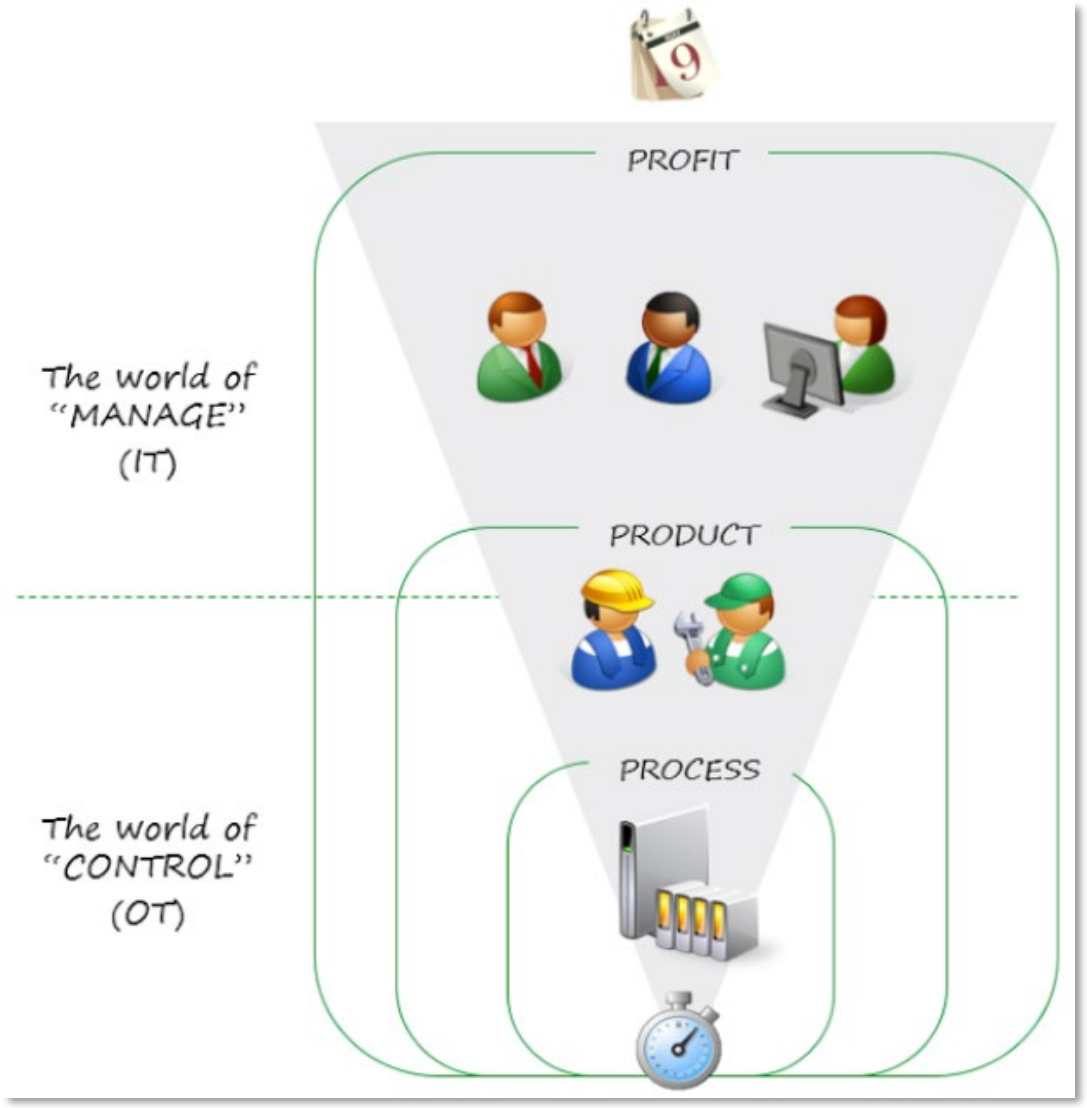
A SeConSys megközelítése szerint az OT rendszerek esetében az AIC fontos, szükséges, de nem elégséges követelmény, mivel az ipari (aktuálisan energetikai) rendszerekkel szembeni további két fontos követelmény – a megbízhatóság, továbbá az (embert, technológiát és környezetet megvédeni hivatott) (fizikai) biztonság, nem jelenik meg benne. A SeConSys megközelítése szerinti IT-OT funkciókat a 16.3. ábra mutatja.



322 D. Scali. "Developing a Security Strategy to Cover ICS Assets." FireEye https://www.fireeye.com/blog/executive-perspective/2016/08/developing_a_securit.html/ (Letöltve: 2022.01.14.)

16.3. ábra: CIA vs. SR+AIC (SeConSys megközelítés)

Az IT és OT terjedelmi és funkcionális sajátosságait a 16.4. ábra mutatja.



16.4. ábra: IT és OT funkciók, terjedelmek [323] [80]

[323] Operations Management Systems Evolution. "OT/IT Convergence "What does it mean in the Industrial World?"" http://operationalevolution.blogspot.com/2015/02/otit-convergence-what-does-it-mean-in.html (Letöltve: 2022.01.14.)

2.2. Tételes sajátosságok: különbözőségek

Számos forrás tesz kísérletet arra, hogy tételesen megfogalmazza az IT és OT közötti különbözőségeket. E forrásokat áttekintve, szintetizálva és strukturálva a SeConSys a 16.1. táblázat szerint fogalmazza meg a különbözőségeket, vastagítással kiemelve a legfontosabbakat.[324,325,326,327,328,329,330]

[81] [82] [83] [84] [85] [86] [87]

[324] J. Weiss. (2014.) "Industrial Control System (ICS) Cyber Security for Water and Wastewater Systems" In: Securing Water and Wastewater Systems (pp.87-105) DOI:10.1007/978-3-319-01092-2_3

[325] P. Peeters. "Towards a Digital (manufacturing) Future – Part 5 : Cybersecurity" Agorira https://www.agoria.be/en/manufacturing/innovation/towards-a-digital-manufacturing-future-part-5-cybersecurity (Letöltve: 2022.01.14.)

[326] B. Russel, D. V. Duren (2018.). Divergence in IT and OT security fundamentals In: Divergence in IT and OT security fundamentals https://subscription.packtpub.com/book/business/9781788832687/1/ch01lvl1sec16/divergence-in-it-and-ot-security-fundamentals

[327] R. M. Krieg. (2020.) "The Journal of Critical Infrastructure Policy". JCIP https://viewer.joomag.com/journal-of-critical-infrastructure-policy-volume-1-number-2-fall-winter-2020/0332765001608321823 (Letöltve: 2022.01.14.)

[328] Fortinet. "A Solution Guide to Operational Technology Cybersecurity" https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-operational-technology-design-guide.pdf (Letöltve: 2022.01.14.)

[329] S. Fluchs. "Why OT has different needs than IT". FluchsFriction https://fluchsfriction.medium.com/why-ot-has-different-needs-than-it-18ba9baa36e7 (Letöltve: 2022.01.14.)

[330] D. Harcharan, S. H. Houmb, E. A. Engum. "Safeguarding OT From Cyber Threats." ISSSource https://isssource.com/safeguarding-ot-from-cyber-threats-2/ (Letöltve: 2022.01.14.)

16.1. táblázat: IT és OT sajátosságok

Témacsoport	Téma	IT	OT (ICS, SCADA)
Elvi alapok	**Definíció**	**Adat vagy információ tárolása, keresése, átvitele és feldolgozása**	**Érzékelés és működés kiváltása a fizikai eszközök, folyamatok és események közvetlen megfigyelése és felügyelete révén**
	Fókuszterület	**Az adat**	**A felügyelt technológia, folyamat**
Üzleti alapok	Üzleti misszió	Az üzlet támogatása	A fizikai folyamatok működtetésével bevétel termelése
	Az üzleti cél teljesítésének magas szintű feltételei (prioritási sorrendben)	Confidentiability (financial, costumer, partner, IP data) Integrity Availability	Safety (worker & costumer) Reliability Availability Integrity Confidentiability (process, IP formulations)
	Támadás lehetséges üzleti hatásai	**Megszakadó működés**	**Megszakadó működés mellett fizikai folyamat kontrollvesztése/leállása.**
		Többnyire alacsonyabb bevételkiesés az OT elleni támadáshoz képest	**Akár közepes vagy nagy bevételkiesés**
		Adatvesztés, -lopás (személyes azonosító adatok, üzleti adatok, szellemi tulajdon stb.)	**Adatvesztés, -lopás mellett Lehetséges haláleset, sérülés, környezeti kár**
		Megrendelői bizalomvesztés	Bizalomvesztés mellett akár nemzetbiztonsági kockázat is (pl. közszolgáltatások elvesztésével)
		Ellátási lánc lehetséges megszakadása	Ellátási lánc lehetséges megszakadása mellett akár olyan közszolgáltatások elvesztése, mint a villamosenergia- és vízellátás

Témacsoport	Téma	IT	OT (ICS, SCADA)
Szabályozási alapok	Szabványok	A kommunikációs szabványok jellemzően nyíltak (RFC-kben rögzítettek), a használt fájlformátumok közt viszont található több zárt (proprietary) is.	Szabványos és egyedi: soros és egyéb régebbi protokollok. Elmozdulás a szabványos protokollok irányába, vegyes szoftver környezetet eredményezve
	Szabályozások	Adatvédelem, minőségirányítás, gazdasági kockázatok menedzselése	A termelés vagy a szolgáltatások működőképességére és a veszélyes események vagy határérték-túllépések elkerülésére vonatkozó követelmények
Kockázati alapok	**Kockázatkezelési elvárások**	Adatmenedzselés	A fizikai világ felügyelete
		Az adat bizalmassága, sértetlensége (integritása), és rendelkezésre állása az elsődleges fontosságú	**Az emberi biztonság és a folyamat biztonsága az elsődleges, majd ezt követi az adat rendelkezésre állása, sértetlensége és bizalmassága**
		A hibatűrés kevésbé fontos, egy rövid állásidő többnyire nem kritikus, fontosabb a hiba gyors és biztos elhárítása.	**A hibatűrés alapvető fontosságú, még rövid állásidő sem engedhető meg, akár a hiba érdemi javításának (patch-elésének) elhúzódása árán is.**
		A fő kockázati hatás az üzleti műveletek késedelme	**A fő kockázati hatás az élet, a berendezések vagy a termelés elvesztése, a környezeti hatások**
Performancia jellemzők	**Erőforrás korlátok**	**A rendszerek tipikusan megfelelő erőforrással rendelkeznek a járulékos, olyan harmadik fél általi alkalmazásokhoz, mint a biztonság**	**A meglévő rendszerek adott ipari folyamatok támogatására vannak méretezve és többnyire nincs elég memóriájuk és processzor kapacitásuk, illetve bővíthetőségük, hogy járulékos (biztonsági**

Témacsoport	Téma	IT	OT (ICS, SCADA)
			vagy egyéb) alkalmazásokat is támogassanak. **További kötöttség lehet, ha a szállítói licenc- és szolgáltatási megállapodás kizárja harmadik féltől származó (akár kiberbiztonsági) alkalmazás telepítését.**
	Rendszer működés (operációs rendszerek)	A rendszereket tipikus operációs rendszerekkel való használatra tervezték, így a hardvergyártótól független lehet az operációs rendszer választás	Eltérő és esetleg szabadalmaztatott operációs rendszerek, melyeket a hardver gyártója köt ki, gyakran beépített biztonsági képességek nélkül
		A frissítés egyszerűbb az automatizált telepítési eszközök elérhetőségének köszönhetően	A szoftver váltásokat óvatosan kell végezni, általában a szoftver szállító által, a speciális felügyeleti algoritmusok és esetlegesen módosuló hardver és szoftver miatt. A frissítési lehetőségek korlátozottak, tipikusan ritkábban jelennek meg az IT-ben megszokotthoz képest.
	Kommunikáció, hálózatok	Szabványos kommunikációs protokollok	Szabadalmaztatott, szabványos vagy egyedi – kizárólag az adott gyártó által használt – ipari protokollok
		Elsődlegesen vezetékes adatkapcsolat, némi helyi vezetéknélküli kapcsolati képességgel	Több fajta átviteli rendszer, eszköz van használatban, beleértve a dedikált vezetékes és vezetéknélküli (rádió vagy műholdas) kapcsolatokat
		Adatvezérelt, optimális kihasználás szempontú IT hálózati struktúrák	**A hálózatok gyakran a technológiai oldali szempontok szerint alakulnak**
		Nagy méretű, jól skálázható, gyakran változhat	**Ritkán változó topológia**

Témacsoport	Téma	IT	OT (ICS, SCADA)
		Hálózati komponensek százai, ezrei, jól csoportosítható szerepkörökkel	**Általában kevesebb hálózati komponens, de több egyedi kezelés szükséges**
		Dinamikusan változó felhasználói elvárások	**Ritkán változó felhasználói elvárások**
	Rendelkezésre állási, megbízhatósági követelmények	Megengedhetők a válaszreakciók (pl. újraindulás)	A folyamat rendelkezésre állási követelmények miatt kerülendők az olyan válaszreakciók, mint pl. az újraindulás
		A rendelkezésre állási hiányosságok jobban tolerálhatók a rendszer üzemeltetési követelményeitől függően	**A rendelkezésre állási követelmények redundáns rendszereket tehetnek szükségessé**
		Előnyös minél előbb tervezni a karbantartásokat és üzemszüneteket, de többnyire tolerálható a rövid vagy értesítés nélküli előfordulás	A kieséseket napokkal/hetekkel előre kell tervezni és ütemezni
			A magas rendelkezésre állás kimerítő tesztelést igényel a telepítés előtt
		Jobban tolerálható a válaszidő szórása. Sok helyen emberi reakcióidőkhöz mért válaszidő elvárások	Kritikus válaszidő (akár milliszekundomos léptékben)
	Élettartam, ciklusidő	**3-5 év, de nem ritka a 10+ éves élettartam sem**	**Tipikusan 10-15 év nagyságrend (de akár hosszabb is lehet)**
	Támadás utáni újraindítás	Az újraindítás előtt annyira alapos forensic végzendő, amennyire csak lehet, olyan gyorsan, amennyire csak lehet. Az újraindulás során az alapkiépítéshez képesti degradált – pl. kevesebb redundanciát, kevesebb erőforrást tartalmazó – működés is elfogadható lehet.	Az újraindítás előtt annyira alapos forensic végzendő, amennyire csak lehet, olyan gyorsan, amennyire csak lehet. Az újraindulás során szinte bizonyosan nem megengedett az alapkiépítéshez képesti degradált működés. Az újraindulás az összetett, a technológiát is érintő - nyilvánvalóan

Témacsoport	Téma	IT	OT (ICS, SCADA)
		A forensichez szükséges adatok rögzítése utáni lehető legrövidebb idő alatt	technológiai ismereteket is igénylő - tesztelések sikeres elvégzése után lehetséges
	Frissítések, hibajavítások	**Gyakran, akár hetente javasolt**	**Rendszertelen, akár éves nagyságrendű periódusok. Növekvő kockázat, sűrítés javasolt**
	Karbantarthatóság, sérülékenység javítás	**Relatíve gyakori, előre tervezett karbantartások**	**Kizárólag a technológia tervezett leállásakor lehetséges teljes karbantartás**
Kibervédelmi jellemzők	**Megelőzés, védekezési ismeretek**	**A hatásos megelőzéshez, védekezéshez nem szükséges a rendszer által kiszolgált technológiai sajátosságok mély ismerete**	**A hatásos megelőzés, védekezés előfeltétele a fizikai technológiai sajátosságok ismerete**
	Anti-vírus védelem	Elterjedtek, könnyen telepíthetők, frissíthetők és paraméterezhetők	A meglévő rendszerek gyakran csak egyedi, utólagos megoldásokkal védhetők, minden esetben az erőforrásigény alapos elemzése mellett
	Támadáselhárító intézkedések	**Automatikus, szóba jöhet a whitelisting. Számos elterjedt prevention, detection, reaction eljárás és szoftver áll rendelkezésre.**	**A generikus eszközök nehezen használhatók, többnyire kerülendők az automatikus beavatkozások (a téves forgalmi/szoftver korlátozások hatása összemérhető lehet a támadással)**
	Jogosultságkezelés	**A biztonsághoz szükséges mértékűen szigorú hozzáférési rendszer alakítható ki és működtethető**	**Kritikus a vészhelyzeti jogosultság azonosítás. A rendszerhez és rendszerelemekhez való hozzáférést szigorúan szabályozandó és ellenőrizendő. Ugyanakkor jogosultság azonosítás nem akadályozhatja esetleges vészhelyzeti beavatkozást.**

Témacsoport	Téma	IT	OT (ICS, SCADA)
	Incidens kezelés és kivizsgálás	Kidolgozott technológiák léteznek rá, a fő probléma ezek ára és a házon belüli szakértelem hiánya	Az elsődleges cél a technológia működésének helyreállítása/biztosítása, a megszokott általános módszertanok alkalmazása nehézkes a speciális igények miatt
	Rendszerek biztonságának fejlesztése	Egyre inkább a fejlesztések, illetve a fejlesztési módszertanok természetes része	Hagyományosan nem része a rendszer fejlesztésének. Az OT szállítók ugyan fejlődnek, de tipikusan lassabban, mint az IT-sek.
	Változásmenedzsment	A változtatásokat az IT-esek végzik, gyakoriak a beszállítói, illetve kiszervezett tevékenységek	A változtatásokat gyakran beszállítók végzik (gyakran távoli eléréssel, szélső esetben tekintet nélkül a biztonsági és az auditálhatósági szempontokra)
		A szoftverváltozásokat alaposan tesztelni kell, és nagy méretű rendszer esetén fokozatosan kell bevezetni. A frissítések és változások telepítésré jól használható támogató eszközök állnak rendelkezésre. A szervezetek biztonsági politikája jellemzően külön kitér a változásmenedzsmentre	A szoftverváltozásokat alaposan tesztelni kell, és fokozatosan kell bevezetni a rendszerben, hogy az ellenőrzési rendszer integritása megmaradjon. Az ICS-kieséseket gyakran hetekkel vagy hónapokkal előre kell tervezni és ütemezni. Az ICS olyan operációs rendszereket használhat, amelyek már nem támogatottak.
	Informatikai rendszer homogenitása	Megfelelő tervezés és változásmenedzsment esetén viszonylag homogén tud maradni	Az akár extrém hosszú életciklus miatt többnyire nagymértékben inhomogén – emiatt pl. nehezen megvédhető – rendszer

Témacsoport	Téma	IT	OT (ICS, SCADA)
	IDS-től[331] IPS[332] felé történő elmozdulás hatása	Szolgáltatásminőségi és üzemeltetési okok miatt kedvező	Az IDS olyan működési kockázatot és potenciális zavarokat jelent, amelyek ipari környezetben elfogadhatatlanok
Üzemeltetés	Támogatás	Különféle támogatási formák és rendelkezésre állások választhatók	A szervíz támogatást többnyire rendszerenként egyetlen beszállító biztosítja, de több beszállító esetén korlátozott ill. akadozó lehet közöttük az együttműködés
	Teszt, audit	**Modern módszerek használhatók. A rendszerek kellően robusztusak és ellenállók, hogy kezeljék ezeket az értékelési módszereket**	**A tesztelési módszertant a rendszerhez kell igazítani. A rendszer működése általában nem módosítható szabadon a tesztek idejére sem**
		Az ellenőrzéshez való hozzáférés szigorúan korlátozott lehet a biztonsághoz szükséges mértékben	**Az ICS-hez való hozzáférést szigorúan ellenőrizni kell, de nem akadályozhatja vagy zavarhatja az ember-gép vagy gép-gép interakciót**
	Üzembe helyezési eljárások	Az alapfunkcióktól eltekintve többnyire nem követelmény valamennyi funkció tételes tesztelése és dokumentálása	Valamennyi funkció tételesen tesztelendő és dokumentálandó
	Behatolás/betörés-tesztelés (pentest) alkalmazhatósága	**Megszokott, kezelhető kockázatú művelet**	**Az esetleges technológiai hatások lehetséges safety jellegű következményeire tekintette pentest működő fizikai technológiai rendszer mellett nem végezhető**

[331] DS: Intrusion Detection Systems
[332] IPS: Intrusion Prevention Systems

Témacsoport	Téma	IT	OT (ICS, SCADA)
	Teszt környezet (testbed) alkalmazhatósága	Megszokott, kezelhető költségű vizsgálati módszer	Megszokott és kezelhető testbedek léteznek a gyártóknál az alapvető funkciókra. Azonban költsége és nehéz megvalósíthatósága miatt a fizikai folyamatokkal való kölcsönhatásokra ez nem terjed ki.
Környezeti jellemzők	Működési környezet	Adatközpontokban, vagy egyéb ellenőrzött helyeken	Mind ellenőrzött, mind szétszórt – akár tűz- és robbanásveszélyes – környezetben működhet. Meleg, hideg, nedvesség, szennyezés, rezgés és villamos hatások is érhetik
		Könnyű elérhetőség	Lehetséges terepi és/vagy nehéz megközelíthetőségű elhelyezkedés
	Az összetevők elhelyezkedése	Az összetevők többnyire egy helyen (telephelyen) vannak és könnyen elérhetők	A komponensek elszigeteltek, távoliak lehetnek, és a hozzájuk való hozzáférés jelentős előkészítést igényelhet

16.1. táblázat: IT és OT sajátosságok

2.3. Tételes sajátosságok: egyezőségek

Amennyire a kölönbözőségeket sok forrás tárgyalja, addig az egyezőségekről alig található ilyen, miközben a s zükségesnek tartott konvergencia hajtómotorjai éppen ezek lehetnének.

A kézikönyv következő aktualizálása során lehetőség szerint az egyezőségek is bemutatásra kerülnek.

2.4. A „hídépítés" lehetőségei

Az IT és OT közötti „híd" építése hosszú, de szükségszerű folyamat. Kulcskérdés, hogy a felek értsék – és megértsék – a 16.3. ábra szerinti prioritásokat, avagy kényszerpályákat:

- azaz az IT oldali embereknek el kell fogadniuk, hogy akkor és csak akkor van bevétel (és ezzel nekik munkájuk), ha az OT oldal a magas követelményeket folyamatosan teljesítve támogatja az értékteremtő technológia (a core bussiness) zavartalan működését. Ennek részeként azt is el kell fogadniuk, hogy a Purdue modell OT szintjein elsődlegesen a safety és security követelményeknek való megfeleléshez – ezzel a zavartalan bevételtermeléshez – akár az IT-nél lényegesen szigorúbb (és gyakran OT-specifikus) – követelményeknek való megfelelés feltételeit is biztosítani kell.
- az OT oldali embereknek el kell fogadniuk, hogy az informatikai robbanás olyan paradigmaváltással felérő új technológiákat hoz magával, mint az IIoT, az 5G adatkapcsolat, amelyek a kellő megbízhatósági szint elérésekor minden bizonnyal az OT-rendszerek részévé válnak. Nyitottnak kell lenniük olyan léptékű paradigmaváltásra, mint amely '80-as években zajlott a hagyományos, elektromechanikus védelmeknek digitálisra történt cseréjekor.

Elsődlegesen a SolarWinds/Orion incidens tükrében mind az OT, mind az OT oldali megrendelők jogos elvárása, hogy elsődlegesen a szoftver tervezők, gyártók, szolgáltatók (de a lehetséges backdoorolásra tekintettel a hardver beszállítók is) a jelenleginél lényegesen magasabb szintű garanciákat adjanak elsődlegesen termékeik, szolgáltatási integritása – és a 16.3. ábra szerinti többi követelmény teljesítése – tekintetében.

Az IT és az OT viszonyrendszerét, a konvergencia humán és adminisztratív aspektusait külön anyag is bemutatja.[333]

3. Képzés

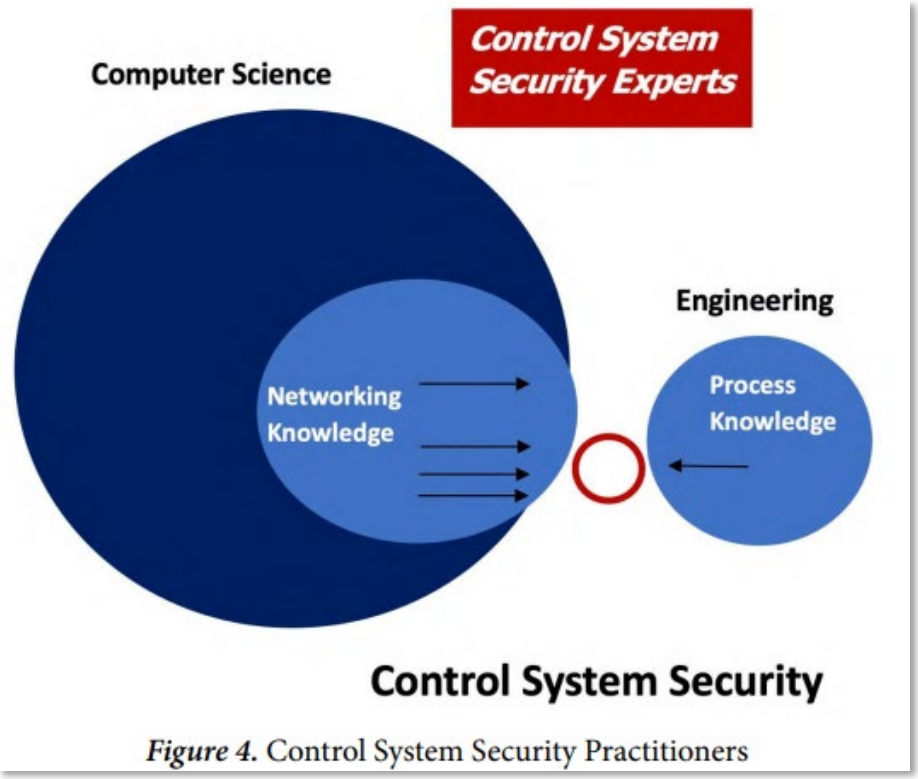
3.1. A helyzet

[333] alverad-ot-human-aspektusok-FIN.pdf

Világjelenség, hogy technológia felügyeleti rendszereket (ICS) is üzemeltető társaságok esetében fennakadások vannak az IT és OT rendszereket tervező, létesítő, de legfőképpen üzemeltető szakemberek együttműködésében. A problémák gyökere a két terület szakembereinek általában eltérő képzettsége és szemlélete, egymás szakterületi sajátosságainak, lehetőségeinek és korlátjainak elégtelen ismerete, a „szakadék" áthidalása szükségességének fel nem ismerése, avagy az áthidalásra vonatkozó képesség elégtelen volta.

Az egyre inkább az ICS-eket is érő támadások közepette elemi érdek e „szakadék" áthidalása. Ennek előfeltétele a jelenleg aktív, továbbá a jövőben munkába lépő szakemberek mindkét területre vonatkozó, komplex ismeretekkel történő felruházása.

Az ideális állapot az lenne, ha a két terület szakembereit mindkét területre vonatkozó ismeretekkel rendelkező szakértők segíthetnék:



16.5. ábra: Az IT és OT közötti szakmai hídszerepet nyújtani képes, azaz speciális képzésben részesítendő szakemberek lehetséges szerepe[334] [88]

[334] J. Weiss (2020) Control System Cyber Security In: Journal of Critical Infrastructure Policy 1. Évfolyam 2. Szám https://www.jcip1.org/weiss.html (Letöltve: 2022.01.14.)

A jelenlegi helyzetben, első lépésként már az is sikernek tekinthető, ha sikerül elősegíteni az IT-s és OT-s szakemberek egymás felé történő nyitását.

Ennek eszköze az oktatás, képzés.

Ennek átfogó célja az érzékenyítés egymás szakterületi sajátosságaira, lehetőségeire és korlátjaira.

A szaktudás és az elsajátítás módja többszintű megközelítést igényel. Kiberbiztonságnál az egyik legnagyobb kihívást az jelenti, hogy a támadások és az ott alkalmazott módszerek mindig „világszínvonalúak", így a védekezést is ehhez kell igazítani. Viszont minden rendszer egyedi, így a nemzetközi trendek és tudás mindig csak a helyi rendszerek komplex ismeretével, ahhoz alkalmazkodva építhető be, tehát alapvető feladat a hazai iparban dolgozó IT és OT szakemberek tudásának komplex továbbfejlesztése.

Az eddig meglévő szaktudás nem „felesleges", – ezért szükségtelen, életszerűtlen „lecserélni" a meglévő IT és OT szakembereket egy közös tudással rendelkező állományra. Nem célszerű sem az IT szakembereket OT szakemberré képezni, sem fordítva. Viszont

- egyrészről szükséges az érzékenyítés, azaz az IT ill. OT szakemberek látókörének kölcsönös bővítése a másik oldali szakterületek felé,
- másrészről olyan új kompetenciák megadására is szükség van, amelyek birtokában a szükséges és elégséges mértékben kölcsönösen értenek egymás szakterületeihez, de legfőképpen ahhoz, hogy a két terület között hidat képezhessenek.

Speciálisan villamosenergia-rendszerek esetén ez azt jelenti, hogy például a diszpécsereknek rendellenes mérési értékek fogadásakor, vagy valamilyen kommunikációs csatorna kiesése esetén már gyanakodniuk kell egy potenciális kiberbiztonsági kockázatra és az „IT oldallal" azonnal felvenni a kapcsolatot. Ehhez hasonlóan az IT infrastruktúra üzemeltetésben látható folyamatok alapján jelzéseket érdemes továbbítaniuk a diszpécserek számára, amivel a fizikai infrastruktúra állapotával is mérsékelhetik a potenciális káros hatást. A teljes folyamatot, interakciót és a rendszerszintű kockázatot pedig olyan szakemberek felügyelik, akik mindkét területre rálátnak.

A hazai képzések segítése szerves részét kell képezze a SeConSys működésének (célkitűzéseinkkel összhangban). Ezek közül is elsődleges a tudatosság növelése, az interdiszciplináris tudásanyag megfelelő helyekre való eljuttatása. A SeConSys ajánlások kidolgozásával segítheti a folyamatot, melyre különösen alkalmassá teszi nonprofit jellege és pártatlansága; így az iparági szereplők aktív bevonását is hatékonyan tudja biztosítani.

A következő két alfejezetben röviden áttekintjük a képzési típusokat, valamint a képzésekhez szükséges infrastruktúrát, fókuszálva a SeConSys által nyújtható támogatásra.

3.2. Képzési lehetőségek

A képzések lehetséges célcsoportjai egyrészt egyes közép- és felsőfokú képzések hallgatói, másrészt aktív IT-s, OT-s szakemberek, továbbá közép- és felsővezetők.

Az ismeretátadás történhet:

- a közoktatásban, a szak- és felnőttképzésben,
- szervezeti belső képzésben,
- külső szolgáltató által nyújtott képzésben

A fenti főbb képzési formák mindegyikében szükséges az eddigi szemlélet felülvizsgálata, az egymás területei felé nagyobb mértékű érzékenyítésre, illetve a fentebb is említett szakterületeket összekötő „híd" kompetenciára is.

A képzést tágabban értelmezve kiemelt fontosságú, hogy a közép- és felsővezetők látókörének bővítését segítsük, hiszen egy vezető kizárólag azt tudja megkövetelni a szervezetétől, amelynek létezéséről és fontosságáról ismerettel rendelkezik. Ebben különös jelentősége van a külső szolgáltató általi képzésnek. A tömör, ugyanakkor informatív képzés célszerű eleme a profilba vágó legutóbbi és legkomolyabb támadások és azok céges – reputációs, árbevételi stb. – hatásainak lényegre törő bemutatása. A vezetők limitált idejét figyelembe véve, az ismeretet, netán figyelmeztetést inkább hajlamosabbak elfogadni egy külsős szakértőtől, mint a saját beosztottjaitól.

A hagyományos köz-, szak- és felsőoktatás továbbra is az iparági tudás alapját adják, ezért szintén kiemelt figyelmet érdemel a terület. Az átfutás azonban lassabb, hiszen egy tanterv reform után évek telnek el, mire kikerülnek az első szakemberek az iparba, és még további évek, mire ezen szakemberek eljutnak középvezetői pozíciókba.

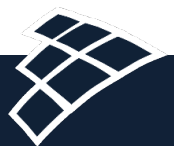
A belső képzésekre való igényt részben a fenti két képzési forma generálja, amivel az új kollégák betanulási időszaka rövidítheti, illetve az iparági új ismeretek közvetíthetők a meglévő kollégák számára.

A képzések elvégzését tágabb értelemben a regulációs környezet szabja meg az üzleti igények/érdekek mellett.

Az egyes képzési formák számára – többek között – az alábbi támogatást nyújthatja a SeConSys:

3.2.1. A SeConSys lehetséges szerepe a köz-, szak- és felnőttképzésben

- Közvetítheti a mindennapi üzemvitel során jelentkező releváns szempontokat, nehézségeket.



- A múltban előforduló helyzetekről esettanulmányokat készíthet, a gyakorlati nehézségekre fókuszálva – szükség szerint anonimizálva.
- Összesítheti, közvetítheti az iparági igényeket, melynek révén azok konzisztenciája javul, hatékonyabban épülhetnek be a tananyagokba annál.
- Hidat biztosíthat a szakmai gyakorlatok számára (pl. külső labormérések, gyakorlati foglalkozások, látogatások szervezésével).

3.2.2. A SeConSys lehetséges szerepe a szervezeti belső képzések terén

- Kapcsolatot tartva az egyetemekkel, kutatókkal (akár nemzetközi szervezetekkel és cégekkel is) a cégek számára közvetítheti a szakirányú trendeket, a nemzetközi regulációs irányokat.
- Segítheti a releváns tudás összegyűjtését.
- Cégeken átívelő szakmai tematikákat nyújthat.
- Segítheti az iparágban tevékenykedő cégek közötti kommunikációt, a képzések során gyűjtött tapasztalatok cseréjét.

3.2.3. A SeConSys lehetséges szerepe a külső szolgáltatók által nyújtott képzések terén

- Közvetítheti a hazai iparági igényeket a szereplők felé, melyre ők így könnyebben reagálhatnak, mint egy-egy cég egyedi megkeresése esetén.
- Előminősíthet, értékelhet, ajánlhat képzéseket a hazai szereplők számára.

3.2.4. A SeConSys lehetséges szerepe a képzési infrastruktúra biztosításában

A képzések fontos eszköze lesz egy olyan környezet, amely képes a releváns folyamatokat, mindennapokban használt eszközöket felvonultatni, de az éles rendszer kockázatai nélkül. Már a jelenben is léteznek olyan valós idejű szimulációs eszközök, melyekkel a fizikai folyamatok megfelelően kis időlépcsővel, megfelelő részletességgel emulálhatók ahhoz, hogy a SCADA, PAC és egyéb rendszerek ne tudják megkülönböztetni a valóságos világtól. Az IT biztonságnál pedig léteznek magas interaktivitású honeypotok és honeynetek, mely koncepciót szükséges bővíteni az OT sajátosságokkal. Így létrehozható egy integrált virtuális környezet, melyen egyszerre, azonos rendszerben lehet gyakorlatozni, sőt elemzéseket végezni, vagy pentestet, red team-blue team gyakorlatokat is folytatni.

Továbbá:

- A belső, kooperációs gyakorlati képzések lebonyolítására vonatkozó jó gyakorlatának gyűjtése és megosztása.
- A képzésekhez használt eszközrendszer alapjainak közös kialakítása:
  - Híd képzése a cégek és az egyetemek/kutatók között, ahol összefogásban megvalósulhatna az alapkérdések részletes vizsgálata.
  - Addig, amíg a cégek belső kompetenciában nem tudják megvalósítani a saját tréning rendszereiket, támogathatja egy közös gyakorlati platform koordinált létrehozásához és közös felhasználásához szükséges feltételek megteremtését.

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. augusztus 26.)

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

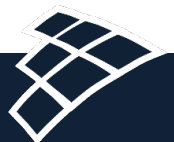
[7] L. Obregon. „Secure Architecture for Industrial Control Systems." SANS Institute. https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327 (Letöltve: 2020. augusztus 26.)

[8] M. C. Hurd, M. V. McCarty (2017) "A Survey of Security Tools for the Industrial Control System Environment" doi.org/10.2172/1376870

[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?" AutomationWord. 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.)

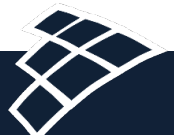
[19] A. Cherepanov, „Win32/Industroyer: a new threat for industrial control systems.” Eset. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf (Letöltve: 2020. 08. 28.)

[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.)

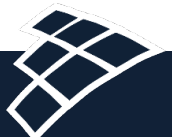
[30] C. McMahon. „Exclusive: EirGrid targeted by 'state sponsored' hackers leaving networks exposed to 'devious attack'." Independent.ie. https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html (Letöltve: 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] R. K. Knake. „A Cyberattack on the U.S.s Power Grid, Center for Preventive Action" https://www.cfr.org/report/cyberattack-us-power-grid (Letöltve: 2022. 01.14.)

[40] K. D. Bose. "NERC Cyber Security Supply Chain Risks: Staff Report and Recommended Actions Docket No. RM17-13-000" North American Electric Reliability Corporation https://www.eenews.net/assets/2019/05/29/document_ew_02.pdf (Letöltve: 2022. 01.14.)

[41] GAO. "Information Security: Supply Chain Risks Affecting Federal Agencies". U.S. Government Accountability Office https://www.gao.gov/products/gao-18-667t (Letöltve: 2022. 01.14.)

[42] 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: 2022. 01. 13.)

[43] K. Backman. "When Intrusions Don't Align: A New Water Watering Hole and Oldsmar." Dragos https://www.dragos.com/blog/industry-news/a-new-water-watering-hole/ (Letöltve: 2022. 01. 13.)

[44] I. Jibilian, K. Canales. "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal." Business Insider https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 (Letöltve: 2022. 01. 13.)

[45] P. Paganini: "SolarWinds Attack: Microsoft sheds lights into Solorigate second-stage activation." Security Affairs https://securityaffairs.co/wordpress/113681/apt/microsoft-solorigate.html/ (Letöltve: 2022. 01. 13.)

[46] "What You Need to Know About the Massive Solarwinds Hack." ExcalTech https://www.excaltech.com/what-you-need-to-know-about-the-massive-solarwinds-hack/?nowprocket=1/ (Letöltve: 2022. 01. 13.)

[47] B. Barett. "Security News This Week: Russia's SolarWinds Hack Is a Historic Mess" https://www.wired.com/story/russia-solarwinds-hack-roundup/ (Letöltve: 2022.01.14.)

[48] icscybersec. "A SolarWinds incidens tanulságai Magyarországon". ICS Cyber Security Blog https://icscybersec.blog.hu/2021/01/30/solarwinds-tanulsagok-magyarorszagon (Letöltve: 2022. 01. 13.)

[49] W. Turton, K. Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." Bloomberg https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (Letöltve: 2022. 01. 13.)

[50] J. Panettieri. "Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details." MSSPAlert https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/ (Letöltve: 2022. 01. 13.)

[51] Kovács László: A kibertér védelme, Hadtudomány, Ludovika Kiadó 2018.

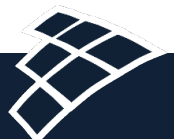
[52] M. Zeller. (2011) Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator? Schweitzer Engineering Laboratories, Inc., IEEE 10.1109/CPRE.2011.6035612

[53] Swearingen, M., Weiss, J., Huber, D. „What You Need to Know (and Don't) About the AURORA Vulnerability.": https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/ (Letöltve: 2022. 01. 13.)

[54] J. Weiss. "ICS cyber security is the second coming of the Maginot Line – and the Chinese have breached it." Energy Central https://energycentral.com/c/iu/ics-cyber-security-second-coming-maginot-line-%E2%80%93-and-chinese-have-breached-it (Letöltve: 2022. 01. 13.)

[55] J. Weiss. "Do the Chinese "own" our electric grids and other infrastructures?" Control Global https://www.controlglobal.com/blogs/unfettered/do-the-chinese-own-our-electric-grids-and-other-infrastructures/ (Letöltve: 2022. 01. 13.)

[56] J. Weiss. "Large electric transformers are subject to cyber attacks which can cause outages of months to years." ControlGlobal



https://www.controlglobal.com/blogs/unfettered/large-electric-transformers-are-subject-to-cyber-attacks-which-can-cause-outages-of-months-to-years/ (Letöltve: 2022. 01. 13.)

[57] National Intelligence Estimate. "Climate Change and International Responses Increasing Challenges to US National Security Through 2040." National Intelligence Council https://www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf (Letöltve: 2022. 01. 13.)

[58] Secure the Grid Coalition. "Improving Executive Branch Policies to Secure the United States Electric Grid." https://securethegrid.com/wp-content/uploads/2021/02/STG-Coalition-Letter-DOE-OMB.pdf (Letöltve: 2022. 01. 13.)

[59] 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.)

[60] Office of Electricity. "Department of Energy's Electricity Advisory Committee Establishes the Grid Resilience for National Security Subcommittee". https://www.energy.gov/oe/articles/department-energy-s-electricity-advisory-committee-establishes-grid-resilience-national/ (Letöltve: 2022. 01. 13.)

[61] FireEye "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor" https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor (Letöltve: 2022. 01. 13.)

[62] Department of energy. "Prohibition Order Securing Critical Defense Facilities" https://www.energy.gov/sites/prod/files/2020/12/f81/BPS%20EO%20Prohibition%20Order%20Securing%20Critical%20Defense%20Facilities%2012.17.20%20-%20SIGNED.pdf (Letöltve: 2022. 01. 13.)

[63] The White House. " Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis" https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-protecting-public-health-and-environment-and-restoring-science-to-tackle-climate-crisis/ (Letöltve: 2022. 01. 14.)

[64] Executive Office of the President. "America's Supply Chains", Executive Order 14017 https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains (Letöltve: 2022. 01. 13.)

[65] Office of Cybersecurity, Energy Security, And Emergency Response. "DOE Announces $8M to Build Robust and Cyber-Resilient Energy Delivery Systems"

https://www.energy.gov/ceser/articles/doe-announces-8m-build-robust-and-cyber-resilient-energy-delivery-systems/ (Letöltve: 2022. 01. 13.)

[66] Department of Energy "Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats" (Letöltve: 2022. 01. 13.) https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0v

[67] Energy Department. "Revocation of Prohibition Order Securing Critical Defense Facilities" https://www.federalregister.gov/documents/2021/04/22/2021-08483/revocation-of-prohibition-order-securing-critical-defense-facilities (Letöltve: 2022. 01. 13.)

[68] The White House. "Executive Order on Improving the Nation's Cybersecurity" https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (Letöltve: 2022. 01. 13.)

[69] T Axelrod. "White House sends out memo to private sector on cyberattack protections" The Hill https://thehill.com/policy/cybersecurity/556625-white-house-sends-out-recommendations-to-private-sector-on-protections (Letöltve: 2022. 01. 13.)

[70] The White House. "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems" https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (Letöltve: 2022. 01. 13.)

[71] IndustrialCyber. "CISA sets up latest cyber defense initiative to defend critical infrastructure" https://industrialcyber.co/article/cisa-sets-up-latest-cyber-defense-initiative-to-defend-critical-infrastructure/ (Letöltve: 2022. 01. 13.)

[72] Department of Energy. "Progress Report: 100 Days of the Biden Administration's Industrial Control Systems (ICS) Cybersecurity Initiative and Electricity Subsector Action Plan." https://www.energy.gov/articles/progress-report-100-days-biden-administrations-industrial-control-systems-ics (Letöltve: 2022. 01. 13.)

[73] The White House. "FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity" https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/ (Letöltve: 2022. 01. 13.)

[74] R. Walton. " 'Maybe it's not the right approach anymore' — FERC Chair Glick mulls new security paradigm for power sector" https://www.utilitydive.com/news/maybe-its-not-

the-right-approach-anymore-ferc-chair-glick-mulls-new-se/607594/ (Letöltve: 2022.01.14.)

[75] Cybersecurity & Infrastructure Security Agency. "CRITICAL INFRASTRUCTURE CONTROL SYSTEMS CYBERSECURITY PERFORMANCE GOALS AND OBJECTIVES" https://www.cisa.gov/control-systems-goals-and-objectives (Letöltve: 2022.01.14.)

[76] 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.)

[77] Energy Central Community. „FERC versus NERC." Energy Central. https://energycentral.com/c/iu/ferc-versus-nerc (Letöltve: 2020. augusztus 30.)

[78] M. Wopata "5 Industrial connectivity trends driving the IT-OT convergence." IoT. Analytics https://iot-analytics.com/5-industrial-connectivity-trends-driving-the-it-ot-convergence/ (Letöltve: 2022. 01. 13.)

[79] D. Scali. "Developing a Security Strategy to Cover ICS Assets." FireEye https://www.fireeye.com/blog/executive-perspective/2016/08/developing_a_securit.html/ (Letöltve: 2022. 01. 13.)

[80] Operations Management Systems Evolution. "OT/IT Convergence "What does it mean in the Industrial World?"" http://operationalevolution.blogspot.com/2015/02/otit-convergence-what-does-it-mean-in.html (Letöltve: 2022. 01. 13.)

[81] J. Weiss. (2014.) "Industrial Control System (ICS) Cyber Security for Water and Wastewater Systems" In: Securing Water and Wastewater Systems (pp.87-105) DOI:10.1007/978-3-319-01092-2_3

[82] P. Peeters. "Towards a Digital (manufacturing) Future – Part 5: Cybersecurity" Agorira https://www.agoria.be/en/manufacturing/innovation/towards-a-digital-manufacturing-future-part-5-cybersecurity (Letöltve: 2022. 01. 13.)

[83] B. Russel, D. V. Duren (2018.). Divergence in IT and OT security fundamentals In: Divergence in IT and OT security fundamentals https://subscription.packtpub.com/book/business/9781788832687/1/ch01lvl1sec16/divergence-in-it-and-ot-security-fundamentals

[84] R. M. Krieg. (2020.) "The Journal of Critical Infrastructure Policy". JCIP https://viewer.joomag.com/journal-of-critical-infrastructure-policy-volume-1-number-2-fall-winter-2020/0332765001608321823 (Letöltve: 2022.01.14.)

[85] Fortinet. "A Solution Guide to Operational Technology Cybersecurity" https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-operational-technology-design-guide.pdf (Letöltve: 2022. 01. 13.)

[86] S. Fluchs. "Why OT has different needs than IT". FluchsFriction https://fluchsfriction.medium.com/why-ot-has-different-needs-than-it-18ba9baa36e7 (Letöltve: 2022. 01. 13.)

[87] D. Harcharan, S. H. Houmb, E. A. Engum. "Safeguarding OT From Cyber Threats." ISSSource https://isssource.com/safeguarding-ot-from-cyber-threats-2/ (Letöltve: 2022. 01. 13.)

[88] J. Weiss (2020) Control System Cyber Security In: Journal of Critical Infrastructure Policy 1. Évfolyam 2. Szám https://www.jcip1.org/weiss.html (Letöltve: 2022. 01. 13.)

Felelős kiadó:

Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet

Budapest

Az 1. kiadást szerkesztette:

Dr. Bonnyai Tünde

Görgey Péter

Dr. Krasznay Csaba

A 2021. és 2022. évi kiadást szerkesztette:

Görgey Péter

Dr. Krasznay Csaba

ISBN 978-615-82042-3-1

>>SeCONSys

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI
KIBERVÉDELMI INTÉZET