Villamos rendszerek kiberbiztonsága az Ukrajnával kapcsolatos történések tükrében

Csatár János[1], Görgey Péter[2], Holczer Tamás[3*]

[1]Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamos Energetika Tanszék, Budapest, Magyarország
[2]Magyar Elektrotechnikai Egyesület, Budapest, Magyarország
[3]Budapesti Műszaki és Gazdaságtudományi Egyetem, Hálózati Rendszerek és Szolgáltatások Tanszék, Budapest, Magyarország
[*]Levelező szerző, e-mail: holczer@crysys.hu

Beérkezett: 2023. október 31.; elfogadva: 2023. november 20.; Online megjelent: 2024. március 28.

Összefoglalás

Minden fejlett ország erősen függ a villamosenergia-rendszerek működésétől, ami az idő előrehaladtával várhatóan növekedni fog. A stabil működést számos faktor befolyásolja, ezek egy része véletlenszerű (pl. időjárás), de az emberi tényező is nagy hatással van a megbízhatóságra. Ebben a cikkben a szándékos károkozás azon speciális eseteivel foglalkozunk, amikor a támadó a rendszert felügyelő és irányító számítógépes rendszeren keresztül befolyásolja károsan a villamosenergia-rendszer alapvető működését. Ehhez áttekintjük a két rendszer összefonódását, megvizsgáljuk az elmúlt nyolc évben Ukrajnában történt ilyen eseteket. A cikkben összegezzük és elemezzük a történéseket, valamint javaslatokat teszünk, hogy mit lehet tenni az ilyen káros események elkerülése érdekében, szem előtt tartva a „megelőzés, észlelés, reagálás" elvét.

Kulcsszavak: villamos rendszer, kritikus infrastruktúra, kibertámadás

Cyber security of electric power systems in light of the events related to Ukraine

János Csatár[1], Péter Görgey[2], Tamás Holczer[3]

[1]Budapest University of Technology and Economics, Department of Electric Power Engineering, Budapest, Hungary
[2]Hungarian Electrotechnical Association, Budapest, Hungary
[3]Budapest University of Technology and Economics, Department of Networked Systems and Services, Budapest, Hungary

Summary

All developed countries are highly dependent on the operation of electric power systems, and this dependence will probably increase. Many factors influence stable operation, some of which are random (weather or failures of devices and cables); however, human activities also have a significant impact on reliability. In this paper, we deal with special cases of attacks that achieve a detrimental effect on the electric power system by compromising the controlling and monitoring computer systems. To support the reader, we first analyze the key components of the physical and cyber parts of the system to provide an understanding of the intertwining of these domains – it is a cyber-physical system. We further elaborate on how an event can spread from one part to the other through domains. Then, a series of actual examples underlines the importance of this topic, focusing on malicious acts committed with the goal of sabotaging the power system. Thereafter, we analyze cyber-attacks committed during the last eight years in Ukraine. Most of these attacked the Ukrainian electric power system, aiming for blackouts and device destruction. Some of the attacks had severe consequences in other European countries as well. However, some attacks were successfully stopped before any harm was made. After analyzing the events, we conclude that threat actors' focus shifted from causing short-term blackouts to device destruction and long-term breakdowns. In the last part of our paper, we enumerate mitigation methods for operators. Our enumeration is based on the PreDeCo principle, namely prevention, detection, and correction. In conclusion, the defender must separate its different purpose networks, use strong authentica-

tion and authorization, and have proper patch management policies. These techniques must be verified with regular penetration tests. As the Ukrainian examples show, the threat actor sometimes can avoid prevention techniques; thus, good detection is necessary. The detection is based on analyzing the output of intrusion detection systems and detailed logging facilities. The analysis should be done in the security operations center by experts with knowledge of both cyberspace and electric power systems operations. In case of an incident, the security operations center must make corrective steps with the possible help of external experts. The corrective steps include the understanding of the incident, the recovery from the incident, the prevention of future similar incidents, and the digital forensic of the incident.

Keywords: electric power system, critical infrastructure, cyberattack

1. Bevezetés

A villamosenergia-rendszer legfőbb feladata a villamos energia biztosítása a termeléstől a fogyasztásig, ebbe beleértve a megfelelő helyre való eljuttatást is. Ma már a teljes Európát átszelő, összekapcsolt rendszer biztosítja ezt nálunk, mely számos más infrastruktúrától függ, és számos más infrastruktúra működésének alapja. Az energiahatékonyság, a megújuló energia integrálása, valamint a szén-dioxid-kibocsátás csökkentése egyaránt az elektrifikációt növeli, így a villamos energia a jövőben még inkább meghatározza az országok működését. Jelen cikkben a villamosenergia-rendszer kiberbiztonsága kerül fókuszba, amelynek az Ukrajna területén az elmúlt években tapasztalt történések jelentős aktualitást és európai relevanciát adnak.

A témát igyekszünk holisztikusan megközelíteni, ennek keretében a következő fejezet a villamosenergia-rendszer működésének sajátosságait világítja meg, azután az ukrajnai történések részletezése következik, végül a kiberbiztonsági kockázatok elemzésére, csökkentésére vonatkozó javaslatok zárják a sort.

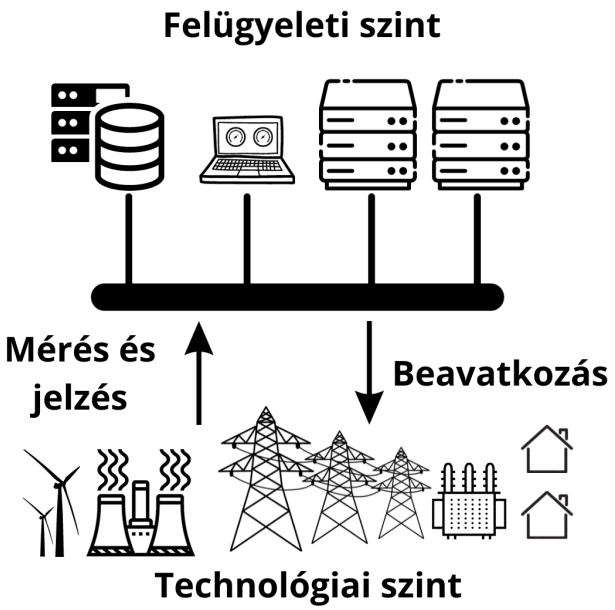
A témában számos általános és hazánkra specifikus tartalom érhető el a SeConSys kézikönyvében *(Angyal et al. 2023)*, amit minden érdeklődő olvasónknak ajánlunk.

2. A villamosenergia-rendszer működése kiberbiztonsági szempontból

A villamosenergia-rendszer kiberbiztonságának holisztikus kezeléséhez a következő alfejezetekben először a kiberfizikai működést világítjuk meg, majd a rendszer működésének alapjait, a lehetséges támadási pontokat mutatjuk be, végül pedig a rendszer kiberbiztonsági sérülékenységeit szemléltető példákat hozunk.

2.1. A villamosenergia-rendszer mint kiberfizikai rendszer

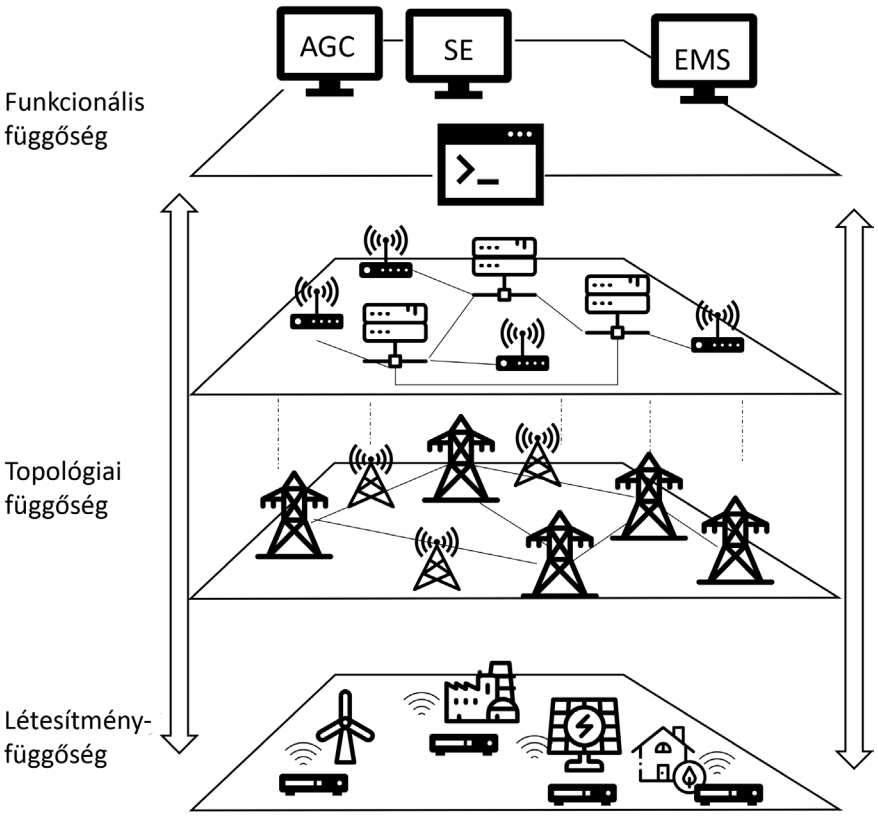
A villamosenergia-rendszer működése bár ma már folyamatos, de az állandósult állapotot érzékeny, gyors tranziens folyamatok alakítják. A mai, lényegében kontinensnyi rendszer üzemének irányítása és felügyelete már meghaladja az emberek áttekintőképességét és reakcióidejét; akár másodpercnél rövidebb válaszidő is szükséges. Ezen feladatokra ma már digitális eszközökre és kommunikációra támaszkodik a rendszer, így a kibertérnek, az algoritmusok szerepének jelentősége nemcsak megnőtt, hanem szerves részévé is vált a működésnek. A kiberfizikai rendszer azt jelenti, hogy a *„fizikai”* folyamat hat a *„kiber”* folyamatokra is, továbbá a visszahatás is legalább ennyire jelentős (lásd *1. ábra*).



1. ábra A villamosenergia-rendszer szemléltetése kiberfizikai rendszerként

Forrás: saját szekesztés Xu Guo 2023 alapján

Egy esetleges támadás is tetszőleges útvonalon fejtheti ki hatását, váltogathat a kiber és fizikai hatások között, kombinálhatja őket. A holisztikus megközelítésnél ezen két területet egyenrangúként, összekapcsoltan vizsgáljuk, melyhez az irodalomban az úgynevezett CPPS (cyber-physical-power-system, vagyis kiberfizikai villamosenergia-rendszer) terminológia jelent meg 2017 környékén *(Dai–Zhao–Chen 2017)*, és ezen megközelítés egyre több teret nyer a kutatásoknál. A villamosenergia-rendszer kiberfizikai leírásának irodalmi áttekintése mellett egy lehetséges keretrendszerére tesz javaslatot *(Xu et al. 2021)*, miáltal ez a holisztikus megközelítés részletesen modellezhető, biztosítva az egyes területek



2. ábra A villamosenergia-rendszer kiberfizikai rendszerként értelmezett függőségei

Forrás: saját szerkesztés Xu et al. 2021 alapján

egyenrangúságát. Erre egy példa volt az időjárás következtében a villamos és kommunikációs hálózat egyidejű meghibásodása 2008-ban és 2016-ban Kínában. A megközelítés közérthetőbb, rövidített formában is elérhető *(Xu–Guo 2023)*. Jelen cikk szempontjából különösen a többszintű függőség megjeleníthetősége lényeges, melyet a *2. ábra* szemléltet.

2.2. Az üzemirányítás szintjei

Az összekapcsolt villamosenergia-rendszereket csak elosztottan, koordináltan lehet üzemeltetni. Jelenleg a nagyobb területekért az átviteli engedélyesek (rendszerirányítók – TSO[1]) felelősek, ezek országonként 1-3 szervezetet jelentenek, melyek egymással szoros együttműködésben, valós időben felügyelik az országhatárokon átnyúló átviteleket, valamint a rendszer makró szempontú egyensúlyát. Az elosztói engedélyesek (DSO[2]) a rendszerhasználók (termelők és fogyasztók) közvetlen kapcsolódását biztosítják a rendszerhez. Ehhez más elosztókkal és az őket ellátó rendszerirányítóval, valamint a rendszerhasználókkal szintén szoros együttműködésre van szükség. Az általuk felügyelt entitások száma miatt általában a DSO-n belül is hierarchikusan több szintre bontott az üzemirányítás.

A szervezeti hierarchiával párhuzamosan, ahhoz hasonlóan, a villamosenergia-rendszer fizikai feszültségszintjei is hierarchikusan épülnek egymásra, melyek között transzformátor állomások (alállomások) biztosítják a kapcsolatot. A kisebb feszültségű szintek (elosztó hálózat) a rendszerhasználókhoz közel üzemelnek, a nagyobb feszültségszintek inkább az átvitelre szolgálnak. A hálózaton általában kevesebb és hosszabb vezeték biztosítja a nagy távolságú átvitelt, míg sok és rövidebb összeköttetés az energia elosztását.

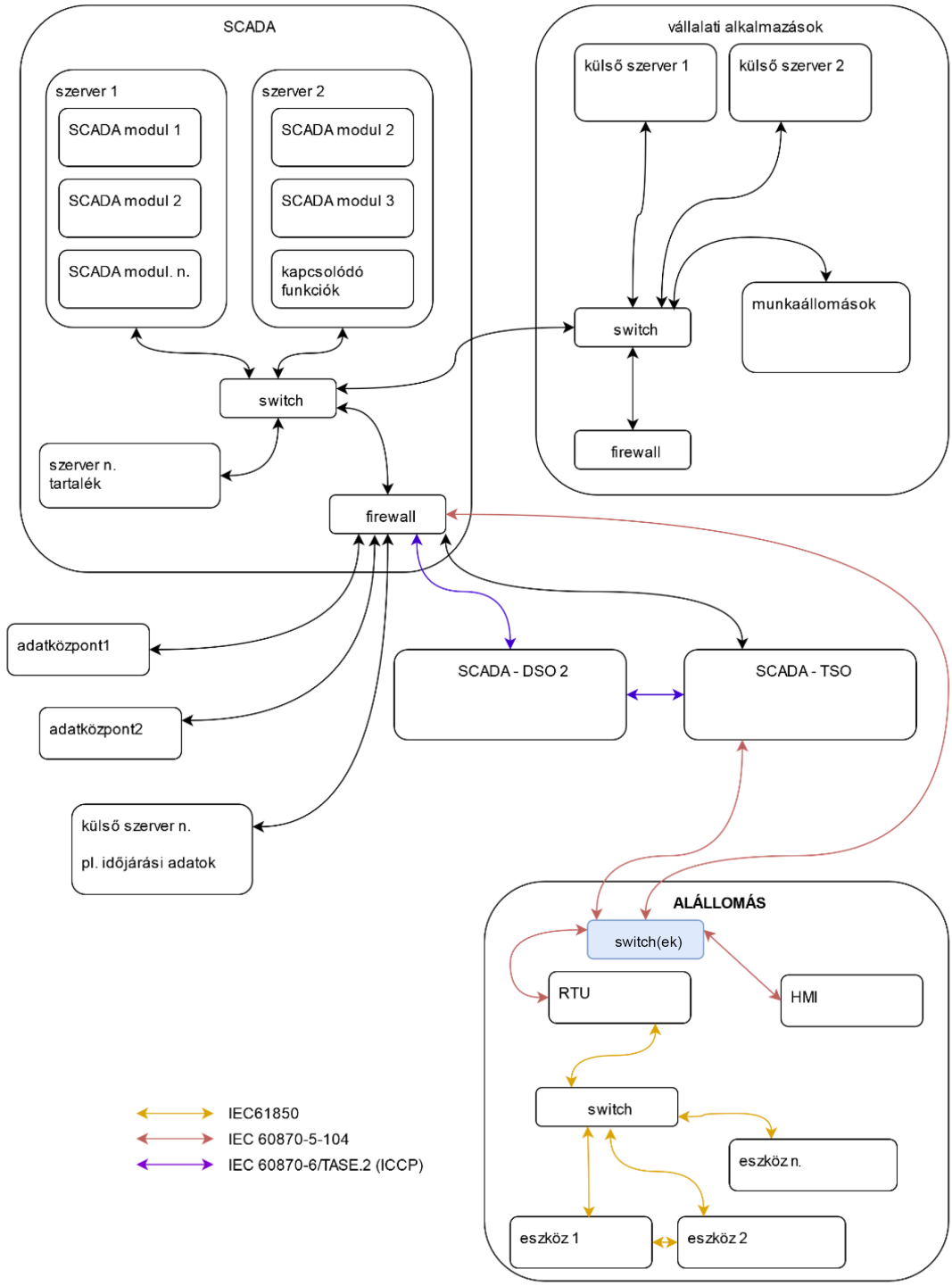
Mindegyik szintnél nagy földrajzi távolságok jellemzőek, melyek felügyeletéhez a mérések, jelzések és parancsok átvitelére van szükség, az irányítóközpontok csak ezeken a kapcsolatokon keresztül érzékelik a rendszer állapotát.

2.3. Üzemirányítási ICT infrastruktúra

A villamosenergia-rendszer üzemirányításához minden rendszerirányító hasonló struktúrát alkalmaz, ahol az üzemirányítási központ az alállomásokkal, kihelyezett szenzorokat felügyelő adatkoncentrátorokkal és más üzemirányító központokkal tart kapcsolatot. Az üzemirányítás központi eleme a SCADA rendszer (supervisory control and data acquisition), amely nemcsak

[1] TSO: Transmission System Operator (átviteli rendszerirányító).
[2] DSO: Distribution System Operator (elosztóhálózati rendszerirányító).

a rendszer felügyeletét biztosítja, hanem interfészként is szolgál számos automatizált funkció számára. Az iparágban elterjedt kommunikációs protokollok rendszerirányítási szinten, Európában az IEC 60870-5-104 és az IEC 60870-6 (ICCP TASE.2), valamint alállomáson belül ezen felül még gyártóspecifikus egyedi protokollok mellett az IEC 61850 szabványcsalád által definiált protokollok. Az iparági specifikus protokollokon kívül az általános ICT feladatokra itt is előfordulnak általános megoldások (távoli asztal kapcsolat, ssh stb.). Egy tipikusan hazai felépítésre mutat példát a *3. ábra*. A SeConSys által gondozott kiberbiztonsági kézikönyv mellékletében további részletek is találhatók ezen aspektusról *(Angyal et al. 2023)*.



3. ábra A villamosenergia-rendszer üzemirányítási rendszerének szemléltetése

Forrás: saját szerkesztés

2.4. A villamosenergia-rendszer sérülékeny pontjainak áttekintése

Az üzemirányításhoz szükséges és megkövetelt adathozzáférések, kitettségek alapján több potenciális támadási pont is kirajzolódik:

- A jogi reguláció miatti, illetve a működéshez szükséges, automatizált adatcsere biztosítja például a szomszédos üzemirányító hálózati állapotának ismeretét, de akár konkrét beavatkozási parancsok is ezen alapulnak, mint például a zárt hurkú szabályozásba bevont erőművek.
- A földrajzi kiterjedtség és a rendkívül szigorú rendelkezésre állás követelménye miatt ma már elkerülhetetlen a távoli hozzáférés alkalmazása, például személyzet nélkül működő alállomások, vagy akár beszállítók távoli munkavégzése is.
- Az üzemirányítási rendszer komplex, számos beszállító és harmadik fél együttműködésén alapul. Így ennek bármely eleme – a beszállítói láncot is beleértve – potenciális támadási pont.

A fenti, inkább külső felek felé meglévő kitettségek mellett a belső, a rendszer hierarchiai szintjeinél meglévő sérülékenységekre is érdemes példákat hozni:

- Maga a SCADA rendszer értelemszerűen kritikus eleme az üzemirányításnak, és így a támadások egyik potenciális célpontja is. Ezen keresztül egy pontról átvehető az irányítás a rendszer felett. Emiatt általában ez az egyik legjobban védett része a belső informatikai rendszereknek.
- A SCADA rendszerhez számos interfész kapcsolódik, amelyek mindegyike potenciális támadási felületet jelent, hiszen hozzáférhet kritikus folyamatokhoz, illetve kritikus adatok áramlanak keresztül rajta. Szintén védett, viszont az interfész már nyíltabb rendszerekhez is kapcsolódik, így könnyebben támadható.
- A SCADA rendszer számos adatforrásból táplálkozik, logikai kapcsolatban áll egyéb üzleti folyamatokkal (például menetrendezés, tervezett munkálatok, villamosenergia-piaci folyamatok). Így ezen adatok támadása a SCADA vagy interfészeinek közvetlen érintése nélkül is hatással lehet az üzemirányításra. Ezek támadásához tehát már nem szükséges az üzemirányítás legbelső rendszerének érintése vagy ismerete.
- A kommunikációs infrastruktúra általános ICT eszközökön is alapul, így ezek is támadási felületet jelentenek (kapcsolók, útvonalválasztók, tűzfalak), továbbá a földrajzi kiterjedtség miatt fizikailag nem is tartható a rendszer folyamatos ellenőrzés alatt.
- Az alállomások a SCADA rendszerekkel általában RTU (remote terminal unit – fejgép) eszközökkel tartanak kapcsolatot. Ily módon ennek támadása elvághatja a központi irányítást a konkrét beavatkozó és mérő eszközöktől. Lokálisan komoly hatással járhat, regionális hatásokhoz azonban egynél több alállomás támadására van szükség.
- Végponti eszközöknek tekinthetők a mérő és beavatkozó eszközök. Ezek támadása olyan helyzetet eredményezhet, melynél a helyreállítás csak a helyszínen oldható meg, mely kellő számosság mellett hosszú folyamatot, és így tartós hatást eredményez.

2.5. Megtörtént, releváns példák a villamosenergia-rendszer sérülékenységére

A villamosenergia-rendszer kiberbiztonsági szempontú sérülékenységeinek sokszínűségére az alábbi példák mutatnak egy betekintést kronologikus sorrendben.

- A 2003-ban történt incidens a Blaster nevű féreg nem szándékolt mellékhatása volt. Itt a támadók általában minden Windows frissítését célozták, mely így viszont kihatott az üzemirányítás-környéki eszközökre is. Végül a mérések, parancsok késve vagy egyáltalán nem értek célba, így sok tízmillió rendszerhasználó tapasztalt kimaradásokat *(Moyer 2011)*.
- 2010-ben a Stuxnet volt az első széles sajtónyilvánosságot kapó, és így az egyik legtöbbet hivatkozott olyan kiberbiztonsági incidens, mely fizikai károkat is eredményezett. Ez egy speciálisan erre kifejlesztett kártevő volt, potenciálisan többéves előkészítő fázissal *(McDonald et al. 2013)*.
- Ukrajnát több ízben is érte támadás, leginkább a 2015-ös eset kapott visszhangot. Ezekről a következő fejezet fog részletesen értekezni.
- 2020-ban a portugál EDP energetikai céget érte az eddigi egyik legnagyobb, publikált ransomware-támadás *(Osborne 2020),* ahol fogyasztói adatok voltak érintettek.
- Szintén 2020-ban az egyik legnagyobb kiberbiztonsággal foglalkozó céget, a SolarWinds-et ért incidensnél a hivatalos, gyártó által kiadott szoftverben jelent meg kártékony kód *(SolarWinds 2021)*. Ennek következtében hónapokig hozzáférést nyertek az érintett szoftvert telepítő ügyfelek rendszereiben a támadók. Az eset jól demonstrálja a beszállítói láncok jelentette kockázatokat.
- 2021-ben a Colonial Pipeline-t ért támadás *(Turton–Mehrotra 2021)* a számlázási rendszert érintette, viszont a fizikai elosztás leállítását vonta magával a további veszteségek és a fertőzés terjedésének megállítására tett erőfeszítések eredményeként. Ez az üzleti és üzemirányítási folyamatok egymásra hatásának egyik legtöbbet hivatkozott példája.
- 2021-ben a Log4J nyílt forráskódú szoftvermodul sérülékenysége került napvilágra (a sérülékenység egyébként már 2013 óta létezett), amivel a támadóknak távoli kód futtatására adott lehetőséget a modult implementáló minden szoftver esetén *(IBM 2023)*. Az eset bemutatta, hogy a mai komplex rendszerek fejlesztésénél már egy-egy szoftverfejlesztő cég sok más, akár nyílt forráskódú részre épít (melyről a megrendelő esetleg nem is tud). Ez a villamos energetikában is

meglévő hosszú beszállítói láncoknál kritikus sérülékenységet eredményezhet a végső rendszerben.
- 2022-ben a Vodafone portugáliai rendszereit érte kritikus támadás *(Demony 2022)*, mely a teljes távközlési infrastruktúra leállását eredményezte. Az eset példája annak, hogy akár a teljes kommunikációs infrastruktúra kiesése is vizsgálandó a villamos energetika területének kiberbiztonsági kockázatelemzése során.

További, folyamatosan frissülő példákat tartalmaz a SeConSys kézikönyve *(Angyal et al. 2023)*.

3. Az ukrán villamosenergia-rendszer elleni kiber- és fizikai támadások és azok tanulságai

Az ukrán villamosenergia-rendszer ellen 2015 óta zajlanak támadások. Ezeket – továbbá az orosz-ukrán konfliktushoz kapcsolódó, szintén energetikai célpontokat érintő egyéb támadásokat – elemezve mintázatok azonosíthatók, kirajzolódnak a támadások szakaszai, általános céljai és konkrét célpontjai.

3.1. A támadások szakaszai

Az aktuális (2023. októberi) állapot szerint öt jól elkülöníthető támadási szakasz azonosítható, melyeket a *4. ábra* szemléltet.

E szakaszolás indokai és az egyes szakaszok jellemzői az alábbiak:

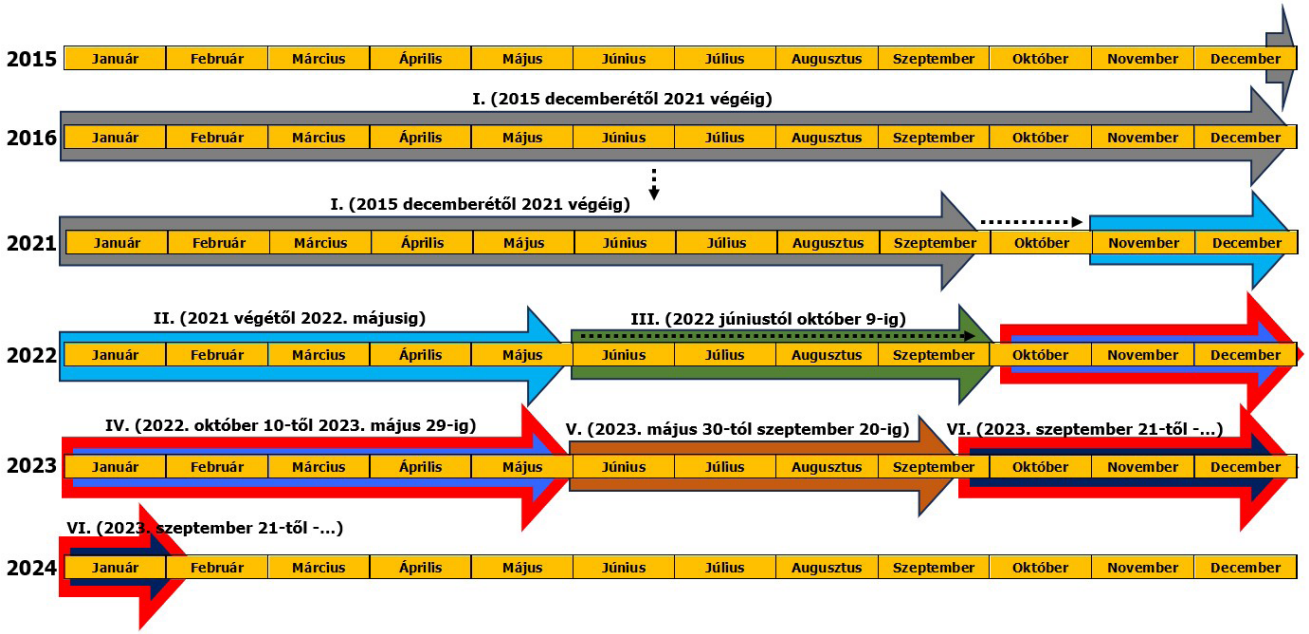
3.1.1. I. szakasz (2015 decemberétől 2021 végéig)

E szakasz meghatározó eseményei a 2015. december 23-ai, majd 2016. december 17-ei kibertámadások.

2015. december 23.: támadás ukrán DSO-k ellen

Hat DSO-t (ukrán elnevezéssel: oblenergo-t) ért támadás, amely három DSO esetében hosszú (3-6 óra időtartamú) és jelentős (mintegy 130 MW-nyi teljesítményt és 225 000 fogyasztót érintő) áramszüneteket okozott. Ennek közvetlen oka az volt, hogy az érintett DSO-k üzemirányítói mintegy 57 db 110 és 35 kV-os alállomás esetében nemcsak elveszítették a távfelügyelet lehetőségét, de mintegy 40 perces időtartamban (15:30 és 16:10 között) a három DSO üzemirányító központjaiból kezelői beavatkozás nélkül, az üzemirányítókat kizárva kerültek kiadásra megszakító kikapcsolási parancsok. Az üzemirányítók végül csak a SCADA-k teljes lekapcsolásával tudták megakadályozni azt, hogy a támadó további kapcsolásokat végezhessen.

A támadás eszköze a BlackEnergy3 malware volt. A támadó ezt a DSO-k rendszereibe adathalász e-mailek küldése (phising) révén tudta bejuttatni *(Lipovsky 2016)*. A támadó a Microsoft Active Directory szervereibe bejutva egyebek mellett megszerezte az üzemirányítók felhasználó azonosítóit. Ezzel hozzáférést és távkapcsolási jogosultságot szerzett az üzemirányító rendszer operátori felületein. A támadó mintegy 17 db SCADA HMI-hez hozzáférve, 50 alállomáson vált képessé az alállomási



4. ábra Az ukrán villamosenergia-rendszer elleni támadási szakaszok (a vastagított nyilak az ukrán villamosenergia-rendszer elleni súlyos fizikai támadások időszakait jelölik)

Forrás: saját szerkesztés

megszakítók kikapcsolására, ezzel kiterjedt áramszünet előidézésére.

Az illetéktelen kapcsolások mellett a támadó egyebek mellett az alállomási RTU-k Windows-alapú, integrált HMI firmware-jét is felülírta, ezzel akadályozva a kikapcsolt megszakítók helyszíni, kézi visszakapcsolását, vagyis a fogyasztók ismételt ellátását *(Styczynski–Beach–Westmoreland 2019)*.

A kibertámadás komplexitása miatt a villamosenergia-szolgáltatás végül csak órákkal később, az alállomásokra kiküldött üzemeltető személyzet helyszíni, kézi kapcsolásaival volt visszaállítható *(Lee–Assante–Conway 2016)*.

A támadó a támadást manuálisan hajtotta végre. Egyes jelek szerint a támadásban egyszerre több személy is részt vehetett.

A támadó valószínűsíthetően az orosz katonai hírszerzéshez, a GRU-hoz köthető Sandworm nevű APT[3] egység volt[4] *(Görgey 2020)*.

2016. december 17.: támadás a pivnichnai alállomás ellen

Míg a 2015. évi támadás sok, de főelosztó-hálózati alállomást, addig a 2016. évi csak egyetlen, de a Kijev északi részének villamosenergia-ellátását biztosító, Pivnichna-észak 330/110/10 kV-os átviteli hálózati alállomást érintette. Ismeretlen számú, összességében mintegy 200 MW teljesítményigényű fogyasztó maradt bő 1 óráig ellátatlan.

December 17-én, nem sokkal éjfél előtt az alállomáson üzemirányítói szándék nélkül megszakítók kezdtek sorozatban kikapcsolódni, ellátatlanul hagyva fogyasztókat.

A támadás eszköze az Industroyer-nek (más elnevezés szerint CrashOverride-nak) elnevezett malware[5] volt. Ez a BlackEnergy3-nál lényegesen fejlettebb, moduláris, a támadást – és annak részeként a kapcsolásokat – automatikusan végrehajtó eszköz volt. A támadást követő vizsgálatok eredménye szerint az Industroyer célja nem adatgyűjtés, hanem kifejezetten áramszünetek előidézése, sőt akár fizikai kár okozása volt. Az érintett fogyasztók ellátását másnap 01:05-re sikerült helyreállítani.

Az elemzések szerint a malware egyik moduljának kifejezetten az RTU-k támadása és a megszakítók kikapcsolása volt a feladata. Egy másik modul feladata volt szolgáltatásmegtagadás (DoS[6]) kiváltása az alállomás SIEMENS SIPROTEC védelmein, míg egy harmadik modulnak az alállomás távfelügyeletének lehetőségét kellett blokkolnia. A támadó még az üzemzavar utáni helyreállítás nehezítésére is gondolt azzal, hogy egy wiper (törlőprogram) modul csak másnap 02:20-kor lépett működésbe, fontos konfigurációs és rendszerfájlokat törölve. A malware az alállomáson ugyancsak működő ABB-eszközök egyes fájljainak törlésére is fel volt készítve, de szerencsés módon e készülékekben nem talált kihasználható sérülékenységet *(Slowik 2019)*.

A támadás kiemelt célpontjai voltak tehát az alállomási RTU-k. Az elemzések szerint a malware az IEC 101, 104 vagy 61850 protokollt alkalmazva az alállomási RTU-kban képes volt végtelen ciklusokat kiváltani. Ezek okozták egyrészt a megszakítók kikapcsolását, másrészt esetleges bekapcsolási távparancs esetén ismételt kikapcsolásukat. Ezzel végképp lehetetlenné vált a megszakítók távoli visszakapcsolása.

Villamos szakmai szempontból kulcsfontosságú mozzanat volt a pivnichnai alállomás villamos védelmeinek támadása. Még 2015. július 21-én ismertté vált a SIEMENS SIPROTEC 4 és SIPROTEC Compact védelmek sérülékenysége. Ezt megelőzően a SIEMENS ki is adta a sérülékenységet orvosló firmware frissítést. Nincs arra vonatkozó információ, hogy a támadás időpontjáig a pivnichnai alállomás SIPROTEC védelmein végrehajtották volna a firmware-frissítést.

Az elemzések szerint a malware DoS jellegű terhelést és firmware-frissítést idézett volna elő a SIPROTEC védelmekben. A védelmek korlátozott erőforrásai (főleg memóriája) miatt mindez a villamos védelem alapfunkciójának, azaz védelmi képességének elvesztését jelentette volna, közvetlen fizikai kár kockázatát teremtve az egyébként általa védett technológiai elem, berendezés vonatkozásában. Szerencsés körülmény, hogy a támadó kódolási hibát vétett, így a malware nem volt képes bénítani a SIPROTEC védelmeket *(Siemens 2018)*.

A valószínűsíthető támadó ugyancsak Sandworm csoport volt *(Görgey 2020a, 2020b)*.

3.1.2. II. szakasz (2021 végétől 2022. október 9-ig)

A 2022. február 24-ei inváziót megelőző hónapokban a kibertérben megkezdett orosz előkészítő műveletek új szakasz kezdetét jelezték. Az ukrán kritikus infrastruktúrák – így a villamosenergia-rendszer – felügyeleti rendszereiben meg nem erősített hírek szerint wiperek jelentek meg, ezzel zavarva meg a működésüket.

Február 24. után a kibertámadások mellett elkezdődtek az ukrán villamosenergia-rendszer elleni közvetlen fizikai támadások is (2022. február 24-től szeptember 30-ig 58 találat) *(Kostin 2023)*.

Az időszak néhány konkrét esete:

2022. február 24.: támadás a VIASAT KA-SAT műholdas kommunikációs rendszer ellen

Az Ukrajna elleni háború első napjára időzített támadás nem energetikai célú volt, ám hatásában mégis Európaszerte érintett energetikai objektumokat. A támadás a VIASAT KA-SAT műholdas rendszer földi modemjei ellen irányult. Célja az volt, hogy megzavarja az ezen

[3] APT: Advanced Persistent Threat (fejlett tartós fenyegetés, de a gyakorlatban az ilyen fenyegetésre képes állami hátterű támadók megnevezése).

[4] Bár egyes támadások esetén több csoport érintettsége is felmerülhet, de itt és a későbbiekben is a publikus adatok alapján valószínűsíthető domináns támadót nevesítjük.

[5] Malware: Malicious Software (rosszindulatú/kártékony szoftver/program).

[6] DoS: Denial of Service (szolgáltatásmegtagadás).

műholdas rendszeren is zajló ukrán műveleti kommunikációt. Azonban a támadásnak vélhetően nem szándékolt „mellékhatásai" is voltak. Például megbénult a német ENERCON GmbH mintegy 5800 (!) db, 11 GW összteljesítményű szélturbinájának távfelügyelete. A támadás eszköze az AcidRain nevű, kifejezetten modemek és routerek ellen tervezett wiper volt. Az esetek döntő többségében a modemek javíthatatlanul károsodtak, csak Európában mintegy 30 000 db. A támadásra egy rosszul konfigurált VPN adott lehetőséget *(Greig 2022)*.

A valószínűsíthető támadó orosz volt.

2022. március–április: támadások a Deutsche Windtechnik és a Nordex cégek ellen

A háború kezdeti szakaszában két olyan kibertámadás is történt, amelyek bár nem az ukrán villamosenergia-rendszer ellen irányultak, ám meghatározó európai energetikai cégek voltak a célpontok.

A Nordex dán szélturbinagyártó és üzemeltető óriást először 2021 novemberében érte támadás. A támadó a LockBit ransomware-t alkalmazta. Aztán a céget 2022. március 31-én újabb támadás érte. Szerencsére a cég a támadást korán azonosítani tudta. Az informatikai rendszereiket és a szélturbinák távoli hozzáféréseit azonnal leállították. Ezzel sikerült megakadályozni a támadó hozzáférését a cég egész rendszeréhez.

A támadást az ugyancsak orosz hátterű Conti csoport vállalta magára *(Williams 2017)*.

Április 11-én éjjel a Deutsche Windtechnik német szélturbina céget érte kibertámadás. A cég rendszerei a védelme érdekében minden külső rendszerrel megszakította a kapcsolatot. Ennek egyik következményeként mintegy 2000 szélturbina maradt 1 napra távfelügyelet nélkül *(Drügemöller 2022)*.

A támadó nem ismert.

2022. április: újabb támadás az ukrán villamosenergia-rendszer ellen (Industroyer2)

A támadás célja egyértelműen ismételt tömeges áramszünet kiváltása volt. A támadás eszköze a 2016. évi támadásnál alkalmazott Industroyer malware jelentősen továbbfejlesztett változata, az Industroyer2 volt.

A támadás elemzése szerint bár a malware már 2022. március végén „benn volt" az ukrán villamosenergia-rendszerben, azonban az április 8-ra tervezett támadást a CERT-UA – a Microsoft és az ESET közreműködésével – időben fel tudta deríteni, majd hatását jelentősen korlátozni *(ESET 2022)*. Ezzel együtt egyes, meg nem erősített hírek szerint a támadó egyes admin jogokat meg tudott szerezni.

A támadó képes volt az Ukrenergo informatikai (IT) hálózatáról az ipari vezérlőrendszer (ICS) hálózatára lépni. A CERT-UA az ESET szlovák kiberbiztonsági céggel és a Microsofttal együttműködve képes volt helyreállítani és megvédeni a megcélzott hálózatot *(Greenberg 2022; Kapellmann et al. 2022)*.

A támadó ebben az esetben is valószínűsíthetően a Sandworm csoport volt *(Wright 2022)*.

2022. április: támadás PLC-k ellen (Pipedream)

A Pipedream egy kifejezetten PLC-k ellen kifejlesztett, tűzfalak, határvédelem, hitelesítés, titkosítás megkerülésére, jelszavak megszerzésére, belső kommunikáció megszakítására, PLC átprogramozására, memória törlésére stb. képes, fejlett technológiai szinttel rendelkező, moduláris keretrendszer.

Az OT rendszerek kibervédelmének egyik meghatározó cége, a DRAGOS elemzése szerint a Pipedream nem OMRON-, SCHNEIDER-, azaz gyártóspecifikus, hanem szinte bármely más PLC-re veszélyes lehet. A DRAGOS vizsgálati eredményei alapján a támadás célja egyértelműen a fizikai károkozás volt. Összességében a Pipedreamet *„állami szintű, háborús képességnek"* minősítette.

A vélhetően sikeres védekezésnek köszönhetően nincs arra vonatkozó információ, hogy a Pipedream Ukrajnában sikerrel működésbe tudott volna lépni.

A támadó valószínűsíthetően a Chernovite nevű orosz csoport volt *(Dragos 2022)*.

2022. augusztus 14.: támadás szentpétervári 110 kV-os alállomás ellen (Operation Smoked)

Augusztus 14-én, Szentpéterváron támadás érte a Rosseti Lenenergo cég 110/35 kV-os alállomását. A támadó a SCADA rendszeren keresztül hozzáférést szerzett az alállomási UPS-hez, azon belül az akkutöltőhöz is. A támadó a töltőáram valószínűsíthető manipulálásával képes lehetett túlmelegíteni az akkumulátorokat. Ezzel fizikailag károsíthatta azokat és azok érzékelőit is. A jelek szerint a támadás célja a fizikai károkozás volt.

A támadó valószínűsíthetően az ukrán szimpatizáns OneFist csoport volt *(Béres 2022)*.

3.1.3. III. szakasz (2022. október 10-től 2023. május 29-ig)

E szakaszban domináns módon közvetlen fizikai támadások (rakéta, manőverező robotrepülőgép, drón) zajlanak. Nem érhető el információ arra vonatkozóan, hogy az ukrán villamosenergia-rendszert ebben az időszakban a korábbiakhoz mérhető súlyosságú kibertámadás érte volna.

A 2022. október 1. és 2023. február 20. közötti időszakban az ukrán villamosenergia-rendszert 197 találat érte.

3.1.4. IV. szakasz (2023. május 30-tól 2023. szeptember 20-ig)

Május 30-án súlyos, kiterjedt üzemzavar volt az ukrán villamosenergia-rendszerben, egy bejelentés szerint fő-

leg annak keleti részén[7] *(Görgey 2023)*. Az ilyen esetekben szokásos kivizsgálás annak gyanúját vetette fel, hogy valójában kibertámadás történt. Egyes meg nem erősített hírek szerint az RTU-kben az Industroyer2 nyomaira lehetett bukkanni. A jelek arra utalhattak, hogy a malware a téli támadások után megindult helyreállítási munkák során kerülhetett be a rendszerbe, hátsó ajtókat biztosítva a támadó számára. Ha ez a „beszivárgás" valós, akkor súlyos kockázatot jelent a 2023. évi téli időszakra, amikor egyáltalán nem zárható ki az ukrán villamosenergia-rendszer elleni támadások újraindulása, immár a fizikai és kibertámadások együttes alkalmazásával.

3.1.5. V. szakasz (2023. szeptember 21-től …)

Az V. támadási szakasz jelenleg is zajlik. Oroszország mintegy háromhavi szünet után szeptember 21-én ismételt légitámadást indított az ukrán villamosenergia-rendszer ellen.

A háború új mozzanata, hogy szeptember 29-én, majd 30-án immár Ukrajna mért csapást orosz energetikai célpontokra.

A kézirat lezárásának pillanatáig újabb jelentős, energetikai célpontot érő támadásról nem áll rendelkezésre publikus információ.

3.2. A támadásokból levonható következtetések

A vizsgált 8 év támadásait elemezve több hangsúlyos elem is kiemelhető:

– A villamosenergia-rendszer mint „legkritikusabb" kritikus infrastruktúra egyre inkább akár kiber-, akár fizikai támadások lehetséges célpontja. A veszély mértékét mutatja, hogy kritikus infrastruktúrákat érő kibertámadások csaknem 40%-át teszik ki az energetikai célpontok *(Security 2023)*.
– A kibertámadások a kezdetben végrehajtott, „csak" jogosulatlan kikapcsolások után egyre inkább a célpont fizikai károsítását is célozzák. A károkozás mértéke valamely digitális eszköz tönkretételétől (lásd KA-SAT modemek) egészen a technológiai berendezések javíthatatlan károsításáig (lásd Rosseti Lenenergo akkumulátorok) terjed.
– A villamosenergia-rendszer berendezései között kiemelt célpontnak látszanak az RTU-k, illetve a PLC-k. Ez vélhetően abból a logikából fakad, hogy ezek a Purdue modell szerinti 1. szinten lévő eszközök a megzavarni, károsítani kívánt technológia – villamosenergia-rendszer esetében megszakítók, transzformátorok, turbinák, generátorok – közvetlen közelében vannak. Nem véletlen, hogy a Stuxnet támadás hangsúlyos célpontjai is az uráncentrifugákat közvetlenül vezérlő PLC-k voltak.

De az RTU-k (PLC-k) már önmagukban is azért célpontok, mert például firmware-jük átírásával, avagy wiper alkalmazásával működésképtelenné tehetők, amely hozzájárul az előidézett üzemzavar elhúzódásához.

- Az ukrán villamosenergia-rendszer elleni elmúlt téli támadások célpontjai egyértelműen az előző pontban említett villamos főberendezések voltak. Ezek kifejezetten drága, gyakran egyedi, ezért csekély mértékben tartalékolt, időigényes gyártású, méretük és/vagy súlyuk miatt nehezen szállítható berendezések. E tulajdonságaik miatt fizikai károsításokkal jelentős mértékben és hosszan elhúzódóan zavarható meg a villamosenergia-ellátás. Mivel a sorolt főberendezések is egyre inkább digitalizáltak, szintén Purdue 1. szintű eszközökkel felügyeltek, sőt vezéreltek, ezért egyre nagyobb az ezeket fenyegető kockázat. E berendezések esetében egyértelműen beazonosíthatóak azok az egyre inkább digitalizált alrendszerek, amelyek működésének megzavarásával (például téves adat bejuttatásával, azaz FDI, False Data Injection révén) a főberendezések tényleges és súlyos fizikai károsodása idézhető elő.
- Összességében a fentiek azt is jelentik, hogy a támadók egyre mélyebb szakmai ismeretekkel rendelkeznek a megtámadott technológiai berendezésekről és az azok ellátási rendszerben játszott szerepéről éppúgy, mint például egy üzemzavar kezelésének módjáról, így megzavarásának lehetőségeiről is. A történtek tükrében súlyos hiba lenne alábecsülni a támadó technológiai ismereteinek minőségét.

Mindezek azt jelzik, hogy a támadási képességek bizonyított fejlődése egyre inkább lehetővé teszi technológiai berendezések fizikai károsítását. Egyes esetekben a támadó már a gyakorlatban is bizonyította ez irányú képességét. Az elmúlt évek eseményeinek áttekintése után térjünk rá, hogy mit tehetnek és tesznek az üzemeltetők, hogy elkerüljék a hasonló eseményeket.

4. Védekezés

A támadásokból levont tapasztalatok és a szakmai gyakorlat alapján össze lehet állítani a védekezés főbb technikai lehetőségeit. A védekezés többrétű, kezdve a szabályozással, a képzéssel, majd a technikai védekezésen át az incidensek kivizsgálásáig és a rendszerek sérülékenységvizsgálatáig. Jelen írás a védekezés technológiai lehetőségeire fókuszál.

A kiberbiztonság esetén a védekezésnek három összefüggő mozzanata van, ezek a megelőzés, észlelés és reagálás (Prevention, Dection, Correction, PreDeCo) *(ISA 2007)*. A megelőzés folyamán megpróbáljuk elkerülni a sikeres támadásokat, vagy a támadások hatását próbáljuk meg minimalizálni. Ugyan a hatékony megelőzés létfontosságú, de nem létezik tökéletes védelem. A támadó előbb vagy utóbb be tud jutni a célpontra, és ott valamilyen tevékenységet tud végezni. Ebben a szakaszban már

[7] Ukrenergo Telegram poszt: https://t.me/Ukrenergo/2113.

inkább az a fontos, hogy ezt a rosszindulatú tevékenységet minél előbb észlelni tudják az üzemeltetők. Iparági statisztikák esetén a behatolás és az észlelés között eltelt idő több hónap is lehet, ami tág teret ad a támadónak a célja elérésére. Az észlelés feladata ennek az időintervallumnak a leszorítása (ami az utóbbi években jelentősen sikerült is a 2011-es globális medián 416 napról 24 napra 2020-ra – *Mandiant 2021*). Az észlelt támadás után az üzemeltető feladata a normál működés minél gyorsabb helyreállítása. – Ezt támogatja a reagálás művelete. A következő alfejezetekben ennek a három összetevőnek a villamosenergia-rendszer specifikus tényezőit tekintjük át röviden. Alaposabb áttekintés érdekében a SeConSys együttműködés keretében készült kézikönyvet *(Angyal et al. 2023)* javasoljuk tanulmányozni.

4.1. Megelőzés

A megelőzés többrétű feladat, aminek a célja a sikeres támadások kivitelezésének megelőzése vagy a hatásuk minimalizálása. Ennek első lépése a sebezhetőségek felmérése. Ezt ideális esetben egy független szereplő hajtja végre előre egyeztetett időpontokban, rendszeresen. A feladat kihívása, hogy míg hagyományos IT-rendszerekben sokan tudnak sérülékenységvizsgálatot végrehajtani, addig villamosenergia-rendszerek esetén speciális szaktudás és eszközkészlet szükséges. További probléma lehet, hogy nem kellő helyismerettel végrehajtott tesztelés önmagában is szolgáltatáskiesést okozhat. Emiatt élő rendszer ellen veszélyes ilyen tesztet végrehajtani, de a rendszerek leállítása tipikusan nem lehetséges; legalábbis nem olyan gyakorisággal, ami a sérülékenységvizsgálat szempontjából kívánatos lenne.

Akár normál üzemeltetés folyamán, akár az előbb említett sérülékenységvizsgálat következtében kiderülhet, hogy egy rendszerhez rendelkezésre áll olyan javítás, ami sérülékenységet szüntet meg. Ezt minél előbb érdemes alkalmazni, de csak akkor, ha az alkalmazása nem okoz további kockázatot. Villamosenergia-rendszerek esetén a karbantartási ablakok ritkasága, illetve az előzetes alapos tesztelés hosszú ideje nehezíti meg a javítások gyors bevezetését.

Rendkívül fontos a felügyelő és irányító rendszerek szeparálása a többi rendszertől, illetve a rendszeren belüli elválasztások is. Ezt tipikusan tűzfalak és egyéb határvédelmi megoldások szolgáltatják. Ezeknek a tervezése közben a lehető legteljesebb szeparációra kell törekedni. Tehát például, ha nem szükséges, hogy a szomszédos alállomások egymással kommunikáljanak, akkor az ilyen irányú forgalmakat is korlátozni kell. Természetesen az operátoroknak hozzá kell férniük a felügyelt eszközökhöz, de ezt csak jól beállított virtuális magánhálózatokon keresztül szabad engedélyezni, megfelelő hitelesítés és jogosultságkezelés után. Ha ez nem sikerül jól, akkor tudnak a támadók például az előző fejezetben említett 2022. februári módszerrel bejutni a hálózatba. A többfaktoros hitelesítés használata is javasolt, amivel meg lehet nehezíteni a 2015. decemberihez hasonló támadásokat. A hitelesítést és jogosultságkezelést nemcsak a humán operátorok esetében érdemes alkalmazni, hanem gép-gép kommunikáció esetén is. Ezzel elkerülhető, hogy jogosulatlan felhasználók utasításokat tudjanak kiadni, mint ahogy történt az előző fejezetben tárgyalt 2015. és 2016. decemberi esetekben.

Természetesen a hitelesítés és jogosultság ellenőrzése csak akkor ér valamit, ha a létező kapcsolatokba a támadók nem tudnak beleszólni. Ezt a célt szolgálja a kommunikációs protokollok titkosítása és legfőképpen integritásvédelme. A villamosenergia-rendszerekben használt régebbi protokolloknak nincs megfelelően védett verziójuk (például Modbus), vagy nem széles körben támogatott, mint az IEC 60870-5-104 esetén a TLS vagy IPsec használata. Modernebb protokollok, mint például az IEC 61850 esetén viszont rendelkezésre állnak megfelelően védett alverziók is. Ilyen megoldásokra ad iránymutatást például az IEC 62351, valamint egyéb protokollok használata is felmerül. Ezeknek a modern megoldásoknak a használatát viszont tipikusan csak az újabb eszközök támogatják, amelyekre való áttérés jelentős költséget róhat az üzemeltetőre.

Azonban a legalaposabban kidolgozott megelőzés esetén is előfordulnak incidensek, amiket észre kell venni. Ezeket a technikákat mutatja be a következő alfejezet.

4.2. Észlelés

Az észlelés alapvető feltétele, hogy az operátorok tudják, mi történik a saját hálózataikban és más hasonló hálózatokban. Az utóbbi célt hatékony információmegosztással lehet elérni, mind az iparágon belül, mind nemzetközi szinten. Ezt a célt támogatja például az ENISA az Európán belül a NIS1 direktíva alapján létrehozott, majd a NIS2 alapján megerősített CSIRTs[8] hálózata.

A saját hálózatok megfigyelése leginkább behatolásdetektáló rendszerek futtatásával, naplózással és a naplók folyamatos elemzésével valósul meg. A behatolásdetektáló rendszerek a tipikus támadási mintázatokat tudják felismerni, vagy a normális működéstől való eltérést. Naplózás folyamán minden fontosabb eseményről bejegyzés készül, aminek az elemzésével időben észre lehet venni a nem kívánt eseményeket. A naplózás lehet akár lokális is, de elemezhetőség szempontjából szerencsésebb a központi naplógyűjtés. Nagyon fontos a naplók integritásának megőrzése, hiszen egy módja a támadás elrejtésének, ha a támadó törölni tudja a saját lépéseihez tartozó bejegyzéseket.

A nagy méretű naplóállományok feldolgozása automatikus módszereket tesz szükségessé. Erre alkalmasak

[8] https://csirtsnetwork.eu/.

a SIEM[9] megoldások. Ezek a megoldások lehetővé teszik a naplók automatikus ellenőrzését, a független események korrelációját, és ezáltal a lényeges események kiemelését a humán operátor számára. Az operátorok a SIEM jelzéseit és a hálózat állapotát figyelembe véve tudják időben észlelni, hogy támadás alatt állnak. A feladat talán legnagyobb kihívása, hogy az operátoroknak egyszerre kell érteniük a kiberbiztonsághoz és a villamosenergia-rendszerek működéséhez is. A villamosenergia-rendszer teljesítményátvitelt közvetlenül végző része olyan, a fizikai folyamatokra alkalmazott védelmi és automatika megoldásokkal is rendelkezik, melyek annak fizikai meghibásodása esetén működnek. Ezekre azonban ritkán kerül sor, viszont ilyenkor kritikus a megfelelő működés. A nagyon ritka események ugyanakkor megnehezítik a megfelelő detekciós szabályok felállítását (ezek tipikusan a tesztidőszak alatt nem fordulnak elő), illetve hamis pozitív jelzéseket generálhatnak.

4.3. Reagálás

Az észlelt incidenseket kezelni kell. Az incidensekre való reagálás nem az incidensekkel kezdődik, hanem sokkal korábban. Ideális esetben egy belső csapatot készítenek fel az incidensek kezelésére, de gyakran szükség van külső szakértőkre is. A felkészítés során rendszeres oktatás és szituációs gyakorlatok váltják egymást. Az így felkészített csapat képes lehet elemezni az eseményeket, körülhatárolni a kompromittálódott rendszereket és támogatni a helyreállást. Jó példa a hatékony reagálásra az előző fejezetben említett 2022. áprilisi események, míg kevésbé hatékony reagálás történt például 2015 decemberében, ami a támadássorozat első része volt, továbbá vélhetően a 2023 nyarán történt eseményeket is egy nem tökéletes helyreállás alapozta meg. A helyreállás tipikusan egy mentett állapot visszatöltését jelenti, amihez nélkülözhetetlen a rendszeres mentések elkészítése. Emellett nagy segítséget jelent, ha az utolsó felhasznált konfigurációk egy jól strukturált és védett helyről elérhetők, ezzel elkerülve egy korábbi inkonzisztens, már nem aktuális állapotra való visszaállásból következő további problémákat.

5. Összefoglalás

Jelen cikkben általánosságban áttekintettük a villamosenergia-rendszerek kitettségét a kibertér felől jövő támadásokra. Számba vettük, hogy milyen fontosabb részekből áll a rendszer, és azoknak a kompromittálódása milyen hatással lehet az egész rendszer működésére. Ezek után megvizsgáltuk, hogy az elmúlt években milyen kibertámadások érték az ukrán villamosenergia-rendszert, és ezt miként lehet jelentősebb szakaszokra bontani, illetve milyen következtetéseket lehet levonni a publikus információkból. Végül azt vizsgáltuk meg, hogy milyen ellenintézkedéseket tehet egy operátor a támadások káros hatásainak elkerülésének vagy csökkentésének érdekében.

A hazai villamosenergia-rendszer éves szinten jelentős villamosenergia-importtal rendelkezik[10], melynek eddig az egyik legjelentősebb forrása Ukrajna volt. Egy következő értekezésben érdemes lenne megvizsgálni, hogy az ukrajnai eseményeknek milyen hatásuk volt és van a magyar ellátásbiztonságra, illetve mit lehet tenni az ellátásbiztonság további fokozása érdekében.

Köszönetnyilvánítás

Ennek a publikációnak a megszületését részben a Nemzeti Kutatási Fejlesztési és Innovációs Alap FIEK 16-1-2016-0007 számú projektje támogatta.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

6. Irodalomjegyzék

Angyal I., Arató Gy., Bakos B., Baranya Zs., Bocsok V., Bogáncs T., ... Zámbó M. (2023) Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve. Nemzeti Kibervédelmi Intézet. ISBN 978-615-82042-3-1

Béres K. (2022) Pro-ukrainian hacker group claims hacked Rosseti Lenenergo's SCADA system. CyberThreat. Report

Dai, H., Zhao, S., & Chen, K. (2017) A chaos-oriented prediction and suppression model to enhance the security for cyber physical power systems. Journal of Parallel and Distributed Computing, Vol. 103. pp. 87–95. ISSN 0743-7315. https://doi.org/10.1016/j.jpdc.2016.11.015

Demony, C. (2022) Vodafone Portugal hit by hackers, says no client data breach. https://www.reuters.com/technology/vodafone-portugal-hit-by-hackers-says-no-client-data-breach-2022-02-08/ [Letöltve: 2023. 10. 30.]

Dragos Inc. (2022) CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS). https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/ [Letöltve: 2023. 10. 12.]

Drügemöller, L. (2022) Erpressung aus dem Cyberraum. https://taz.de/Cyber-Attacken-auf-Windenergiebranche/!5848854/ [Letöltve: 2023. 10. 12.]

ESET (2022) Industroyer2: Industroyer reloaded. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ [Letöltve: 2023. 10. 12.]

[9] SIEM: Security Incident and Event Management (Biztonsági információk és események kezelése).

[10] https://www.mavir.hu/web/mavir/brutto-energia-eves.

Görgey P. (2020a) Kibertámadások Ukrajnában: áramszünetek és tanulságok. Elektrotechnika, Vol. 110. No. 11. pp. 22–24. https://www.mee.hu/files/files/et2020-11.pdf [Letöltve: 2023. 10. 12.]

Görgey P. (2020b) Kibertámadások Ukrajnában: áramszünetek és tanulságok. (II. rész) Elektrotechnika, Vol. 110. No. 11. pp. 22–24. https:// www.mee.hu/files/files/et2020-11.pdf [Letöltve: 2023. 10. 12.]

Görgey P. (2023) Az ukrán villamosenergia-rendszer átmenetileg két részre szakadhatott. CyberThreat.Report. https://www.cyberthreat.report/az-ukran-villamosenergia-rendszer-atmenetileg-ketreszre-szakadhatott/ [Letöltve: 2023. 10. 12.]

Greenberg, A. (2022) Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine. WIRED. https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/ [Letöltve: 2023. 10. 12.]

Greig, J. (2022) Viasat confirms report of wiper malware used in Ukraine cyberattack. The Record. https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack [Letöltve: 2023. 10. 12.]

IBM (2023) What is the Log4j vulnerability?. https://www.ibm.com/topics/log4j [Letöltve: 2023. 10. 30.]

ISA (2007) ISA-62443-1-1-2007 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models, International Society of Automation. https://www.isa.org/products/isa-62443-1-1-2007-security-for-industrial-automat [Letöltve: 2023. 10. 30.]

Kapellmann, Z., Leong, D., Leong, R., Sistrunk, C., Proska, K., Hildebrant, C., Lunden K., & Brubaker, B. (2022) INDUSTROYER.V2: Old Malware Learns New Tricks. Mandiant. https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks [Letöltve: 2023. 10. 12.]

Kostin, A. (2023) Пресконференція Андрія Костіна про роботу прокуратури за рік повномасштабної агресії РФ (Andriy Kostin's press conference on the work of the prosecutor's office during the year of full-scale aggression by the Russian Federation). https://www.gp.gov.ua/ua/posts/preskonferenciya-andriya-kostina-pro-roboti-prokuraturi-za-rik-povnomasstabnoyi-agresiyi-rf [Letöltve: 2023. 10. 12.]

Lee, R. M., Assante, M. J., & Conway, T. (2016) Analysis of the Cyber Attack on the Ukrainian Power Grid. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf [Letöltve: 2023. 10. 12.]

Lipovsky, R. (2016) New wave of cyberattacks against Ukrainian power industry. ESET spol s.r.o. https://www.welivesecurity.com/en/company/contact-us/ [Letöltve: 2023. 10. 12.]

Mandiant (2021) M-Trends 2021, Fireeye Mandiant Special Report. https://services.google.com/fh/files/misc/m-trends-report-2021-en.pdf [Letöltve: 2023. 10. 28.]

McDonald, G., O Murchu, L., Doherty, S., & Chien, E. (2013) Stuxnet 0.5: The Missing Link. https://docs.broadcom.com/doc/stuxnet-missing-link-13-en [Letöltve: 2023. 10. 30.]

Moyer, M. (2011) Expert: A Virus Caused the Blackout of 2003. Will the Next One Be Intentional?. https://blogs.scientificamerican.com/observations/expert-a-virus-caused-the-blackout-of-2003-will-the-next-one-be-intentional/ [Letöltve: 2023. 10. 30.]

Osborne, C. (2011) Energy company EDP confirms cyberattack, Ragnar Locker ransomware blamed. https://www.zdnet.com/article/edp-energy-confirms-cyberattack-ragnar-locker-ransomware-blamed/ [Letöltve: 2023. 10. 30.]

Security (2023) Energy sector faces 39% of critical infrastructure attacks Security. https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure [Letöltve: 2023. 10. 12.]

Siemens (2018) Siemens SIPROTEC Denial-of-Service Vulnerability. https://www.cisa.gov/news-events/ics-advisories/icsa-15-202-01 [Letöltve: 2023. 10. 12.]

Slowik, J. (2019) CRASHOVERRIDE: Reassessing the 2016 Ukraine. Electric Power Event as a Protection-Focused Attack. Dragos Inc.

SolarWinds (2021) SolarWinds Security FAQ. https://www.solarwinds.com/sa-overview/securityadvisory/faq [Letöltve: 2023. 10. 30.]

Styczynski J., & Beach-Westmoreland, N. (2019) When the Lights Went Out. Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure. Booz Allen Hamilton Inc. https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf [Letöltve: 2023. 10. 12.]

Turton, W., Mehrotra, K. (2021) Hackers Breached Colonial Pipeline Using Compromised Password. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [Letöltve: 2023. 10. 30.]

Williams, B. (2017) Hackers' methods feel familiar in Ukraine power grid cyberattack. https://www.c4isrnet.com/home/2017/01/29/how-a-power-grid-got-hacked/ [Letöltve: 2023. 10. 12.]

Wright, R. (2022) Industroyer2: How Ukraine avoided another blackout attack. TechTarget. https://www.techtarget.com/searchsecurity/news/252523694/Industroyer2-How-Ukraine-avoided-another-blackout-attack [Letöltve: 2023. 10. 12.]

Xu, L., Guo, Q., Sheng, Y., Muyeen, S.M., & Sun, H. (2021) On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective. Renewable and Sustainable Energy Reviews, Vol. 152. ISSN 1364-0321, https://doi.org/10.1016/j.rser.2021.111642

Xu, L., & Guo, Q. (2023) Integrated Modelling, Analysis and Optimization for Cyber-Physical Power Systems Considering the Impacts of Communication Networks. Cigré Science & Engineering, Vol. 28. pp. 160–181. ISSN 2426-1335