NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 3. szám 40–57. • DOI: 10.32561/nsz.2019.3.4

Kralovánszky Kristóf[1]

A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész)

Cyber- and National Security Risks of the Electric Energy System (Part One)

A villamosenergia-rendszer helye a kritikus infrastruktúrák között nem minden esetben tükrözi azt a valós veszélyeztetettséget, amelyet más kritikusinfrastuktúra-ágazatok számára jelent. E tanulmány első része példákon keresztül mutatja be a villamosenergia-rendszer bizonyos kibersérülékenységeit,[2] az ezeket kihasználó támadások valós kockázatait és a támadást követő helyreállási képességének kiemelt fontosságát. Áttekinti a kibertámadásokkal szembeni védekezés erőforrásigényeit, annak állami és gazdasági szereplőit, illetve nemzetbiztonsági kapcsolatait.

Kulcsszavak: kiberbiztonság, villamosenergia-rendszer, kritikus infrasturktúra, helyreállási képesség

The placement of the electric energy subsector among critical infrastructures does not always reflect the real threat they pose to other sectors of critical infrastructures. With different examples, the first part of our study shows certain cyber-vulnerabilities of the electric energy system, the actual risks of attacks thereon and the real necessity of systems' resilience. The study investigates the organisational and theoretical resources required for the cyber defence of the electric energy sector, including its state-, commercial- and national security players.

Keywords: cybersecurity, electric energy system, power grid, critical infrastructure, resilience

[1] Kralovánszky Kristóf doktorandusz, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, ORCID: 0000-0002-5560-3525

[2] Kibersérülékenység az angol cyber vulnerability szakkifejezés tükörfordítása. A kibertér – mint tartomány – elemeinek (rendszereinek/eszközeinek) sérülékenységeit jelenti.

Bevezetés

A létfontosságú rendszerelemek[3] valódi súlyát, illetve fontosságát vizsgálni rendkívül nehéz feladat, mert a vizsgálat számos okból könnyen válhat szubjektívvé. A vizsgálat azonban nem állhat meg az adott rendszerelemnél, így vizsgálni kell annak más rendszerelemekkel való kapcsolatát, azoktól való függését, vagy azok kiszolgáltatottságát a tárgyi infrastruktúrának – vagyis az interdependenciákat. Ezt követően lehet csak megalapozott véleményt nyilvánítani.

Ezért is fontos, hogy kiemelt hangsúlyt kapjon az adott környezetben történő vizsgálat, és ne egy ágazat általános kitettsége, kockázata alapján, automatikusan történjen a minősítés vagy kategóriába sorolás. Ennek a megkülönböztetésnek igaznak kell lennie ágazaton belül is, de ágazatok között is – amely utóbbi sajnos sokszor nem valósul meg. A hatályos magyar jogi szabályozás szerint nemzeti létfontosságú rendszerelemet, európai létfontosságú rendszerelemet és alapvető szolgáltatást nyújtó szereplőket különböztetünk meg a kijelölt ágazatokban.[4]

Bármely ágazat függőségi viszonyait tekintjük, minden esetben szükség lesz energiára, ami vagy villamos energia, vagy valamilyen más energiahordozó, amely erőgépek hajtásához vagy villamosenergia-előállításhoz szükséges. Az erőgépek hajtásához szükséges hajtóanyag gyártási folyamata sem nélkülözi a villamos energiát – tehát kijelenthető, hogy a forrás, amelyre minden ágazatnak szüksége van: a villamos energia. Áttekintve az energiaszektoron kívüli, jogszabályban meghatározott ágazatokat,[5] a villamos energia mint legszükségesebb eredő megállapítható a közlekedés, az agrárgazdaság, az egészségügy, a társadalombiztosítás, a pénzügy, az infokommunikációs technológiák, a víz, a közbiztonság és védelem, valamint a honvédelem ágazataiban egyaránt.

A téma nagysága és nemzetközi kapcsolódásai miatt e tanulmányt két részben közöljük. Az első rész főként a villamosenergia-alágazat[6] (és ahhoz közvetlenül kapcsolódó) kiberbiztonsági kockázatok néhány aspektusát vizsgálja, míg a második rész ágazati és alágazati, regionális és szövetségi kapcsolatok által biztosított kibervédelem egy lehetséges mátrixát fogja áttekinteni.

---

3 Hatályos honi jogi szabályozás szerint (2012. évi CLXVI. törvény) a hivatalos megnevezés létfontosságú rendszerelem, amely nemzetközileg elfogadott elnevezés szerint: kritikus infrastruktúra. Írásunkban a két kifejezést egymás szinonimáiként használjuk.

4 Hatályos honi szabályozás szerint a következő ágazatokban értelmezhetők létfontosságú, nemzeti létfontosságú rendszerelemek, illetve alapvető szolgáltatásokat nyújtó szereplők: energia (kivéve atomenergiát termelő infrastruktúrák), közlekedés, agrárgazdaság, egészségügy (a gyógyszergyártás nem tartozik ide), társadalombiztosítás, pénzügy, infokommunikációs technológiák, víz, közbiztonság-védelem, honvédelem. 2012. évi CLXVI. törvény.

5 2012. évi CLXVI. törvény 1., 2., 3. mellékletében meghatározott magyarországi kritikusinfrastruktúra-ágazatok.

6 Jogszabályi megnevezéssel: villamosenergia-rendszer létesítményei alágazat. A továbbiakban a villamosenergia-rendszer alágazat fogalmán az előbbit értjük.

Villamosenergia-rendszer mint kritikus (információs) infrastruktúra-alágazat

A villamosenergia-ellátás részeit rendszerszemléletben vizsgálva meg kell állapítanunk, hogy nem lehet a különböző alrendszerei között súlyozni: ugyanolyan fontosságú a termelési oldal, a szállítási oldal és a megtermelt energia fogyasztók közti elosztásának, vagy régebbi terminológiával élve, a terhelés elosztásának képessége.[7] Az utóbbi kettőnek pedig elengedhetetlen alapjai az infokommunikációs rendszerek, hiszen csak így tud adatcsere történni a különböző alrendszerek között – akár regionális, akár nemzeti, akár nemzetközi viszonylatban.

Az előbbi felsorolás a villamosenergia-rendszert főként horizontális síkon rendszerezte, egy országos átviteli hálózat szemszögéből.[8] Ennek a síknak az összefüggései ugyanúgy léteznek vertikális síkon is: az országos, átviteli hálózat[9] és az elosztóhálózat tökéletesen egymásra utalt, hiszen az elosztóhálózaton jelenik meg a végfelhasználó. Mivel az elosztóhálózat tulajdonosa (és üzemeltetője) eltér az országos hálózat szereplőitől, kettejük között a zökkenőmentes infokommunikációs adatcsere ugyanannyira kritikus, mint az országos átviteli hálózat horizontális síkjában.

Furcsán hangzik, de a villamosenergia-alágazat (így a villamosenergia-rendszer létesítményei) is ugyanúgy igényli az elektromos áramot, hiszen alapfeladatként energia-előállítást, illetve energiahordozó szállítást/feldolgozást végez, de a vezérléshez nem direkt módon használja fel a termelt/szállított/feldolgozott energiát.[10]

A szállítási oldal külön érdekessége, hogy az átviteli hálózati nagyfeszültségű távvezetékoszlopok ma már nem csupán elektromos, hanem adatátviteli feladatokat is ellátnak, az oszlopok tetején futó földelőkábel közepén lévő optikai szálak segítségével.[11] Magyarországon ez adja az MVM Net Zrt. által üzemeltetett Nemzeti Távközlési Gerinchálózat optikai alaphálózatának meghatározó részét.[12] Így tehát egy önmagában kritikus infrastruktúra (távvezeték-hálózat) kritikus információs infrastruktúrává is válik, vagyis két külön okból is védelmet igényel.

---

7 Jelen tanulmány a terheléselosztás energetikai alrendszereit a szállítási oldalhoz sorolja. A szállítási oldal részeként tekinti mind az átviteli hálózatot, mind az elosztói hálózatot.

8 Magyarországon ez az átviteli engedélyes a Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR ZRt.).

9 Országos, átviteli hálózat feszültségszintjei 132, 220, 400 és 750 kV, az elosztóhálózati feszültségszintek pedig 10, 20, 35 és 132 kV. Az átviteli hálózat juttatja el a villamos energiát az elosztói hálózatokba.

10 Egy 750kV – 400kV transzformátor vezérlését és felügyeletét (részben) ugyanúgy egy 230V feszültségen üzemelő infokommunikációs eszköz látja el.

11 Angol elnevezéssel ezt a típusú kettőscélú vezetőt hívják Optical Ground Wire-nek, rövidítve: OPGW. E vezetékekben akár 400-at (!) is meghaladó optikai szál lehet, a jellemző mennyiség ma általában a 24/48/96 elemi szál.

12 Ez az optikai gerinchálózati hossz Magyarországon jelenleg 6000 km nagyságrendű, maximális adatátviteli képessége (számos technikai paraméter függvényében) a több száz gbit/s sebességet is elérheti: *MVM Net hálózati technológia.* Elérhető: www.mvmnet.hu/bemutatkozas/technologia/ (A letöltés dátuma: 2019. 05. 04.)

Szolgáltatói felelősség

Amíg egy szolgáltató a teljes hálózatát saját felügyelete és üzemeltetése alatt tudja tartani, a felelőssége tisztán értelmezhető és fenntartható. Abban az esetben, ha ezt a hálózatot rajta kívül álló személyek/szervezetek kétoldalú módon használják (vagyis nem csupán kivesznek belőle), abban az esetben is meg kell őrizni a szolgáltató eredő felelősségét, de ebben az esetben egészen új problémák jelenhetnek meg.

Az energiaszektorban és szűkebb értelemben a villamosenergia-alágazatban a termék, illetve a gyártmány a villamos energia maga, amely nem szükségszerűen csak nagy erőművekből származhat. Az elmúlt években jelentősen gyarapodott a házi, 0,4 kV-os hálózatban termelt villamos energia, amely jellemzően napelemek[13] segítségével jön létre. Az így termelt elektromos áram fel nem használt részét a végfelhasználó általában visszatáplálja a fogyasztói elosztóhálózatba. Példánkban olyan vegyes használatú végpontokról van szó, amelyek termelik is és fel is használják a villamos energiát, és a nem engedélyköteles és háztartási méretű kiserőművek közé tartoznak. 2018 végére a teljes magyarországi bruttó teljesítőképesség (8560 MW) 3,7%-át tudja adni (maximális kapacitásával) a nem engedélyköteles kiserőművek összessége (lásd az 1. táblázatot).[14]

1. táblázat

Nem engedélyköteles és háztartási méretű fotovoltaikus erőművek teljesítőképessége Magyarországon 2012–2018 között[15]

	2012	2013	2014	2015	2016	2017	2018
Teljesítőképesség (kW)	12 530	31 210	68 127	127 540	164 080	239 960	319 700
Kiserőműszám (db)	n/a	n/a	n/a	15 220	20 401	29 593	39 456
Termelés növekedése az előző évhez képest (%)	334,6	149,1	118,3	87,2	28,6	46,2	33,2

Forrás: Összefoglaló a nem engedélyköteles – ezen belül a háztartási méretű – kiserőművek adatairól (2008–2017) (2018)[16]; Jelentés a negyedévente újonnan belépő háztartási méretű kiserőművekről (2018 Q1-Q3) (2019)[17]

13 Pontos megnevezéssel: fotovoltaikus rendszer.

14 A valós nettó erőművi teljesítőképesség a 8560MW-nál kevesebb, vagyis a napenergia teljesítőképességi aránya ideális időben magasabb lehet.

15 A 2018-as adatok a forrásban 2018. III. negyedévéig állnak rendelkezésre. Az összehasonlíthatóság érdekében a 2018. IV. negyedéves adatokat az I. negyedévvel egyenlőnek tekintettük. Ezért a teljes 2018. évre vonatkozó adat csak becsült.

16 *Összefoglaló a nem engedélyköteles – ezen belül a háztartási méretű – kiserőművek adatairól (2008–2017)* (2018). Elérhető: www.mekh.hu/download/7/28/60000/nem_engedelykoteles_es_hmke_beszamolo_2008_2017.pdf (A letöltés dátuma: 2019. 04. 30.)

17 *Jelentés a negyedévente újonnan belépő háztartási méretű kiserőművekről (2018 Q1-Q3)* (2019). Elérhető: www.mekh.hu/download/2/23/90000/jelentes_a_negyedevente_ujonnan_belepo_haztartasi_meretu_kiseromuvekrol_2018q3.pdf (A letöltés dátuma: 2019. 04. 30.)

Egy sugaras hálózatban,[18] ahol az utolsó ágon van 50 fogyasztó, a fizikai törvényszerűségek miatt az utolsó fogyasztónál alacsonyabb lesz a feszültség, mint a vonal elején az első fogyasztónál (ezt hívjuk feszültségesésnek), tehát a szolgáltatónak úgy kell kalibrálnia a hálózatát, hogy az utolsó fogyasztónál is még a szabványos tűréshatáron belül legyen a feszültség. Amennyiben viszont az utolsó fogyasztók valamelyike saját maga termel villamos energiát, és azt a hálózatba visszatáplálja, akkor az utolsó fogyasztóknál akár jelentősen is növekedni fog a feszültség szintje, amely vélhetően még a szabványos keretek közt marad, de már el fog térni a szolgáltató által számított értéktől. Ugyanez igaz egy transzformátor csatlakozási pontjához közel eső fogyasztók viszonyára is. Ha a csatlakozási ponthoz közel eső fogyasztók valamelyike termel villamos energiát, nem biztos, hogy annak környékén még szabványon belül marad a feszültségszint (a megengedettnél magasabb lesz), ami a végfelhasználó elektromos árammal működő eszközeit (különösen az elektronikus eszközöket) károsíthatja.

A hálózaton biztosított energiaszabványoknak való megfelelősége jogi értelemben (is) a szolgáltatót fogja terhelni, így számára a felügyelet és vezérlés lehetősége nem kérdés, hanem szükségszerűség. Ahogy egyre több „termelő" jelenik meg a hálózatban, egyre inkább szükségessé válik az egymás közötti kommunikáció (termelő–termelő, termelő–szolgáltató), illetve a szolgáltató irányába történő információszolgáltatás, hiszen a szolgáltatónak a termeléshez kell igazítania saját üzemi paramétereit, és biztosítania kell, hogy az előbbi példában bemutatott folyamatos túlfeszültség ne jöhessen létre. Ez a kommunikáció két módon tud történni: szenzorok segítségével, amelyek a szolgáltatónak biztosítják a szükséges hálózati információt, és a „termelők" betáplálási pontjainak felügyeletével. Tovább bonyolítja a helyzetet, hogy a szolgáltatónak a termelő–termelő közötti kommunikációról is kell információval rendelkeznie, mert az ugyanúgy rendszertechnikai befolyással bírhat és potenciális kockázatot jelenthet – különösen, ha nem valós adatokat továbbítanak egymás között.

Mindezek elengedhetetlenül szükségesek (lesznek) ahhoz, hogy a villamosenergia-szolgáltató megfelelően felügyelhesse a kétirányúsított fogyasztói végpontokat, kis- és mikroszakaszokat, hogy szükség szerint beavatkozhasson és a termelőt korlátozhassa, vagy szélsőséges esetben kizárhassa a hálózatra való feltáplálásból.

Látható tehát, hogy villamosenergia-alágazat jelentősen támaszkodik az összekapcsolt infokommunikációs rendszerek részben vagy teljesen autonóm kapcsolattartására. Tartalmi értelemben ez az összekapcsoltság és az önálló, intelligens kommunikáció (és azt követő gépi döntéshozatal) egyben az Ipar 4.0[19] alapvető meghatározása is. Ahogy más ágazatokra is egyre jellemzőbb, az új technológiákat alkalmazó okoseszközök várhatóan mind inkább az Ipar 4.0 szerinti felépítéseket és adatcserét fogják használni, vagyis a termelés vezérlése, illetve a hálózat irányítása (annak minden szegmensében) általánosságban is ezek segítségével, egyre növekvő autonómiával fog történni.[20]

---

18 A sugaras hálózatok végén az utolsó fogyasztónál végződik az ellátókábel, ellentétben a hurkolt hálózatokkal, ahol az ellátókábel az összes fogyasztó érintése után visszatér a betáplálási pontba.

19 Az Ipar 4.0 (Industry 4.0) fogalom jelen értelmezésében a szakirodalomban általánosan elfogadott olyan új ipari forradalmat jelent, ahol az infokommunikációs technológiák a gyártási és automatizálási folyamatokkal egyre szorosabban fonódnak össze: Nagy 2017.

20 Kovács 2018.

A rendszerek és szenzorok közötti kommunikáció történhet IP[21]-alapú és nem IP-alapú kommunikáció segítségével. Nem szabad figyelmen kívül hagyni, hogy különösen jelentős növekedés előtt állnak a nem IP-alapú vezeték nélküli kommunikációt használó eszközök is, amelyek jellemzően Bluetooth- vagy NFC[22]-alapon működnek, és valamilyen érzékelőként alkalmazzák azokat. Jelenleg nem tudjuk, hogy 4-5 év távlatában (ami hozzávetőleg két technológialéptetési ciklust jelent) az IoT[23]-eszközök mennyire fogják a nem IP-alapú szenzorokat kiszorítani, illetve, hogy egymáshoz viszonyított arányuk hogyan alakul majd. Szintén nyitott kérdés, hogy az 5G-s mobil távközlés milyen ütemben fog lefedettségben terjedni nagyvárosi környezeten kívül,[24] és milyen hatással lesz az érzékelők és a rendszerek közötti kommunikáció megvalósítására (így az alkalmazott átviteli technológiára).[25] Itt (is) abban rejlik a veszély, hogy az eszközök hamisíthatók, és a kommunikáció is manipulálható.

Villamosenergia-szolgáltatóknál az érzékelők számának és a kommunikáció mértékének (jelentős) növekedése éppen a végfelhasználói hálózati szegmensben fog megszületni, ahol ez ma még csak kis mértékben létezik, de különösen a kertvárosi területeken lesz robbanásszerű. Az így létrejövő hálózati forgalom kezelése a szolgáltatóra fog hárulni, hiszen az ő érdeke (és feladata) a zökkenőmentes üzem biztosítása. A külön kihívást pedig az jelenti majd, hogy az ilyen mértékű infokommunikációs hálózatüzemeltetés jelenleg nem elvárás a fogyasztói elosztóhálózat tulajdonosaitól, ezért sem tapasztalatuk, sem erőforrásuk, sem rendszerszintű eszközparkjuk nincs hozzá. Természetesen opció lehet egy internetszolgáltatóval történő együttműködésük, ami azonban szükségszerűen a két hálózat (publikus internet- és villamosenergiaelosztás-vezérlés) legalább logikai szintű[26] elkülönítését igényli. Ez a szétválasztás megvalósulhat számos technológia alkalmazásával, de egy több ezer vagy több tízezer végpontot felügyelő rendszer esetében nagyon komoly plusz üzemeltetési kapacitást igényel mind anyagi, mind humánerőforrás-vonatkozásban.

Hálózatok szegmentálása

Biztonságtechnikai rendszerek IP-alapú átvitelre váltásakor jelent meg először a normál infokommunikációs és a biztonságtechnikai rendszerek elkülönítésének, a hálózatok szétválasztásának kérdése. Ebben az időszakban erre számos logikai lehetőség

21 IP – Internet protokoll.

22 Az NFC – Near Field Communication – képes elektronikai eszközök (megfelelő szabványok szerint) egymáshoz nagyon közeli helyzetben (2-3 cm) vagy egymáshoz érintve, egymással adatkommunikációt végezni.

23 IoT – (Internet of Things – dolgok internete).

24 Nagyvárosi környezeten kívülinek tekintjük az elővárosi és kertvárosi területeket, különösen akkor, ha nincsenek fő- és/vagy tömegközlekedési vonalak közvetlen szomszédságában.

25 Mindkét vonatkozásban rendkívül ambiciózus tervekkel rendelkeznek mind a gyártók, mind a szolgáltatók – de ezek hangsúlyosan csak tervek, amelyek megvalósításához szükséges anyagi erőforrások mértéke jelentősen alábecsült lehet. Véleményünk szerint a technológia a tervezett ütemnél lassabban fog terjedni, mivel a felhasználói céleszközök penetrációja várhatóan nem fogja elérni a szolgáltatók által becsült és rentábilis üzemhez megkívánt szintet – kivéve, ha a vezetékes hálózati szolgáltatások rendelkezésre állásának csökkentésével nem fogják a fogyasztókat átkényszeríteni az új (5G) adatátvitel használatára.

26 Biztonsági szempontból sokkal célszerűbb a fizikai szétválasztás, ami ritkán valósítható meg, de egy bizonyos vezérelt területméretet meghaladóan elengedhetetlen.

kínálkozott, például a különböző alhálózatok használata vagy a virtuális hálózati elkülönítés (VLAN[27]). E kettőnek a legnagyobb előnye a költséghatékonyság volt, vagyis nem kellett külön hálózatot üzemeltetni. Számos kritikus helyen azonban hamar felismerték az ebben rejlő óriási veszélyt, hiszen a hálózat kompromittálódása az irodai munka infokommunikációs kiszolgálás (e-mail, internetelérés) és a biztonságtechnika (kamerák képei, beléptetőrendszerek stb.) kiesését egyaránt jelenthette. Megoldásként létrehoztak tehát egy második fizikai hálózatot, amely dedikáltan csak a biztonságtechnikai rendszert szolgálta ki, az eredeti, első rendszer pedig megmaradt az irodai alkalmazások számára. Azokban a gyárakban, ahol a termelésirányítás jelentősen támaszkodott számítógépes vezérlésre, az (mint technológiai rendszer) megjelent egy újabb szegmensként, és ismét az eredeti probléma vetődött fel: „összerakható-e" a termelésirányítás és az irodai munka hálózati forgalma? Kritikusabb területeken (például vegyipar, gyógyszeripar, energia) hamar megszületett a döntés, hogy itt is szükséges a különválasztás. E három önálló rendszer utána kiegészülhetett még a különböző vezeték nélküli (wifi-) hálózatokkal,[28] jellemzően (és célszerűen) részben önálló VoIP[29] hang kommunikációs rendszerrel, illetve veszélyes ipari üzemek esetében elkülönült szenzorrendszerrel,[30] amelyek például az országos adatbázisokba szolgáltatnak információt a terület meghatározott paramétereiről (például veszélyes vegyi anyag jelenléte a levegőben).

Egy villamos nagyerőmű[31] vagy vegyipari üzem esetében tehát megjelenik legalább kettő, de ideális (és szakmailag elvárt) esetben öt vagy hat egymástól fizikailag is elkülönítetten működő IP-alapú hálózat saját kábelezésével, aktív eszközeivel és rendezőivel.[32]

Valós kockázatok

Ahogy a következő példák is bemutatják, a kritikus infrastruktúrák infokommunikációs rendszereinek célzott támadási kockázatát azok tulajdonosai/üzemeltetői sokszor jelentősen alábecsülik. Ennek egy része hiányos felkészültségként, míg egy másik része elhárítási képességek és erőforrások részleges hiányaként jelenik meg.[33] Tekintsünk át két esetet, amelyek egyértelműen alátámasztják, hogy létfontosságú

27 VLAN – (Virtual Local Area Network – virtuális helyi hálózat).

28 Nagyobb gyáraknál ilyenből legalább 2-3 szegmens üzemel (általános, vezetői, speciális).

29 VoIP – (Voice over IP – internet protokollon keresztüli hangátvitel).

30 Ilyen Magyarországon az Országos Katasztrófavédelmi Főigazgatóság MoLaRi (Monitoring és Lakossági Riasztó) rendszere, az alsó és felső küszöbértékű veszélyes vegyi ipari üzemek körzetében, országos kiterjedésű, magas rendelkezésre állású, redundánsan működő adatátviteli hálózatra épülő meteorológiai és vegyi monitoring, valamint lakossági riasztó feladatokat látja el. *MoLaRi-rendszer.* Elérhető: www.katasztrofavedelem.hu/index2.php?pageid=iparbiztonsag_molari (A letöltés dátuma: 2019. 04. 30.)

31 Magyarországon villamos nagyerőműnek tekintendő az 50 megawatt feletti teljesítményű villamos erőmű.

32 Hazánkban 10-es nagyságrendben vannak ilyen üzemek, amelyek között nem szerepel a Paksi Atomerőmű – ott lényegesen összetettebb és eltérő szabályok szerint működő rendszerekről van szó. A nagyságrend a szerző számítása, az ismert villamos erőművek, vegyipari és gyógyszeripari gyártók ismeretében.

33 Mindkét rész természetesen bontható még további fontos területekre.

rendszerek esetében, különösen a vegyiparban[34] és az energiaágazatban rendkívül valós és kiemelten kezelendő kockázatokról van szó.[35]

Norsk Hydro

Kritikus infrastruktúra lehet (ágazattól függetlenül, nemzetgazdasági és világgazdasági hatásai miatt)[36] egy olyan cégcsoport is, amely „csak" alumíniumgyártással és -feldolgozással foglalkozik, de a világ tizedik legnagyobb alumínium-előállítója. (Kínán kívül pedig az ötödik).[37] Ez a norvég Norsk Hydro[38] óriáscég, amely infokommunikációs rendszerét 2019. március 18-án, 23:00 óra után kibertámadás érte.[39] Ennek során (jelenlegi ismereteink szerint) a LockerGoga zsarolóvírus lekódolta a különböző hálózaton lévő számítógépek háttértárait, használhatatlanná téve azokat.[40] Mivel a szervezet több országban végez gyártási tevékenységet, és rendszereik egymással összekapcsoltak, ezért nem csak Norvégiában következett be üzemzavar, hanem a cég katari és brazíliai gyáregységeiben is.[41] Szerencsére az alumíniumolvasztókat és -kohókat át tudták állítani manuális üzemmódra, így ott nem történt komolyabb kár. A kész alumíniumot feldolgozó rendszerek nagyobb részét azonban le kellett állítani. Az elsődlegesen becsült kár 40 millió USD nagyságrendű volt, amely a hónapokig tartó teljes kárelhárítás[42] végére vélhetően jelentősen növekedni fog. A támadást követően az alumínium világpiaci ára 1,4%-kal növekedett. A támadást követő negyedik napon még mindig csak teljes gyártókapacitásának 50%-án működött a vállalat.[43] Ugyanez

[34] Magyarországon az „ipari veszélyes anyagok előállítása, tárolása és feldolgozása" alágazatot (a nagyobb vegyipari gyártók döntő többsége ide tartozik), illetve a gyógyszergyártás alágazatot a közigazgatási bürokráciacsökkentésről szóló 2015. évi CLXXXVI. törvény kivette a kritikusinfrastruktúra-alágazatok közül.

[35] Írásunknak nem célja az elkövetők azonosítása, vagy motivációjuk keresése.

[36] Magyarországon az ágazati besoroláson kívül a kritikus gyártókapacitások nem tartoznak a kritikus infrastruktúrák közé. Ezzel szemben az Amerikai Egyesült Államok besorolásában megtalálható a „kritikus gyártás" (critical manufacturing) mint ágazat. *Presidential Policy Directive – Critical Infrastructure Security and Resilience* 2013. Elérhető: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (A letöltés dátuma: 2019. 05. 04.)

[37] *The world's leading primary aluminum producing companies in 2017, based on production output (in million metric tons)* 2019. Elérhető: www.statista.com/statistics/280920/largest-aluminum-companies-worldwide/ (A letöltés dátuma: 2019. 05. 03.)

[38] A Norsk Hydro ASA vállalatcsoport 2017-es éves árbevétele meghaladta a 12,6 milliárd USD-t, alkalmazotti létszáma 35 ezer fő, a világ 40 országában van jelen. *Fontos tények.* Elérhető: www.hydro.com/hu-HU/a-hydro-bemutatasa/fontos-tenyek/ (A letöltés dátuma: 2019. 04. 30.)

[39] *Norway's Norsk Hydro hit by ransom cyber-attack* 2019. Elérhető: www.thelocal.no/20190322/norways-norsk-hydro-hit-by-ransom-cyber-attack (A letöltés dátuma: 2019. 04. 30.)

[40] Zsarolóvírusok esetében, amíg akár egy fertőzött gép is van az adott alhálózaton, az képes az összes többi, még nem fertőzött vagy már megtisztított gépet megfertőzni, ezért általában hálózati szegmensek vagy a teljes hálózat azonnali leállítása után kezdődhet meg a helyreállítás, lépésről lépésre. Ennek ütemében lehetséges a funkcionális visszaállás is. Mivel a szervezet informatikai szakemberei a visszaállással vannak elfoglalva, így ezen idő alatt az egyéb információtechnológiai üzemeltetés gyakorlatilag szünetelni fog, tovább nehezítve ezzel a rendszerek és így a teljes szervezet napi üzemmenetét.

[41] FOUCHE–SOLSVIK 2019.

[42] ADOMAITIS 2019.

[43] *Norsk Hydro Unit Begins Operating at 50% of Capacity After Cyber Attack* 2019. Elérhető: www.insurancejournal.com/news/international/2019/03/21/521324.htm (A letöltés dátuma: 2019. 04. 30.)

az érték a támadást követő hetedik napon 60% volt.[44] Vagyis egyhetes (vélhetően megfeszített) munka csak 10% javulást tudott eredményezni.

Ki kell emelni, hogy a támadás pár óra alatt le is zajlott, így a behatolást követően rendkívül kevés idő állt rendelkezésre a hatékony védekezésre. Más megközelítésben a gyár informatikai üzemeltetőinek vélhetően minimális esélye volt a rendszer kompromittálódását követő, (további) károkozást megállító beavatkozásra. A kohók manuális továbbműködtetése a belső kárenyhítés szempontjából volt fontos, hiszen így nem semmisültek meg a gyártóberendezések a visszaszilárduló fémtől, illetve a gyártás alatt lévő folyékony fém nem veszett kárba. Van azonban egy teljesen más aspektus is, ez pedig a villamosenergia-felhasználás. Ilyen méretű – különösen kohászati – gyárak villamosenergia-felhasználása tervezetten történik, vagyis az országos villamosenergia-teherelosztásban előre meghatározott kapacitások állnak számukra rendelkezésre (és kötelezően használandók fel), amelytől akár felfelé, akár lefelé történő jelentős eltérés komoly problémákat okozhat az országos rendszerben. Ez a típusú üzemzavar pedig kihatással lehet a rendszer más felhasználóira is, a hirtelen keletkező többletkapacitás megjelenése miatt.

Nagyon fontos kezelendő kockázat tehát egy gyártási folyamat technológiai leállása felügyeleti képességének megőrizhetősége, ami a fejlett országokban egyre kevésbé lesz műszaki kérdés, és egyre inkább lesz infokommunikációs probléma.

Tasnee

2017 második felében kibertámadás érte Szaúd-Arábia Tasnee[45] vállalatcsoportjának egyik petrolkémiai üzemét. A művelet részleteit először 2017 decemberében kezdték publikálni, amiből kiderült, hogy kifejezetten kritikus infrastruktúrák vészleállító rendszereit támadó kártevőről van szó, azon belül is a Schneider Electric Triconex Safety Instrumented System vezérlőiről, amelyek folyamatosan monitorozzák a felügyelt technológiai folyamat paramétereit, és eltérés esetén úgy avatkoznak be, hogy a normál működést megkísérlik visszaállítani, illetve ennek sikertelensége esetén leállítják a kritikussá vált folyamatot: egyfajta automatikus, de biztonságos vészleállítást hajtanak végre.[46] A kártevő – amit Tritonnak neveztek el – jelenléte véletlenül derült ki, ugyanis annak aktiválását követően nem történt meg a rendszer leállása, hanem a rendszer üzembiztos állapotba tért vissza.

Megállapítást nyert, hogy a kártevő kifejezetten fizikai károkozási céllal készült. Nyilvánvalóvá vált, hogy a készítői rendkívül komoly technológiai ismeretekkel rendelkeztek, ugyanis pontosan tudták a Triconex rendszer szoftveres működési paramétereit, amelyet egyébként a gyártó semmilyen módon nem publikált.[47]

---

44 *Norsk Hydro Returns Major Production Division to 60% of Capacity After Cyber Attack* 2019. Elérhető: www.insurancejournal.com/news/international/2019/03/26/521674.htm (A letöltés dátuma: 2019. 04. 30.)

45 A vállalat hivatalos neve: National Industrialization Company, de a „Tasnee" rövid nevet is használják. 2017-es árbevételük meghaladta a 2,7 milliárd USD-t. Fő tevékenységi területük a vegyipar és a petrolkémia.

46 Osborne 2017.

47 *Triton Malware Hits Critical Infrastructure in Saudi Arabia* 2017. Elérhető: https://resources.infosecinstitute.com/triton-malware-hits-critical-infrastructure-saudi-arabia/#gref (A letöltés dátuma: 2019. 04. 30.)

Érdemes egy lépéssel továbbgondolni a folyamatot. Ha az elkövető által készített kártevő képes beavatkozni a vészleállító rendszerbe, akkor egy valós vészhelyzet vagy technológiai hiba esetén képes a leállítórendszert vagy nyíltan akadályozni, vagy annak bemenő adatait manipulálni és már kritikus értékeket normál értékekre felülírni – mindezt úgy, hogy a felügyelet adott esetben észre sem veszi. E képesség birtokában pedig egy megfelelően létrehozott üzemzavar igen jelentős károkat képes okozni – nem csupán anyagi vonatkozásban, hanem egy petrolkémiai gyárban környezeti katasztrófa formájában is.

2019 áprilisában a Triton-csoport nyomai ismét megjelentek egy eddig még meg nem nevezett ország kritikus infrastruktúrájában.[48] Az anyagi haszonszerzés céljának hiánya, az elkövetés módja és a különösen óvatos előkészítés[49] mind arra utal, hogy a Triton-csoport mögött állami szereplő állhat.

Az iparban a kibertámadások egyik jelentősen alábecsült része a politikai konzekvencia. A Triton helyes működése esetén az adott gyár 2017-ben fizikailag is megsemmisült volna.[50] Szaúd-Arábia nyilván komoly ellenlépéseket tett volna, ami önmagában sem kis probléma.[51] Az Amerikai Egyesült Államok egyik legnagyobb szövetségeseként vélhetően az amerikai támogatás sem maradt volna el, ha a támadás és annak közvetett hatásai során amerikai érdekek is sérülnek.

A két példa nyomán érdemes elgondolkodni azon, hogy egy gyógyszeripari technológiába történő (a Tasnee-hoz hasonló) sikeres és így észrevétlen beavatkozás egy olyan piaci penetrációval rendelkező cég esetén, mint a Norsk, milyen következményekkel járhat.[52]

A védelem szükséges, de nem elégséges feltétele az ellenálló képesség

Nem minősítési célzattal, de meg kell állapítani, hogy sem a Norsk, sem a Tasnee ellenálló képessége nem volt megfelelő, hiszen ha az lett volna, az eseményből nem lett volna incidens.[53] Kritikus infrastruktúrák esetében a sebezhetőségek kivédése

48 Whittaker 2019.

49 A Tasnee esetében az előkészítés 2014-ben indult el. Miller et al. 2019. A vállalat nem először szenvedett el kibertámadást, 2017 januárjában számítógépeik egy részének merevlemezét törölték, és egy szír kisgyermek fényképét helyezték el rajtuk, aki Szíriából menekülve a török partoknál a tengerbe fulladt. Perlroth–Krauss, 2018.

50 Perlroth–Krauss, 2018.

51 Az ellenlépések megvalósulhatnak direkt vagy indirekt módon. Utóbbira jellemző példa lehet a vélt elkövető ellenségének kiemeltebb támogatása, például Szíriában az Amerikai Egyesült Államok még erősebb támogatása.

52 Amennyiben egy Norskhoz hasonló piaci penetrációval rendelkező gyógyszeralapanyag-gyártó termelési kapacitása olyan időtartamra és mértékben esik ki, mint a Norsk esetében az alumínium előállítása, akkor az jelentős ellátási zavarokat eredményezhet. Sokkal veszélyesebb a felvetés akkor, ha nem a gyártáskiesést tekintjük kockázatnak, hanem például a receptúra (ideiglenes) módosítását.

53 A magyar és az angol terminológia fordítva használja a két kifejezést, mert míg az angolban (és az idegennyelvű szakirodalomban) az esemény (event) az alsóbbrendű történés és a kezeletlen (nem kezelhető) esemény válik incidenssé (incident), addig magyar terminológiában az incidenst tekintik eseménynek. E tanulmány az angol jelentéstartalom szerinti szóhasználatot követi.

jelenti az első védelmi vonalat, hiszen, ha minden sebezhetőséget ki lehetne iktatni (klasszikus értelemben ezt nevezhetjük teljes ellenálló képességnek), akkor azzal megvalósulna a tökéletes biztonság. Ilyen azonban nem létezik, ezért fontos, hogy minél több sebezhetőség azonosítható legyen, amelyek kihasználási (bekövetkezési) kockázatának szakszerű elemzését követően lehet különböző védelmi terveket kialakítani.

Angol szakirodalomban egyre sűrűbben lehet találkozni a „resilience" szóval, ami magyarul rezilienciaként is használatos és sokszor tévesen rugalmas ellenállási képességnek fordítják.[54] Ez azért félrevezető, mert keveredik a rezisztencia és a reziliencia jelentése: az előbbi az ellenálló képességet írja le, az utóbbi, a „resilience" szó egy pluszdimenziót is jelent, a helyreállás képességét (és logikailag feltételezi, hogy az ellenállás részben vagy egészben sikertelen volt). A „rugalmas ellenállás" egy sajátos módon persze jelenthet az eredeti állapotba történő visszatérést, de nem hordozza magában a sérülés és a helyreállás tartalmat, inkább csak nagyfokú idomulási képességre igyekszik utalni. Írásunkban a reziliencia fogalmát a továbbiakban helyreállási képességként fogjuk használni.

Ahogy a Norsk Hydro példáján is láttuk, rendkívül komoly erőforrásokat igényel a bekövetkezett helyzet kezelése, a további károkozás megakadályozása, az érintett infokommunikációs rendszer teljes megtisztítása a kártevőtől, az indirekt károk felszámolása, a termelési képesség és teljesítmény eredeti állapotra történő visszaállítása és az egyéb járulékos veszteségek megfelelő rendezése.

Támadási kockázat számításánál szükségszerűen vizsgálni kell a védekezési képességet. Ha a támadás-védekezés kérdését szűkítjük a villamosenergia-hálózatra, és elfogadjuk, hogy e hálózat (annak teljességében) egy adott ország legkritikusabb infrastruktúrája, akkor vizsgálnunk kell azt is, hogy milyen képességeknek és erőknek kell rendelkezésre állniuk az alágazat védelméhez. Az üzemeltetés szereplői azonban jellemzően gazdasági társaságok, amelyeknek elsődleges feladata alaprendeltetésük és működésük fenntartása, vagyis villamos energia előállítása, továbbítása vagy átalakítása. Hírszerzési képességük (ami egy várható támadásról szolgálna adatokkal) kimerül a nyílt forrású hírszerzésben, elhárítási képességük pedig a normál üzletmenetben elvárható mértékig áll rendelkezésre. Komoly hálózati adatgyűjtési és elemzési lehetőségeik nincsenek, hiszen nem ez a feladatuk. Egy lehetséges támadás megelőzéséhez azonban pontosan ezekre a képességekre lenne szükségük, amelyben ezért állami szerepvállalásra van szükség.

Ha igaznak fogadjuk el, hogy a megelőzés a legtöbb esetben sokkal kisebb költséggel jár, mint a bekövetkezett kár elhárítása, akkor nem kíván további bizonyítást, hogy a helyreállási képesség arányosan rövidül (és lesz hatékonyabb) az ellenálló képesség növekedésével és erősségével. Számokra átfordítva elmondhatjuk, hogy amennyiben egy rendszer szakmai alapokon nyugvó, szakértő kockázatelemzést követő védelmi tervének megvalósítása 100 egységbe kerül, akkor a megfelelő védelem részleges hiányából származó kár egészen biztosan meg fogja haladni a 100 egységet. Ugyanígy igaz lesz, hogy a 100 egységes védelmi költségvetés takarékossági okokból történő csökkentése nem lineárisan fogja növelni a kockázat (várható kár) mértékét. Nyilvánvaló tény ugyanis, hogy 100 egységnyi érték védelmére nem fog

[54] *Reziliencia*. Elérhető: https://idegen-szavak.hu/keres/reziliencia (A letöltés dátuma: 2019. 04. 30.)

senki 100 egységnyi védelmet fordítani, hiszen akkor nincs értelme a védelemnek, mert a kárérték megegyezik a védelem költségével. Ezért (racionális körülmények között) a védelem jellemzően két nagyságrenddel alacsonyabb költséget jelent, mint a védendő érték.[55]

A helyreállás folyamatának és képességének egy igen fontos (szükséges, de nem elégséges) része a katasztrófahelyreállási terv,[56] ami része az üzletmenetfolytonossági tervnek.[57] Míg a DRP lényege, hogy egy bekövetkezett, minősített helyzetben[58] a pontos teendőket írja le a normál üzemi állapotra történő visszatéréshez, addig a tágabb BCP a normál üzemi állapot (és körülmények) folyamatos fenntarthatóságának szervezetre adaptált szabályrendszere. Mindezek azonban nem koncepcionális problémakezelést jelentenek, hanem az adott (gazdasági) szereplő saját működési képességének megőrzését, illetve eredeti állapotra történő visszaállását, vagyis az adott szervezet hozza létre saját magának, egy bekövetkezett esemény által elszenvedhető károk megakadályozására/minimalizálására és saját (gazdasági) képességeinek maximalizálására.[59] Nem foglalkozik azonban a rajta kívül álló másodlagos hatásokkal – vagyis a tőle függő, más infrasturktúrákban/rendszerekben keletkezett fennakadások/zavarok elhárításával, amelyeket maga a káresemény okozott.

Amikor nem csupán az adott társaság önnön érdekeit vizsgáljuk, hanem a teljes ellátási láncban betöltött szerepét, akkor lényegesen szélesebb szempontrendszer alapján kell eljárnunk, mert ilyen esetekben inkább foglalkoznunk kell az okozott külső hatásokkal, amelyek a társaság interdependencia-mátrixából vezethetők le. Nagyon gyorsan meg lehet találni az ágazatközi kapcsolatokat, és hamar kiderül, hogy az ágazati csoportosítás szükséges bár, de ugyanennyire szükséges a teljes nemzetgazdaság (államigazgatás) szempontjából is vizsgálódni, ahogy nem elhanyagolható a regionális szintű kapcsolatrendszer áttekintése sem. Utóbbi főként környezetvédelmi, illetve nem gazdasági területeken lehet kiemelkedően fontos, ahol a bekövetkezett esemény határoktól függetlenül fog kárt okozni.

A védekezés szükségszerű eszköze

Vitatható, hogy egy védelmi rendszer felügyelete igényel-e a humán erőforrást, vagy sem. A kérdés persze nem ennyire egyszerű, de a komplexitás és a védendő érték növekedésével mégis egyre inkább válhat indokolttá a szakértő felügyelet. A rendkívül összetett automatizált döntési algoritmusok a kialakuló helyzeteket nagyon magas arányban képesek sikeresen kezelni, de mindig lesznek olyan helyzetek, ahol

55 Az arányok természetesen rendkívül sok paramétertől függenek és ágazatról ágazatra változnak, de a védelmi költségnek (racionális keretek között) szinte soha nem szabadna meghaladnia a védendő érték 5%-át. Nagyon nehéz ugyanakkor szubjektív fogalmakat (például biztonságérzet) számszerűsíteni. Az 5%-os mérték a szerző saját kockázatbecslésein és kivitelezési tapasztalatain alapul.

56 Angol kifejezéssel: Disaster Recovery Plan (DRP).

57 Angol kifejezéssel: Business Continuity Plan (BCP).

58 Minősített helyzet – a normál üzemmenettől eltérő körülmények között történő munkavégzés/működés. Ilyen lehet például az infokommunikációs rendszer kibertámadás miatti részleges hozzáférhetetlensége.

59 Az ISO 27000 tanúsítási rendszer követelményeként fogalmazza meg a rendszert alkalmazótól a BCP meglétét és folyamatos felülvizsgálatát (ezzel szükség szerinti módosítását).

elengedhetetlen a szakmai tapasztalat a kialakult helyzet valóban helyes megítéléséhez. A Tasnee példáján is kiválóan látszik, hogy nem megengedhető kizárólag automatikára bízni technológiai irányítási folyamatokat, hiszen ha az automatika kompromittálódik, akkor az azt követő folyamatok – és így az automatizált döntések – már (részben) fertőzöttek lesznek.

A hálózatok szegmentálása részben láttuk, ahogy külön rendszereket képez a gyártási (alaptevékenységi) technológia, a biztonságtechnika és az infokommunikáció, úgy ezek felügyeletének is külön kell megvalósulnia. Kibervédelmi vonatkozásban ezt az elkülönült felügyeletet nevezzük biztonsági műveleti központnak, angol nevén Security Operations Centernek, rövidítve SOC-nak.[60]

Az elsődlegesen nem infokommunikációval foglalkozó vállalatok esetében, különösen Magyarországon, nagyon ritka, hogy saját SOC-vel rendelkezzenek. Aki rendelkezik ilyennel, ott pedig publikusan nem áll rendelkezésre információ annak működéséről. A feladat kiszervezhető ugyan külső szolgáltatóhoz, de beavatkozási hatékonyságában (kerülve az alul-, illetve a túlreagálást) a saját, szervezeten belüli megoldás – nagyobb vállaltok esetében – általában célravezetőbb, a napi szintű helyés rendszerismeret, de főként a nem infokommunikációs szakmai és technológiai tudás házon belüli rendelkezésre állása miatt.[61]

Az SOC mellett, amely monitorozást és irányítást végez, rendelkezni kell eseménykezelési képességgel is, amely az adott intézkedéseket fizikai szinten is képes végrehajtani. Vagyis az SOC mint aktív monitorozó (és adott esetben irányító, koordináló) ügyelet működik, az eseménykezelést pedig az erre dedikált számítógépvészhelyzetkezelő csapat (Computer Emergency Response Team, a továbbiakban: CERT) vagy számítógépbiztonságiincidens-kezelő csapat (Computer Security Incident Response Team, a továbbiakban: CSIRT) végzi.[62] A CERT vagy CSIRT működhet a SOC szervezetén belül vagy önálló szervezetként is. Léteznek törvény által meghatározottan működő CERT-k, amelyek egy ország szakmailag szétválasztott, de azon belül teljes kiber-incidenskezelését hivatottak végrehajtani. Magyarországon három ilyen szervezet van: a Nemzetbiztonsági Szakszolgálat által működtetett Eseménykezelő Központ (korábbi nevén Kormányzati Eseménykezelő Központ), a Katonai Nemzetbiztonsági Szolgálat keretein belül működő katonai eseménykezelő központ (MilCERT) és az Információs Hivatal által működtetett IntCERT.[63]

---

60 Hámornik 2018.

61 Magyarországon is több „magán" SOC/CERT/CSIRT működik, amelyek szolgáltatásait bármilyen gazdasági szereplő igénybe veheti. Magyar gazdasági társaság természetesen külföldi SOC/CERT/CSIRT-et is használhat. A házon belüli vagy kiszervezett SOC/CERT/CSIRT kérdésének eldöntése jóval összetettebb, amit e tanulmány második része részletesen vizsgál tovább.

62 A CERT és a CSIRT tartalmilag nagyjából megegyező fogalmak, így akár szinonimaként is használhatók. Megjegyzendő, hogy a CERT rövidítés intézmény nevében történő használata engedélyhez kötött, mivel az a Carnegie Mellon Egyetem bejegyzett védjegye 1997 óta. Az engedélyezéshez a szervezet megfelelőségét (is) kell igazolni.

63 2019. január 1-jével a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (BM OKF LRLIBEK) a klasszikus, nem kormányzati eseménykezelő feladatait átvette a régi nevén GovCERT-ként ismert, a Nemzetbiztonsági Szakszolgálat által működtetett Eseménykezelő Központ. (2018. évi CXXI. törvénnyel módosított 2013. évi L. törvény alapján). Ezeken kívül több önálló gazdasági társaság van Magyarországon, amelyek szolgáltatásként végeznek eseménykezelési tevékenységet.

Az SOC-k monitorozási tevékenysége nem csupán eseménykövetést jelent, hanem egyre inkább támaszkodik a fenyegetettségek, veszélyeztetettségek azonosítására (Threat Intelligence) – részben ez az, amivel proaktívvá tud válni. E feladatok miatt is elengedhetetlen a nemzetbiztonsági szervezetek aktív részvétele az SOC-k és CERT-k munkájában, illetve információval való ellátásában – akár áttételesen is.[64]

Képességalapú védekezés

Ahogy az infokommunikáció is egyre inkább szerteágazó, és különböző területei egyre mélyebb ismereteket igényelnek a hatékony védekezésben, az SOC-k hatékony működéséhez is mind inkább külön szakembereket fognak igényelni a különböző területek. Látható, hogy a szenzor- és adatátviteli hálózatok mindenhol megjelennek, és egyre nagyobb teret követelnek maguknak már most is, mind vezetékes, mind vezeték nélküli technológiákkal. Hangsúlyozni kell, hogy a főbb adatátviteli gerinchálózatok továbbra is vezetékesek, ám technológiájukat tekintve nem réz-, hanem egyre inkább optikai alapúak. Nem szabad figyelmen kívül hagyni, hogy a kommunikációs csatorna zavarásával adott esetben legalább ugyanakkora kárt lehet okozni, mint az átviteli csatornában az adatok módosításával. Ugyanakkor igaz az is, hogy az átvitt adatok megismerése és fedett módon történő manipulálása hosszabb távon több nagyságrenddel nagyobb kárt tud okozni, mint a zavarási tevékenység – de ezek egymástól jelentősen eltérő területek, és nagyon különböző eszközöket, illetve szaktudást igényelnek. E tevékenységek – amelyek katonai változatát elektronikai hadviselésnek nevezzük – olyan ismereteket és tapasztalatot követelnek, amelyek egy „hagyományos" biztonságtechnikával foglalkozó vagy egy infokommunikációs szakembernek nem állnak rendelkezésére.[65] A támadói oldalon ezek a képességek alkalmazás szinten is megjelennek, tehát nem lehet kérdés a megfelelő védekezéshez való rendelkezésre állásuk sem.

A támadások legnagyobb részénél a támadó pontos személye vagy a támadócsoport pontos személyi összetétele nem állapítható meg. Ugyanígy, gyakorlatilag lehetetlen direkt bizonyítékot szerezni, hogy az elkövető állami szereplő volt-e, vagy hogy a végrehajtók egy állami szereplő megbízásából hajtották-e végre a cselekményt. Vannak azonban olyan jelek, amelyekből az állami szereplő jelenlétére nagyon nagy bizonyossággal lehet következtetni. Ilyenek lehetnek a következők:[66]

1. nem profitszerzési céllal végzik a műveletet, függetlenül attól, hogy a kivitelezéshez jelentős anyagi erőforrásokra volt szükség;
2. a felhasznált programok, eszközök egyedileg a konkrét támadáshoz készültek, máshol még soha nem használták;
3. rendkívül hosszú (akár többéves) előkészítés előzte meg a műveletet;
4. titkosszolgálati jellegű eszközöket is felhasználtak az előkészítés során.[67]

64 Mindezek részletes kifejtését e tanulmány második része tartalmazza.
65 Haig et al. 2014.
66 Több paraméternek kell egyidejűleg teljesülnie.
67 A szerző saját kutatási eredménye, számos különböző forrás szintézise és kiegészítése alapján.

Ha a fent említett „nagy bizonyosság" rendelkezésre áll, még mindig komoly problémát jelenthet, hogy az azt megalapozó információk nyílt vagy titkos forrásból származnak-e. Amennyiben inkább az utóbbi igaz, nagyságrendileg nehezebbé válhat a válaszlépések hiteles elfogadtatása a közvéleménnyel – hiszen nem megfelelően áll rendelkezésre bemutatható direkt bizonyíték.

Tisztán látszik azonban, hogy olyan képességekről van szó, amelyek semmilyen formában nem nélkülözhetik az állami szerepvállalást a védelemben, amibe ugyanúgy beleértendők egy ország polgári titkosszolgálatai, mint a különböző kiberképességekkel[68] rendelkező katonai szervezetei, akik az elektronikai hadviselés legmagasabb szintű képviselői.

Kritikus infrastruktúrák támadása ugyanis már nem elsősorban gazdasági céllal történik, hanem jól látható/érezhető problémát[69] vagy fennakadást kíván okozni. Ezzel egyben félelmet is kelt, hiszen sikeres támadás esetén a társadalom egy részének valamilyen alapellátását akadályozza. Képes ugyanakkor instabilitást is kelteni, ha az adott ország látványosan nem tudja a támadást kezelni, vagy bármilyen okból azt nem (vagy nem megfelelően) előzte meg. Eredményeiben tehát a terrorizmussal sok párhuzamot mutat, de eszközrendszerében gyökeresen eltérő és a terrorizmus kezeléséhez képest nagyságrendekkel komolyabb és jelentősen differenciáltabb szaktudást és rendkívüli tapasztalatot igényel – a megelőzésében is. Így válik kiemelten kezelendő nemzetbiztonsági feladattá is, amely megoldására a modern, információs társadalomnak (mint környezetnek és társadalmi berendezkedésnek) válaszokat kell tudnia adni. E válaszok a szakértő nemzeti és nemzetközi intézmények és intézményrendszerek kialakításával, üzemeltetésével és azok egymás közötti hatékony információcseréjével jönnek létre. A megfelelő reagálóképesség pedig nem opcionális, hanem létkérdés.

A tanulmány második része fog a lehetséges szervezeti felépítésekkel foglalkozni, milyen struktúra képes hatékony válaszokat adni a különböző komplex kihívásokra, illetve hogyan lehetséges vállalati, országos és nemzetközi szinten is hatékony feladatellátásra képes rendszert létrehozni.

Összefoglalás, következtetések

A kritikus infrastruktúrák védelme az államtól elvárt társadalmi igény. Ehhez az állam szabályzókat hozhat létre, amelyeken keresztül a kritikus infrastruktúrák üzemeltetőit egyfajta szabványosított védelemre kötelezi – helyesen. A szabályzók dogmatizálódása azonban legalább akkora probléma egy rendkívül dinamikusan változó környezetben, mint a szabályzók hiánya. Nem védekezhet tehát az állam azzal, hogy a szabályzói rendszere létezik és a szolgáltatói oldal nem tartja be, ha e rendszer fölött jelentősen elhaladt az idő, és a rendelkezésre álló technológiák már adott esetben egy gyökeresen más szabályozást igényelnének. A jövőbe tekintve ugyanígy elmondható, hogy szintén nem lehet felmentés egy kifutóban lévő technológiához igazítani a szabályozást, ha már látható az újabb technológia megjelenése. Nagy kihívás ugyanakkor

[68] Kiberképességen a kibertérben végzett aktív és passzív műveleteket és tevékenységeket értjük.
[69] Amely probléma lehet politikai, társadalmi, gazdasági, vagy a három kombinációja.

olyan jogszabályi környezetet létrehozni, amely legalább részben képes a technológiai változások követésére. Ennek egyik lehetséges módja, hogy logikai folyamatokat igyekszik lekezelni, amit egy rugalmas intézményrendszeren keresztül hajt végre. Vagyis törvényi szinten nem mikromenedzsment, hanem koncepcionális gondolatiság jelenik meg, amire építve az alsóbb, minisztériumi szintek rendelik hozzá a szükség szerint változó technikai tartalmat.

Ugyanakkor, megfelelően életképes és üzemképes szabályozást létrehozni egy jelentősen differenciált technológiai környezetben sokkal nagyobb kihívás lehet, mint egy piaci szereplőnek önmaga számára biztonságosan üzemeltetni az adott rendszert. A komplex és valós védelem azonban nem nélkülözheti – sőt alapként épít – a stabil és szakmailag megfelelő szabályzókra, amelyek egyben a szükséges interdependenciák működését is támogatják. Ezzel pedig visszakanyarodtunk az államtól elvárt igényhez, hiszen az államnak erősebb érdeke fűződik az egymáshoz kapcsolt rendszerek megfelelőségéhez, mint azok üzemeltetőinek – az előbbi esetben egy szűkebb gazdasági érdekről, míg utóbbiban egy tágabb, társadalmi, nemzetgazdasági, nemzetbiztonsági érdekről van szó.

A szabályozási rész nyilvánvalóan államigazgatási feladat, amely szakági egyeztetéseken és tárcaközi folyamatokon alapul, de országos szinten politikai szükségszerűségként is megjelenik, rendkívül magas destabilizálási képessége miatt: amikor ugyanis egy nagyobb regionális vagy egy országos kritikus infrastruktúra-rendszer[70] a társadalom által még tolerálható szint alatt teljesít, az elégedetlenség nem kívánt eseményekké válhat, tovább növelve az állam számára a megoldandó feladatok számát.

Hangsúlyozni kell az egyensúly fontosságát is az állam és a piaci szereplők között, így egyik sem várakozhat a másikra. Összességében nem lehet egy alá-fölérendeltségi rendszerről beszélni, mert akkor nem partneri kapcsolatról van szó. Csak partnerségen keresztül tud megvalósulni a különböző szerepek megfelelő elismertsége is – az állam soha nem fog rendelkezni saját piaci tapasztalatokkal, és a piaci szereplők sem fognak saját államigazgatási háttérrel rendelkezni. Ezeket azonban egymással meg kell és meg tudják osztani, vagyis egymásra vannak utalva, amit a szó legpozitívabb értelmében kell kezelni mindkét oldalon, mert így tud megvalósulni a valódi védelmük, aminek üzembiztos eredménye össztársadalmi érdek.

Különösen igazak a fentiek egy ország legkritikusabb infrastruktúra-rendszerére, a villamosenergia-alágazatra és közvetlenül kapcsolódó alrendszereire. Ezen belül egy adott gazdasági szervezetnek meg kell hagyni a szabadságát, hogy alapfeladatát tudja végezni, de biztosítani kell számára minden körülményt, hogy ezt az alapfeladatot maradéktalanul el tudja látni (amit meg is kell követelni). Amennyiben valamelyik feltétel nem teljesül, garantáltan csorbulni fognak a képességek. Ennek pedig egyenes következménye az adott ország teljes kritikusi infrastruktúra-rendszere[71] sérülési lehetőségének (vagy támadásokkal szembeni kitettségének) növekedése.

[70] Ilyen regionális vagy országos kritikusinfrastruktúra-rendszer lehet a villamosenergia-rendszer távvezeték-hálózata, országos vezetékes hírközlő gerinchálózat, regionális ivóvízvezeték-hálózat.

[71] Vagyis az ország kritikus infrastuktúrái összességének.

Felhasznált irodalom

HÁMORNIK Balázs Péter (2018): A Security Operations Center (SOC): a kiberbiztonsági csapatmunka és kihívásai. *Hadmérnök*, 13. évf. 2. sz. 393–408.
KOVÁCS László (2018): *A kibertér védelme*. Budapest, Dialóg Campus Kiadó.
HAIG Zsolt – KOVÁCS László – VÁNYA László – VASS Sándor (2014): *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem.

Jogi források

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
2015. évi CLXXXVI. törvény a közigazgatási bürokráciacsökkentéssel összefüggő törvénymódosításokról

Internetes források

ADOMAITIS, Nerijus (2019): *Norsk Hydro's initial loss from cyber attack may exceed $40 million.* Elérhető: https://uk.reuters.com/article/us-norway-cyber/norsk-hydros-initial-loss-from-cyber-attack-may-exceed-40-million-idUKKCN1R71X9 (A letöltés dátuma: 2019. 04. 30.)
Fontos tények. Hydro. Elérhető: www.hydro.com/hu-HU/a-hydro-bemutatasa/fontos-tenyek/ (A letöltés dátuma: 2019. 04. 30.)
FOUCHE, Gwladys – SOLSVIK, Terje (2019): *Aluminium producer Hydro hit by cyber attack, shuts some plants.* Elérhető: www.itnews.com.au/news/aluminium-producer-hydro-hit-by-cyber-attack-shuts-some-plants-522286 (A letöltés dátuma: 2019. 04. 30.)
Jelentés a negyedévente újonnan belépő háztartási méretű kiserőművekről (2018 Q1-Q3) (2019). Magyar Energetikai és Közmű-Szabályozási Hivatal. Elérhető: www.mekh.hu/download/2/23/90000/jelentes_a_negyedevente_ujonnan_belepo_haztartasi_meretu_kiseromuvekrol_2018q3.pdf (A letöltés dátuma: 2019. 04. 30.)
MILLER, Steve – BRUBAKER, Nathan – KAPELLMANN ZAFRA, Daniel – CABAN, Dan (2019): *TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping.* Elérhető: www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html (A letöltés dátuma: 2019. 04. 30.)
MoLaRi-rendszer. Belügyminisztérium – Országos Katasztrófavédelmi Főigazgatóság. Elérhető: www.katasztrofavedelem.hu/index2.php?pageid=iparbiztonsag_molari (A letöltés dátuma: 2019. 04. 30.)
MVM Net hálózati technológia. Elérhető: www.mvmnet.hu/bemutatkozas/technologia/ (A letöltés dátuma: 2019. 05. 04.)
NAGY Judit (2017): *Az ipar 4.0 fogalma, összetevői és hatása az értéklánc*ra. Budapesti Corvinus Egyetem. Elérhető: http://unipub.lib.uni-corvinus.hu/3115/ (A letöltés dátuma: 2019. 04. 30.)

Norsk Hydro Returns Major Production Division to 60% of Capacity After Cyber Attack. Elérhető: www.insurancejournal.com/news/international/2019/03/26/521674.htm (A letöltés dátuma: 2019. 04. 30.)

Norsk Hydro Unit Begins Operating at 50% of Capacity After Cyber Attack (2019). Elérhető: www.insurancejournal.com/news/international/2019/03/21/521324.htm (A letöltés dátuma: 2019. 04. 30.)

Norway's Norsk Hydro hit by ransom cyber-attack (2019). Elérhető: www.thelocal.no/20190322/norways-norsk-hydro-hit-by-ransom-cyber-attack (A letöltés dátuma: 2019. 04. 30.)

OSBORNE, Charlie (2017): *Hackers use Triton malware to shut down plant, industrial systems.* Elérhető: www.zdnet.com/article/hackers-use-triton-malware-to-shut-down-plant-industrial-systems/ (A letöltés dátuma: 2019. 04. 30.)

Összefoglaló a nem engedélyköteles – ezen belül a háztartási méretű – kiserőművek adatairól (2008–2017) (2018). Magyar Energetikai és Közmű-Szabályozási Hivatal. Elérhető: www.mekh.hu/download/7/28/60000/nem_engedelykoteles_es_hmke_beszamolo_2008_2017.pdf (A letöltés dátuma: 2019. 04. 30.)

PERLROTH, Nicole – KRAUSS, Clifford (2018): *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.* Elérhető: www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html (A letöltés dátuma: 2019. 04. 30.)

Presidential Policy Directive – Critical Infrastructure Security and Resilience (2013). Elérhető: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (A letöltés dátuma: 2019. 05. 04.)

Reziliencia. Elérhető: https://idegen-szavak.hu/keres/reziliencia (A letöltés dátuma: 2019. 04. 30.)

Triton Malware Hits Critical Infrastructure in Saudi Arabia. Elérhető: https://resources.infosecinstitute.com/triton-malware-hits-critical-infrastructure-saudi-arabia/#gref (A letöltés dátuma: 2019. 04. 30.)

WHITTAKER, Zack (2019): *The hacker group behind the Triton malware strikes again.* Elérhető: https://techcrunch.com/2019/04/09/triton-malware-strike/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cud2lyZWQuY28udWsvYXJ0aWNsZS93aXJlZC1hd2FrZS0xMDA0MTk&guce_referrer_cs=qQIvtyPC6YLec-Y73T1siQ (A letöltés dátuma: 2019. 04. 30.)

The world's leading primary aluminum producing companies in 2017, based on production output (in million metric tons) (2018). Elérhető: www.statista.com/statistics/280920/largest-aluminum-companies-worldwide/ (A letöltés dátuma: 2019. 05. 03.)