STATUS OF CYBER PROTECTION REGULATION OF THE HUNGARIAN ELECTRICITY SYSTEM

A MAGYAR VILLAMOSENERGIA RENDSZER KIBERVÉDELMI SZABÁLYOZÁS HELYZETE

DÉR Attila[1]

Abstract

Critical infrastructures are the focus of attention around the world. Not without reason, as they play a key role in every aspect of life in every country, including our own. In Hungary, there are several of them, such as the health care system, transport and transportation, energy supply systems, etc. In this study, the focus will be on the electricity system within the energy supply systems. Unfortunately, based on the experience of the last years, the number of cyber attacks has increased sharply, especially in the energy sector. The spread of digitalisation throughout the management and control systems of electricity supply plays a major role in this. As a consequence, it is important to have an appropriate domestic legislative framework to ensure cyber security. This article makes proposals for this existing legislative framework to reduce the vulnerability of the Hungarian electricity system in a strategic and legislative context. Possible adaptation of the Swiss model in Hungary through EU-level directives Advantages, disadvantages, taking into account the specificities of the electricity supply system.

Keywords

Cybersecurity, electricity supply, critical infrastructure, digitalisation

Absztrakt

A kritikus infrastruktúrákat az egész világon kiemelt figyelem övezi. Nem véletlenül, hiszen minden országban és természetesen hazánkban is kulcsfontosságú szerepet töltenek be az élet minden területén. Magyarországon több ilyen is van, mint például az egészségügyi rendszer, közlekedés és szállítás, energiaellátó rendszerek stb. Ebben a tanulmányban az energiaellátó rendszereken belül a villamosenergia rendszere lesz fokuszálva. Sajnos az utóbbi évek tapasztalataiból kiindulva a kibertámadások száma erőteljesen megnőtt, különösen az energiaszektorban. Nagy szerepet játszik ebben a digitalizáció elterjedése a villamosenergia ellátás teljes irányítási és szabályozási rendszereiben. Ennek következtében fontos, hogy megfelelő hazai jogszabályi keret legyen a kiberbiztonság megteremtéséhez. A cikk erre a meglévő jogszabályi környezetre tesz Javaslatokat a magyar villamos-energiaellátó rendszer sérülékenységének csökkentésére stratégiai és jogszabályi összefüggésében. Európai Uniós szintű irányelveken keresztül a svájci modellnek a lehetséges adaptációja Magyarországon Előnyök, hátrányok, villamos-energiaellátó rendszer sajátosságainak figyelembe vételével.

Kulcsszavak

Kiberbiztonság, villamosenergia-ellátás, kritikus infrastruktúra, digitalizáció

[1] der.attila@uni-obuda.hu | ORCID: 0009-0008-9547-102X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

DOI: https://doi.org/10.12700/btsz.2024.6.4.73

BEVEZETÉS

A villamosenergia-rendszer fő célja a villamosenergia-termelése, -átvitele és –szállítása az erőművektől a végfelhasználókig, amelyek közé tartoznak a háztartások, a kereskedelmi épületek és az ipar. Az átviteli és az elosztó hálózati rendszerek feszültségszinteknek megfelelően lettek besorolva. Közvetlenül az erőműből természetesen a legnagyobb feszültségű vezetékek szállítják az elektromos áramot. A nagyfeszültségű vezetékek Magyarországon 750kV-, 400kV és 220kV értékek között szállítják a villamos-energiát alap átviteli hálózatként. Ennek a gerinc hálózatnak a feszültségszint határa letranszformálva 120kV feszültségszint, ahol már az elosztó hálózat kezdődik. Az elosztó hálózatot üzemeltetők tovább csökkenti a 120kV feszültségszintet ipari fogyasztók számára szükséges különféle 35kV-, 20kV és 10kV középfeszültségű szintekre. A lakossági fogyasztóknál, pedig a 0,4kV kisfeszültségű hálózatot, mint a legkisebb tovább nem transzformált feszültség értéket figyelhetjük meg.[1] [2]

Magyarországon az erőművek feladatuk szerint lehetnek közcélúak, ahol egy ország ipari vagy kommunális fogyasztóinak ellátása a cél vagy nem közcélúak, ahol pedig csak egyes speciális üzemeknek az energiaellátása a feladat. Továbbá lehet a magyar villamosenergia-rendszerrel együttműködő, ahol a teherelosztást a diszpécserközpont végzi vagy nem együttműködő csak egy létesítményt szolgál ki. Kihasználtság szempontjából három csoportot különböztetünk meg az egyik az alap erőművek, ilyen például a paksi. A másik a villamosenergia igény változásai szerint működő menetrendtartó erőművek, mint a Mátrai és a Dunamenti. A harmadik típusúak pedig a csúcserőművek, amelyek nyilván a nevükből is kikövetkeztethetőek, hogy csak maximális energiafogyasztásnál termelnek. Későbbi leírásnál fontos lehet még, hogy mely szervezetek irányítják a magyar villamosenergia-rendszert, amely több szintet különböztet meg egymástól. Az egyik ilyen szervezet a Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR Zrt), amely országos szinten felel az ellátásbiztonságért. Továbbá gondoskodik fogyasztás pillanatnyi egyensúlyának fenntartásáért, ellenőrzi a hálózat túlterheltségét, illetve megfelelő feszültségszintjét. A területi áramszolgáltatóknál a Körzeti Diszpécseri Szolgálatok végzik az üzemirányítást, ahol a 120 kV-os és alacsonyabb feszültségszintű elosztóhálózatok helyezkednek el. Végül a legalsóbb feszültségszintű elosztóhálózatokat Üzemirányító Központok működtetik, felügyelik és karbantartják. A magyar energiaszektor piacának és ellátásbiztonságának szabályozásáért felelős hatóság a Magyar Energetikai és Közmű-szabályozási Hivatal. Kiberbiztonság területén fontos elemként létrehozta az információmegosztó és elemző központot, amely az érintett energiaellátó szervezetek közötti fenyegetésfelderítési adatfolyam megosztásában, elemzésében és a korai felderítésben kulcsfontosságú szerepet tölt be.[3]

SZABÁLYOZÁS

Európai Uniós szabályozás

Az Európai Unió magasabb szinten csak a 2000. évektől kezdte el komolyabban vizsgálni a tagállamok infrastruktúráinak védelmi helyzetét. Ehhez nagymértékben hozzájárult több terrortámadás, amely főként kritikus infrastruktúrák ellen irányult globális és európai szinten. Az első ilyen kezdeményezés a kritikus infrastruktúrák védelméről szóló európai programcsomag (European Programme for Critical Infrastructure Protection) volt.

Majd ebből lett egy irányelv, amelynek a frissítése 2008.-ban 114/2008/EK irányelvként volt ismeretes, amelyben már olyan fontosabb pontokat is megemlítenek, mint az energia és közlekedés ágazatok prioritásként történő kezelése; sebezhetőségi pontok meghatározásának kötelezettsége; azonosítás és kijelölés folyamatának meghatározása stb.[14]

Az Európai Parlament és Tanács kritikus szervezetek ellenállóképességéről szóló Irányelve (CER) a statikus fizikai rendszerszemléletről a rezilienciára, ellenállóképességre tolja el a szabályozás irányát, amely a rendszer minél kisebb megszakítását vagy a már megtörtént incidensek mielőbbi visszaállítását célozza meg. Ebben az ajánlásban a kritikus infrastruktúráknak is bővült a körük, így nem csak az energia és a közlekedésre koncentrál, mint az előző szabályozások, hanem a többi kulcsfontosságú nemzetgazdasági ágazatra is.[15]

A Hálózati és Információs Rendszerek (Network and Information System) röviden: NIS, amely 2016/1148 irányelvként lett kiadva már részletesen lefekteti a kiberbiztonsági alapokat az egész Unió területén. Különösebben nem foglalkoznék ezzel a NIS-el inkább az újabb verziójával a NIS2 2022/2555 irányelvre térnék ki, amely például az előbb említett CER direktívával kézen fogva szabályozza a kritikus infrastruktúrákat, úgy hogy az egyik szabályozás ne üsse a másikat. A NIS2 kiberbiztonsági kockázatok nem jelennek meg a CER-ben, de amiket nem fektetett le a NIS2 azokat a rizikófaktorokat viszont tartalmazza a CER.[13]

ENISA (European Network and Information Security Agency), amely az Unió egyik legfontosabb kiberbiztonsági szervezete. Tanácsadó szervezetként különféle ajánlásokkal, dokumentumokkal segíti a tagállamokat stratégiáik kialakításában. Bizonyos kritikus infrastruktúráknál a bejelentési kötelezettséget ír elő, ha valamilyen váratlan incidens éri a kiemel rendszerelemet. Az Európai tagállamok, mint Magyarország is nagyon közel van a NIS2 irányelv bevezetéséhez, amely 2024.10.18.-tól már hatályba fog lépni.

Külön a pénzügyi szektorra is készült rendelet, amely a bankok informatikai biztonsági előírásait szigorítja a digitális működési ellenálló képességről szóló rendelet (Digital Operational Resilience Act, DORA)

Magyar szabályozás

2007. évi LXXXVI. törvény a villamos energiáról ennek a törvénynek a legfőbb csapásvonala a biztonságos villamosenergia versenypiac kialakítása.[16]

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyarországon ez az első törvénybe iktatott szabályozás, ahol konkrétan a kritikus infrastruktúrákról szól, habár nem ezzel az elnevezéssel szerepel a törvényben. Nyílván a legfontosabb célja a törvénynek, hogy kijelölje nemzeti létfontosságú rendszerelemeket, ahol az üzemeltetői azonosítás vizsgálat elkészítését követően az ágazati kijelölő szakhatóság dönt, hogy ki tartozik ezen törvény hatálya alá. A törvény megemlíti a hatóság és a már besorolt létesítmények közötti kapcsolat biztosítására szolgáló összekötő személy kötelező kijelölését és feladatát. Továbbá a hivatásos katasztrófavédelmi szervet kijelöli, hogy hatósági eljárásokban hivatalosan járjon el. A jogszabály meghatározza, hogy mely rendszerelemek kapcsolódhatnak az Európai Unió rendszereihez és létesítményeihez. Végül az 1. számú mellékletében 10 darab ágazatot sorol fel, ahol az energia ágazatnál említi meg a villamosenergia rendszer létesítményeit kivétel Paks nukleáris biztonságának kérdéskörét.[17]

Az előző törvény tartalmának konkrét gyakorlati megvalósítását a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló rendelet részletesen tárgyalja. Megtalálhatjuk például az 1. mellékletében a horizontális elvárásokat vagy a 2. mellékletében az üzemeltetői biztonsági terv részletes tartalmi követelményeit.[20]

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról a magyar kiberbiztonság általánosságban megfogalmazott alapjait célját és feladatait fekteti le. Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat a NIS ezt egészítette ki, de villamosenergia szektor problematikájával nem foglakozik.[18]

Magyarországon a 2013. évi információbiztosági törvény(Ibtv) fektette le elsőként két legfontosabb információs rendszerek biztonsági felügyeltét megszervező intézményt. Az egyik a Nemzetbiztonsági Szakszolgálat a civil platformot képviseli, itt is főként az államigazgatási szerveket. A másik a Katonai Nemzetbiztonsági Szolgálat, amely a katonasággal kapcsolatos biztonsági eseményeket kezeli. Ezen eseményközpontok feladatait eljárásaikra vonatkozó általános rendelkezéseit a „187/2015. (VII. 13.) Korm. rendelet részletezi az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelőfeladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról".[19][21]

„271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól biztonsági események bejelentéséről szól." [22] A kritikus infrastruktúrák sérülékenységvizsgálatát a polgári nemzetbiztonsági szolgálat végzi, hogy megvizsgálja ezen elektronikus rendszerek ellenálló képességét. A megtalált hiányosságokat a hatóság informatikai szakemberei górcső alá helyezik, kiértékelik és ezekre javaslatokat, megoldásokat tesznek, hogy az érintett kritikus rendszereket még biztonságosabbá tegyék.

2020. évi CLXXVI. törvény a villamos energiáról szóló 2007. évi LXXXVI. törvény módosításáról főként energiaközösségeket, átviteli rendszerirányítói feladatokat és elosztói rugalmassági szolgáltatásokat érint.[24]

Viszont a Nemzeti Energiastratégiában már megemlítik a villamosenergia szektor infókommunikációs védettségét és ezekkel összefüggő elhárítási lehetőségeit. Ugyan ebben az évben jelent meg a 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, amelyben a kibertér kutatására és fejlesztésére és annak védelmi összetevőire hívja fel a figyelmet. Továbbá rávilágít arra a tényre is, hogy ebben a témában kutatással és fejlesztéssel foglalkozó intézmények jóval kevesebben vannak jelen Magyarországon, mint más nagyobb nyugat-európai országban, mint például Németországban vagy Franciaországban. Ezzel összhangban az oktatás fejlesztését is figyelembe kell venni, mivel a fenti törekvések alapja és kiindulópontja. [1163/2020. (IV. 21.) Korm.]

A villamosenergia-rendszer hatókörében lévő kiemelt kockázatú infrastruktúrák ágazati besorolására a Magyar Energetikai és Közmű-szabályozási Hivatalt jelölte meg a 374/2020. (VII. 30.) Korm. rendelet, mint eljáró hatóság. Megemlítésre kerül a hazai és Uniós kiemelt kockázatú rendszerelemek besorolása különböző paraméterek szerint. Fontos jelenség a rendeletben, hogy pontosan meghatározza a kritikus zavarokat, küszöbértékeket és a kiemelkedő kockázatú eseményeket.[23]

Sajnos az 526/2022. (XII. 16.) Korm. rendelet sem említi a kibevédelemet csak az orosz-ukrán háború következtében kialakult vészhelyzeti intézkedéseket, amely a villamos energiáról szóló 2007. évi LXXXVI. törvény eltérő alkalmazásából fakadóan adtak ki. Ugyan ez a helyzet a 2021. évi XCIII. törvénnyel kapcsolatosan is, amely szintén nem szól kiberbiztonságról se energetikai biztonságról.[25][26]

Viszont a legfrissebb kiberbiztonsági törvényünk: 2023. évi XXIII. törvény, amelyet a 10/2023. (V. 15.) Szabályozott Tevékenységek Felügyeleti Hatósága azaz röviden SZTFH rendelete egészíti ki. Nyilván ezek és a fent említett szabályzatok a NIS2 irányelvvel összhangban vannak, sőt mint Európai Uniós tagállamként ez kötelező keretrendszerrel bír még, akkor is, ha élesítve csak ez év végén lesz. [27]

A kiberbiztonsági törvénybe az (EU) 2019/881 uniós rendelet szövegét illesztették be tanúsítási hatóság feladatainak meghatározásához. Magyarország területén belül e törvényben meghatározott kiberbiztonságot érintő rendszereket a következő csoportosításba tehetők alap (alapvető kockázatok), jelentős (korlátozott szakértelemmel és erőforrásokkal rendelkező) és magas (jelentős szakértelemmel és erőforrásokkal) szintekbe. Ellenőrzésre kijelöltek körét, így határozta meg a törvény: kiemelten kockázatos, kockázatos és olyan vállalkozások, amelyek elektronikus információs technológiához szorosan köthetőek. Ezeket a felügyelt piaci vagy nem piaci szegmenseket kétévente független auditor fogja megvizsgálni, akiket SZTFH elnöke biz meg az ellenőrzésre.[28]

NIS2 IMPLEMENTÁLÁSA MAGYARORSZÁGON

A NIS2-irányelv kiterjeszti elődjének tárgyi hatályát új ágazatokra, amelyek kockázatos és kiemelten kockázatos kategóriába vannak besorolva, illetve vannak még olyan NIS2-es szabályozás alá eső piaci szegmensek, akik az információbiztonság szempontjából meghatározó jelentőségűek.

A 2022/2555-ös európai direktíva hatálya alá tartozó szervezetekre korábbinál sokkal szigorúbb követelmények vonatkoznak, mint például a kiberbiztonsági szintek tesztelésének és a titkosításának hatékonyabb használatának feltételei vagy akár megemlíthető a vizsgálandó rendszerek biztonsági réseire vonatkozó szigorítások is. Az új szabályozás az incidensek jelentése terén is pontosabb rendelkezéseket tartalmaz. Ezen túlmenően a tagállamok megkövetelhetik, hogy az alapvető és fontos szervezetek kötelezően tanúsítsák a termékeket, szolgáltatásokat és folyamatokat a kiberbiztonsági törvényben előírt európai tanúsítási rendszereknek megfelelően. Az 5G hálózati elvárásokkal összhangban a kritikus infrastruktúrák kockázatértékelése is sokkal komplexeben lesz. Így ildomos lenne az Európai Unión belül a kockázatos ellátási láncok megfelelő felügyeletét a tagállamoknak az ENISA-val együttműködve ellátni. Újdonság még a kockázatkezeléssel kapcsolatosan, hogy a piaci és az állami szereplők legfelsőbb vezetőinek meghatározott felelősséggel kell majd rendelkezniük. Továbbá bevezetése kerül majd a jogsértések visszaszorítására szolgáló nagyobb pénzbírság is.[4][13]

IS2 menetrend Magyarországon

Az első és lefontosabb dolog, hogy megállapítást nyerjen az érintettség jogi aktusa a NIS2 direktívában meghatározottak szerint. A menetrend első szakasza 2024 január elsejétől 2024 június 30.-ig terjedő időszak, ahol az érintett szervezeteket osztályba sorolják, a

hatóság lajstromba veszi, illetve információbiztonságért felelős vezetőt kijelölik. 2024 október 18-án a tagállamokban és hazánkban is hatályba lép a 2022/2555-ös direktíva. 2024 december 31-ig kell az érintett szegmenseknek szerződni az auditorokkal, akiket Szabályozott Tevékenységek Felügyeleti Hatósága választ ki és a névjegyzékébe felveszi őket. 2025 december 31.-ig kötelező lesz lefolytatni az első kiberbiztonsági ellenőrzési vizsgálatot, majd a következőt 2 év múlva 2027-ben, illetve kettő évente kell ismételten lefolytani, igazodva az első audithoz eredményeihez.[5]

Fontosabb felkészülési feladatok

Első lépés a 2022/2555 irányelv alá tartozó infrastruktúrák vagy szolgáltatók kockázatelemzése meghatározott paraméterek szerint, majd ezek kiértékelése. Az értékelések alapján létrejön egy hiányosságokat feltáró GAP-elemzés. Ennek az analízisnek az eredményéből születik, majd egy forgatókönyv, amelynek tartalmaznia kell az érintett létesítmények biztonsági réseinek javítását és a jövőre vonatkozó fejlesztési javaslatokat. Következő lépésben lehetne konkretizálni a vizsgált rendszerek, illetve a technikai összetevők szabályzatit az adott rendszerelemeknél. Feladatok közé tartozik még a NIS2 által előírt technikai kontrollok bevezetése (pl. SIEM, többfaktoros hitelesítés, hálózati eszközök integrációja, sérülékenységek kezelése stb.). A kutatásom tárgyából fontosabb megemlítenem a főként kritikus infrastruktúráknál előforduló információs technológia(IT) és az operatív technológia(OT) megfelelő szintű szabályozása. Az IT-nél érdemes a frissített Nemzeti Szabványügyi és Technológiai Intézet (NIST) 800-53 rev5. amerikai szabványát alkalmazni, míg az OT-nél a NIST 800-82 biztonsági előírásokat. Továbbá előírás még, hogy az érintett szervezeteknél ki kell jelölni egy információbiztonsági vezetőt, aki a kibertan törvényben meghatározott végzettséggel és szakmai tapasztalattal rendelkezik és a törvényben meghatározott feladatokért egyetemlegesen felel.[6]

SVÁJCI MODELL

Röviden a svájci villamosellátás felépítéséről a felelhető legfrissebb adatok alapján mintegy 610 aktív hálózatüzemeltető működök az alpesi ország teljes területén. Ezek összesen mintegy 5,65 millió fogyasztót látnak el, és mintegy 5,9 millió mérési pontot szolgálnak ki. Az ország természeti adottságiból kifolyólag jelentős eltérések vannak a szolgáltatók között, mivel a legnagyobb szolgáltató több mint 300 000 fős ügyfelkörrel rendelkezik, addig a legkisebbnek mindössze csak 45 fogyasztó csatlakozik. Egyébként az átlagos ügyfélkörrel rendelkező hálózatüzemeltetők megközelítőleg 1620 háztartást vagy egyéb ipari fogyasztót látnak el. [7]

Általánosságban is elmondható, hogy Svájc helyzete Európában eléggé egyedi, ami megmutatkozik villamosenergia piacának kialakításával kapcsolatosan is. Ugyanis ebben a kis államban a piaci versenyhelyzet korlátozott volt bizonyos kritikus infrastruktúrák tekintetében. Míg a nagy ipari fogyasztók nemrégiben lehetőséget kaptak arra, hogy megválaszszák szolgáltatójukat, addig a kisebb ipari szegmenseket vagy magánfogyasztókat továbbra is többnyire helyi monopóliumnak számító önkormányzati közműszolgáltatók látják el. [8]

„Svájc nem termel szénhidrogéneket. Az ország energiatermelése 2021-ben atomenergiából (45%), vízenergiából (28%), bioenergiából és hulladékból (25%) állt, és csak kis arányban (2,8%) váltakozó megújuló energiákból.” [9]

A hazai termelés a teljes energiaszükséglet 50%-át fedezi, a fennmaradó rész pedig importált fosszilis tüzelőanyagokból áll. Ettől függetlenül a kis alpesi országban a villamosenergia-ellátás biztonsága nagyon magas színvonalon áll. Európa többi tagállamához hasonlítva a legelitebb országokhoz tartozik, mint például Németország vagy Dánia. [9]

Svájcban a közelmúltban csak önkéntes intézkedések és ajánlások voltak érvényben a kritikus infrastruktúrák területén, nyilván ez a hagyományos politikai berendezkedésből is fakadt. Mostanra viszont – a cikkem bevezető részére is utalva a kibertámadások gyakoriságára - már nem kérdéses, hogy egyes intézkedések kötelező jellegűek a magas kockázatú intézmények számára.

Energetikailag és így nyilvánvaló kiberbiztonságilag is a környező országokkal (Németországgal, Franciaországgal, Olaszországgal és Ausztriával) területi elhelyezkedéséből fakadóan szimbiózisban van.

Svájcban az első kifejezetten elektronikus támadások elleni intézkedésekre a 2018.-ban kiadott nemzeti kiberbiztonsági stratégia adott konkrét javaslatokat és válaszokat. Előtérbe került a kritikus infrastruktúrák elektronikus és infókommunikációs védelmének hathatós előmozdítása vagy az incidensek vonatkozó bejelentési kötelezettségek és a válságkezelési gyakorlatok forgatókönyveinek fontossága.

A Szövetségi Gazdasági Ellátási Hivatalra (FONES) együttműködve tevékenykedik a Svájci Villamosenergia-ipari Társaságok Szövetségével (AES)

„A gyakorlatias megközelítés és az „egy az egyben" megoldásra való svájci törekvés eredményeként született meg a Minimum standards for improving ICT resilience (Swiss Federal Office for National Economic Supply, 2018) és egy kapcsolódó értékelési eszköz, amelyben a NIST kiberbiztonsági keretrendszerén (identify, protect, detect, respond, recovery) alapuló 106 pontból álló, visszafogott ellenőrző lista segítségével a vállalatok ellenőrizhetik kiberbiztonsági érettségi szintjüket. Az egyes ellenőrzési pontok olyan nemzetközi szabványokra hivatkoznak, mint többek között a NIST kiberbiztonsági keretrendszer, az ISO 27001 és az ISO 27019." [8]

Svájci modell elemzése

Az Uniós Intelligens hálózati munkacsoport már 2014-ben ajánlotta a kiemelt rendszerelemek üzemeltetőinek, hogy kiberbiztonsági intézkedéseit igazítsák az ISO/IEC 27001, ISO/IEC27002 és ISO/IEC27019 szabványaihoz. Később 2018-ban a Svájci Szövetségi Energiaügyi Hivatal (SFOE) a Nemzeti Szabványügyi és Technológiai Intézet (National Institute of Standards and Technology, röviden: NIST) amerikai szabvány mintája alapján alkotta meg az infókommunikációs technológiára épülő úgynevezett minimumszabványt.

Fabian Heymann felmérése a svájci villamosipar résztvevőinek operatív technológia (OT) és információs technológia (IT) fejlettségére irányult. A kutatás szerint a NIST fokozatait felhasználva az információs technológia fejlettsége a legtöbb kategóriában el sem éri az 1. alapszintet. A legnagyobb átlagértéket Svájcban az operatív technológia érte el 1,10-es fokozattal. Ez többnyire annak volt köszönhető, hogy a múltban nagyobb hangsúlyt fektettek a megelőző képességekre, mint az észlelésre és a reagálásra. A villamosipari infrastruktúrák felügyeleti és vezérlő rendszerei Svájcban még most is a beszállítók általi szab-

ványok alapján védettek. Amivel első olvasatra nem is lenne gond, csak éppen nincs összhang a két fél között, nincs közös oda-vissza csatolás és közös kutatás kiberbiztonsági és egyéb védelmi szempontokat figyelembe véve. [8]

A svájciak általában minden döntést azon a szinten hozzák meg és hajtják végre, ahol a legnagyobb szakértelemmel rendelkeznek az érintettek. Nincs ez másként az elektronikus eszközök védelmével sem, ami azt az alomáliát eredményezi, hogy az egyik kanton energiaágazata korszerűbben van felvértezve logikailag és fizikailag, mint a másik térség, pedig egy államról beszélünk. Habár az Európai Uniónak nincs közel sem, olyan joghatása a svájci döntéshozatalra, mint hazánknak, ennek ellenére bizonyos Uniós rendelkezéseket saját biztonságuk érdekében érdemes lenne átvenniük. Nyílván vannak erre már kezdeményezések, mint például a villamosenergia-rendszer kooperációja a szomszédos államokkal, ahol nem lehetőség hanem kötelező a szükséges mértékű európai szabályozás harmonizálása. [8]

Érdemes megemlíteni ebben a fejezetben a kibervédelem fontos védvonalát a Számítógép-biztonsági Incidenskezelő Csoportokat (Computer Security Incident Response Team), ahol szintén erőteljesen érvényesül Svájcra oly jellemző szerződés szabadság elve. Ennek következtében a nagy autonómia miatt, kevés kötelező jellegű jogi szabályozás vonatkozik ezekre a csoportokra. Így az egységes szabályozás erősen háttérbe szorul, amelyre Svájcnak igencsak oda kellene figyelnie majd a közeljövőben. [10]

Végül Pozitívumként a svájci szakpolitika már évek óta több innovációs stratégiát kidolgozott, amelyben a villamosenergia-ellátás jelenlegi állapota jól fejleszthető. Egyik ilyen „eszköz” például sandbox magyarul homokozó, ahol olyan biztonsági teszteléseket tudnak végrehajtani a villamosiparban, amelyek jelenlegi szabályozás keretek között nem lehetne megvalósítani. A homokozók szolgáltatások kifejlesztésére is módot adhat, ahol új intézkedések jelenlegi hiányosságait lehetne felderíteni és koordinálni anélkül, hogy az egész élő rendszert megbolygatnánk. [11]

A SVÁJCI MODELL ADAPTÁCIÓJA MAGYARORSZÁGON

Elsőként szeretném hangsúlyozni, hogy mivel hazánk az Európai Unió közösség tagja, így hiába van annyiféle modell és irányelv szerte a világban, mindenféleképpen prioritást élveznek az EU-s jogi normák a magyar szabályozásra. Gondolok itt például a kutatás szempontjából releváns NIS2 irányelvre, amelyet előző fejezetben már kifejtettem. Ennek ellenére érdemes elemezni más országok sajátos ipari rendszereit és stratégiáit. Mivel valóságos ipari környezetben szerezhetünk tapasztalatokat, amelyeket lehetetlen volna leteszteln szimulációs szoftverekkel. Így került előtérbe például a svájci modell, amely hasonló méretű ország, mint Magyarország, de eltérő ipari adottságokkal és szabályozásokkal rendelkezik, amelyek tanulságosak lehetnek hazánk energiabiztonsága számára. Ennek megfelelően szakértői interjúk és a Secosys csoport ajánlását figyelembe véve egy lehetséges adaptáció lehetne a Common Criteria, amely a 2022/2555 Uniós keretrendszerrel harmonizál, több éves szakmai tapasztalaton nyugszik, a beszállítóknak nemzetközi elfogadást biztosít és hazai bevezetése viszonylag rövid időn belül kivitelezhető lehetne. Első lépésként egy forgatókönyvet kellen elkészíteni, amelyben már tesztüzem értékelése és a problémák feltárása elkezdődik. Majd a további lépéseknél ISO 27000-es szabványcsaládot alapul véve a svájci gyakorlat hibáinak kiszűrésével hazai jól bevált módszertanokra épülve kialakítani egy elfogadható és precíz villamosenergia rendszert védő kibervédelmi szabályozást. [12]

Másfajta megközelítésben a villamos ágazat tanúsítási és ellenőrzési rendszerét differenciáltan kockázati kategóriák mentén kellene növelni a követelményeket a korábban említett Svájci modell kapcsán, ahol sok kisebb villamosenergia elosztó szolgáltató kibújt a központi kötelezettség alól, mivel se szakmailag se gazdaságilag nem volt indokolt bevezetésük.

ÖSSZEFOGLALÁS

Nem kétséges, hogy a magyar kritikus infrastruktúra egyik legmeghatározóbb képviselője a villamosenergia ágazat teljes rendszere. Így védelmére különösen nagyobb hangsúlyt kell fektetni, mint általában más ágazatokra, mivel a többi kritikus infrastruktúra működésére is jelentős hatást gyakorol. Mivel a technológiai és fizikai adottságai megkövetelik, ezért folyamatos a nap 24 órájában üzemeltetni kell ezeket a rendszereket. Pár perces kiesés is hatalmas problémákat okozhatnak az ország villamosenergia-ellátásban. Kutatásomban inkább jogszabályi oldalról közelítettem meg az elektronikus információs rendszerek védelmének problémakörét. Ennek következtében a NIS2-es európai szintű szabályozást emeltem ki, amely 2024 október 18-tól már teljes hatállyal Magyarországot is fogja érinti. Természetesen implementálása hazánkban már folyamatban van, ahogy ezt a cikkben ki is fejtettem. Továbbá megvizsgáltam a svájci villamosenergia-rendszer sajátosságait az európai normatívákat figyelembe véve és ezekre a tapasztalatokra építve kialakítottam egy javaslati szinten lévő magyar adaptációt. Nyílván több ország szakági gyakorlatát is lehetett volna elemezni, de ennek a cikknek meghaladta volna a terjedelmét. A jövőben biztosan kiterjesztem majd a kutatásomat más európai és/vagy Európán kívüli országokra is. Összefoglalva a kutatással kapcsolatos tapasztalataimat a következő fontosabb javaslataim lennének: célszerű lenne az Európai Unión belül a kockázatos ellátási láncok megfelelő felügyeletét a tagállamoknak az ENISA-val együttműködve ellátni. A tagállamok közötti információmegosztás intézményesítésére létre kellen hozni egy európai sajátoságokra épülő szabványcsaládot. Továbbá javaslom az IT-nél alkalmazott NIST 800-53 rev5. és az OT-nél a NIST 800-82 biztonsági előírásokat Uniós sajátosságokra tovább fejleszteni. [3]

FELHASZNÁLT IRODALOM

[1] Faludi , Andor és Szabó, László, *Villamosenergia-rendszer üzeme és irányítása*, 2012. kiad. Budapest, Hungary: BME.

[2] P. J. Horváth, É. S. Somossy, és T. Tóth, „A decentralizált villamosenergia-rendszerek fejlődésének nemzetközi és hazai szempontjai”, *Közgazdasági Szemle*, köt. 69, sz. 6, o. 697–720, jún. 2022, doi: 10.18414/KSZ.2022.6.697.

[3] C. Krasznay és G. Gyebnar, „Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems”, in *2021 13th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia: IEEE, máj. 2021, o. 171–188. doi: 10.23919/CyCon51939.2021.9468289.

[4] A. Besiekierska, „Legal Assessment of the National Cybersecurity System in Poland in the Light of the New Developments in the NIS2 Directive”, in *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, Opatija, Croatia: IEEE, máj. 2023, o. 1474–1477. doi: 10.23919/MIPRO57284.2023.10159958.

[5] Tóth Tamás, „A NIS2 irányelv az Európai Unió kiberbiztonsági szabályozása”. [Online]. Elérhető: https://nis2iranyelv.hu/
[6] H. Altaleb és Z. Rajnai, „Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures”, in *2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, Pula, Croatia: IEEE, szept. 2023, o. 000625–000630. doi: 10.1109/SISY60376.2023.10417951.
[7] Swiss Federal Electricity Commission ElCom, „Report on the activities of ElCom 2022”, Bern, 6/2023, 2023. Elérés: 2024. május 28. [Online]. Elérhető: https://www.elcom.admin.ch/elcom/en/home/documentation/reports-and-studies/taetigkeitsberichte.html
[8] F. Heymann, S. Henry, és M. Galus, „Cybersecurity and resilience in the swiss electricity sector: Status and policy options”, *Utilities Policy*, köt. 79, o. 101432, dec. 2022, doi: 10.1016/j.jup.2022.101432.
[9] INTERNATIONAL ENERGY és AGENCY, „Switzerland 2023 Energy Policy Review”, Switzerland, Review, 2023. Elérés: 2024. május 30. [Online]. Elérhető: https://iea.blob.core.windows.net/assets/b6451900-e6ef-45a8-922d-117520e09a82/Switzerland2023.pdf
[10] P. Meyer és S. Métille, „Computer security incident response teams: are they legally regulated? The Swiss example”, *Int. Cybersecur. Law Rev.*, köt. 4, sz. 1, o. 39–60, márc. 2023, doi: 10.1365/s43439-022-00070-x.
[11] F. Heymann, J. Schmid, M. Vazquez, és M. Galus, „Regulatory sandboxes in the energy sector - review and learnings for the case of Switzerland”, in *CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution*, , Online Conference: Institution of Engineering and Technology, 2021, o. 3229–3233. doi: 10.1049/icp.2021.1730.
[12] Bonnyai, Tünde, Görgey, Péter, és Krasznay, Csaba, *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve*. Budapest, Hungary: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, 2023. [Online]. Elérhető: https://seconsys.eu/wp-content/uploads/2023/02/SeConSys_kezikonyv_aktual_2023_jan.pdf

JOGSZABÁLYOK

[13] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/ 1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)*
[14] *A TANÁCS 2008/114/EK IRÁNYELVE az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.*
[15] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2557 IRÁNYELVE (CER) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről*.
[16] *2007. évi LXXXVI. törvény a villamos energiáról*.
[17] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*.

[18] *1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról*.
[19] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*.
[20] *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról*.
[21] *187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról*.
[22] *271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól*.
[23] *374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*.
[24] 2020. évi CLXXVI. törvény a villamos energiáról szóló 2007. évi LXXXVI. törvény módosításáról.
[25] *2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról*.
[26] *526/2022. (XII. 16.) Korm. rendelet a villamos energiáról szóló 2007. évi LXXXVI. törvény veszélyhelyzet ideje alatt történő eltérő alkalmazásáról*.
[27] *2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről*.
[28] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály.

KÖSZÖNETNYILVÁNÍTÁS

Egyetemi Kutatói Ösztöndíj Program-Kooperatív Doktori Program keretében megvalósuló kutatás, amelyet az Óbudai Egyetem Kutatási és Fejlesztési Alapból finanszírozott.