CURRENT CYBER SECURITY OF THE ELECTRICITY SYSTEMS

VILLAMOSENERGIA-RENDSZEREK AKTUÁLIS KIBERBIZTONSÁGA

DÉR Attila[1]

Abstract

We have built ourselves an infrastructure system that supports our daily lives and makes them more comfortable, but these systems rely almost entirely on IT systems. But everything requires electricity. The electricity system has changed significantly over the last decade, becoming more complex, more sophisticated and increasingly indispensable. This highlights the crucial role of security of supply. The need for research is also underlined by the fact that cyber-attacks on critical infrastructure are increasing year on year. The research objective of this paper is to explore the current state of security of electricity supply systems and to define the security of the domestic energy supply systems in the light of this. In terms of research methods, I compare several critical infrastructures at international and national level. Current cyber security risks will be assessed, analysed and evaluated through expert interviews. Furthermore, I will evaluate existing data on the protection of energy supply systems and make recommendations based on this data.

Keywords

cyber security, cyber defence, electricity system, critical infrastructure, electricity supply

Absztrakt

Kiépítettünk magunknak egy olyan infrastruktúra rendszert, amely a mindennapi életünket támogatja, komfortosabbá teszi, azonban ezek a rendszerek szinte teljes mértékben az informatikai rendszerekre támaszkodnak. Mindenhez azonban villamos energiára van szükség. A villamosenergia-rendszer az elmúlt évtized óta jelentős változásokon ment keresztül összetettebb, bonyolultabb és egyre nélkülözhetetlenebb lett. Mindez abszolút rávilágít az ellátásbiztonság kulcsfontosságú szerepére. A kutatás szükségességét az a tény is alátámasztja, hogy kibertámadások a kritikus infrastruktúrák tekintetében évről évre növekszik. Jelen cikk kutatási célja feltárni a villamosenergia-rendszerek jelen helyzetű védelmi helyzetét, és ennek tükrében meghatározni a hazai energiaellátó rendszerek védelmét. A kutatási módszerek tekintetében összehasonlítok több kritikus infrastruktúrát nemzetközi és hazai szinten. Az aktuális kiberbiztonsági kockázatokat felmérem, elemzem és szakértői interjúk segítségével kiértékelem. Továbbá az energiaellátó rendszerek védelméről meglévő adatokat kiértékelem és ennek alapján ajánlásokat teszek.

Kulcsszavak

kiberbiztonság, kibervédelem, villamosenergia-rendszer, kritikus infrastruktúra, villamosenergia-ellátás

[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

BEVEZETÉS

A villamosenergia-rendszerek kialakulása a múlt század legelejére tehető, amikor még a fogyasztó csak egyetlen villamos hálózattal volt összekötve az erőművel. Ez azt jelentette, hogy hibák és karbantartások esetén kiesések lehettek a fogyasztói hálózaton a termelő egység teljes tartalék tartását követelte meg. Ennek következtében a fogyasztók ellátásának biztonsága érdekében meghatározott körzetekben lévő villamos termelő létesítményeket összekapcsoltak, hogy a tartalékok és terheléseloszlásokat kiegyenlítsék a különböző erőművek között. Végül ezekből a kisebb kooperációkból napjainkra már kontinens méretű együttműködés alakult ki. Magyarországon, mint villamosenergia-rendszer hivatalosan 1949-ben lett kialakítva VER néven, amely később 2011-től lett tagja ENTSO-E RG CE (Europian Network of Transmission system Operators for Electricity, Regional Gro up Continental Europe)

Amikor már nem közvetlen kapcsolat van a fogyasztó és az energiaellátást biztosító intézmény között és egyre nagyobbak a távolságok, akkor már komoly szállításról, illetve átvitelről beszélünk, amelyek már külön kategóriát képviselnek a villamosenergia-rendszeren belül. 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 750kV-, 400kV és 220kV értékek között mozoghatnak, attól függően, hogy milyen teljesítményű erőművekre csatlakoznak. Fontos viszont megemlíteni, hogy a nagyfeszültségű hurkolt vagy alap átviteli hálózat és az elosztó hálózat közötti feszültségszint határa a 120kV, ahol a 400/120kV és 220/120kV-ra transzformált feszültséget transzformátorokkal csökkenti tovább középfeszültségűszintre, azaz 35kV-, 20kV és 10kV elosztó hálózati szintre. Itt már megjelenek már a különféle ipari fogyasztók is, mint például gyárak, üzemek vasúti szállítás stb. Végül a legkisebb feszültségű hálózatok 0,4kV-val üzemelő a kisfeszültségű hálózatok, amelyek már a főként lakossági fogyasztókkal vannak összefüggésben. [1]

VILLAMOSENERGIA-RENDSZER RÖVID ÁTTEKINTÉSE

A cikk megírásával kapcsolatban releváns bemutatni ennek a három hálózati szintnek a topológiáját is, mivel kibertámadások alkalmával egyáltalán nem mindegy, hogy milyen elrendezésűek ezek a rendszerek. Az alap nagyfeszültségű hálózat hurkolt, nem véletlenül nevezik a teljes rendszer gerincének. Míg a középfeszültségen sugaras kialakítású a táppont és a fogadó pont között egy átviteli út van. A középfeszültségű elosztó hálózat fogadó pontjai a középfeszültségű elosztó hálózati gyűjtősínek, transzformátorállomások. Az azonos feszültségszinten sugarasan üzemelő vezetékeken az energiaellátás folyamatosságának és így a fogyasztók ellátása biztonságának növelésére bontási helyeket (összekapcsolási lehetőségeket) alakítanak ki, ezáltal a sugarasan ellátott körzetek nagysága változtatható. A vidéki szabadvezetékes elosztóhálózat jellemző feszültségszintje 20 kV, a városi kábelhálózatok zöme 10 kV névleges feszültségű. A kisfeszültségű hálózatokra általában a sugaras topológia a legjellemzőbb, de meg lehet találni speciális hurkolt kialakítást is, ahol a sugaras vezeték összeillesztését biztosító eszköz segítségével oldják meg. [1]

Mint már említettem a bevezetőben 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. A hagyományos energetikai hálózataink az elmúlt évek során átalakult egy speciális intelligens hálózattá, amely a kiber-fizikai rendszert is magában foglalja, mint ahogy egyes kutatásokban Smart Grid (SG) és Cyber-Physical System (CPS), mint angol kifejezéseket már együtt használják. A hagyományos elvek szerint a villamosenergia-rendszernek két tartópillére van az egyik a fizikailag kiépített rendszer, mint például erőművek, alállomások, átviteli vezetékek, okos mérőberendezések stb. és a másik az információs és kommunikációs technológiákon alapuló irányítási rendszer. Természetesen a hagyományos felépítés nem változott meg alapjaiban, hanem csak a vezérlés és az irányítás technológiája fejlődött napjainkra óriási léptéket. Így a már említett kiber-fizikai rendszer összekapcsolása intelligens hálózatokkal felvetett egy újfajta csoportosítást, amelyben négy kulcsfontosságú elem található. Az első elem a villamosenergia-rendszer a második elembe tartoznak a méréseket, érzékelőket és az aktuátorokat irányító rendszer, a harmadik a vezérlő egységeket magába foglaló rendszer és negyedik a kommunikációs rendszer. Ennek megfelelően az intelligens hálózati rendszerek alrendszereiben is megtalálhatók a védelem és az áramellátás kapcsolatában az intelligens elektronikával felszerelt eszközök, távoli elérésű terminálegységek (RTU), relék, áram- és feszültségszabályozók, feszültségszint átalakítására szolgáló transzformátorok, valamint különféle méretű és fajtájú megszakítók. A villamosenergia-rendszer felügyeletéhez és működtetéséhez szükséges elektromos jelek mérését is az intelligens elektronikával felszerelt eszközök, távoli elérésű terminálegységek (RTU) és a fázismérő egységek szolgáltatják. Ezeket a mérési adatokat az alállomások adatgyűjtő egységei összegyűjtik és továbbítják a villamosellátást irányító központokba.[2]

Az irányítóközpont felelős az energiarendszer felügyeletéért, biztonságáért és stabilitásáért. Az állapotbecslő alkalmazások tervezéséhez a SCADA-rendszerből kapott mérési adatokat használja fel a villamosenergia-rendszer működésének becsléséhez. Az állapotbecslő alkalmazások ezután elemzik a villamosenergia-rendszer biztonságát és stabilitását.[3]

NEMZETKÖZI KITEKINTÉS

Egyesült Államok

Ebben a fejezetben egy rövid kitekintést tennék más országok villamosellátásával kapcsolatosan, hogy összehasonlítás nyújtson hazánk helyzetével. Az egyik ilyen kiemelkedő fontosságú ország az Amerikai Egyesült Államokban, ahol hatalmas kiterjedésű és rendkívül összetett rendszer van. A nagyságrendek érzékeltetéséhez két adatot említenék: körülbelül 3300 szolgáltató van az Amerikai Egyesült Államokban, amely 200000 mérföldnyi átviteli hálózattal rendelkezik. Mivel az Egyesült Államok rengeteg államból áll, így az egész országra kiterjedő egységes szabályozás igencsak nehéz. Van egy úgynevezett Észak-Amerikai Villamos Megbízhatósági Tanács a NERC(North America Electric Reliability Council)[4], amely a kritikus infrastruktúra előírásaival egyetemben kidolgozott megbízhatósági szabványokat a villamosenergia rendszerek védelmére. Ezek az egyes államokra kötelező jellegű szabályozások különböző szempontokra terjednek ki, mint például a rendszer és a vezérlés biztonságának kezelésére, a személyzet képzésére, a kritikus kibereszközök azonosítására, fizikai biztonságra és helyreállítási tervek elkészítésére stb. A 45 követelményt és kilenc szabványt tartalmazó előírás jelentősen befolyásolja és biztosítja a nagy

teljesítményű villamosenergia-rendszerek nagyfokú megbízhatóságát. Ennek ellenére az észak-amerikai közművek felére vonatkoznak kötelező jelleggel. Felmérések szerint az amerikai villamoshálózat ellen intézett támadások jellentő kárt tudnának okozni az energiaellátásban, akár több tíz millió fogyasztónál lehetne elérni időlegesen áramszünetet. Az amerikai Nemzeti Szabványügyi és Technológiai Intézet a NIST (National Institute of Standards and Technology) létrehozta a NISTIR 7628 Rev. az intelligens hálózatok kiberbiztonságára vonatkozó iránymutatások (Guidelines for Smart Grid Cybersecurity) jelentését, amelyben egy speciális keretrendszert dolgozott ki a hatékony kiberbiztonsági stratégiák kidolgozásához. Az Intelligens Hálózatokban részvevők kockázatértékeléshez, valamint a kockázatok azonosításához és a megfelelő biztonsági követelmények alkalmazáshoz használhatják. A NISTIR 7628 Rev.1. 2014-ben vezették be, hogy felváltja a NISTIR 7628 iránymutatást, amely a 2010. évben jelent meg. Ez a szabvány már megemlíti, hogy az elektromos hálózatok átalakulóban vannak viszonylag zárt rendszerből egy összetett, nagymértékben összekapcsolt környezetté. Továbbá fontos szempontként kiemeli, hogy az egyes kritikus infrastruktúráknak együtt kell fejlődniük karöltve a technikai fejlődéssel, hogy elkerüljék az elmúlt években megsokszorozódott hálózat biztonságát fenyegető veszélyek elkerülését.[3][5]

Európai Unió

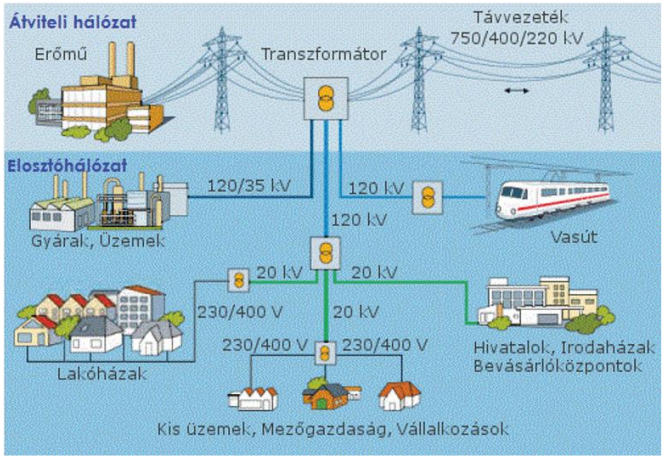
A Európai Unióban három főbb szabályozás vonatkozik a villamosenergia rendszerekre az EU Tanács által kiadott 2008/114/EK irányelve, amely az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szól. A második Az Európai Uniós Kiberbiztonsági Ügynökség(ENISA) vonatkozásában az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). Végül a harmadik komponens a Hálózati és információs rendszerek biztonságáról (NIS2) szóló irányelv.[6]

Az Európai Bizottság 2017/1485 számú rendelete a villamosenergia-átviteli hálózat üzemeltetésére vonatkozóan módszertani javaslatokat fogalmaz meg az egyes hálózati elemek kiesésének relevanciája kapcsán (Európai Unió 2017). Fontos mérföldkő ennél a rendeletnél, hogy a rendszerirányítóknak modellezések és szimulációk segítségével egy olyan módszertant kell kialakítani, amelyben képesek az átviteli és elosztórendszerek létfontosságát megvizsgálni és kiértékelni. Utána kettő év múlva lett kihirdetve az Európai Parlament és a Tanács 2019/941 rendelete a villamosenergia-ágazati kockázatokra való felkészülés vonatkozásában, amelyben minden tagállamnak nemzeti kockázati tervet kell kidolgoznia a regionális és tagállami villamosenergia-ellátási válságforgatókönyvek alapján (Európai Parlament és Tanács 2019).[7] Minden megújuló technológia ott hasznosulna a rendszerben, ahol a legjobbak a földrajzi adottságok: a nagy szélerőműparkok a tengerpartokra, a naperőművek az intenzív besugárzású területekre, a vízerőművek a hegyvidéki övezetekbe stb. települnének.[8]

HAZAI VILLAMOSENERGIA-RENDSZER HELYZETE

Magyarországnak 23 nagyerőműve van, amelyek bruttó beépített teljesítménye 6.756,9 MW, de ez a teljesítmény nem használható ki teljes mértékben az erőművek önfogyasztása, valamint az állandó hiány miatt. A rendszerszintű koordinációban mind a 23 villamos termelő egység jelentős kapacitással vesz részt. Ebből a legjelentősebb a Paksi Atomerőmű, amely nagyjából az összes hazai beépített teljesítmény egyharmadát adja nagyjából 2000MW-ot.[9]

A hazai villamosenergia-rendszer működéséért, az ellátásbiztonságért és a fogyasztás pillanatnyi egyensúlyának fenntartásáért a Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR Zrt) gondoskodik nap, mint nap. Legnagyobb mértékben természetesen működése a magyar átviteli hálózatra tevődik, ezért különös figyelmet fordít a feszültség értékekre, meddő teljesítményre és terhelési szögekre. Továbbá folyamatosan monitorozza a hálózat túlterheltségét, illetve megfelelő feszültségszintjét. Gyakran tartanak kiesés vizsgálatokat és szimulációs gyakorlatokat, amelyben a beállított hálózati részeket kikapcsolják, hogy a megterhelt vezetékeken átfolyó áram nem okoz-e túlterhelődést más közelben lévő részekre. A MAVIR ezeket a számításokat periodikusan egész nap az év 365 napjában teszteli.



1. ábra átviteli és elosztóhálózat, forrása:[9]

Az európai országokban is megvannak a MAVIR-hoz hasonló rendszerirányító központok, amelyek egyébként napjainkban már teljes belépő és kilépő villamos hálózata össze van kötve egymással. Így a magyar villamosenergia-rendszer szimbiózisban van a többi tagország rendszereivel, ami azt jelenti, hogy bármely nagyobb nemzeti üzemzavar vagy szabályozás az egész európai rendszert érinti. Ennek következtében nagyon fontos, hogy ezen kritikus infrastruktúra irányítói szoros kooperációban együttműködjenek egymással és egy teljes részt alkossanak az Európai Unió zökkenőmentes energiaellátásának biztosítása érdekében.[9]

Kockázatok és sérülékenységek a villamosenergia ellátásban

Természetesen már a legelején le szeretném szögezni, hogy kutatásomban előforduló kockázatokat és sérülékenységeket csak specifikusan a témával szorosan összefüggő adatok és elemzések alapján vizsgáltam a teljesség igénye nélkül. A megújuló alapú villamosenergia-termelés aránya az elmúlt években exponenciálisan nőt és az elkövetkezendő évekre is ez a tendencia lesz majd érvényes. Ezeket a zöld energiával rendelkező egységeket is el kell látni megfelelő kommunikációs hálózati csatornával illetve hozzá kapcsolódó protokollokkal, hogy egységesen lehessen őket kezelni egy nagy kiterjedésű térség (EU, USA) vagy ország energetikai ellátás láncában. Ennek következtében egyre növekvő Kiberbiztonsági kockázatot is jelentenek évről évre a villamosenergetikai rendszerekben. További kockázatok lehetnek még az ipari felügyeleti rendszerek nyílt forráskódú elérhetőségei vagy a SCADA rendszerek gyártói támogatásának, frissítésének megszűnése. Egyébként az ipari rendszerek legtöbb gyártója sincs felkészülve a különböző kiberfenyegetésekkel szemben, mivel nincs meg a kellő tapasztalatuk és gazdasági érdekük ezzel kapcsolatosan. Így az energetikai rendszerek irányító testületeinek kell olyan beszállítókat találni vagy szerződéseket kötni, ahol markánsan jelen vannak az erre szakosodott védelmi mechanizmusok. Vannak próbálkozások, de sajnos nem kielégítőek egy meghatározó követelményrendszer megalkotásához, amelyek az információs technológia és ICS/SCADA rendszerek legalapvetőbb logikai követelményszintjének megfelelően megalapoznának egy erős védelemhez szükséges feltételrendszert.[6] Ugyan így vannak forgatókönyvek, amelyekben már bekövetkezett eseményeket dolgoznak fel vagy lehetséges fenyegetésekre való felkészülést is tartalmazhatnak. A cél mindig a fenyegetések elleni hatékony megelőzés illetve a már bekövetkezett támadás elhárításának leggyorsabb és leghatásosabb eredeti állapotok visszaállítása. Egy megvalósítható fenyegetéseseménynek négy elemet kell tartalmaznia: az eseményt kezdeményező fenyegetés forrását, a fenyegetésesemény célobjektumát, a célobjektum sebezhetőségét és a sebezhetőséget kihasználó fenyegetés forrását. Ha a potenciális fenyegetés forrása, a sebezhetőség és a sebezhetőséget okozó fenyegetés vektorát azonosítottuk és megértettük, akkor megkaphatjuk a megvalósítható fenyegetésesemény teljes tartalmát**.**[10]

Az elektromos hálózat intelligens hálózatokra történő átalakítása további biztonsági problémákat vett fel a hagyományos elektromos hálózattal ellentétben, amely a Felügyeleti irányítás és adatgyűjtő SCADA-rendszerre támaszkodik a felügyelet és az irányítás tekintetében. Míg az Intelligens hálózatok a hatékonyabb ellenőrzésre és felügyleti pontosság növelésére az információ- és kommunikációstechnológiát (IKT) és Fázismérő egységeket használják. Viszont ennek a technológiának az a hátrány például, hogy a fázismérő egységek feszültség- és áramfázis méréseket továbbítanak meghatározott központi egységek felé kommunikációs csatornákon keresztül, és erre ugyanaz a központi egység vezérlőjeleket ad vissza a fázismérőnek cserébe. Így a felügyeleti és szabályozási folyamatot sérülékenyebbé teszi kibertámadásokkal szemben, ami csökkenti a teljes energiaellátás biztonságát.[2]

Az intelligens hálózatok ellen intézett kibertámadások a rosszindulatú támadások széles skáláját jelentik, amelyek célja a villamos hálózatok adatainak, kommunikációs rendszereinek sebezhetőségének kihasználása. Az ilyen támadások veszélyeztethetik az adatok titkosságát, sértetlenségét és rendelkezésre állását, megzavarhatják a hálózati működést, áramkimaradásokat és egyéb súlyos következményeket eredményezhetnek. Néhány gyakori kibertámadás a villamosenergia rendszer ellen, mint például szolgáltatásmegtagadással járó

támadás (DoS), hamis adatinjekció (FDI), közbeékelődéses támadás man-in-the-middle, malware, adathalászat, terhelésmódosítás, visszajátszás és spoofing támadások.[10]

Intelligens hálózatok valós idejű nyomon követésére és ellenőrzésére SCADA-rendszereket alkalmaznak. Rendszeres időközönként adatokat szereznek az intelligens mérőórák leolvasásából, állapotérzékelőkből és egyéb forrásokból, lehetővé téve a hatékony folyamatirányítást. Ezek a rendszerek távoli elérésű telemechanikai terminál egységekből és programozható logikai egységekből állnak, amelyek távoli érzékelőkkel és működtetőkkel kommunikálnak egymással. Az összegyűjtött adatokat ezt követően egy központi fő terminálegységhez küldik el elemzésre. A SCADA-rendszerek tartalmaznak egy HMI-egységet is, amely lehetővé teszi a kezelők számára a rendszer működésének valós idejű nyomon követését és módosítását. Ezen felügyeleti és adatgyűjtő konstrukciók fő célja az elosztott rendszerek megfelelő felügyelete és kezelése, ami költségmegtakarítást, jobb karbantartást és az energiaellátás megbízhatóságának növelésélést eredményezi. Funkciójának ellátásához azonban a SCADA-nak a kibertámadásokkal szembeni valamennyi biztonsági célkitűzésnek meg kell felelnie. Különböző biztonsági technológiák, mint például a behatolásérzékelő rendszerek (IDS), virtuális magánhálózatok (VPN), internetprotokoll-biztonság, stb. (IPsec) és tűzfalak, amelyeket a SCADA-hálózatokban alkalmaznak a következők védelmére biztonságukat és megbízhatóságukat.[3]

A bevezetésben már említettem a villamosenergia-ellátás topológiáját, amely nagyban függ a hálózat feszültségszítjétől, átviteli vagy elosztó hálózat és az adott térség földrajzi adottságaitól. Ezeket a topológiákat jól lehet vizsgálni és kiértékelni különböző aspektusokban. Ennek hatására kutatásokban gráfelmélet alapján próbálják meg lemodellezni egy lehetséges kibertámadást főként átviteli villamos rendszer hálózatait és csomópontjait figyelembe véve. Meglepetésre a 132kV vezetékek eltávolítása jelentette a legnagyobb sérülékenységet. Ennek oka, hogy ezen élek eltávolítása a gráf több részre eséséhez vezet, szigetüzemű ellátási területeket létrehozva. Ezeknél a tanulmányoknál jól látható, hogy a csomópontok jelentősebbek, mint az élek. A hazai villamosenergia átviteli hálózat két központi alállomását 80%-ban biztosan érinti egy nagyobb kibertámadás. Kombinált támadásoknál általában a keleti országrészben lesznek érzékelhetők a támadások hatásai. Magyarország gerincvezetékét alkotó hurkolt 400kV-os vezetékrendszer szerencsére egyszeres vezetékkiesésre ellenálló.[7][11]

Fontos észrevételem, hogy villamosenergia rendszerben és a leggyakrabban előforduló irányítási és ellenőrző egységek ICS/SCADA-nál kiberbiztonsági kockázatértékelés ne csak papíron legyen, hanem gyakorlatban is ki legyen építve, illetve tesztelve erre tervezett szimulációval vagy akár valós helyzetű gyakorlatokkal. A határvédelemnél nagyobb figyelmet kellene fordítani a hozzáférési lista létrehozására, a port szintű biztonsági alkalmazások megfelelő ellenőrzésére. A tűzfal szabályokat rétegelt stratégiával kell kiépíteni behatolás észlelő és megelőző rendszer kompatibilitásának megőrzése mellett. A hálózati behatolás megelőző rendszer mellett érdemes minden egyes hálózati szegmensbe is hálózati észlelő eszközt telepíteni. Az operatív vagy más néven üzemeltetési technológia hálózataiba behatolás megelőző rendszer helyett inkább a behatolás észlelő rendszert érdemes betervezni. Sőt az érzékeny adatok védelmére ajánlott kriptográfiával titkosított protokollt alkalmazni. Mindig ellenőrzött beszállítótól szerezük be a szükséges rendszerelemeket.

ÖSSZEFOGLALÁS

Villamosenergia rendszer egy dinamikusan felépülő valós idejű folyamat, amelyben olyan visszacsatolásos szabályozás vagy direkt irányítás történik, ahol kiesésnek nincs helye. A Gyors és precíz reagálás ennél a kritikus infrastruktúránál elengedhetetlen feltétele, hogy üzembiztosan működjön. Így a kibervédelmeket is, mint más egyéb védelmeket úgy kell megtervezni, illetve a már meglévőt átalakítani, hogy semmilyen körülmények között se lassítsa az elvárt reakcióidőt. Fontos elvárás az üzemeltetőktől, hogy kialakítsanak egy erre az ágazatra kiélezett eljárásrendet, amely a támadás elhárítása után az eseményeket megfelelően kiértékeli. Továbbá rendelkezik egy saját eseménykezelő csapattal, Biztonsági eseménykezelési szabályzattal és tervezettel. Nemzetközi összehasonlításban kimondható, hogy a magyar villamosenergia-rendszer kibertámadás szempontjából megbízhatóbb, mint az amerikai vagy globálisan nézve az egész Európai Uniós rendszer. Nyílván gazdasági okokra is visszavezethetően nem rendelkezik a legújabb intelligens hálózatok üzemeltetéséhez szükséges információs technológiával – amely nem biztos, hogy mindig hátrány -, de a hálózati topológia kialakítása és a manuális rendszerelemek megléte nagyban hozzájárul ezen tény megállapításához. Az Európai Unió kiberbiztonsági stratégiája és villamosenergia specifikus szabályzatai nagymértékben hozzájárulnak a tagállamok és így hazánk villamosenergia-ellátásának biztonságához és megbízható működéséhez. A jövőre váró ajánlás egy olyan kibervédelmi ellenálló képességére vonatkozó keretrendszer megtervezése, amelyben mesterséges intelligencia által támogatott automatizált helyreállítás, incidensekre való reagálás szervezését biztosítja majd az uniós tagállamok nemzeti szintű igényeihez. [12]

FELHASZNÁLT IRODALOM

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

[2] K. Bitirgen és Ü. B. Filik, „A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid”, *International Journal of Critical Infrastructure Protection*, köt. 40, o. 100582, márc. 2023, doi: 10.1016/j.ijcip.2022.100582.

[3] M. K. Hasan, R. A. Abdulkadir, S. Islam, T. R. Gadekallu, és N. Safie, „A review on machine learning techniques for secured cyber-physical systems in smart grid networks”, *Energy Reports*, köt. 11, o. 1268–1290, jún. 2024, doi: 10.1016/j.egyr.2023.12.040.

[4] „NERC”. Elérés: 2024. május 12. [Online]. Elérhető: https://www.nerc.com/AboutNERC/Pages/default.aspx

[5] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, „Guidelines for smart grid cybersecurity”, National Institute of Standards and Technology, NIST IR 7628r1, szept. 2014. doi: 10.6028/NIST.IR.7628r1.

[6] 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

[7] B. Hartmann, „Hogyan befolyásolja a villamosenergia-hálózatról rendelkezésre álló információ a fizikai támadások által okozott sérülékenységről alkotott képet?: A hazai energiaszolgáltatás túlélőképessége”, *ScientSec*, köt. 2, sz. 2, o. 155–163, okt. 2021, doi: 10.1556/112.2021.00030.

[8] 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.

[9] G. Kovács, „Az országos villamosenergia-rendszer irányítása”, *Légkör*, köt. 67, sz. 3, o. 157–162, 2022, doi: 10.56474/legkor.2022.3.5.

[10] X. Song, J. Zhao, H. Yuan, Z. Li, Y. Zhi, és X. Zhang, „Network Attack Scenario Analysis and Threat Identification”, in *2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, Chongqing, China: IEEE, okt. 2019, o. 1055–1059. doi: 10.1109/IMCEC46724.2019.8984024.

[11] N. D. Fîţă, M. D. Marcu, D. Păsculescu, F. G. Popescu, és T. Lazăr, „Security Risks Assessment on the 400/275/25 kV Elvanfoot Power Substation from Scotland in Order to Ensure Resilience and Energy Security”, in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Cape Town, South Africa: IEEE, nov. 2023, o. 1–6. doi: 10.1109/ICECET58911.2023.10389271.

[12] K. Fysarakis *és mtsai.*, „PHOENI2X – A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange”, in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, Venice, Italy: IEEE, júl. 2023, o. 538–545. doi: 10.1109/CSR57506.2023.10224995.