

60. Tudományos Diákköri Konferencia
Kiberbiztonság szekció
Budapest, 2024. november 13.
Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

**Kritikus információs infrastruktúrák elleni kibertámadások hatásai az egészségügyi és
villamosenergia ágazatokban**

Szerző: Rubint Péter
Konzulens: Prof. Dr. Rajnai Zoltán

Lezárás időpontja: 2024. 11. 07.

2024.

„A KULTURÁLIS ÉS INNOVÁCIÓS MINISZTERIUM 2024-2.1.1 KÓDSZÁMÚ EGYETEMI KUTATÓI ÖSZTÖNDÍJ
PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT
SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.”



Tartalomjegyzék

Problémafelvetés	4
Kutatási célok.....	5
Kutatási módszerek	5
Hipotézisek	5
I. FEJEZET – A kritikus infrastruktúrák szerepe a társadalom működésében.....	6
Kritikus infrastruktúrák Magyarországon.....	7
II. FEJEZET – Az energetikai szektort érintő kibertámadások elemzése	8
Az elkövetők motivációi	8
Pénzügyi.....	8
Politikai aktivizmus	8
Terrorizmus, megfélemlítés	9
Állami szervezetek.....	9
A villamosenergia-átviteli hálózatok információs infrastruktúrája.....	10
Támadási módszerek.....	10
Sérülékenységek kihasználása	10
Kártékony programok használata	11
Ellátási lánc kompromittálása	11
Sikeres kiber-fizikai támadások a közelmúltban	12
Stuxnet	12
Industroyer/CrashOverride	12
Védekezés	12
Kritikus infrastruktúra védelem hazánkban és a globálisan	12
Határkeresztező villamosenergia-áramlás	14
Összegzés.....	16

III. FEJEZET – Egészségügyi rendszerek kiberbiztonsági kockázatai.....	17
Egészségügyi információs infrastruktúrák.....	17
Kórházi információs rendszer	17
Képarchiváló és kommunikációs rendszer.....	17
Elektronikus Egészségügyi Szolgáltatási Tér	19
Az egészségügyi rendszereket fenyegető kibertámadások típusai.....	20
Adatok ellopására vagy manipulációjára irányuló.....	20
Üzemzavar előidézésére, károkozásra irányuló	20
Zsarolóvírusos támadások következményei az egészségügyi ágazatban.....	21
Orvosi ellátásra és gyógyulási kimenetelekre gyakorolt hatás	21
Adatszivárgás és adatvesztés	22
Anyagi károkozás.....	22
Súlyos kórházi kibertámadások a közelmúltban.....	23
Düsseldorfi Egyetemi Kórház.....	23
Health Service Executive	23
Összegzés.....	24
KONKLÚZIÓ	25
HIVATKOZOTT IRODALOM.....	26

Problémafelvetés

A mindennapi élethez elengedhetetlen, alapvető szolgáltatások biztosításához szükséges ipari rendszerek, szervezetek és infrastruktúrák mind informatikai hálózatba vannak kapcsolva. Ez megkönnyíti ugyan az üzemeltetést, de új támadási felületeket is megnyit a kibertér rosszindulatú felhasználói számára.

Az Internet elterjedésével azonos ütemben kialakult az információs hadviselés új módszere, a kiberhadviselés, így mára az információs tér ugyanolyan hadszíntérnek minősül, mint a föld, víz, levegő és a világűr. Kormányzati szervek, aktivisták, bűnözők hajtanak végre kibertámadásokat számos érdekből, általában hétköznapi számítógépek és hálózatok ellen, azonban egyre gyakrabban fordul elő, hogy létfontosságú rendszereink kerülnek célkeresztbe. Kíváncsú célpontok ezek, mert az itt található számítógépek fizikai folyamatokat irányítanak, ezek megzavarásával pedig lehetséges maradandó kárt tenni a megtámadott intézményben, az így okozott üzemzavarok hatását a társadalom szinte azonnal érzékeli. Oroszország is ezt a taktikát alkalmazta 2016-ban, amikor egy kibertámadással áramszünetet okoztak Kijevben. Előszeretettel vesznek célba kritikus rendszereket, például kórházakat a kiberbűnözők is zsarolóprogramjaikkal, az általuk okozott üzemzavar ugyanis súlyos következményekkel jár, így váltságdíj követeléseik gyakrabban teljesülnek.

A létfontosságú rendszerek közül a két legfontosabb az energetikai és egészségügyi infrastruktúrák védelme. A villamosenergia hálózatok elleni támadások megzavarják az áramszolgáltatást, ez pedig az összes többi kritikus rendszer, például a kórházi ellátás működtetéséhez elengedhetetlen. Továbbá a modern gyógyászati intézmények napi üzemeltetéséhez is létfontosságúak a kommunikációs infrastruktúrák és az elektronikus orvosi műszerek is. Ugyanakkor ezek is ki vannak téve a kibertérből érkező támadásoknak, ezért nagyon fontos szem előtt tartani, hogy ha egy ilyen behatolás megzavarja a kórházi informatikai rendszert, az befolyásolja a betegek ellátását, és komplikációkat, sőt haláleseteket is eredményezhet.

Létfontosságú rendszereinknek tehát fontos szerepe van az életszínvonal és a társadalmi rend fenntartásában, ezért nem engedhetjük meg, hogy az információs térben egyre gyakoribb fenyegetések bármilyen módon kárt tegyenek bennük.

Kutatási célok

Az egészségügyi és energetikai infrastruktúrák kiberbiztonsági fenyegetettségének felmérése, az elkövetők motivációjának, és leggyakoribb elkövetési módszereinek bemutatása, valamint a védelmi intézkedések és biztonságtudatosság fontosságának szemléltetése.

Kutatási módszerek

A kutatási módszerek területén elengedhetetlen volt a komplex megközelítés a kutatási témám vizsgálatakor, összetettségéből adódóan interdiszciplináris szemléletet követelt meg. A tudományos probléma megoldása során az empirikus módszerek közül a megfigyelést és a dokumentumelemzést alkalmaztam, a logikai módszerekből az indukciót és a dedukciót, az analízist és a szintézist, az absztrakciót, a fogalomalkotást, valamint az adaptációt.

A szakterület irodalmának áttanulmányozása külön témakörökre bontva történt. Nagyon sok szempontot sikerült megismerni, feltárni és begyűjteni, amelyek felhasználásával készítettem el dolgozatomat.

Hipotézisek

Feltételezem, hogy az egészségügyi rendszerek kiberbiztonsága nem kielégítő, és egy támadás esetén a páciensek szenzitív adatai, egészsége vagy élete is veszélybe kerülhet.

Egy egészségügyi és energetikai rendszereket érintő összehangolt információs támadás kifejezetten súlyos következményekkel járna.

I. FEJEZET – A kritikus infrastruktúrák szerepe a társadalom működésében

Jelen korunk társadalmáról elmondható, hogy működésének szerves része az információáramlás és az infokommunikációs technológiák, ezért gyakori az információs társadalom vagy digitális társadalom elnevezés. Az emberek többsége mindennapjait folyamatos információáradat közepette, állandó kommunikációval, egy digitális áramlatban tölti, amelynek sok hasznos tulajdonsága van ugyan, azonban végső soron az élet minden területét informatikai eszközöktől teszi függővé. De mi történik, ha ezek működése megghiúsul? Felborulhat a napi rutin, az alapvető szolgáltatásokhoz való hozzáférés hirtelen lelassul vagy teljesen megszűnik, a társadalom érintett tagjainak biztonságérzete lecsökken, ami bizalmatlanságot és pánikot eredményezhet.

Elektromos árammal működnek a számítógépek, az egészségügyi ellátás, a banki rendszerek és szinte minden olyan dolog, ami a modern társadalom alapvető szükségleteinek kiszolgálásához elengedhetetlen, így egy villamos energia hálózat kiesése sürgető és szerteágazó problémákat képes okozni. Minden olyan rendszert, létesítményt, szervezetet vagy eszközt, amely működésében bekövetkező hiba vagy leállás az előbbi példához hasonlóan súlyos problémákat váltana ki, kritikus infrastruktúrának nevezünk. [1], [2]

Kifejezetten a társadalom és a kormányzás információs igényeinek kielégítésére hivatottak a kritikus információs infrastruktúrák. Szerepük van a létfontosságú rendszerek működtetésében is, ide tartoznak például a kórházi számítógépes rendszerek, vagy a villamosenergia-ellátás berendezéseit vezérlő ipari irányítási rendszerek. [3]

Fontos kiemelni, hogy az ilyen létfontosságú rendszerek egymással is függésben vannak, ezért, ha összehangolt támadás ér egy vagy két elemet, láncreakció alakulhat ki, és idővel az egész infrastruktúra hálózatban jelentkeznek a káros hatások. A legjobb példa az interdependenciára a villamosenergia-ipar központi szerepének vizsgálata. Ha egy ország elektromos szolgáltatása leáll, az súlyosan befolyásolja minden egyéb infrastruktúra működését is. Minden olyan intézmény, ami nem rendelkezik vészhelyzeti generátorral képtelenné válik a társadalmi szerepének betöltésére. A kórházak műszerei és információs rendszerei nélkül nincs ellátás, szivattyúk nélkül megtelnek és túlsordulnak a szennyvíztelepek, üzleti rendszerek nélkül leáll a logisztika és felborulnak az ellátási láncok. [3]

Kritikus infrastruktúrák Magyarországon

Hazánkban az alapvető szolgáltatásokat nyújtó vagy azok fenntartásához szükséges infrastruktúra elemeket a 2012. évi CLXVI. törvény „*létfontosságú rendszerelemek*” -ként azonosítja, és 10 ágazatba csoportosítja őket. A létfontosságú rendszerelemek által támogatott legfontosabb szolgáltatások a törvény szerint az egészségügyi ellátás, a pénzügyi és szociális szolgáltatások, illetve a lakosság biztonsága és a honvédelem. [4]

Ágazat	Alágazat
Energia	- Villamosenergia-rendszer (az atomerőmű kivételével) - Kőolaj- és földgázipar, távfűtés
Közlekedés	- Közúti-, vasúti-, légi-, víziközlekedés - Logisztikai központok
Agrárgazdaság	- Mezőgazdaság - Élelmiszeripar - Elosztó hálózatok
Egészségügy	- Fekvőbeteg-ellátás - Mentésirányítás - EÜ tartalékok és vérkészletek - Magas biztonsági szintű biológiai laboratóriumok - Gyógyszer-nagykereskedelem
Társadalombiztosítás	TB igénybevételhez szükséges informatikai rendszerek és nyilvántartások
Pénzügy	- Kereskedelmi, fizetési, klíring- és elszámolási infrastruktúra és rendszerei - Bank- és hitelintézeti biztonság - Készpénzellátás
Infokommunikációs technológiák	- Internet szolgáltatás és infrastruktúra - Elektronikus hírközlési szolgáltatások és hálózatok - Műsorszórás - Postai szolgáltatások - Meteorológiai infrastruktúra - Kormányzati elektronikus információs rendszerek
Víz	- Ivóvíz-szolgáltatás - Felszíni és felszín alatti vizek minőségének ellenőrzése - Szennyvízelvezetés, -tisztítás - Vízbázisok védelme - Árvízi védművek, gátak
Honvédelem	Honvédelmi rendszerek és létesítmények
Közbiztonság-védelem	Rendvédelmi szervek infrastruktúrái

II. FEJEZET – Az energetikai szektort érintő kibertámadások elemzése

Az elkövetők motivációi

Pénzügyi

Mint minden bűncselekménynél, az elkövetés egyik fő motivációja a kiberbűnözés esetében is az anyagi haszonszerzés lehetősége. A kibertérben elkövetett támadások közül messze a legelterjedtebb a zsarolóvírusos, azaz ransomware támadás. Az érintett szervezet rendszereit a támadók egy rosszindulatú programmal megfertőzik és a számítógépeken tárolt adatok titkosításával használhatatlanná teszik, majd váltságdíjat követelnek a titkosítás feloldásáért cserébe. Bár a hatósági és kormányzati szervek nem javasolják, sőt bizonyos helyeken kifejezetten tiltják a váltságdíj kifizetését, a ransomware használatával végrehajtott támadások elkövetői összesen több, mint 1 milliárd amerikai dollárnak megfelelő hasznot zsebeltek be 2023-ban. A Sophos brit kiberbiztonsági cég által publikált „*The State of Ransomware 2023*” jelentés szerint egy vállalat által kifizetett váltságdíj átlagosan 1.5 millió dollár körül mozgott, és az érintett szervezetek 46%-a fizetett a zsarolóknak. [5], [6]

Az energetikai szektorban található létfontosságú rendszereket ritkábban érintik zsarolóvírusos támadások, de ez sem példa nélküli. A magukat *DarkSide*-nak nevező hackercsoport 2021. május 7.-én ransomware támadást hajtott végre az amerikai egyesült államokbeli Colonial Pipeline benzint és kerozint szállító vezetékrendszert üzemeltető vállalat ellen. Ennek következtében az USA keleti partján a cég öt napra leállította a vezetéket, ami hatalmas anyagi károkhoz és üzemanyaghiányhoz vezetett, mivel a vezeték által szállított nyersanyag a térség szükségleteinek 45% százalékát szolgáltatta ki. Az üzemzavar hatására Észak- és Dél-Karolina, illetve Virginia és Georgia államokban átlagosan a benzinkutak 40%-a, illetve 7 repülőtér maradt üzemanyag nélkül. A hírek hallatára az emberek pánikvásárlásba kezdtek, ami tovább súlyosbította a már eddig is katasztrófával fenyegető helyzetet. Ezen tényezők hatására a vállalat végül 4.4 millió dollárnyi váltságdíjat fizetett, a támadók feloldották a titkosítást és a vezetéket május 12.-én ismét üzembe helyezték.[7]

Politikai aktivizmus

Számos olyan hacker közösség tevékenykedik világszerte, ami célpontjait kifejezetten politikai célból választja meg. Általában kormányzatok nagy port kavaró, széles körben vitatott cselekedeteire válaszul intéznek csapást az adott ország információs infrastruktúrái ellen. Talán a

legismertebb ilyen kollektíva az Anonymus, egy globális hacker közösség melynek tagjai a 2010-es évek óta hajtanak végre kibertámadásokat politikai indokkal. Ezeket a hadjáratokat meg sem próbálják titokban tartani, a sikeresen feltört oldalakon figyelemfelkeltő üzeneteket hagynak és a támadások során ellopott adatokat is rendszeresen közzéteszik. Célba vették többek között Iránt, Oroszországot és Izraelt is. Háborús és elnyomó cselekedeteik miatt az érintett országok közigazgatási, kormányzati és katonai információs rendszereit sorra kompromittálták az Anonymus tagjai. Üzeneteiket igyekeznek minél nagyobb közönséghez eljuttatni, ezért a közösségi média mellett az általuk feltört weboldalakon is elhelyezik és többször sikeresen megszakították a televíziós műsorszórást is, hogy saját tartalmaikat közreadhassák. Ezek a támadások leginkább a kritikus információs infrastruktúrát érintették, azonban előfordulnak olyan esetek is, ahol egyéb létfontosságú rendszerek, például az energetikai vagy vízügyi ágazat került a célkeresztbe. [8]

Terrorizmus, megfélemlítés

Az alapvető szolgáltatások megzavarása komoly pszichológiai hatásokkal is járhat. Ha nincs áramszolgáltatás vagy leáll az orvosi ellátás, az emberek bizalmatlanságot érezhetnek a kormányzat felé, ez csökkenti a biztonságérzetet. Minél tovább áll fent egy súlyos üzemzavar a kritikus infrastruktúra rendszerekben, annál szerteágzóbbak lehetnek a fizikai és pszichológiai hatásai egy adott országon vagy régión belül.

Állami szervezetek

A 2010-es évek óta az energetikai kritikus infrastruktúra rendszereket egyre gyakrabban érik katonai szervezetek által elkövetett, sokszor fizikai károkozással is összehangolt informatikai támadások. A kibertér ma már ugyanúgy hadszíntérnek tekinthető, ahol különböző érdekcsoportok csapnak össze, gyakran egy fizikai térben is folyó harc kiegészítéseként. A kibertérben folyó műveletek célja lehet az ellenfél kritikus infrastruktúráinak gyengítése, a döntéshozást támogató rendszerek befolyásolása, információszerzés vagy zavarkeltés is. A háborús helyzetekben végrehajtott kibertéri műveleteket összefoglaló néven kiberhadviselésnek nevezzük. [3]

A 2014-ben kirobbant orosz-ukrán háború az egyik első olyan konfliktus, amelyben már a kiberhadviselés is nagy szerepet kapott. Talán a leghíresebb példa az orosz katonai hírszerzésnek tulajdonított kibertámadás, ami 2015-ben Ukrajna több régióját is érintő áramszünetet okozott.

Azóta folyamatosan érkeznek a hírek a két ország egymás ellen irányuló kiberműveleteiről, ezeket gyakran bombázásokkal vagy egyéb hadműveletekkel egyidőben hajtják végre, így nagyobb zűrzavart és pusztítást okozva. [9]

A villamosenergia-átviteli hálózatok információs infrastruktúrája

Kiberbiztonsági szempontból a legnagyobb kockázatot az alállomások és egyéb létesítmények elavult ipari irányítási eszközei jelenthetik. Ezeket extrém környezeteknek ellenállónak tervezték, a fő szempont a hosszú ideig tartó zavartalan üzem biztosítása és az eszközök egymáshoz illeszthetősége volt. Ennek eredményeként olyan termékeket hoztak létre, amelyeknek élettartama akár húsz év is lehet, gyakran nehezen elérhető helyen vannak, működésüket nem lehet megszakítani frissítésekkel vagy karbantartásokkal, és sokszor nélkülözik a megfelelő biztonsági funkciókat. Egymással gyakran az üzem belső hálózatán keresztül kommunikálnak, azonban a távoli felügyelet és irányítás megvalósításához szükséges, hogy ez a belső hálózat elérhető legyen az Internet felől is. A végeredmény tehát egy olyan távolról is elérhető ipari hálózat, aminek elemei elavultak lehetnek, nem mindig alkalmaznak kiberbiztonsági intézkedéseket, viszont a működésük a fizikai környezetükre is hatással van. Mindezek következményeként lehetségessé vált olyan kibertámadások végrehajtása ipari rendszerek és az általuk vezérelt kritikus infrastruktúrák ellen, ahol az információs térben végzett műveletek fizikai kárt is képesek okozni. A villamosenergia ágazatban ez még súlyosabb problémát jelent, mivel egy ilyen támadás az áramszolgáltatás teljes leállításához vezethet, ami kihatással lehet a többi ágazat infrastruktúráinak működésére. [10]

Támadási módszerek

Sérülékenységek kihasználása

Az ipari irányítási eszközök speciális szoftvereiben és a munkavégzéshez szükséges általános irodai programokban is előfordulhatnak a gyártó és felhasználók számára ismeretlen sérülékenységek. Ezek felkutatásához és kiaknázásához magas szintű szakmai tudás szükséges. Azonban előfordul, hogy a feketepiacon értékesítik a kihasználáshoz szükséges adatokat, így jóval szélesebb körben elérhető a hackerek számára. Az ilyen sérülékenységek nagyon veszélyes fegyverek a rosszindulatú csoportok kezében, védekezni ellenük szinte lehetetlen. A gyártók folyamatosan közzéteszik az általuk felfedezett sérülékenységeket orvosoló frissítéseket és információkat, ezért létfontosságú a kiberfenyegetettségi információk nyomonkövetése, és az

eszközök szoftverének rendszeres frissítése, illetve az elavult, gyártó által már nem támogatott komponensek cseréje. Az ipari rendszerek szempontjából ez kifejezetten nehéz feladat, mert az eszközök gyakran olyan folyamatok részei, amelyek nem állíthatók le frissítés céljából. [10]

Kártékony programok használata

A villamosenergia-ellátást biztosító üzemek és alállomások az ipari irányítási rendszerek mellett hagyományos számítógépes eszközöket, hálózatokat is alkalmaznak a munkavégzéshez. A dolgozók munkaállomásait, és a szervezet adattárolóit ismeretlen sérülékenységeknél sokkal gyakrabban fenyegetik kártékony programok. Zsarolóvírusok, kémprogramok vagy adatpusztító kódok (wiper) terjedhetnek szét rajtuk akár egy óvatlan kattintás eredményeképpen. Ez minden szervezetnél problémát jelent, azonban a kritikus infrastruktúrákat üzemeltetőknél az adatszivárgások és leállások komolyabb következményekkel járhatnak. Ha a támadók hozzáférnek például egy transzformátor-alállomáson dolgozó személy számítógépéhez, kémprogramokkal kifigyelhetik az elektromos ipari berendezések kezelésének módját, vagy hozzáférési adatokat lophatnak el, ezek felhasználásával később zavart okozhatnak az áramellátásban. Emellett megjelentek a kifinomultabb, kifejezetten ipari irányítási rendszerek megzavarására készített malware programok is. Ezek már képesek az ilyen környezetekben használt speciális protokollokon keresztül irányítani az ipari eszközöket, így akár olyan műveleteket is végrehajthatnak, amik fizikailag tönkre teszik a berendezéseket, megnehezítve a katasztrófa utáni helyreállítást.

Ellátási lánc kompromittálása

A kártékony programok ipari rendszerekbe juttatásának több módja is van, például az üzemeltető személyzetet célzó phishing e-mail-ek küldésével, vagy a szervezet beszállítóinak kompromittálásával. Az IKT-termékek, szolgáltatások gyártói nem minden esetben alkalmaznak megfelelő kiberbiztonsági intézkedéseket, és a rendszereikbe való bejutással a támadók hozzáférést szerezhetnek az eredeti célpontjukhoz a beszállító csatornáin keresztül. A 2013.-ban felfedezett Havex malware is így terjedt el Európában, több száz energetikai ipari rendszert fertőzött meg észrevétlenül. A behatolók számos energetikai témájú weboldalt feltörték, és a látogatókat egy hamisított oldalra irányítva malware-t telepítettek az eszközeikre, illetve több ipari szoftver letöltési oldalán is lecserélték az elérhető programcsomagokat egy vírusos verzióra. [10], [11]

Sikeres kiber-fizikai támadások a közelmúltban

Stuxnet

A jelenkor talán legismertebb kritikus infrastruktúra ellen intézett, fizikai károkozással járó hackertámadás a Stuxnet vírus bevetése volt 2010 körül. Célpontja az Irán által titokban, több nukleáris egyezményt megsértve létrehozott urándúsító üzem ipari irányítási rendszere volt. Az Egyesült Államok és Izrael közreműködésével létrehozott Stuxnet egy szofisztikált és komplex program, ami kifejezetten a dúsítóüzemben alkalmazott Siemens gyártmányú programozható logikai vezérlőket (PLC) és az ezeket felügyelő rendszereket manipulálta. Az urán gáz dúsítását végző centrifugák forgási sebességének, és nyomásszintjeinek bizonyos időközönkénti módosításával elérte, hogy az üzemi berendezések kárt tegyenek saját magukban működés közben. Eközben a szenzoroknak és felügyeleti rendszereknek hamis állapotinformációkat továbbítva elérte, hogy az üzemeltető személyzet hosszú időn keresztül ne fedezze fel a szabotázsakciót. Az üzem biztonsági intézkedései kifejezetten szigorúak voltak, ám a Stuxnet készítői mégis olyan részletes információkhoz jutottak, amelyek segítségével meg tudták alkotni az Irán nukleáris törekvéseit évekkel hátráltató kártékony programot. [12]

Industroyer/CrashOverride

A kifejezetten ipari irányítási rendszerek szabotálására tervezett vírusok családjába tartozó Industroyer vagy Crashoverride malware-t orosz állami támogatású hackerek használták a 2016-os kijevi áramszünet előidézéséhez. Ez a program talán az első nyilvánosan ismert vírus, amit villamosenergia-hálózatok megzavarására készítettek. Komplex és testreszabható eszköz, egy energiaszolgáltató cég hálózatába építve hozzáférést ad az üzemeltetők munkaállomásaihoz, és a villamosiparban használatos protokollcsaládokat is képes alkalmazni. Biztosítékokkal, relékkel és egyéb, alállomásokon található berendezésekkel kommunikál, így a támadók távolról ugyanúgy átkapcsolhatják ezeket mintha a helyszínen lennének. Beépített port szkennelő funkcióval is rendelkezik, ezért használható az ipari hálózatok feltérképezésére, valamint adattörlő modult is tartalmaz, ami a fertőzött gépek teljes adatállományát megsemmisíti. [13]

Védekezés

Kritikus infrastruktúra védelem hazánkban és a globálisan

A 2000-es évek óta a nagy horderejű kibertámadások száma egyre gyorsabban növekszik, ezek közül egyre több incidens érinti a társadalom működését támogató létfontosságú rendszereket is.

Ezt a felismerve az Európai Unióban és szerte a világon elkezdődtek a kiberbiztonság fejlesztésére irányuló törekvések, például a szükséges jogi háttér kialakítása. Számos kiberbiztonsági szervezet és jogszabály jött létre a fokozódó kiberbiztonsági fenyegetések elleni hatékony reziliencia megalapozására.

Az EU 2004-ben megalapította az Európai Unió Hálózat- és Információbiztonsági Ügynökséget (ENISA), az Egyesült Államokban létrehozták a CISA-t (Cyber and Infrastructure Security Agency), hazánkban pedig a Nemzeti Kibervédelmi Intézetet (NKI) és a Nemzeti Kiberkoordinációs Tanácsot. A magyar Országgyűlés 2012-ben bevezette a *2012. évi CLXVI. törvényt a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*. Ebben meghatározásra került az európai és nemzeti létfontosságú rendszerelemek fogalma, azonosításukhoz szükséges kritériumok és az üzemeltetők, illetve a hatóságok feladatai a kritikus infrastruktúrák védelmében. [4], [14]

Megjelentek az Európai Parlament és Tanács hálózati és információs rendszerek biztonságára vonatkozó irányelvei, amelyek NIS és NIS-2 (Network and information security directive) néven ismertek. Az irányelvek célja az egységes és magas szintű kiberbiztonság elérése a tagországokban, és ezek kötelezően vonatkoznak a kritikus infrastruktúrákat üzemeltető vállalatokra. A 2023. januárjában hatályba lépett NIS-2 direktíva előírja a hatálya alá tartozó szervezeteknek a kiberbiztonsági kockázatelemzés és üzletmenetfolytonossági terv elkészítését, az ellátási láncok ellenőrzését és a biztonsági incidensek 24 órán belüli jelentését. A megfelelést egy külső audit sikeres teljesítésével kell igazolniuk, és súlyos bírságok szabhatóak ki az irányelvekben meghatározott határidők elmulasztása vagy a biztonsági intézkedések hiányosságai miatt. Magyarországon az irányelvet a 2023. évi *“XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről”* foglalja törvényi keretek közé, a végrehajtásért és ellenőrzésért felelő hatóság szerepét pedig a Szabályozott Tevékenységek Felügyeleti Hatóságára (SZTFH) ruházza. A kiberbiztonsági incidensek bejelentéseit az NKI által üzemeltetett incidenskezelő központ (CSIRT – Computer Security Incident Response Team) fogadja, segítséget nyújt az elhárításban és információkat szolgáltat a fenyegetésről érdekelt feleknek, például üzemeltetők vagy a többi tagország CSIRT-jeinek részére. [12], [16]

Határkeresztező villamosenergia-áramlás

A villamosenergia-továbbító hálózatok az európai államok leginkább létfontosságúnak tekinthető infrastruktúrái. Mivel az egyes tagországok különböző mennyiségű erőforrásokkal, eltérő energiatermelési kapacitással és felvevőpiacokkal rendelkeznek, szükségessé vált a villamosenergia-rendszereik összekapcsolása. Az így létrehozott közös határkeresztező villamosenergia hálózat lehetővé teszi az országok közötti villamosenergia-átvitelt, viszont az összekapcsolás miatt a hálózat egy részét érintő kibertámadás könnyen áterjedhet több tagállam infrastruktúráira is, ez pedig hatalmas kockázatot jelent. A NIS-2 által előírt intézkedések bevezetése megfelelő kiindulási alapot nyújt a kritikus villamosenergia-rendszereket üzemeltetőknek a kiberbiztonság fejlesztéséhez, azonban a határkeresztező energiaáramlást biztosító rendszereknél szigorúbb szabályokra van szükség. Ennek ellenére 2024 előtt nem létezett ágazatspecifikus Unió-s szabályozás, ami előírná a tagállamokat összekötő villamosenergia rendszer elemeinek kiemelten kritikus szerepéből eredően szükséges szigorú kiberbiztonsági intézkedéseket. [17]

Az Európai Bizottság 2024/1366. számú rendelete, a Network Code on Cybersecurity (NCCS) az első olyan rendelet, ami kifejezetten a határkeresztező villamosenergia-ellátásra vonatkozó szabályokat határoz meg. A rendelet négy fő területről tartalmaz előírásokat, ezek a kiberbiztonsági kockázatértékelésről, közös kiberbiztonsági minimumkövetelményekről, tervezésről, jelentéstételről és nyomonkövetésről, illetve válságkezelésről szólnak. A fentebb említett NIS-2 irányelvvel közösen alkalmazható magas szintű kiberbiztonság kialakítására minden olyan kis-közép- és nagyvállalatnál, ami szerepet játszik a határokon átvelő áramszolgáltatásban. Az érintett szervezeteket az NCCS második cikke határozza meg a villamosenergia ipar minden részén, tagállami, regionális és európai szinten. Az Unió-s szintű együttműködést, kockázatelemzéseket és a rendelet végrehajtásához szükséges információkat, például a kibertámadások hatásainak felmérésére alkalmazható indexeket vagy beszállítói javaslatokat három szervezet biztosítja: az ENISA, az Európai Unió-s Energiaszabályozói Együttműködési Ügynökség (ACER), valamint a villamosenergia-továbbító hálózatokat összefogó ENTSO-E. Emellett minden tagországban szükséges a rendelet végrehajtását elősegítő és ellenőrző illetékes hatóságot kijelölni, hazánkban ez a Magyar Energetikai és Közmű-szabályozási Hivatal (MEKH).

A hatóság a rendelettel kapcsolatosan számos feladat végrehajtásáért lesz felelős, úgymint:

- a határkeresztező villamosenergia-áramlás folytonosságára kritikus- és nagyhatású szervezetek azonosítása az ENTSO-E által közzétett módszertan alapján
- kapcsolattartás a nemzeti és nemzetközi társszervezetekkel (NKI, SZTFH, ACER, ENISA)
- kiberbiztonsági incidens bejelentések fogadása a kritikus- és nagyhatású szervezetektől
- ellenőrzési és tanúsítási rendszer kidolgozása, ellenőrzések folytatása
- nemzeti és regionális kibergyakorlatok lebonyolítása

Az NCCS a határkeresztező villamosenergia-áramlás magas szintű kiberbiztonságát átfogó Unió, regionális, nemzeti szintű kockázatelemzések elkészítésével és az ezekre kidolgozott kockázatkezelési tervekkel, közös kiberbiztonsági keretrendszer és szolgáltatók közti kommunikációs, „korai figyelmeztető” rendszer kiépítésével kívánja biztosítani. [17]

A közös kiberbiztonsági keretrendszernek való megfeleléshez az érintett szervezeteknek leltárat kell készíteniük minden eszközről, folyamatról és információról, ami befolyásolja a határkeresztező villamosenergia-továbbítást. Minden azonosított elemet be kell sorolni kritikus- vagy nagy hatásúként, védelmükre alapszintű vagy továbbfejlesztett kiberbiztonsági szabályokat kell alkalmazni. Az alapszintű és továbbfejlesztett intézkedések listáját az illetékes hatóság dolgozza ki, az előzetes verzió 2025 második negyedévében, a végleges 2027-ben kerül publikálásra. Az intézkedések alkalmazására, kezelésére egy kiberbiztonsági irányítási rendszer szükséges, már létező szabványos rendszerekhez hasonlóan (pl.: ISO27001). Bevezetés után 24 hónappal, utána pedig háromévente kötelező a rendszer ellenőrzése. Kötelező egy biztonsági elemzőközpont, azaz Security Operations Center (SOC) kialakítása is, amelynek feladata a naplófájlok és hálózati forgalom ellenőrzése, behatolások észlelése és megfelelő védelmi intézkedések végrehajtása. Ez a szervezeti egység kifejezetten fontos az incidenskezelés, információgyűjtés és a biztonság nyomonkövetésének szempontjából. [17], [18]

Az érintett szervezetek működéséhez szükséges IKT-rendszerek, eszközök és szolgáltatások biztonságos forrásból történő beszerzéséhez az ENTSO-E közzétesz egy listát az ajánlott beszállítókról, amit releváns kockázatelemzések, auditok és egyéb alkalmazható szabványok vagy technikai dokumentumok alapján készítenek és frissítenek. A listán szereplő beszállítók alkalmazása nem kötelező, minden érintett saját belátása szerint jár el, azonban a kockázatkezelési tervében ki kell térnie az ellátási lánc kockázatainak kezelésére, és a fentebb tárgyalt

kiberbiztonsági irányítási rendszernek tartalmaznia kell a biztonságos beszerzésre vonatkozó alapvető és továbbfejlesztett intézkedéseket. [17], [18]

A kiberbiztonsági incidensek hatékony megelőzéséhez és kezeléséhez elengedhetetlen az érintett szolgáltatók és felügyeleti szervek közötti hatékony kommunikáció létrehozása. Az NCCS értelmében minden hatálya alá tartozó szervezet köteles 4 órán belül az illetékes hatóság és nemzeti CSIRT felé jelentést tenni minden incidensről, ami hatással lehet a határkeresztező villamosenergia-ellátásra. A bejelentést fogadó szervezetek feladata ezután az incidens elhárításában való segítségnyújtás, az eset kivizsgálása és az Unió szervezetei, illetve a többi tagország CSIRT-jeinek tájékoztatása. [17], [18]

Összegzés

A villamosenergia-ipar digitalizációjával egyre nő a kibertámadásoknak kitett eszközök és létesítmények száma. Elmondható, hogy a kibertéri hadviselést folytató felek érdekeltek az ellenséges ország elektromos hálózatának megzavarásában, erre már kifejezetten ipari irányítási rendszerekre szabott kártékony programokat, taktikákat alkalmaznak. A kiberbiztonság folyamatos fejlesztésére tehát égető szükség van az alapvető szolgáltatások biztonságának fenntartásához. Az NCCS és NIS 2 intézkedéseinek bevezetése hosszadalmas és költséges folyamat, azonban megvalósításuk nagy előrelépést fog jelenteni az Európai Unióban található létfontosságú rendszerek kiberbiztonságának korszerűsítésében és az alapvető szolgáltatások biztonságának fejlesztésében.

III. FEJEZET – Egészségügyi rendszerek kiberbiztonsági kockázatai

Egészségügyi információs infrastruktúrák

Ezek a rendszerek és hálózatok segítik az egészségügyi szakembereket a minőségi és folytonos ellátás biztosításában. Fontos információkat tárolnak és szállítanak, kiemelt szerepük van a döntéstámogatásban és az ellátás szervezésében is. A legfontosabbak a szakmai támogató folyamatok, például az elektronikus kórtörténetek, labor- vagy képalkotó funkciók, amelyek az alapellátás biztosításához szükségesek. Emellett az intézmény működését támogató folyamatokat, logisztikát, pénzügyet, készletnyilvántartást is digitális eszközökkel kezelik. Az egészségügyi információs infrastruktúrákat érintő biztonsági incidensek több szempontból is komoly következményekkel járnak, hiszen például kiszivároghatnak a betegek érzékeny adatai, vagy üzemzavar léphet fel, ami korlátozza az egészségügyi intézmények működését.

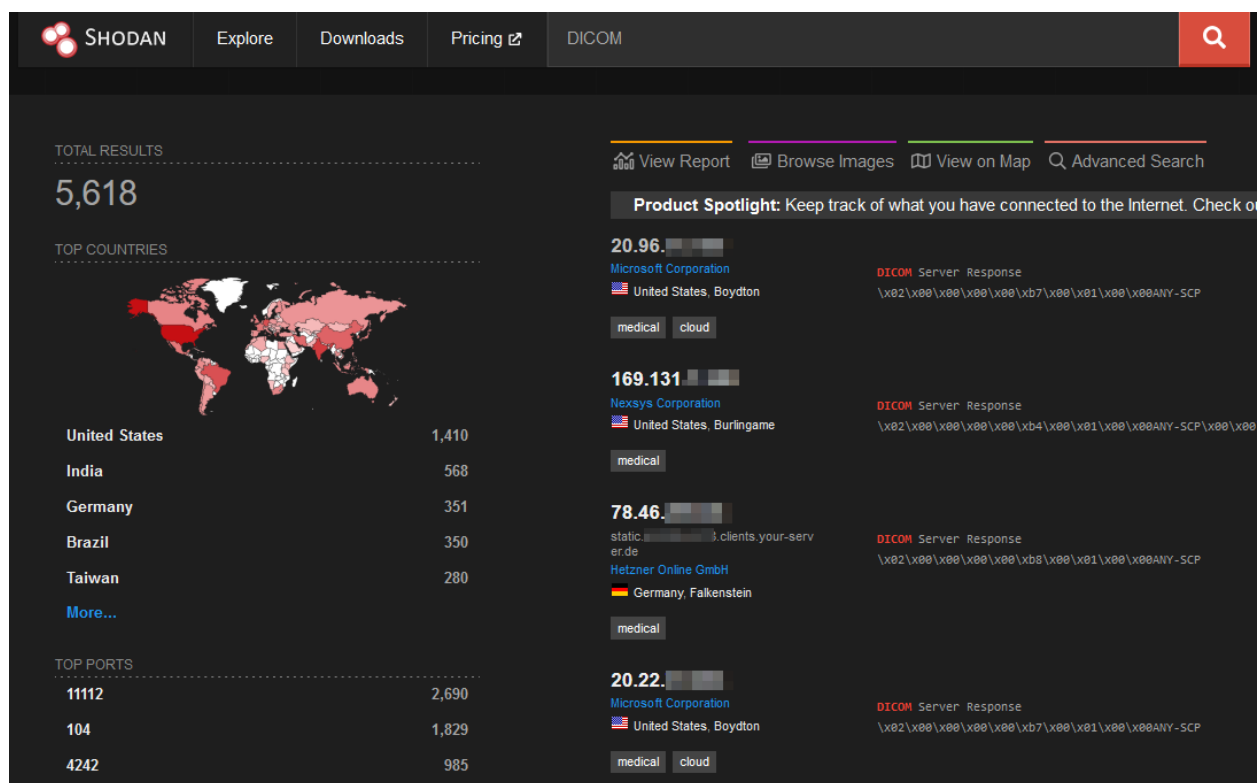
Kórházi információs rendszer

A modern kórházak működésének egyik legfontosabb eleme a kórházi információs rendszer, vagy HIS (Hospital Information System). Itt találhatóak a páciensek adatlapjai, az előjegyzések, a vizsgálatokról készült feljegyzések, leletek, sőt, akár számlázási információk is. Ez a digitális ökoszisztéma szükséges az ellátás folytonosságához, nélküle az intézmény folyamatai lelassulnak, csökken a kapacitás. Informatikai rendszer lévén ugyanúgy ki van téve kiberbiztonsági incidenseknek, melyek súlyosságát megsokszorozza a tény, hogy zavar esetén romlik az ellátás minősége, ezért veszélybe kerülhet a páciensek élete. [19], [20]

Képarchiváló és kommunikációs rendszer

A képalkotós eljárások, például röntgen, CT vagy MR által készített képi információk hatékony tárolását és megjelenítését leggyakrabban egy képarchiváló- és kommunikációs rendszerrel (PACS) valósítják meg. A konstrukció lényege, hogy összekapcsolja a képalkotó orvosi eszközöket, az adatbázist és az orvosok számítógépeit, így az elkészült képeket gyorsan és hatékonyan lehet tárolni és megtekinteni, nem szükséges azokat kinyomtatni és manuálisan szállítani. Az átvitel megvalósítására a DICOM (Digital Imaging and Communications in Medicine) szabvány által előírt fájlformátumot és TCP/IP protokollt alkalmazzák. Egy tipikus PACS implementáció négy fő részből áll: a képalkotó orvosi eszköz, egy biztonságos hálózat, az archívum és az orvosi munkaállomás. [21]

Ezek a képarchiváló rendszerek az orvosi információs infrastruktúrák fontos részét képezik, és az általuk kezelt adatok kifejezetten érzékenyek. Sajnálatos módon azonban előfordul, hogy a képek megjelenítéséhez és továbbításához alkalmazott szoftvereket figyelmetlenül telepítik, és azok nyíltan elérhetővé válnak nem csupán a belső hálózatról, hanem akár az Internetről is. A kutatás során a shodan.io internetes keresőmotorral a „DICOM” paraméterrel indított kereséssel 5618 egyedi eszközt találtam, amelyek az Internet felé nyitott DICOM porttal rendelkeznek. Ez azt jelenti, hogy illetéktelen személyek erre alkalmas szoftverek segítségével jelenleg ennyi eszközre csatlakozhatnak és megtekinthetik a tárolt felvételeket és páciens adatokat.



1. ábra: Internet felé nyitott DICOM portok 2024.10.20. -án (A szerző saját felvétele)

Elektronikus Egészségügyi Szolgáltatási Tér

Magyarországon az orvosi ellátás során keletkező adatok központi rögzítése, tárolása és intézmények közti megosztása a 2017-ben bevezetett Elektronikus Egészségügyi Szolgáltatási Tér-en (EESZT) keresztül történik. Az EESZT egy összetett informatikai rendszer, ami az összes egészségügyi intézmény kórházi információs rendszerét összeköti. Ez lehetővé teszi a kezelőorvosok részére a páciens kórtörténetéhez és alapadataihoz való gyors hozzáférést, illetve az új adatok, dokumentumok és receptek felvitelét.

Az eBeutaló modulban rögzíthetők az orvos által kiállított beutalók, amik azonnal megjelennek az illetékes szakrendelő rendszerében is, így nem szükséges a papír alapú beutalók használata. Minden ellátási eseményről bejegyzés készül az Eseménykatalógusba, amely tartalmazza az ellátó orvos és intézmény adatait, a vizsgálat időpontját és a felállított diagnózist. A betegellátás során keletkező dokumentumok, leletek pedig az eKórtörténetbe kerülnek, ahol a páciens és kezelőorvosai is könnyen hozzáférhetnek. A képalkotási módszerekkel készült felvételek a kórházak PACS rendszeréből az EESZT-be is feltöltődnek, illetve lehetőség van az elkészült felvételek intézmények közötti azonnali továbbítására is egy képküldő funkcióval. Az eProfil oldalon elérhetőek a páciens ritkán változó adatai, illetve alapállapotra, rendszeresen szedett gyógyszerekre vagy vércsoportra vonatkozó információi. Vényköteles gyógyszerek kiváltásához szükséges recepteket írhat az orvos az eRecept rendszer segítségével, az ide felírt gyógyszerek azonnal megtekinthetők a gyógyszerterákból, ezzel lényegesen egyszerűbb a receptre írt készítmények kiváltása. [22], [23]

Az EESZT tehát egy olyan szerteágazó információs infrastruktúra, ami nagyban megkönnyíti az egészségügyi szakemberek munkáját, az egészségügyi intézmények közötti hatékony információcsere biztosításával. Nagyban hozzájárul a lakosság tájékoztatásához is, az állampolgárok az EESZT felületén könnyen megtekinthetik saját adataikat. Emiatt viszont nagy mennyiségű titkos adatot tartalmaz, ezek kiszivárgása vagy elvesztése súlyos következményekkel járhat. Egy sikeres kibertámadás esetén az elkövetők potenciálisan hozzáférhetnek számos beteg adataihoz, hamis recepteket állíthatnak ki, vagy üzemzavart idézhetnek elő, súlyos csapást mérve az egészségügyi ellátásra országszerte.

Az egészségügyi rendszereket fenyegető kibertámadások típusai

Adatok ellopására vagy manipulációjára irányuló

A kórházi és intézményeket összekapcsoló informatikai rendszerek nagy mennyiségű titkos egészségügyi információt tartalmaznak, emiatt gyakran kerülnek a hackerek célkeresztjébe. A megszerzett adatokkal ellophatják a páciensek személyazonosságát, zsarolást vagy biztosítási csalásokat hajthatnak végre és eladhatják a feketepiacon. Az adatlopásra irányuló kibertámadások fő módszere a phishing, megtévesztő e-mailek vagy SMS üzenetek formájában. Ilyenkor a támadó magát egy megbízható személynek vagy szervezetnek kiadva, hamis információkkal próbál meg bejelentkezési adatokat kicsalni az áldozatától, vagy elérni, hogy egy gyanús linkre kattintva rosszindulatú programot telepítsen a számítógépére. A megszerzett belépési adatokkal ezután hozzáférhet érzékeny adatokat tartalmazó email fiókokhoz, munkaállomásokhoz vagy akár kórházi rendszerekhez. Egy ilyen adathalász támadás következtében 2015. februárjában mintegy 78 millió rekord szivárgott ki az Anthem Inc. (2022 óta Elevance Health) amerikai egészségbiztosítást kínáló cégtől, mert egy beszállító munkatársa rákattintott egy phishing emailre. A támadók több, mint 50 felhasználói fiókhoz fértek hozzá, és behatoltak a cég központi adatbázisaiba is. [24], [25]

Világszerte egyre gyakoribbak az adathalász támadások által okozott adatvédelmi incidensek, ezért kiemelten fontos megfelelően védekezni ellenük, főleg az olyan létfontosságú szektorokban, mint az egészségügy. Az első és legfontosabb a munkavállalók megfelelő biztonságtudatossági képzése. Hangsúlyozni kell a phishing támadások súlyos következményeit, és a dolgozók felelősségét az ilyen támadások megakadályozásában. Ajánlott phishing gyakorlatokat végezni, ezek folyamán adathalász emaileket küldünk ki a szervezetben, és megnézzük hány alkalmazott kattintott rá, így felmérhető az adathalászat elleni felkészültség szintje. Az emberi tudatosság mellett technikai megoldásokat is szükséges alkalmazni, például hatékony email szűrőket, amelyek törlik a nemkívánatos leveleket, hálózatzbiztonsági szoftvereket, melyek megakadályozzák az ismert támadó IP címek felé történő kommunikációt, és kétfaktoros hitelesítést, hogy az ellopott belépési adatokkal ne lehessen azonnal bejelentkezni.

Üzemzavar előidézésére, károkozásra irányuló

Az adathalászat mellett a másik legelterjedtebb, egészségügyet is érintő támadási forma a zsarolóvírusos támadás. A támadók behatolnak a rendszerbe, és a lehető legtöbb számítógépre

kártékony programot telepítenek, ami egy bizonyos idő elteltével, vagy manuális aktiválás után megtámadja és használhatatlanná teszi az eszközt amire telepítették. Ezután az érintett szervezet részére egy váltságdíj követelést továbbítanak, ebben pénzt követelnek a támadás leállításáért cserébe. Az egészségügyi létesítmények létfontosságú szolgáltatást biztosítanak, erre azonban képtelenek az információs rendszereik kiesése esetén. Ilyen helyzetben az ellátás akadózni kezd, a pácienseknek többet kell várniuk a kezelésre, a kritikus állapotban lévők kezelése is nehezebbé válik, műtéteket kell elhalasztani és más intézményekbe átirányítani az újonnan érkezőket. Minél tovább áll fent az üzemzavar, annál jobban romlanak a betegek kilátásai, növekszik az ellátási komplikációk száma és halálesetek is előfordulhatnak. [24], [26]

Ha egy intézmény nem rendelkezik megfelelő üzletmenet-folytonossági és katasztrófaelhárítási eljárásrendekkel, akkor valószínűbb, hogy kifizeti a váltságdíjat. Pontosán emiatt a zsarolóvírusos kampányok jövedelmező lehetőséget jelentenek a kiberbűnözőknek, mára már egész „iparág” alakult ki az internetes zsarolásból. Megjelentek a zsarolóvírus-kölcsönző, azaz Ransomware-as-a-Service (RaaS) szervezetek is. Ezeknek a „vállalkozásoknak” az üzleti modellje a következő: a zsarolóprogram fejlesztői előfizetésért cserébe biztosítják az eszközeiket és infrastruktúrájukat, amit bárki használhat támadások végrehajtására. Az előfizetők nem csak az eszközökhöz kapnak hozzáférést, hanem útmutatókat és támogatást is biztosítanak a fejlesztők, így bárki könnyedén elkezdhet zsaroló kampányokat indítani, ha a megszerzett váltságdíjat megosztja a RaaS csoporttal. A világon elkövetett ransomware támadások 24 százalékát tette ki 2023-ban az egyik legismertebb RaaS szervezet, a LockBit. Sajnálatos módon ez a módszer egyre elterjedtebbé válik, az Egyesült Államok Nemzeti Hírszerzési Igazgatósága által közzétett statisztikák szerint 2022 és 2023 között a duplájára nőtt az egészségügyi intézmények ellen elkövetett ransomware támadások száma. [27], [28]

Zsarolóvírusos támadások következményei az egészségügyi ágazatban

Orvosi ellátásra és gyógyulási kimenetelekre gyakorolt hatás

Amikor egy egészségügyi intézmény rendszerei elérhetetlenné válnak, az ellátás minősége sérül. Minden, egyébként számítógépek segítségével végzett feladatot analóg módon papíron, telefonon kell folytatni, ami gyakran kifejezetten bonyolult és nem minden esetben kivitelezhető. A személyzet leterheltsége megnő, a munkavégzés hatékonysága pedig lecsökken. Ennek következtében romlik az egészségügyi ellátás, bizonyos funkciók teljesen leállnak és az intézmény

befogadóképessége is korlátozódik. Kutatások igazolják, hogy egy kórház kevesebb beteget tud fogadni, miközben zsarolóvírusos támadás alatt áll és a kezelési folyamatok lassulása miatt a pácienseknek több időt kell eltölteniük az intézményben. A csökkentett befogadóképességből következik, hogy a környező intézmények forgalmában is emelkedés mutatható ki az átirányított betegek érkezése miatt, így a kiesés a régió egészségügyi ellátórendszerét is leterhelheti. Az ellátás minőségének romlása egyúttal a páciensek gyógyulását és kilátásait is befolyásolja, a kórházi rendszerek kiesése esetén megnő a komplikációk és a halálozások száma is. Például műtétek elhalasztása, nem megfelelő gyógyszerek beadása a páciens adatlapjának hiányában, vagy mentővel érkező sérültek átirányítása miatt könnyedén előfordulhatnak egyébként elkerülhető halálesetek. [29], [30]

Adatszivárgás és adatvesztés

Az egészségügyi adatok bizalmosságára minden országban szigorú törvényi előírások vonatkoznak. Magyarországon a 2011. évi CXII. információs önrendelkezési jogról és az információszabadságról alkotott törvény így határozza meg az egészségügyi adat fogalmát: *“egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.”*[31]. Ezek az érzékeny információk tehát a betegek személyéről, kórtörténetükről és egyéb magánjellegű részletekről szólnak. Rossz kezekbe kerülve felhasználhatóak zsarolásra, személyazonosság eltulajdonítására vagy biztosítási csalások elkövetésére. Éppen ezért értékesnek számítanak bűnözői körökben, fekete piacokon, így a kiberbűnözők egyre gyakrabban fosztanak ki egészségügyi rendszereket és adatbázisokat haszonszerzés céljából. [24], [32]

Anyagi károkozás

Zsarolóvírusos támadás esetén az érintett szervezetnek megfelelő vészhelyzeti tervek és tartalékok nélkül súlyos anyagi megterheléssel kell számolnia. Például, ha kifizeti a zsarolók követeléseit, amelyek igen nagy összegeket érhetnek el. Ellenkező esetben pedig a megfertőzött infrastruktúra helyreállítása is rengeteg pénzt emészt fel. Az alkalmazott vírus működésétől függően lehetséges a kompromittált számítógépek újratelepítése és üzembe helyezése, azonban előfordul, hogy az adatok titkosítása tönkretesz olyan kritikus programokat is, amik nélkül egyes alkatrészek vagy eszközök használhatatlanná válnak és cserére szorulnak. [29]

A rendszer leállása alatt a kórházi folyamatok lelassulnak és bonyolultabbá válnak, ezért a munkavállalók terhelése megnő, túlórára és kiegészítő személyzet behívására is szükség lehet, ami további költségeket jelent. A helyreállításnál kiemelten jelentkezik ez a probléma, ha a kórháznak vagy szolgáltatónak nincs, vagy nem megfelelő a saját incidenskezelő és IT üzemeltető személyzete, ekkor harmadik féltől szükséges felbérelni szakértőket. [33]

Egy adatszivárgással járó incidens esetén az egészségügyi szolgáltatókat súlyos bírságok megfizetésére kötelezhetik, mert nem biztosítottak megfelelő védelmet a páciensek érzékeny adatainak. A kiszivárgott adatok, gyógyulási komplikációk vagy halálesetek miatt pert indíthatnak a kórház ellen az érintettek, ennek következtében előfordulhat, hogy a kórháznak kártérítést kell fizetnie. [32]

Súlyos kórházi kibertámadások a közelmúltban

Düsseldorfi Egyetemi Kórház

Egy zsarolóvírus fertőzte meg 2022. szeptemberében a németországi Düsseldorf Egyetemi Kórház hálózatát. A támadás megbénította az ellátás biztosításához szükséges információs rendszereket, így a sürgősségi osztály betegadminisztrációs alkalmazását is, így lehetetlenné vált az újonnan érkezők fogadása. Ennek következtében szeptember 11.-én egy kritikus állapotban lévő embert szállító mentőautót útközben átirányítottak egy 30 kilométerre fekvő másik kórházba. A páciens azonban útközben életét veszítette. Hivatalosan sem a kórház, sem az illetékes hatóság nem mutatott ki kapcsolatot a kiberbiztonsági incidens és a haláleset között, ettől függetlenül feltételezhető, hogy a beteg halálához hozzájárult a kórházi információs rendszerek elérhetetlensége. [34], [35]

Health Service Executive

Írország egészségügyi ellátásért felelős szervezetét 2021. májusában érte kiterjedt ransomware incidens. A Health Service Executive akkoriban 54 kórház működtetését látta el, információs infrastruktúrájában ekkor több, mint 4500 szerver és 70 000 felhasználói eszköz működött. Biztonsági intézkedéseik ellenére egy adathalász email rosszindulatú csatolmányán keresztül a Conti zsarolóvírus szétterjedt a teljes hálózaton, és május 14.-én az összes csatlakoztatott számítógépet működésképtelenné tette. Írország egészségügyi ellátására kifejezetten súlyos hatást gyakorolt a támadás, az okozott károk és az egészségügy szinte teljes elérhetetlenségét látva az

elkövetők május 21.-én önszántukból átadták a titkosítás feloldásához szükséges kulcsot. Válságdíjkövetelésüket az ellopott egészségügyi adatok fejében továbbra is fenntartották, de a HSE nem fizetett, azóta az adatok sorsa ismeretlen. Még a titkosítás kulcsával is több, mint 4 hónapba telt, mire a hálózat minden szolgáltatását helyreállították, ehhez kétségtelenül hatalmas anyagi ráfordításra volt szükség. [29]

Összegzés

Az egészségügyi ellátás hatékony biztosításához minden intézménynek számos információs hálózatra van szüksége. Ezeket a digitális rendszereket létfontosságú szerepük és bizalmas adattartalmuk miatt egyre gyakrabban érik kibertámadások világszerte. Kijelenthető, hogy az egészségügyi rendszerek információs infrastruktúráit érintő kiberbiztonsági incidensek súlyos károkat okoznak, befolyásolják a betegek jólétét és gyógyulását, a gyakran nem megfelelő forrásokkal rendelkező intézményekre pedig óriási anyagi terheket rónak. Sajnos azonban jelenleg még nem létezik olyan ágazatspecifikus szabályozás, ami korszerű intézkedések, például üzletmenet-folytonossági és katasztrófa visszaállítási eljárásrendek bevezetését írná elő az egészségügyi szektor szereplőinek. Az egészségügy magas szintű kiberbiztonságának eléréséhez szükséges jogszabályi háttér és támogatás minden nemzet számára létfontosságúvá vált.

KONKLÚZIÓ

A társadalom jólétének fenntartásához szükséges alapvető szolgáltatások biztosításában szerepet játszó kritikus infrastruktúra rendszerek ma már világszerte infokommunikációs technológiákat alkalmaznak. Ezek az információs rendszerek lehetővé teszik az üzemeltetéshez szükséges adatok hatékony továbbítását és feldolgozását a kibertéren keresztül, egyúttal azonban új támadási felületeket nyitnak meg. A létfontosságú rendszerek ellen elkövetett kibertámadások pedig képesek olyan üzemzavarokat okozni, amelyek a lakosság jólétét és biztonságát fenyegetik.

A villamosenergia-hálózatok a modern világ ütőerei, nélkülük elképzelhetetlen a társadalom működése, az élet minden egyes területére befolyással vannak. Nélkülük számos olyan folyamat leáll, amit a mindennapi életben alapvetőnek tekintünk, hiányuk pedig súlyos következményekkel jár. A digitalizált ipari irányítási rendszerek elterjedésével az áramszolgáltatáshoz szükséges berendezések és üzemek kiberbiztonsági kockázatai jelentősen megnövekedtek. Számos példa van rá, hogy rosszindulatú csoportok az elektromos hálózat megbénításával próbálták elérni céljaikat, kifejezetten erre a célra tervezett kártékony programokkal és támadási technikákkal.

Az egészségügyi intézmények feladata a lakosság egészségének megőrzése színvonalas egészségügyi szolgáltatások biztosításával, ehhez azonban mostanra elengedhetetlenek a jól működő információs rendszerek. Az orvosi ellátást támogató informatikai infrastruktúra nagyban hozzájárul a hatékony munkavégzéshez, elérhetetlenné válása ezért nagy mértékben korlátozza a kórházak kapacitását és az általuk nyújtott szolgáltatások minőségét. Mindez hatással van a páciensek gyógyulására is, elmondható, hogy a kibertámadások növelik a komplikációk és halálozások számát az érintett intézményekben.

A létfontosságú rendszerek, kifejezetten a villamosenergia-hálózatok és az egészségügyi intézmények kiesése katasztrófákat idézhet elő, ezért biztonságuk garantálása minden ország életbevágóan fontos feladata. Minden évben növekszik a világon elkövetett kibertámadások száma, ezért a kritikus létesítményekben található informatikai eszközök védelmére szigorú kiberbiztonsági intézkedések bevezetése szükséges. Ezt felismerve számos közösség tevékenykedik az alapellátás kiberbiztonságának fejlesztésén, napjainkban azonban még gyakoriak a hiányosságok és a felkészületlen szervezetek.

HIVATKOZOTT IRODALOM

- [1] K. László, *A KIBERTÉR VÉDELME*. Budapest: Dialóg Campus Kiadó, 2018.
- [2] „A kritikus infrastruktúra védelmi fogalmi rendszere, hazai és nemzetközi szabályozása”. Katasztrófavédelmi Tudományos Tanács. Elérés: 2024. március 19. [Online]. Elérhető: <https://www.vedelem.hu/letoltes/anyagok/382-a-kritikus-infrastruktura-vedelem-fogalmi-rendszere-hazai-es-nemzetkozi-szabalyozasa.pdf>
- [3] K. László és H. Zsolt, „Kritikus infrastruktúrák és kritikus információs infrastruktúrák”. Katonai Üzemeltető Intézet, 2012.
- [4] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
- [5] „The State of Ransomware 2024”, ransomware.org, 2024. Elérés: 2024. október 12. [Online]. Elérhető: https://ransomware.org/wp-content/uploads/2024/03/2024-State-of-Ransomware-Report_v1.pdf
- [6] „The State of Ransomware 2023”, Sophos, 2023. Elérés: 2024. október 12. [Online]. Elérhető: <https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf>
- [7] J. Beerman, D. Berent, Z. Falter, és S. Bhunia, „A Review of Colonial Pipeline Ransomware Attack”, in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, Bangalore, India: IEEE, máj. 2023, o. 8–15. doi: 10.1109/CCGridW59191.2023.00017.
- [8] S. Firer-Blaess, *The collective identity of Anonymous: web of meanings in a digitally enabled movement*. Uppsala: Acta Universitatis Upsaliensis, 2016.
- [9] N. Beach-Westmoreland, J. Styczynski, és S. Stables, „When the lights went out - A comprehensive review of the 2015 attacks on Ukrainian critical infrastructure”. Booz Allen Hamilton, 2016. november. Elérés: 2024. március 30. [Online]. Elérhető: <https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>
- [10] SeConSys, *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve 2022*. Nemzeti Kibervédelmi Intézet, 2023. [Online]. Elérhető: https://nki.gov.hu/wp-content/uploads/2023/02/SeConSys_online_kezikonyv_aktualizalas_2022_tortenese_kialapjan.pdf
- [11] „Dragonfly: Cyberespionage Attacks Against Energy Suppliers”. Symantec, 2014. július 7. Elérés: 2024. november 3. [Online]. Elérhető: https://web.archive.org/web/20140801093235/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
- [12] A. Cserhádi, „A Stuxnet vírus és az iráni atomprogram”, *Nukleon*, köt. IV., sz. 85, márc. 2011, Elérés: 2024. március 17. [Online]. Elérhető: http://nuklearis.hu/sites/default/files/nukleon/Nukleon_4_1_85_Cserhati_.pdf
- [13] A. Cherepanov, „WIN32/INDUSTROYER A new threat for industrial control systems”. ESET, 2017. június 12. Elérés: 2024. március 30. [Online]. Elérhető: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf
- [14] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS 460/2004/EK RENDELETE az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról*. 2004.

- [15] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022. december 14-i (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv).* 2023.
- [16] 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről.
- [17] *A BIZOTTSÁG (EU) 2024/1366 FELHATALMAZÁSON ALAPULÓ RENDELETE az (EU) 2019/943 európai parlamenti és tanácsi rendeletnek a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjaira vonatkozó ágazatspecifikus szabályokról szóló üzemi és kereskedelmi szabályzat létrehozása révén történő kiegészítéséről.* 2024.
- [18] É. Szolnoki, „Határkeresztező villamosenergia áramlás kibervédelmi szabályozása (NCCS)”, SeConSys, 2024. június 14.
- [19] Xudong Lu, Huilong Duan, Haomin Li, Chenhui Zhao, és Jiye An, „The Architecture of Enterprise Hospital Information System”, in *2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, Shanghai, China: IEEE, 2005, o. 6957–6960. doi: 10.1109/IEMBS.2005.1616106.
- [20] C. Brook, „What is a Health Information System?”, Data Insider. Elérés: 2024. október 17. [Online]. Elérhető: <https://www.digitalguardian.com/blog/what-health-information-system>
- [21] R. H. Choplin, J. M. Boehme, és C. D. Maynard, „Picture archiving and communication systems: an overview.”, *RadioGraphics*, köt. 12, sz. 1, o. 127–129, jan. 1992, doi: 10.1148/radiographics.12.1.1734458.
- [22] J. Kókai, „EESZT Kisokos”. KOPIFO Számítástechnikai Kft., 2017. október 10. Elérés: 2024. október 24. [Online]. Elérhető: <https://web.archive.org/web/20201025022718/http://files.kopifo.hu/200000168-b0fd3b1f6a/EESZT%20kisokos.pdf>
- [23] „Az EESZT működése és szolgáltatási moduljai”, EESZT Információs portál. Elérés: 2024. október 24. [Online]. Elérhető: <https://e-egeszsegugy.gov.hu/az-eeszt-mukodese>
- [24] U.S. Department of Health and Human Services, „Types of Cyber Threat Actors That Threaten Healthcare”, Health Sector Cybersecurity Coordination Center, 2023. június 8. Elérés: 2024. október 17. [Online]. Elérhető: <https://www.hhs.gov/sites/default/files/types-threat-actors-threaten-healthcare.pdf>
- [25] S. Alder, „Healthcare Data Breaches Due to Phishing”, *HIPAA J.*, jan. 2024, Elérés: 2024. október 26. [Online]. Elérhető: <https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/>
- [26] A. M. Freed, „The Impact of Ransomware in the Healthcare Sector”, maliciouslife. Elérés: 2024. október 26. [Online]. Elérhető: <https://www.cybereason.com/blog/the-impact-of-ransomware-in-the-healthcare-sector>
- [27] „Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double”. Office of the Director of National Intelligence, 2024. február 28. Elérés: 2024. október 26. [Online]. Elérhető: https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf
- [28] Kaspersky, „What is ransomware as a service?”, Kaspersky Resource Center. Elérés: 2024. október 26. [Online]. Elérhető: <https://www.kaspersky.com/resource-center/definitions/what-is-ransomware-as-a-service>

- [29] M. I. Mashinchi, T. Acton, és P. M. Datta, „When healthcare becomes sick: Recovering from ransomware”, *J. Inf. Technol. Teach. Cases*, aug. 2024, doi: 10.1177/20438869241279443.
- [30] R. Abouk és D. Powell, „Ransomware Attacks, ED Visits and Inpatient Admissions in Targeted and Nearby Hospitals”, *JAMA*, köt. 331, sz. 24, o. 2129, jún. 2024, doi: 10.1001/jama.2024.7752.
- [31] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
- [32] S. Adler, „Healthcare Data Breach Statistics”, The HIPAA Journal. Elérés: 2024. november 3. [Online]. Elérhető: https://www.hipaajournal.com/healthcare-data-breach-statistics/?utm_source=brevo&utm_campaign=Kiber_III19_20241004&utm_medium=email
- [33] A. M. Stowman és mtsai., „Anatomy of a Cyberattack: Part 1: Managing an Anatomic Pathology Laboratory During 25 Days of Downtime”, *Am. J. Clin. Pathol.*, köt. 157, sz. 4, o. 510–517, ápr. 2022, doi: 10.1093/ajcp/aqab145.
- [34] „Cyber-Angriff auf Uniklinik Düsseldorf: BSI warnt vor akuter Ausnutzung bekannter Schwachstelle”, Bundesamt für Sicherheit in der Informationstechnik. Elérés: 2024. november 3. [Online]. Elérhető: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html
- [35] „Was this the World’s First Fatal Cyberattack?”, SecureWorld. Elérés: 2024. november 3. [Online]. Elérhető: <https://www.secureworld.io/industry-news/fatal-cyberattack-killer-ransomware-attack>