HADMÉRNÖK

XIV. Évfolyam 1. szám – 2019. március

ELEKTRONIKUS HATÁRVÉDELMI RENDSZEREK JELLEMZŐ SEBEZHETŐSÉGEI ÉS VÉDELMÜK LEHETŐSÉGEI

COMMON VULNERABILITIES OF ELECTRONIC PERIMETER PROTECTION SYSTEMS AND POSSIBLE METHODS OF THEIR DEFENSE

KRALOVÁNSZKY Kristóf

(ORCID: 0000-0002-5560-3525)

kralovanszky.kristof@d-systems.hu

Absztrakt

Létfontosságú rendszerelemek (kritikus infrastruktúrák) infokommunikációs rendszereinek megfelelő kibervédelme az üzemeltető társaságok egyre nyomasztóbb kihívása. Jelen írás célja, hogy egy speciális alrendszeren keresztül bemutassa azokat a kiber-sérülékenységeiket, melyekkel szemben védekezniük szükséges. Ismerteti az elektronikai védelemmel kapcsolatos megoldási lehetőségeit, különösen a SIGINT tevékenységek elleni védekezés vonatkozásában. A bizalmasság, sértetlenség és rendelkezésre állás hármassága egyidejű megteremtésének és megtartása szükségességének hangsúlyozása mellett rámutat a megfelelő kiberfenyegetettségi kockázatelemzések elengedhetetlenségére.

Kulcsszavak: *Kritikus infrastruktúra, kibervédelem, elektronikai védelem, elektronikus határvédelmi rendszer, kritikus információs infrastruktúra*

Abstract

Both owners and operators of critical infrastructures are facing a rapidly growing challenge of defending themselves and their infocommunication systems from various cyber threats. This article wishes to demonstrate the cyber vulnerabilities of electronic perimeter protection systems and the need for their adequate protection. Shows certain possibilities of using Electronic Protection (EP) with particular emphasis on protection against various SIGINT threats. Underlines the absolute necessity of cyber threat risk-analysis and assessment, while creating and maintaining system-wide confidentiality, integrity, and availability.

Keywords: *Critical infrastructure, Cyber threat, Electronic protection, Electronic perimeter protection, Critical information infrastructure*

A kézirat benyújtásának dátuma (Date of the submission): 2019.02.12.
A kézirat elfogadásának dátuma (Date of the acceptance): 2019.03.17.

BEVEZETÉS

Határvédelmi (perimeter protection) rendszerek fogalma több különböző telepítési funkciót jelenthet, de a meghatározásokban közös, hogy valamilyen jogi (adminisztratív), vagy katonai terület elhatárolást valósítanak meg fizikai és műszaki (technológiai) eszközökkel. Így tehát ugyanúgy határvédelmi megoldásról beszélünk egy kritikus infrastruktúra[1] külső kerítése esetén, mint egy ország államhatárának vonatkozásában. Számos példa van arra is, hogy többszörös lehatárolást alkalmaznak egy adott létesítményen belül, amennyiben a különböző fizikai biztonsági zónákra osztás valamilyen kockázat kezelése miatt szükséges.[2] Az így megvalósuló zónahatárok ugyanúgy értelmezhetők (és megvalósíthatók) külterületen, mint épületen belül. Utóbbinak egyik leginkább jellemző formája a minősített adatkezelést végző területek elhatárolása a munkavégzés egyéb helyszíneitől.

Döntő többségükben tehát valamilyen fenyegetettség, vagy biztonsági kockázat kezelését végzik a határvédelmi rendszerek, így hatékonyságuk mérésének legjobb módja a fenyegetettségek által meghatározott kockázatok csökkentésének képessége, illetve az üzemelésük során bekövetkező olyan biztonsági incidensek csökkenő mennyisége melyek eredményeként a védett területre illetéktelen belépés történik. Nyilvánvalóan az adott rendszer biztonsági eseményeinek jelentős számát a behatolási próbálkozások, illetve védelmi képességek módosításának, vagy korlátozásának kísérletei fogják adni.

Határvédelmi rendszereknek két fő értelmezése ismert: az egyik a fizikai változat, ahol valamilyen fizikai határvonal védelmét látják el mechanikus és elektronikus eszközök, míg a másik az infokommunikációs megvalósulás, ahol a határvonal egy számítógépes hálózat, vagy alrendszer határa (router, tűzfal, egyéb speciális hardveres és szoftveres védelmi eszközök) és ennek jellemzően IP szintű védelmét / felügyeletét látják el az adott informatikai eszközök (vagyis az utóbbi esetben hangsúlyosan nem mechanikai védelemről van szó). Szinte tökéletesen ugyanarról a logikai vázról van szó mindkét esetben, csupán a felhasznált eszközök fizikai megvalósulása és a rendszerrel felügyelt terület különbözik: az egyik a fizikai térben jelenik meg, míg a másik a kibertérben létezik. Az egyik rendszer logikai folyamatai és kihívásai gyakorlatilag egyenértékűen jelennek meg a másikban.

Határvédelmi rendszerek további jellemzője, hogy majdnem minden esetben legalább egy mechanikai és egy elektronikai alrendszerből állnak.[3] Mechanikai komponens nélkül csupán felügyeleti, vagy megfigyelő rendszerről beszélhetünk. Igaz ugyanakkor az is, hogy az elektronikai részben egyre növekvő arányt képvisel a videotechnikai megfigyelés – részben az elkövetés jogi bizonyíthatósága, részben a magas információtartalma miatt. Bizonyos rendszerek a mechanikai védelem mellett szinte kizárólag videotechnikai megfigyelést valósítanak meg.

A biztonsági kockázatok nem fizikai részének legnagyobb százaléka a kibertérből[4] fog érkezni, mivel a határvédelmi rendszerek elektronikus komponensei hálózatba kapcsolt

[1] Hatályos honi jogi szabályozás szerint (2012. évi CLXVI. törvény) a hivatalos megnevezés létfontosságú rendszerelem. Nemzetközileg elfogadott elnevezés szerint a kritikus infrastruktúra és kritikus információs infrastruktúra megnevezést használjuk.

[2] A többszörös biztonsági zónák jellemzően repülőtereken, robbanóanyagot tároló telephelyeken, vagy jelentős biztonsági kockázat-különbséggel bíró területek elválasztásánál valósulnak meg.

[3] Mindezek kiegészülhetnek egyéb komponensekkel, melyek valamilyen aktív védelmi feladatot látnak el, például kinetikus technológiát alkalmazó kialakítással.

[4] A kibertér fogalmára számos meghatározás létezik, melyek közül a következőt használom: „Ember által mesterségesen létrehozott dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt, és az elektromágneses

infokommunikációs eszközök. Mindezekhez hozzájárul, hogy az ilyen rendszerek által gyűjtött, tárolt feldolgozott és továbbított információ mások számára komoly értéket képviselhet, illetve a támadások a rendszer, vagy az információ sérülése az üzemeltetőinek (vagy felettes szervezetének) komoly kárt okozhat. Ennek elsődleges eredője, hogy a védett területre való bejutás jelentősen könnyebbé válik, a határsértés folyamatának képi dokumentáltsága csökken, vagy egyéb módon megváltozik. Eredményét tekintve tehát, a behatoló azonosíthatósága nehezebb (vagy lehetetlen) lesz, és illetéktelen személyek ismeretlen feladatokat hajthatnak végre a védett területen belül. A folyamat végén pedig akár jelentősen is megnő az adott szervezet sérülékenységi kitettsége, mely kritikus infrastruktúrák és kritikus információs infrastruktúrák esetén akár fokozott nemzetbiztonsági kockázatot is eredményezhet.

Jelen tanulmány fizikai értelmezésben kezeli a határvédelmi rendszereket és célja, hogy bemutassa azok a főbb elektronikai sérülékenységeit, melyek az adott rendszer jelzési képességeit csökkentik, illetve lehetséges megoldásokat javasoljon a védelmi képesség megőrzésére, illetve a támadások bizonyos formáinak megakadályozására.

ELEKTRONIKAI VÉDELEM IGÉNYE

Az üzemeltetett (felügyelt) elektronikus megfigyelő, ellenőrző, feldolgozó és adattovábbító rendszerek nyilvánvalóan védelmet igényelnek, hogy képességeik korlátozása, vagy módosítása jogosulatlan személyek által ne legyen végrehajtható, illetve a bennük tárolt adatok illetéktelenek számára ne legyenek hozzáférhetők (így módosíthatók, vagy törölhetők). Elektronikai hadviselési terminológiát használva ezt nevezzük elektronikai védelemnek. [1]

Hibrid hadviselés[5] során a támadó számára valódi értéket az összes közül azok a kritikus (információs) infrastruktúrák fogják jelenteni, melyek a legkisebb támadási „befektetéssel" a legnagyobb kárt tudják okozni. Fontos különbséget tenni a kinetikus és az elektronikai- és/vagy kibertámadás között: nyilvánvaló, hogy egy jól tervezett és kivitelezett kinetikus támadás hatalmas kárt tud okozni (például egy erőműben) ám annak hatékony megvalósítása rendkívül nehézkes és körülményes. A támadó választása tehát vélhetően az elektronikai megoldásra fog esni – mely szintén képes igen jelentős károkat okozni.[6]

Fontos szempont továbbá, hogy különbséget tegyünk az információbiztonság és az informatikai biztonság között. [2] Mindkettő elérendő cél, illetve teljesítendő feladat, de az ahhoz szükséges eszközök és megoldások jelentősen különbözőek lehetnek. Az egyik a másik nélkül azonban nem fog tudni megvalósulni.

Az alkalmazott érzékelők rendszereinek összetettsége egyenes arányban növekszik a védendő objektum stratégiai, nemzetbiztonsági értékével. Ahogy már nem rendvédelmi szintről van szó és egyre inkább közelítünk (vagy elérjük) a katonai szintű védelmet, fognak megjelenni a bonyolultabb és kifinomultabb rendszerek.

Egy ország államhatárának védelmét végző elektronikus rendszerek rendkívül speciális esetei a határvédelmi megoldásoknak, egyrészt mert általában nagy kiterjedésűek (a védelmi vonal jellemzően meghaladja a 100 km-t) és adott esetben kiemelten komplex kockázatot kezelnek. Sajátosságuk továbbá, hogy honi eszközökkel és erőforrásokkal csak az egyik oldaluk

spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot." [16]

[5] Vö. Szenes Zoltán ny. vezérezredes: A katonai biztonság reneszánsza [17]

[6] Elegendő az iráni urándúsító centrifugákat ért támadások által okozott kárra gondolni, melynek során a Stuxnet számítógépes kártevő jelentős számú centrifugát tett végérvényesen használhatatlanná és vetette hónapokkal, évekkel vissza az iráni atomprogramot.

védhető.[7] Elmondható még, hogy számos párhuzamos szenzorrendszert üzemeltetve és nagy számú egyéb alrendszerre támaszkodva a legösszetettebb és legbonyolultabb megoldások közé tartoznak. [3] Így például regionális vezetési központokból végrehajtva, egységesen koordinálva: a videotechnikai megfigyelő rendszere összeköttetésben lehet az adott ország arcfelismeréshez szükséges biometrikus adatokat tartalmazó rendszerével, gépjármű nyilvántartásával (rendszámfelismeréshez); fel lehet szerelve földbe telepített akusztikus érzékelőkkel, kerítésre telepített rezgésérzékelőkkel; alkalmazhat telepített és kézi üzemeltetésű, látható fény- és infravörös tartományban működő kamerákat; videotechnikai rendszere elektronikus személy- és objektumkövető technológiákkal lehet kiegészítve; reagáló erők képesség alapú vezénylés támogatását végezheti; csatlakozhat más szervek egyéb megfigyelő rendszereihez és azokból automatikusan adatokat emelhet át.

A rendelkezésre álló technológiák csökkenő ára és növekvő elérhetősége ugyanakkor egyre vonzóbbá teszi az ilyen rendkívül összetett rendszerek szélesebb körű polgári alkalmazását, anélkül, hogy ehhez a megfelelő telepítői és üzemeltető szaktudás és tapasztalat szükségszerűen rendelkezésre állna – különösen a rendszerintegrációs oldalon. Ez nagyon könnyen eredményezhet egyrészt hamis biztonságérzetet a rendszer tulajdonosában, másrészt instabil, vagy hibás működést okozhat – főként paraméterezési hibák miatt. Rosszabb esetben a rendszerben sérülékenység jön létre, mely lehetőséget biztosít egy támadónak az adott sérülékenység kihasználására. Amennyiben a kihasználás valamilyen infokommunikációs rendszeren keresztül történik, beszélhetünk kibertámadásról. Adott sérülékenység megjelenése egy rendszerben nem szükségszerűen fog támadást eredményezni, hiszen a támadónak először tudnia kell, hogy a sérülékenység ott egyáltalán jelen van. Igaz ugyanakkor az is, hogy vannak típusos sérülékenységek: például adott gyártók hardvereiben, illetve szoftvereiben meglévő dokumentált hibák. Sokszor ezek akár önmagukban is képesek „meghívóként" szolgálni egy támadó számára.

Minden olyan elektronikus rendszer, ami valamilyen hálózati komponenssel [8] rendelkezik, kitett lesz kibertámadásoknak, melyek bekövetkezési valószínűsége arányosan növekszik az adott rendszer lehetséges sérülékenységeivel, illetve a benne tárolt, feldolgozott, vagy rajta átmenő adatok értékével, A kibervédelem és az elektronikai védelem között nem választani kell, hanem meg kell találni azt az optimális szakmai megoldást, ahogy egymást kiegészítik és támogatják, annak érdekében, hogy az adott rendszernek a lehető legmagasabb védelem biztosítható legyen.

A növekvő számú sérülékenységek ugyanígy növekvő számú kibertámadási lehetőséget hordoznak magukban, vagyis a jelentős technológiai fejlődés szinte automatikusan hozza magával e támadási forma rendkívüli terjedését és az adott rendszerbe való behatolási eszközeként történő kihasználását.

Nem elhanyagolható ugyanakkor, hogy egy támadó és az üzemeltető számára nem mindig ugyanaz és ugyanakkora a megszerzendő / védendő érték, különösen, ha a támadás egy sorozat, vagy folyamat része és a konkrét támadás egy lépcsőfok csupán valamilyen „magasabb" cél eléréséhez.[9]

---

[7] Egy kritikus infrastruktúra esetében igaz ugyan, hogy a védelmet elsődlegesen megvalósító szervezet a saját területi határain belül végezheti csak a tevékenységét, de a terület határán kívül rendelkezésre állnak a honi rendvédelmi erők.

[8] Függetlenül attól, hogy külső (internetes), vagy belső (internet nélküli) hálózatról van szó

[9] A „magasabb" cél természetesen a támadó szemszögéből értendő és az ő céljainak elérése szempontjából értékelt.

ÖSSZADATFORRÁSÚ HÍRSZERZÉSI TEVÉKENYSÉG, MINT A HATÁRVÉDELEM RÉSZE

Legyen szó bármilyen védekezési módról, az első és talán legalapvetőbb – a feladatok meghatározását követően – objektív és alapos, szakmai alapokon nyugvó kockázatelemzés elvégzése, melynek kiemelten fontos része a lehetséges (adott esetben dinamikusan változó) veszélyeztetettség megállapítása (becslése), illetve ezzel párhuzamosan a védendő technológia/infrastruktúra értékének meghatározása. [4]

Változó kockázat esetében a valódi kihívás az aktuális fenyegetettség pontos ismerete, mert nélküle vagy túlzott lesz a védekezés, vagy nőni fog (akár jelentősen is) az illetéktelen behatolók száma. Megjelenhet tehát egyfajta hírszerzési komponens mely a szükséges információs hátteret biztosítja a védekezést ellátó szervezetek felé. Ez az adatforrás lehet a védelmi rendszernek is része, egyfajta korai figyelmeztető/riasztó (early warning) hálózatként, ilyen esetben azonban az adott hálózat védelmét is a teljes rendszer védelmének részeként kell biztosítani.

Államhatár védelmi rendszereknél jelenik meg jellemzően a földi vezérlésű légijárművek[10] által nyújtott képi hírszerzés (IMINT)[11] akár honi, akár idegen, mélységi légtérből. Ugyanígy, jóval nagyobb magasságban, a FRONTEX[12] a 2015-ös migrációs események során kezdett el aktívan használni és a tagállamok között megosztani műholdas megfigyelésből származó IMINT adatokat. [5],[6]

Vizsgáljuk meg, hogy melyek azok a hírszerzési ágak, melyek egy határvédelmi rendszer esetében megjelennek. A felsorolás jellemzően katonai terminológiát használ, de tartalmi elemeiben egy civil rendszernél is ugyanez történik, azzal a kitétellel, hogy minden ág végezhető civilek számára is jogszabályi kereteken belül, így az alkalmazott eszközök és egyéb technikák fogják a határvonalat jelenteni a törvényesen bárki által végezhető és a titkosszolgálati tevékenység között.

Az első nagy csoportban az adott rendszerben az üzemeltetés oldalán az IMINT, illetve a technikai jelfelderítés (MASINT[13]) a két meghatározó forrás. E két felderítési formát maga a telepített technika és a kialakított hálózata valósítja meg, a látható és nem látható fény tartományokban működő kamerák, valamint az egyéb optoelektronikai, radar-, és/vagy akusztikus szenzorok segítségével. Így biztosítható az adott pillanat, vagy következő órák (esetleg egy-két nap) határvonalon, vagy annak szűk környezetében fellépő fenyegetettségeinek megismerése. Más megközelítésben mondhatjuk, hogy ezek jellemzően taktikai, vagy harcászati szintű információk.[14] [7]

A második csoportban, egy rendszer közvetlen tulajdonosa – például egy rendvédelmi szervezet – nem minden esetben rendelkezik titkosszolgálati eszközökkel, de a felettes szerve (irányító szakminisztérium) megfelelő csatornáin keresztül már végez emberi erővel végrehajtott hírszerzést (HUMINT), rádióelektronikai felderítést (SIGINT[15]) és nyílt forrású hírszerzést (OSINT[16]). E három forrásból szerezhetők be azok a rendkívül értékes adatok,

[10] Angol terminológiában Unmanned Aerial Vehicle (UAV).
[11] IMINT – Imagery Intelligence. Nem csupán légijárműből, vagy nagy magasságból végzett, hanem bármilyen képi hírszerzésre vonatkozik.
[12] FRONTEX - Az Európai Unió szárazföldi- és tengeri határ védelmi ügynöksége (European Border and Coast Guard Agency)
[13] MASINT – Measurement and Signature Intelligence
[14] A különböző harcászati szintű információk összesítése és feldolgozása pedig már bőséggel szolgálhatja a hadműveleti, vagy hadászati szintet.
[15] SIGINT – Signals Intelligence
[16] OSINT – Open Source Intelligence

melyek segítségével a közeli (hetek), vagy a távolabbi jövő (hónapok) fenyegetettségeinek egy része megismerhető.

Ha a két nagy csoport hírszerzési forrásait összegezzük és kiértékeljük, jutunk el (vagy jutunk közelebb) a hiteles információhoz - vagyis megállapíthatjuk, hogy komplex tevékenységét tekintve egy határvédelmi rendszer üzemeltetésében kiemelten fontos elem az összadatforrású felderítési (hírszerzési) tevékenység [17], hiszen a főbb ágak (két csoportban bár) megjelennek. [8], [9]

A HATÁRVÉDELMI ADATSZERZŐ SZENZOROK ELLENI FENYEGETÉSEK ÉS VÉDELMI MÓDSZEREK

Érzékelési fenyegetettségek

Tekintsük át, hogy melyek azok a területek, ahol ellenséges hírszerzési tevékenységnek, vagy egyéb támadási lehetőségnek van kitéve egy határvédelmi rendszer.

Koncepcióját tekintve egy rendezési elv szerint a szembenálló félnek célja lehet (1) a rendszer érzékelési képességének megváltoztatására, melybe beletartozik e képesség nullára redukálása; (2) a rendszerben átvitt, illetve tárolt adatok megismerése, vagy módosítása – melybe az adatok részleges, esetleg teljes megsemmisítése is beleértendő.

Az érzékelési képesség megváltoztatása jellemzően az érzékelőnél, vagy annak közvetlen környezetében történhet. Az egyik legegyszerűbb lehetőség a szenzor érzékelésének akadályozása, vagyis mechanikai eszközökkel történő rongálása (kamera objektív beütése, lefestése, érzékelő leverése stb.). Mechanikai károsodás okozható lézerrel is, ami nem igényli a rongáló fizikai kapcsolatát a kamerával, de a képérzékelő átmeneti, vagy maradandó sérülését okozhatja. Ilyen esetben nyilvánvalóvá válik az üzemeltető részére a kár és vélhetően azonnal intézkedni fog a sérült eszköz javítására, vagy cseréjére. Egyben figyelmezteti is a megfelelő szolgálatokat, hogy a károkozás környezetében ellenséges cselekményre lehet számítani.

A védekezés lehetőségei: az érzékelő megközelíthetőségének megakadályozása, illetve a fokozott mechanikai védelem, például a kamera „látását” nem akadályozó, de a repülő tárgyak ellen védő rácsozat készítése. Más megközelítésben a szenzorok többszörözése ugyanígy fokozza a teljes rendszer védelmi hatékonyságát, vagyis a héj-elv szerint egy kieső érzékelő szerepét részlegesen és ideiglenesen át tudja venni egy másik érzékelő.

Kifinomultabb megoldás valamilyen elektronikai zavarással az érzékelőt az érzékelésben akadályozni, vagy korlátozni, különösen, ha ezt szakaszosan teszik. Ilyenkor ugyanis az üzemeltető számára nem egy állandóan hibás eszközről lesz szó, hanem egy nem megbízhatóan működő eszközről, melynél ráadásul a hibát a javítást végző nem fogja tudni provokálni. Komoly szaktudás szükséges ahhoz, hogy az ilyen típusú zavarást a legkevésbé feltűnően lehessen végezni. Korlátozott védelmet biztosíthatnak a különböző árnyékolási megoldások (réz alapú kábelezés esetében), megfelelő védelem kialakításához azonban ismerni kell a pontos támadási technológiát és az ahhoz alkalmazott technikát.

[17] Az összadatforrású felderítésre számos meghatározás létezik. Egy lényegretörő definíció szerint: „... azt jelenti, hogy úgy végzünk felderítési tevékenységet, hogy abban szerepet kap minden elérhető felderítő szerv és szervezet. Vagyis, hogy az összes rendelkezésre álló és a lehető legszélesebb körben elérhető adatszerző forrásokat használjuk, illetve szintén lehetővé válik, hogy egy célobjektumról ezek alapján a lehető legtöbb forrásból szerezzünk adatot.” [18]

Adatátviteli fenyegetettségek és védelem

Az átviteli és tárolási szakaszt az esetek legnagyobb részében valamilyen SIGINT tevékenységgel fogják támadni.[18] Más megnevezéssel kibertámadási eszközökkel történik a végrehajtás. Alkalmazzuk Hayden nómenklatúráját és különböztessünk meg aktív és passzív SIGINT technikát, mely az adat, illetve az információ mozgási állapotából indul ki. [10] Amennyiben álló (tárolt) adatról van szó, akkor nevezzük passzív eljárásnak (melyet a tárolási- és feldolgozási hely fenyegetettségeinél részletesebben megvizsgálunk), ha pedig mozgásban lévő adatról van szó, akkor hívjuk aktív SIGINT tevékenységnek.[19] Alapvetően különböző adatszerzési technológiákról beszélünk a mozgásban (valamilyen adatátviteli csatornában) lévő adat megszerzésére során, vagy egy valamilyen tárolóeszközön lévő adatmennyiséghez való hozzáféréskor.

Mozgásban lévő adat átviteli technológiája lehet vezetékes, vagy vezeték nélküli. A vezetékes részt célszerű két további részre, optikai és nem optikai átvitelre bontani. Mindhárom technológiának megvan a maga eszköztára az átvitt adatok megszerzésére, mely adott esetben rendkívüli nehézségeket is okozhat. Ilyen lehet például egy frekvenciaugratásos rádiórendszeren keresztüli átvitel adattartalmának megszerzése, ahol az átviteli frekvencia egy másodperc alatt akár százas, vagy ezres nagyságrendben változik. E feladatnak lehet persze egyszerű megoldása is, az átvitelbiztonsági kulcs megszerzése, mely az adó és a vevő számára meghatározza a használt frekvencia spektrumát és a frekvenciaváltási paramétereket. E kulcs megszerzése is elvileg lehetséges passzív SIGINT eszközökkel, hiszen a kulcsot vélhetően valamilyen infokommunikációs rendszerben tárolják. Más esetben egyéb hírszerzési ágak feladata lehet a szükséges kulcs beszerzése.[20]

Optikai adatátvitel esetében, hivatalos forrásból 1000 USA dollárért[21] hozzáférhetők az interneten olyan eszközök, melyek segítségével az optikai szálon átvitt adat (bizonyos korlátozások mellett) tükrözhető egy a támadó által választott bármilyen eszközre. Sok esetben a hálózat üzemeltetője talán észre sem fogja venni, hogy az adatfolyamot „lehallgatják” mivel az átviteli vonalon lesz ugyan valamekkora jelveszteség, de a saját végpontok közötti adatátvitelben – a legtöbb esetben – nem lesz hiba.[22]

Réz alapú kábeles adatátvitelnél is könnyedén állnak rendelkezésre azok az eszközök, melyek az átvitt adat 100%-át egy a támadó által választott adathordozóra, vagy alternatív hálózatra irányítják, azzal, hogy az eredeti adatátviteli útvonalat megőrzik.[23]

Könnyű támadási pontok lehetnek az adatátviteli úton a vezérléseket tartalmazó szekrények, itt ugyanis egyszerűen elhelyezhetők azok a fenti eszközök, melyek a támadók számára akár az

---

[18] Természetesen itt is megjelenhet a kinetikus „nyers erő” alkalmazása, például az átviteli kábelek vágása, az elágazási pontok megsemmisítése, melyek nem SIGINT műveletek.

[19] Passzív adat esetében sokszor merül fel a HUMINT tevékenység, mint az adat/információ megszerzésének elsődleges lehetősége – mely azonban nem tekinthető kiber tartományban végzett tevékenységnek.

[20] Jellemzően HUMINT tevékenység végrehajtásával.

[21] Ugyanez a Távol-keletről, „utángyártott” forrásból beszerezve ennek a töredéke

[22] Hálózatok karbantartási és tesztelési feladataira készült, rendkívül egyszerű eszközről van szó, ugyanis rá kell pattintani egy meglévő optikai szálra és az eszköz optikai kimenetén megjelenik ugyanaz a jel, mint az eredeti szál bejövő oldalán. Az eszköz használata nem jár az eredeti optikai szál sérülésével, vagy vágásával és a saját hálózat ellenőrzését, különböző biztonsági incidensek megelőzését és hatékonyabb hibakeresést szolgálja.

[23] Az egyszerű megoldásoknál (mely a legkönnyebben felfedhető is) szükséges a kábelezés megszakítása és a kábel vágásánál új csatlakozókkal való felszerelése. Egy bármilyen egyszerű, menedzselhető switch beiktatásával, az eredeti bejövő oldalt a hálózati kapcsolón (switch) tükrözni kell egy külön aljzatra, az eredeti elmenő oldalt pedig csatlakoztatni egy harmadik aljzathoz. Ezt a feladatot már bármelyik egyszerű, menedzselhető switch megoldja. A bonyolultabb és kompaktabb céleszközök ugyanezt a feladatot látják el, egy sor kiegészítő funkció biztosítása mellett, magasabb áron, de a felfedhetőség csökkentésével.

érzékelők monitorozását és zavarását (adott esetben a támadó által létrehozott alternatív jelfolyam továbbítását), akár az adatátviteli vonal lehallgatását lehetővé teszik. Fontos tehát ezen szekrények megfelelő mechanikai és elektronikai védelme. Törekedni kell továbbá az optikai adatátvitelre való mihamarabbi átállásra, vagyis hogy az érzékelő és az azzal összekötött első hálózati kapcsoló közötti réz alapú átvitel a lehető legrövidebb, illetve a kapcsoló után csak optikai adatátvitel legyen. Az optikai átvitelen – megfelelő jelfolyam vizsgáló berendezések és hozzáértő szakember segítségével – könnyebben megtalálhatók az idegen eszközök és jóval magasabb zavartűrő képesség érhető el (különösen nagy adatátviteli sebességeknél).

Adat – információ - kódolás

Az átvitelnél hangsúlyosan adatokról volt szó. Ahhoz, hogy ez a támadó számára valódi érték is legyen, az adatnak értelmezhetőnek kell lennie, mivel az értelmezést követően válik az adatból információ. Védekezés szempontjából tehát sokkal nagyobb befektetés kell ahhoz, hogy egy adatátviteli hálózatot fizikailag biztonságossá tegyünk, mint ahhoz, hogy az adatok értelmezését nehezebbé tegyük. Ennek pedig a legjobb eszköze a valamilyen kriptográfiai eljárást alkalmazó kódolás. Vagyis védekezésként alapvető fontosságú, hogy minden adatátviteli csatornát kódoljunk, mert annak erősségétől függően a szembenálló fél számára az adatok értelmezése heteket, hónapokat, vagy akár éveket is igénybe vehet. Meggondolandó ugyanakkor az alkalmazott kódolás erőssége, hiszen az időegység alatt átvinni kívánt adatmennyiség függvényében a kódolás erősségének növelése igen komoly beruházást igényelhet a felhasznált kriptográfiai eszközök és erőforrások terén.

A kódolás elengedhetetlensége különösen az aggregált adatátviteli úton igaz, mivel ott már egy harmadik személy által üzemeltetett hálózatról van (lehet) szó. Kivételként meg kell említeni a zártcélú adatátviteli hálózatokat, mint például a Nemzeti Távközlési Gerinchálózat (NTG), ahol a hálózat biztonságát az üzemeltető Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ) biztosítja. A kivétel itt annyit jelent, hogy a kódolást nem a végpont (adatforrás) tulajdonosának kell elvégeznie, hanem az átviteli szolgáltató (NISZ) a saját eszközeivel végzi el. Így eredményét tekintve az aggregált átviteli vonalon már kódolt adatfolyam van.

Olyan esetben, ahol zártcélú rendszer nem áll rendelkezésre és a primer objektum hálózatát elhagyta már az adat, jellemzően egy közcélú (szakaszaiban általában országos) kritikus információs infrastruktúra hálózaton átmenő átvitelről beszélhetünk melyek támadásához gyökeresen eltérő tudás és erőforrások szükségesek. Nyílt átviteli rendszereken pedig még fokozottabb követelményként kell megjelennie a különböző kriptográfiai védelmi eljárásoknak, melynek ilyen esetben egyik kézenfekvő megoldási lehetősége a megfelelően beállított és felügyelt virtuális magánhálózatok (VPN)[24] alkalmazása.

Létezik egy speciális „nyers erő” alkalmazás is, ahol teljes hálózati forgalom alternatív útvonalon történő átvitelével és valószínűsített másolásával éri el célját a támadó. 2016. februárjától közel 6 hónapon keresztül Kanada és a Koreai Köztársaság közötti internetes forgalom egy része Kínán keresztül volt irányítva. 2016. októberében az Egyesült Államok és Olaszország között egy meghatározó angol/amerikai érdekeltségű bank forgalmát irányították Kínán keresztül, ám ez csak órákat tudott működni, mert a kínai végrehajtóknak problémát okozott a forgalom továbbvitele az eredeti végcélba, Milánóba. 2017. április-május hónapokban egy nemzetközi hírügynökség Skandinávia és Japán közötti forgalmát irányították Kínán keresztül. [11] Mindezek mélyreható vizsgálatok után és csak az eltérítést követő hetek, hónapok csomag szintű adatelemzését követően derültek ki részleteiben.

[24] VPN – Virtual Private Network

Az átirányítások a Border Gateway Protocol (BGP) „sérülékenységét” használták ki, ami valójában nem sérülékenység, hanem egy tervezési tulajdonság, mely a tervezés idején nem merült fel, hogy rosszindulatú céllal kihasználható. Főként azért nem, mert egy ilyen eltérítésnek akkor van értelme, ha a forgalom tárolható, amire ekkora mennyiségben még 6-8 évvel ezelőtt sem lett volna racionális erőforrás (meghatározó állami szereplőkön kívül).

Tárolási- és feldolgozási hely fenyegetettségek és védelem

Az adatok végleges feldolgozási és tárolási helyre történő megérkezését követően más eszközök szükségesek azok megszerzéséhez: vagy a belső hálózatba bejutva kell az adatforgalom megszerzését elvégezni, vagy a tárolt adatokhoz szükséges hozzáférni – Hayden csoportosításában ez utóbbi a klasszikusan passzív SIGINT technika. Az adatforgalom lehallgatásához az átviteli útnál alkalmazott eszközök és technológiák szükségesek, azonban az eszközök elhelyezése jóval nehezebb lehet, mivel a kódolás mögötti (kódolatlan) hálózathoz fizikailag észrevétlenül hozzáférni rendkívül nehéz lehet.

A tárolt adatok nem hálózatforgalmi eszközökkel való megszerzéséhez ugyanúgy szükséges a belső hálózathoz való hozzáférés, vagy például lehetséges egy megfelelően preparált hardver eszköz (USB billentyűzet, beépített SSD alapú adattárral) segítségével elvégezni az adatszerzést.

Adatok biztonságos tárolásában rendkívül nagy segítség lehet és adott kockázati szint felett nem megkerülhető a megosztott adattárolás megvalósítása, mely egymástól legalább két független helyen valósul meg. Kiemelten magas kockázat esetén a földrajzi helyükben is eltérnek a redundáns adattárolás elemi részei, alrendszerei. [12]

Ugyanígy problémát jelent a megszerzett adatok kijuttatása is. Ha azt vezeték nélküli technológiával oldja meg a támadó, akkor meg fog jelenni egy rádióadó, ami sugároz és amely a sugárzási paraméterei alapján (adásidő, frekvencia, teljesítmény, stb.) felfedhető. Vezetékes kijuttatás esetén valamilyen telepített vonal szükséges, mely lehet a támadott létesítmény internet hozzáférése is, ahol viszont jól monitorozhatók a hálózati forgalom csomagjainak végpontjai, ami azonban jelentős információbiztonsági erőforrásokkal rendelkező szervezetek számára is komoly kihívás.[25]

A lehetséges védekezési megoldások általában a számítógépes hálózat eszközeinek és felhasználóinak viselkedését és nem a hálózat külső belépési pontjait vizsgálják. Ilyenek az úgynevezett eszköz (hoszt) alapú biztonsági rendszerek (Host Based Security Systems), melyek az adott eszközre egy klienst telepítve monitorozzák folyamatosan az adatáramlást a hálózat különböző irányaiba és a meghatározott szabályrendszerek, valamint öntanuló algoritmusok alapján, gyanús tevékenység esetén riasztást generálnak. [13] Ilyen kliensek nem kizárólag munkaállomásokra, hanem szerverekre is telepíthetőek, így (nagyon leegyszerűsítve) elvileg a szerverekről kiáramló adatmennyiségnek a munkaállomás, vagy másik szerver oldali párja megkereshető. Többek között ez a technológia védi a nagyobb banki rendszereket, illetve az Egyesült Államok Védelmi Minisztériumának minősített adatátvitelét biztosító egyik világméretű hálózatát, melyhez egyéb kormányzati szervek, illetve az USA nagykövetségeinek legnagyobb része is csatlakozik.[26] Hasonló módszerek alkalmazhatók az adatátviteli utak

[25] Nem a SIGINT eszköztárába tartozó megoldás az adathordozó fizikai kijuttatása a feldolgozási helyről. Ezt a megoldást választotta és Bradley Manning 2010-ben és Edward Snowden is 2013-ban a minősített adatok kicsempészéséhez [19]

[26] Ez a rendszer a Secret Internet Protocol Router Network (SIPRNet) és „titkos” minősítésig engedélyezett rajta az adatátvitel.

megfigyelésére is – feltételezve, hogy a hálózati pontok adatforgalma és a hálózati aktív eszközök azonosítottan ismertek.

Közösségi védelmi megoldások

Léteznek úgy Európában, mint az Egyesült Államokban olyan kiberbiztonsági információ megosztó és elemző központok (angol megnevezéssel: Information Sharing and Analysis Center – ISAC), melyek nonprofit szervezetként egy adott ágazatban egyfajta tudásközpont feladatot töltenek be, és melyen keresztül az ágazati szereplők egymással gyorsan és hatékonyan tudnak kommunikálni az őket érő adat-, információbiztonsági és kibervédelmi kockázatok kezelésében, jó gyakorlatok kidolgozásában és a megtörtént események közös elemzésében. [14],[15]

Egy ilyen központ akkor tud igazán hatékony lenni, ha nem kizárólag a szolgáltatók (közvetlen ágazati szereplők) vesznek benne részt, hanem például rendelkezik olyan kormányzati információforrásokkal, melyek akár titkosszolgálati forrásból szerzett és megosztható információkkal látják el. E kapcsolat a kormányzat számára is hasznos lehet, hiszen az ágazati törvényalkotásban olyan tapasztalati tényekre tud támaszkodni, melyek más forrásból nehézkesen, vagy torzulva állnának csak rendelkezésre.

Kiváló példa lehetne egy távközlési szolgáltató megjelenése az adott központ munkájában, mert ezzel egymás számára megismerhetővé válnának az ágazati kommunikációs sajátosságok, így lehetőség lenne a távközlési szolgáltatónak olyan termékeket kialakítani, vagy meglévőket úgy módosítani, hogy még hatékonyabban segítsék és támogassák az adott ügyfelek működését. A távközlési szolgáltató pedig olyan információkra tudna szert tenni, mellyel saját rendszereit tudná felkészültebbé, védettebbé tenni, így egy kibertámadás esetén jelentősen csökkenteni tudná a keletkező károkat és a normál üzemre való visszaálláshoz szükséges időt.

Ugyanez a pozitív kétirányúság igaz minden olyan további kapcsolatra, mely az adott ágazat interdependenciáin alapul, ezzel téve hatékonyabbá és biztonságosabbá mindkét fél számára a saját működési feltételrendszerét.

Európában ilyen információ megosztó és elemző szervezet például az EE-ISAC (European Energy ISAC), mely részben a nemzeti villamosenergia teherelosztókat és átviteli hálózat üzemeltetőket lenne hivatott összefogni, de melynek tagjai közé tartozik például a NATO Kibervédelmi Együttműködési Kiválósági Központja (CCD COE), vagy a Siemens, mint gyártó, vagy egy másik kiemelten fontos intézmény, az Európi Unió Hálózati és Információbiztonsági Ügynöksége (ENISA - European Union Agency for Network and Information Security).[27] A különböző egyetemek tagságán keresztül pedig biztosított a tudományos élet vérkeringésébe történő bekapcsolódás, mely mind a központ, mind az egyetemek számára rendkívül gyümölcsöző lehet – gondoljunk csak a legfrissebb szaktudás és szakemberek kölcsönös és gyors rendelkezésre állására.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Kritikus infrastruktúrák és kritikus információs infrastruktúrák komoly kitettséggel, így jelentős kiberbiztonsági kockázattal rendelkeznek elektronikus határvédelmi rendszereik tekintetében. Nem állami szereplők, nem a banki, energetikai, vagy távközlési ágazatban működő társaságok veszélyeztetettsége kiemelten magasabb, hiszen elsődleges működési feladatuk nem kötődik az egyéni ügyfelek biztonságához, vagy az államigazgatáshoz (beleértve

[27] Jelen írás lezárásakor az EE-ISAC kifejezett magyar taggal nem rendelkezett, képviseletünk (remélhetőleg) csupán Magyarországon is működő multinacionális cégeken keresztül valósul meg. [20]

a honvédelmi és rendvédelmi szervezeteket), hanem jellemzően valamilyen ipari, mezőgazdasági, kereskedelmi, vagy egyéb szolgáltatási tevékenységet végeznek. Ugyanakkor számukra is megoldandó feladat saját fizikai biztonságuk megteremtése, melyet jelentős számú elektronikai és infokommunikációs eszköz segítségével fognak elvégezni.

A határvédelmi technológiák, üzemeltetése során felmerülő igények és problémák jól mutatják, hogy mindezeket interpolálva a teljes vállalati infokommunikációs rendszerre, mekkora kihívásokkal áll szemben az adott szervezet informatikai- és információbiztonságért felelős vezetője. Mennyi kérdést nyit meg és mennyi lehetséges sérülékenységre mutat rá egy egyébként alacsony jelentőségűnek tűnő alrendszer (mint például egy elektronikus határvédelmi rendszer). Ezért is kiemelkedően fontosak a különböző rendszerek interdependenciái, mert olyan összefüggéseket hozhatnak napvilágra, melyek kezelésének szükségessége előtte egyáltalán nem, vagy csak sokkal kisebb súllyal merült fel. Szintén ugyanezért fontos a széleskörű és részletes, szakmai alapokon nyugvó kockázatelemzések elvégzése és folyamatos felülvizsgálata.

A technológia fejlődésének természetéből fakadóan egyre alapvetőbb kihívás lesz a különböző szervezetek[28] saját kibervédelmének megteremtése és fenntartása, bizalmas adataik továbbításának, feldolgozásának és tárolásának védelme, valamint teljes infokommunikációs rendszereik bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása.

A legnagyobb magyarországi vállalatoknál ez mára már nem kérdés, azonban a közepes, vagy kisebb méretű de még a jogszabályok által kritikusnak minősített infrastruktúrák esetében messze nem minden esetben magától értetődő. Pont ők azok, ahol nem szükségszerűen áll rendelkezésre az a tudás és tapasztalat, ami a védelmi rendszerek megfelelő tervezéséhez, kialakításához és üzemeltetéséhez szükséges, különösen azért, mert ágazatonként akár jelentősen eltérő kívánalmak és kockázatok lehetnek, így nem tudnak egy általános megoldást magukra mindenben alkalmazni.

Hatalmas lépés lenne, ha a hazai kritikus infrastruktúrák és kritikus információs infrastruktúrák üzemeltetői közül mind több tagja lenne ISAC szervezeteknek. Nagyon sok esetben ugyanis pont az a tapasztalat hiányzik, melyeket a még nem tagok tudnának a szervezetnek adni, hogy (megfelelő anonimizálást követően) abból utána az összes többi tag tanulni tudjon.

FELHASZNÁLT IRODALOM

[1] KOVÁCS, L.: Az elektronikai hadviselés jelene és lehetséges jövője. Hadmérnök, 1 (2017), 213–232.

[2] HAIG, Zs.: Az információbiztonság komplex értelmezése. Hadmérnök, (2006)

[3] BOGNÁR, E.K.: Szenzorhálózatok határvédelmi alkalmazás a. Hadmérnök, XII (2017), 175–187.

[4] DR. MUHA, L., DR. KRASZNAY, Cs.: Az elektronikus információs rendszerek biztonságának menedzselése. Budapest: Nemzeti Közszolgálati Egyetem, 2014

[5] EUROPEAN UNION SATELLITE CENTRE: Border Surveillance. https://www.satcen.europa.eu/Capdev/services_for_border_surveillance (A letöltés dátuma: 2019. január 6.)

[28] Előbb-utóbb függetlenül attól, hogy kritikus (információs) infrastruktúrának minősülnek-e, vagy sem.

[6] EUROPEAN DEFENSE AGENCY: Persistent SUrveillance Long Term ANalysis (SULTAN). https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-(sultan) (A letöltés dátuma: 2019. január 6.)

[7] KŐSZEGVÁRI, T.: A KATONAI FELDERÍTÉS HELYE, SZEREPE ÉS PROBLÉMÁI A TERRORIZMUS ELLENI KÜZDELEMBEN. Felderítő szemle, 1 (2006), 22–30.

[8] DOBÁK, I.: Elektronikai eszközökkel végzett felderítés − rádiófelderítés. In. A nemzetbiztonság általános elmélete (szerk. Dr. Dobák, I.) Budapest: Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, 2014

[9] GULYÁS, A.: A nemzeti különleges műveleti erők felderítő támogatása. Hadmérnök, (2012), 131–144.

[10] HAYDEN, M. V.: Playing to the Edge. New York: Penguin Press, 2016

[11] DEMCHAK, C.C., YUVAL, S.: China's Maxim – Leave No Access Point Unexploited : The Hidden Story of China Telecom's BGP Hijacking China's Maxim – Leave No Access Point Unexploited : The Hidden Story of China Telecom ' s BGP. Military Cyber Affairs, The Journal of the Military Cyber Professionals Association, 1 (2018)

[12] KRALOVÁNSZKY, K.: Elosztott adattárolás egyes kérdései. Hadmérnök, XIII (2018), 297–305.

[13] PARLIAMENT OF THE UNITED KINGDOM: Defence Committee: Written evidence from McAfee. https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106vw09.htm (A letöltés dátuma: 2019. január 12.)

[14] NYITRAI, M.: Összehasonlító tanulmány az Európai Unió és az Egyesült Államok kritikus infrastruktúra védelem szabályozása és megvalósítása területein. Hadtudományi Szemle, 2 (2017), 232–253.

[15] MOTEFF, J.D.: Critical Infrastructures: Background, Policy, and Implementation: RL30153. Congressional Research Service: Report, (2010), 1–38.

[16] HAIG, Zs.: Információs műveletek a kibertérben. Budapest: Dialóg Campus Kiadó, 2018

[17] SZENES, Z.: A katonai biztonság reneszánsza. Hadtudományi Szemle, 2 (2017), 3–26.

[18] KOVÁCS, L.: Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben. Zrínyi Miklós Nemzetvédelmi Egyetem, 2003

[19] ZETTER, K.: Snowden Smuggled Documents from NSA on a Thumb Drive. wired.com https://www.wired.com/2013/06/snowden-thumb-drive/ (A letöltés dátuma: 2019. január 12.)

[20] EE-ISAC: EE-ISAC Members. http://www.ee-isac.eu/members (A letöltés dátuma: 2019. január 12.)