Paper 43 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

Kritikus infrastruktúrák kiberbiztonsága

Heilmann Márk[1,2]

[1]Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Magyarország, Budapest

[2]Magyar Tudományos Akadémia Agrártudományi Kutatóközpont, Magyarország, Martonvásár

Absztrakt. A következőkben a kritikus infrastruktúrákat[1], majd a kritikus információs infrastruktúrákat mutatom be. Ezek után a Magyarország kiberbiztonsági stratégiájáról és annak szervezeti felépítéséről írok, végezetül olyan kibertérben történt támadások lesz a téma, melyek alátámasztják az informatikai biztonság egyre fontosabb szerepét a kritikus infrastruktúrák védelmében.

Kulcsszavak: kiberbiztonság, kritikus infrastruktúrák, kibervédelem

1 Bevezetés

A kritikus infrastruktúrák (ki) hétköznapi életünk alappillérei, ezért a társadalom részéről elvárás, hogy a legnagyobb biztonsággal üzemeljenek, működjenek. Védelmük, akadálymentes üzemeltetésük komoly biztonsági intézkedéseket igényel. A szerteágazó támadási felületek közül az információs rendszerek kiemelkedő fontosságúak, mert a különböző infrastruktúrák többsége az információs rendszereken alapszik. Napjaink egyik legaktuálisabb biztonságtechnikai problémája a kiberbűnözés, mely a ki-kat is veszélyezteti. Az alábbi fejezetben részletezem milyen rendszereket nevezünk ki-nak.

2 Kritikus infrastruktúrák

Hétköznapi életünk kényelméért, biztonságáért, megélhetésünkért különböző infrastruktúrák felelnek. Fontosságukat csak esetleges hiányukkor észleljük. Ilyen létfontosságú infrastruktúrák az energiaellátás, közlekedés, agrárgazdaság, egészségügy, pénzügy, ipar, infokommunikációs technológiák, vízellátás, kormányzat működése, közbiztonság. Ezeket létfontosságú rendszereknek vagy kritikus infrastruktúráknak nevezzük. [2] Ebből jól látszik mely rendszerek azok, melyek védelme kiemelkedő fontosságú minden nemzet számára, hogy megvédje állampolgárait. A kritikus infrastruktúrákat veszélyeztető események lehetnek természeti katasztrófák, civilizációs és ipari katasztrófák úgy, mint erőművi vagy közlekedési balesetek, fegyveres konfliktusok és terrorizmus. Szinte minden ilyen infrastruktúra informatikai eszközök, hálózatban lévő rendszerek segítségével üzemel [3]. Ezen rendszerek a kibertámadások célpontjai lehetnek, melyek ellen védekezni kell. Ezen a téren Magyarország

[1] „Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.*”[12]*

Paper 43 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

az elsők között kezdett megoldásokat keresni. 2013-ban alakult meg a Kiberbiztonsági Platform (Central European Cyber Security Platform – CECSP). A szervezetben Magyarországon kívül még négy ország vesz részt: Ausztria, Csehország, Lengyelország, Szlovákia. Az együttműködés célja a kiberbiztonság területén szerzett tudás megosztása és közös fejlesztése: képzések, gyakorlatok, kutatások révén. A Magyarországon 2013-ban kiadott kiberbiztonsági stratégiára vonatkozó kormányhatározat 4 csoportban és 11 pontban összegzi a magyar kiberbiztonsági koncepciót.[17] A kiberbiztonság megőrzése folyamatos és dinamikus alkalmazkodást igényel, így a szabályozásoknak is idomulniuk kell a változásokhoz.

A következőkben bemutatom mely kritikus rendszerek sérülékenyek, az informatikai hálózatok oldaláról.

2.1 Mely kritikus infrastruktúrákat kell védeni a kibertérben[2]

A kritikus információs infrastruktúrának nevezzük azokat a rendszereket, melyek magukban is kritikus infrastruktúra elemek vagy olyan infokommunikációs létesítmények, melyek nem rendeltetésszerű üzemelése zavart, meghibásodást okozhat a kritikus infrastruktúrák üzemelésében.[4]

„A kritikus információs infrastruktúrák közé tartoznak az alábbi rendszerek:

- kommunikációs hálózatok,
- energiaellátó rendszerek informatikai rendszerei,
- közlekedési rendszerek informatikai rendszerei,
- víz- és élelmiszerellátó rendszerek informatikai rendszerei,
- egészségügyi rendszerek informatikai rendszerei,
- pénzügyi rendszer informatikai rendszerei,
- egyéb kritikus infrastruktúrák informatikai rendszerei. ”[5]

A felsorolásból jól látszik, hogy szinte az összes kritikus infrastruktúra szegmens érintett, kiberbiztonság szempontjából. Fontos tehát, hogy milyen szervezetek milyen eszközök segítségével foglalkoznak ezen rendszerek biztonságával. A következő részben a magyarországi kiberbiztonsági stratégiát mutatom be.

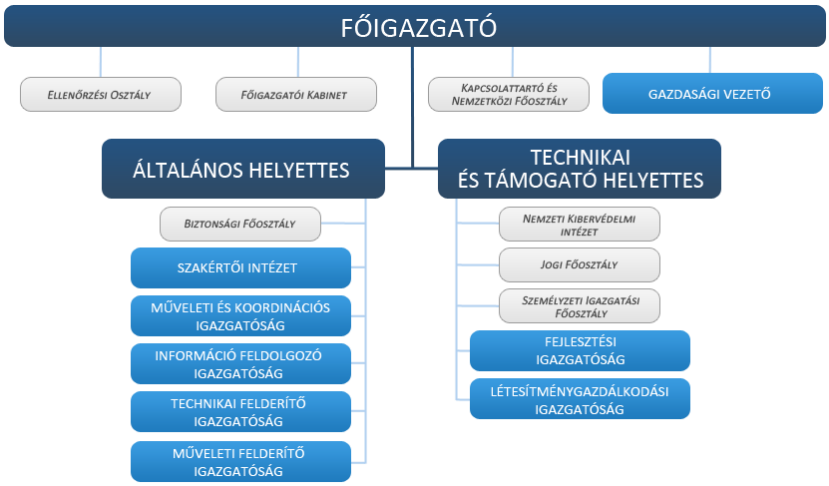
3 Kiberbiztonság

3.1 Nemzeti Kiberbiztonsági Stratégia

[2] „A kibertér a hálózatba kötött számítógépek által létrehozott virtuális valóság világa, annak összes objektumával egyetemben.”[14]

Paper 43 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

Magyarország Nemzeti Kiberbiztonsági Stratégiáját (1139/2013. (III. 21.) Korm. határozat) 2013-ban fogadta el a kormány, melynek keretében létrejött az információbiztonság szervezeti rendszere. 2015-ben az információbiztonsági törvény (Ibtv.) módosításával az addig széttagolt intézményrendszer (Kormányzati Eseménykezelő Központot (GovCERT-Hungary), a Nemzeti Elektronikus Információbiztonsági Hatóság, és az E-biztonsági Intelligencia Központ (NBF-CDMA)) központosításra került. Ahogy az 1. ábrán látszik a Nemzetbiztonsági Szakszolgálaton (NBSZ) belül létrejött a Nemzeti Kibervédelmi Intézet. Itt három különálló szervezeti egység került kialakításra: a Nemzeti Elektronikus Információbiztonsági Hatóság, Kormányzati Eseménykezelő Központ (Gov-CERT), és a Biztonságirányítási és Sérülékenység vizsgálati terület.[6][10][13]



1. ábra Nemzetbiztonsági Szakszolgálat szervezeti felépítése [6]

A Nemzeti Kibervédelmi Intézet különböző szervezeti egységeinek feladatai a következők:

“Nemzeti Elektronikus Információbiztonsági Hatóság feladatai:

- Ügyfelek és rendszerek nyilvántartása
- Biztonsági osztályba és szintbe sorolás ellenőrzése
- Követelmények teljesülésének ellenőrzése
- Sérülékenység vizsgálat elrendelése
- Javaslat létfontosságú rendszer kijelölésére
- Javaslat információbiztonsági felügyelő kirendelésére

- Kormányzati Eseménykezelő Központ incidenskezelési terület feladatai:
  - Biztonsági események kezelése
  - Fenyegetésmenedzsment
  - Ügyeleti szolgálat
  - Elemzés/értékelés
  - Kibervédelmi gyakorlat

Paper 43 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

- Képzés, tudatosítás
- Felelősök kijelölésének támogatása
- Sérülékenység vizsgálat
- Biztonsági esemény kezelés kapcsán együttműködés az internet-szolgáltatókkal
- Rendszeres vezetői tájékoztatás
- Biztonságirányítás és sérülékenység vizsgálat
- Sérülékenység vizsgálat,
- Biztonsági események kivizsgálása
- EMIR / FAIR rendszerekkel kapcsolatos informatikai biztonsági feladatok ellátása"[6]

A következőkben kritikus Infrastruktúrákat ért kibertámadásokat fogok bemutatni, melyek következményeként a megtámadott országok komoly károkat szenvedtek el. Az események bemutatásakor a támadás típusát és célpontjait mutatom be, a kiváltó okokra nem térek ki.

3.2 Kritikus infrastruktúrákat ért kibertámadások

3.2.1 Az orosz−észt kibertámadás

Észtország ellen 2007. április 27-én indult kibertámadás, melynek következtében, fennakadások keletkeztek az online pénzforgalomban, elérhetetlenné váltak az állami intézetek weblapjai és több állami intézményt is le kellett választani a hálózatról. A túlterheléses támadások[3] 178 különböző országból érkeztek és meglehetősen komoly károkat okoztak Észtország infrastruktúrájában. Egy kiemelt példa a károk nagyságrendjére, a Hansabank a május 10-i támadáskor közel 1 millió dolláros kárt szenvedett el.[7]

3.2.2 Stuxnet, Irán

2010-ben derült fény a ma már közismert vírusra, mely a stuxnet nevet kapta. A kártékony szoftver az iráni atomprogramot hivatott visszavetni, mely az erőmű zárt hálózatába egy fertőzött adathordozó segítségével jutott el, ahol már ki tudta fejteni hatását. Egy Siemens S7 PLC (Programmable Logic Controller) működésébe avatkozott be, mely UF_6 (uránhexafluorid) molekulákat feldolgozó centrifuga egyes elemeit vezérelte. Első változata felülírta a tényleges kalibrációs adatokat és hamis értékeket jelzett vissza a kezelőknek. A második verzió esetén a centrifugák sebességének vezérlését állította át, így csökkentve az eszközök élettartamát. A program kifejezett feladata volt, hogy észrevétlenül lapuljon meg a vezérlőhálózaton és írja felül a normál működési funkciókat. A program az iráni erőmű eszközeihez készült, ennek köszönhető, hogy bár a világ nagy részén már fellehető, az iráni erőművön kívül más károkat nem okozott. [8]

[3] *DoS (Denial of Service-szolgáltatásmegtagadással járó támadás), DDoS (Distributed Denial of Service- elosztott szolgáltatásmegtagadással járó támadás) vagy nevezik túlterheléses támadásnak is, jelentése, hogy egy adott eszköz vagy számítógép sebezhető részét támadja, kérésekkel túlterheli, így az adott rendszer, célgép lelassul elérhetetlen lesz és rosszabb esetben a rendszer össze is omlik.[15]*

Paper 43 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

3.2.3 Ukrajnai energiahálózat elleni támadás

Ukrajnában 2015 decemberében kibertámadás érte az ország három regionális energiaszolgáltatóját. Mindhárom szolgáltatónál megtalálták a BlackEnergy[4] malware[5]-t és arról számoltak be, hogy a KillDisk[6] malware segítségével törölték a kiszemelt rendszerekről a működéshez szükséges állományokat. A vírusok, célzott adathalász támadások (spear phishing[7]) segítségével jutottak el a célállomásig. A támadás következtében 225 ezer háztartás maradt villamos energia nélkül.[9][11]

A felsorolt incidensek jól demonstrálják a kiberbiztonsági intézkedések fontosságát. Az elmúlt évtizedben egyre csak növekszik a kibertérben elkövetett bűncselekmények száma, melynek egyértelmű kiváltó oka az informatikai eszközök robbanásszerű elterjedése.

4 Összegzés

Bemutattam, hogy napjaink kiemelkedő fontosságú feladata a kritikus infrastruktúráink korszerű védelme a kibertérben. Az eddig világszerte történt létfontosságú rendszereket ért nagy erejű kibertámadások riasztó példáikkal jelzik, hogy az eddigieknél többet kell tennünk a biztonságunk megőrzése érdekében, úgy mint tudatos felhasználók képzése, a kor elvárásainak megfelelő szakemberek kinevelése, korszerű eszközök, szoftverek használata.

Felhasznált irodalom

[1] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01?_mc=sm_dr_editor_kellyjacksonhiggins

[2] Répás Sándor, Dalicsek István: *Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében*,PRO PUBLICO BONO Magyar Közigazgatás, 2015/4 pp. 22-33. (2015)

[3] Dr. Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor: *A kritikus információs infrastruktúrák meghatározásának módszertana*, http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf,*(2009)*

[4] Muha Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*, Doktori értekezés, (2007)

[5] Gyurák Gábor: *Kritikus infrastruktúrák védelme hálózati behatolás jelző rendszerekkel*,Hadmérnök, X. Évfolyam 2. szám, pp. 223-233. (2015)

[6] http://www.nbsz.gov.hu/?mid=42

[4] Távoli kódfuttatásra és adatlopásra használt kártékony szoftver.
[5] Rosszindulatú szoftver.
[6] Adatok megsemmisítésére szolgáló kártékony szoftver.
[7] Személyre szabott adathalászat.[16]

[7] Bányász Péter, Orbók Ákos: *A NATO kibervédelmi politikája és kritikus infrastruktúra védelme közösségi média tükrében,* HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA XXIII:(1 elektronikus) pp. 188-209. (2013)

[8] Gyebrovszki Tamás: *Stuxnet-mint az első alkalmazott kiberfegyver -a tallini kézikönyv szabályrendszere szempontjából*, Hadmérnök, IX. Évfolyam 1. szám, (2014)

[9] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[10] Müller Tamás: *Kiberfenyegetések és kibervédelem*, infojegyzet 2016/44.

[11] http://icscybersec.blog.hu/2016/03/03/a_department_of_homeland_security_jelentese_a_karacsony_elotti_ukran_villamosenergia-rendszert_erint

[12] 234/2011. (XI. 10.) Korm. Rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[13] Rajnai Zoltán, Fregan Beatrix: *Kritikus infrastruktúrák védelme*, XXI. Fiatal Műszakiak Ülésszaka, Kolozsvár, pp. 349-352 (2016)

[14] http://www.kfki.hu/~cheminfo/hun/olvaso/lexikon/c.html

[15] http://www.virusradar.com/en/glossary/ddos

[16] Dolánszky György: *Informatikai Rendszerek sérülékenység-vizsgálata*, http://users.nik.uni-obuda.hu/poserne/ibst/Frissitett_anyagok_2013/20130508_Serulekenysegvizsgalat_eSec_KURT_DGY.pdf (2013)

[17] Berzsenyi Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése, Nemzet és Biztonság, 2014/6. Szám pp. 110-136. (2014)