dr. Dornfeld László – Keleti Arthur – Barsy Miklós – Kilin Józsefné – Berki Gábor – dr. Pintér István

Műhelymunkák

A virtuális tér geopolitikája

Tanulmánykötet

2016/1. szám

Geopolitikai Tanács Közhasznú Alapítvány – Budapest, 2016
w w w . c g e o p o l . h u

Szerkesztette: Pintér István

A kötetben publikált tanulmányok
a szerzők önálló véleményét tartalmazzák,
így az abban foglaltak nem tekinthetők
a Geopolitikai Tanács hivatalos álláspontjának.

Idézés: Szerző neve (2016) A cikk címe. In: PINTÉR, István: A virtuális tér geopolitikája. Geopolitikai Tanács Műhelytanulmányok, 2016/1. p. oldalszám.HU ISSN 1788-7895. ISBN 978-963-9816-34-3.

Citation: Name of the author (2016) Name of the article. In: PINTER, Istvan: Geopolitics of the Virtual Space. Council on Geopolitics Working Papers, 2016/1. pp.
HU ISSN 1788-7895. ISBN 978-963-9816-34-3.

Tartalom

A kötet szerzői 7
Lektorok 11
Biographies 12
Lectors 16

Bevezető helyett
Frédérick Douzet: Geopolitika a kibertér megértéséhez 19

dr. Dornfeld László
A kibertér főbb nemzetközi és nemzeti szabályozásai 43

Keleti Arthur
A kibertér biztonságának egyes aspektusai 89

Barsy Miklós
A digitális gazdaságról 129

Kilin Józsefné
A kibertér emberi erőforrásai 183

Berki Gábor
Kiberháborúk, kiberkonfliktusok 245

dr. Pintér István
A virtuális tér geopolitikája 285

Keleti Arthur
(keleti.arthur@itbn.hu)

A kibertér biztonságának egyes aspektusai

Általános tanulmány a kiberbiztonság jelenlegi helyzetéről, a SOC-ok és a Threat Intelligence szerepéről a kibertér nemzeti és üzleti védelmében

Absztrakt

A tanulmány azzal a céllal készült, hogy bemutassa a kibervédelem jelenlegi helyzetét, azt, hogy a világban az államok és magánszervezetnek mit tehetnek vagy tesznek annak érdekében, hogy a status quon javítsanak vagy jobban irányításuk alatt tarthassák illetve, hogy milyen eszközöket használnak és milyen lehetőségek és mozgástér áll rendelkezésre a további fejlesztésekre. A tanulmánynak nem célja a témában jártas biztonsági szakembereknek részletes műszaki tanácsokkal szolgálni, igyekszik inkább áttekintő útmutatást adni a geopolitikai összefüggések és hosszú távú stratégia iránt érdeklődő szakembereknek és laikusoknak.

A világban az egyik legfontosabb tényező jelenleg a kiberbiztonság. Ennek hiánya évente több mint 400 milliárd dollár kárt okoz és világviszonylatban sok milliárd dollárt költenek a kár enyhítésére. Még mindig sok probléma van a biztonsági rendszerekkel, melyeket a szakemberek próbálnak beazonosítani és befoltozni. A kiberbiztonsági szakemberek csapatokba és központokba történő szervezése és a SOC létrehozása nemzeti és vállalati szinten fontos feladattá vált. Az ilyen központ minden szervezetnél létfontosságú, nagy mennyiségű technológia és emberierőforrás beruházásra van szükség hozzá és érdemes kiegészíteni Threat Intelligence-szel is. Az új technológiák oldalán figyelemre méltóak a Behavior Based Cyber Security megoldások is.

Kulcsszavak: kibervédelem, kiberbiztonság, biztonsági rendszerek

Abstract

The objective of this chapter of the study was the introduction of the present status of cyber security. What nation states and private companies of the World are doing to develop or take status quo better under their control, what tools are used in the process and what possibilities and room they have for further development. Giving deep technical advice to battle hardened cyber security professionals is not aim of this study, it however provides a general overlook for pros and non-pros interested in contexts of geopolitics.

One of the most important factors of the World today is cyber security. The lack of it causes an annual 400 billion us dollars damage and many billions of dollars are spent on mitigating that damage worldwide. Problems of security systems are present and an ongoing work of security professionals to identify and patch them is a daily task. Grouping cyber security pros, organize them into centers and the making of SOCs is a top level priority of nations and companies. Such a center is vital to organizations, it requires big technological and human resource investment and it is highly advisable to extend it with Threat Intelligence. On the side of new technologies Behavior Based Cyber Security solutions are worth to keep an eye on.

Keywords: cyber security, security systems

1. Bevezető

Jelenlegi tanulmányfejezet azzal a céllal készült, hogy bemutassa a kibervédelem jelenlegi helyzetét, azt, hogy a világban az államok és magánszervezetnek mit tehetnek vagy tesznek annak érdekében, hogy a status quon javítsanak vagy jobban irányításuk alatt tarthassák illetve, hogy milyen eszközöket használnak és milyen lehetőségük és mozgásterük áll rendelkezésre a további fejlesztésekre.

A tanulmánynak nem célja a kibervédelemben mélyen jártas biztonsági szakembereknek részletes műszaki tanácsokkal szolgálni, igyekszik inkább áttekintő útmutatást adni a geopolitikai összefüggések és hosszútávú stratégia iránt érdeklődő szakembereknek és laikusoknak.

A kérdéskör feldolgozásakor az anyag az alábbi struktúrát és tematikát követi:

1. Elsőnek a jelenlegi probléma bemutatásával, a kibertámadások számával, a támadók kilétének és motivációjának sokféleségével, a bonyolult állami és céges folyamatokkal, a nagy adatmennyiséggel és a lassú reakcióidőkkel foglalkozunk.
2. A második szakaszban a fenti probléma megoldására tett erőfeszítések logikájába tekintünk bele a kiberbiztonsági képességek érettségi modelljén (https://www.sbs.ox.ac.uk, 2014), a kiberbiztonsági kapacitások építésén, a Security Operations Center (SOC) felállításán, a Threat Intelligence megoldások igénybevételén és a viselkedés alapú megoldások lehetőségeinek (https://techcrunch.com, 2015) bemutatásán keresztül.
   a) Kiberbiztonsági kapacitások modelljét határozzák meg és
   b) Építenek kapacitást (Az egyes országoknak milyen kiberkapacitásuk van jelenleg, mennyit költenek és főleg mire?)
   c) SOC-ok építése (Mi az, miért van? stb.)
   d) Threat Intelligence igénybe vétele és gyártása (Mi az, miért van? Fő szereplők Cisco, FireEye, TrendMicro, Checkpoint, RSA stb.)
   e) Rövid kitekintés a viselkedés alapú megfigyelési technikákra (Behaviour Based Cyber Security)
3. Az utolsó részben pedig összefoglaljuk a tanulságokat, megállapításokat teszünk és levonjuk a megfelelő konklúziókat.

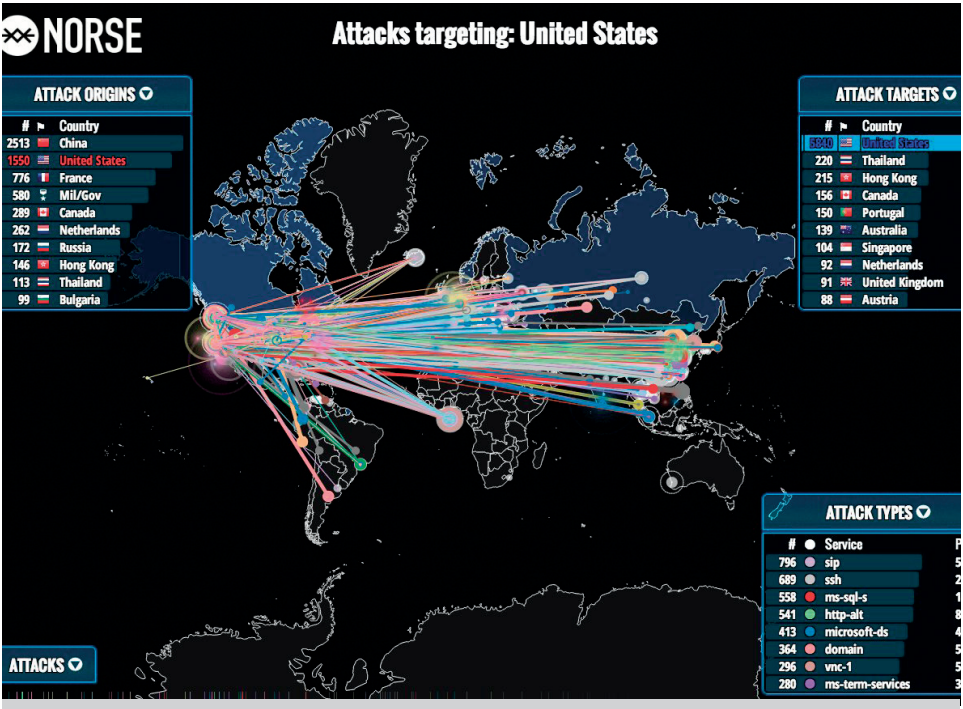
2. Jelenlegi állapot

A nemzetközi és azon belül a magyar kibervédelem nincs sokkal jobb helyzetben, mint a 16. századi európai végvárrendszer: kevés az ember, kevés a pénz és sok a támadó. Ráadásul a védelmi rendszer gyakran elavult, sok helyen lehetnek rések, gyakran azt sem feltétlenül vesszük észre, ami a saját kertünkben zajlik. A globális trendek azt mutatják, hogy a jó szakember ritka mint a fehér holló, az USA-ban például csak 2015-ben több mint 200.000 kiberbiztonsági szakértő állása maradt betöltetlen (www.csoonline.com, 2015), de Magyarországon is hiány van jó informatikai és kiberbiztonsági szakemberekből (www2.deloitte.com, 2016). A cégek gyakran csak azért tartanak fenn kibervédelmi részleget, hogy a belső irányelveknek megfeleljenek és a kliensek által elvárt "biztonságot" megteremtsék, de nem mindig fakad ez belső indíttatásból vagy kellő biztonságtudatból.

A dark weben (amely az internetről egy TOR böngészővel bárki számára elfogadható anonimitást biztosítva elérhető) bárki vehet magának egy-egy hackert vagy bármilyen adatot, csak pénz kérdése a dolog, például 65 millió Tumblr jelszó csak 0.4255 BTC (Bitcoin) ($150) (Deepdotweb, 2016) vagy egy 379 millió bejegyzést tartalmazó adatbázis, amiből 33 millió Twitter jelszó, csupán 10 BTC ($5800) (Mashable, 2016). Az országok dollármilliárdokat (az USA 2017-es költségvetésében 6.7 milliárd dollárt irányoztak elő kiberműveltekre) (www.militaryaerospace.com, 2016) költenek az egymás elleni kiberháborúra, az IT cégek azért hogy a riválisuk előtt járhassanak, bármilyen eszközt bevetnek. Jelenleg a kibertér egy virtuális vadnyugat, ahol lehet fegyver vagy védelem nélkül járkálni, de nem érdemes.

A támadók nagyságrendileg vannak előnyben a védőkkel szemben, míg egy hacker pontosan tudja, mit keres, a védelmi szakembereknek tengernyi adatot kell átfésülniük hogy megtalálják a behatolók nyomát és elhárítsák a fenyegetést. Egy SOC (Security Operations Center) kiépítése és fenntartása cégenként felettébb költséges és az embererő igények miatt könnyedén lehet fenntarthatatlan. A költségek optimalizálása és a szakemberhiány kompenzálása indokolja, hogy a szolgáltatásokat kívülről vásárolják meg a cégek, ezért számtalan szolgáltató van, akik különféle SIM-SIEM (Security information management – Security information and Event Management) szolgál-

(Forrás: map.ipviking.com,2016)

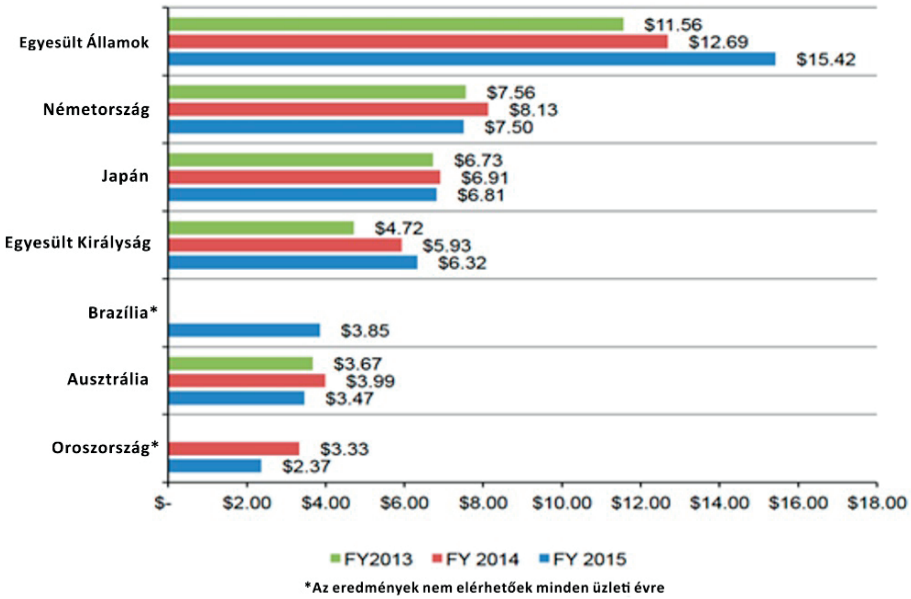


A fenti képen egy threat map látható, amely azt mutatja, hogy mely országokból mely országok felé indulnak az aktuális pillanatban kibertámadások. Ezek azok a támadások, amelyeket az adott szolgáltató rendszere aktuálisan érzékel. Szakmai körökben több kritika érte az ehhez hasonló threat map-eket, mivel nyilvánvalóan nem adnak pontos és akkurátus információt a támadásokról. Ugyanakkor a kiberbiztonsági szakemberek a biztonsággal kapcsolatos legnagyobb problémája a helyzet vizualizációja a releváns döntéshozók számára. Ezt a feladatot tökéletesen ellátja a térkép, mint ahogy konkrétan országokra vagy akár iparági csoportokra leszűrve pedig részletesebb információt is ad, ezért nem ritkán használják SOC-központokban is vagy szakmai bemutatókon.

tatásokat kínálnak (lásd később). De ez nem csak a vállalatokat érintheti. Észtország 2016 nyarán úgy döntött, hogy Angliában helyezi el kormányzati szervereit, mert tart az orosz hackerek támadásaitól (www.ft.com, 2016).

Az „IBM Security Services Cyber Security Intelligence Index," ami 3,700 IBM-kliens részletes analízisét és kiberbiztonsági eseményeit írja le 130 ország-

Ábra 1. A kiberbűnözés összköltsége hét országban
A költségek amerikai dollárban kerültek feltüntetésre (000,000), n = 252 különböző cég



(Forrás: Ponemon Institute: 2015 Cost of Cyber Crime Study: Global, 2015)

A cégeknek egyre több és drágább kihívással kell szembenézni, amint az a fenti ábrából is látható. Hogy jobb áttekintést kapjunk, vizsgáljuk meg a sikeres támadások számát.

2015: 477 támadás 252 szervezetben, avagy 1.9 sikeres támadás cégenként mindent héten

2014: 429 támadás 257 szervezetben, avagy 1.7 sikeres támadás cégenként mindent héten

2013: 343 támadás 234 szervezetben, avagy 1.4 sikeres támadás cégenként mindent héten

2012: 262 támadás 199 szervezetben, avagy 1.3 sikeres támadás cégenként mindent héten

(További értékek és táblázatok: Ponemon Institute© Research Report, 2015 Cost of Cyber Crime Study: Global Benchmark Study of Global Companies Ponemon Institute October 2015.) Ezért van szüksége a cégeknek sokkal alaposabb megközelítésre rendszereik megvédéséhez.

ból, 2012-ben 137,4 millió incidenst említ, amikor valami kártékony tevékenység megpróbált információs rendszereket és adatot ellopni, megzavarni, működés képtelenné tenni vagy elpusztítani. Ez 2.6 millió támadás minden héten, és 0,38 millió minden nap. Ezek közül egymillióból 1,07 volt sikeres. Hogy ezek a támadások mennyi kárt okoztak? A Ponemon Institute becslései alapján egy szervezeti adatbiztonsági incidens átlagban fájlonként 188 dollárba kerül, összesen így 5,4 millió dollárt vesztettek a cégek. De a közvetett költségek és a további implikációk költségei még ennél is magasabbak; egy cég reputációja nagyjából 21%-ot zuhan egy-egy sikeres támadás során, amikor a támadók ügyféladatokat is megszereznek. Ez összesen átlagosan 332 millió dollárt jelent állományonként. A támadások száma az elmúlt 4 évben lényegesen nőtt és az ellopott adatok mennyisége is nagyságrendeket ugrott, a támadások sebességéről nem is beszélve (a 2016-os Anonymous hacker csoport támadásában a Fülöp-szigetek választási rendszere ellen 55 millió választó adatát lopták el és tették közzé órák alatt) (www.hackread.com, 2016), tehát ez az összeg a helyzettől függően 2016-ban már ennek többszöröse is lehet.

3. A probléma megoldása

Az országok és vállalatok döntéshozóinak komoly kihívást jelent a kiberbiztonság kérdése. Egy láthatatlan csatatérbe kell dollármilliókat invesztálniuk, amelynek elég kétes a megtérülése. Milyen opciói vannak tehát annak, aki biztonságban szeretné tudni az állampolgári vagy szervezeti adatait? Az információmegosztásban az, hogy minden cég minden titkát, adatát publikusan elérhetővé tegyen – effektíve nyílt lapokkal játssza –, egy ilyen szinten kompetitív szférában öngyilkossággal érne fel. Tehát a „nekem nincs semmi titkom, nem árthatnak nekem" mint általános irányelv nem állja meg a helyét. Ugyanígy a „kétszer nem csap ugyanoda a villám" sem igaz. A kibertámadások jelentős része nem pillanatszerű, nem egy-egy specifikus dolog az, ami kell a támadóknak, hanem időben hosszan elnyújtott folyamat. Ha egyszer bejutottak egy rendszerbe azok, akiknek nem a károkozás a célja, hónapokig, évekig bujkálhatnak a háttérszervereken, és közben felbecsülhetetlen mennyiségű és értékű adatot bányásznak ki. Még 2016-ban is az átlagos rendszerben

maradó „lappangási ideje" a hackereknek anélkül, hogy észre vennék őket, átlagosan 200 nap (blogs.microsoft.com, 2016).

Hogy biztonságban legyenek az adataink, egy-egy védelmi technológia (pl. tűzfal vagy antivirus) vajmi kevés védelmet nyújt. Több megoldás vagy szolgáltató kombinált szolgáltatásainak fenntartása jár bizonyos előnyökkel, például esetlegesen két nem teljesen azonos adatbázisból dolgoznak vagy eltérő ország és információhátterük van (mint pl. az orosz Kaspersky, a japán TrendMicro vagy az amerikai Intel Security), tehát nagyobb spektrumot fednek le, például Kelet-Európából is érdemes orosz és kínai szolgáltatókat igénybe venni, mivel azok a saját régiójuk tipikus fenyegetéseit jobban ismerhetik, mint egy nyugati szolgáltató. Ugyanakkor különböző fejlesztők szoftvereit összehangolni, karbantartani, a kapott eredményeket értelmezni hihetetlenül nehéz. Egy nagyvállalat szó szerint milliónyi eseményt generál percenként, ráadásul sok esetben ütköző funkciókat tartalmaznak, aminél szükséges egyes dolgok kikapcsolása, az ideális beállítástól való eltérés, ergo biztonsági rések szándékolt bent hagyása a rendszerben. Sajnos általános tapasztalat, hogy ezek a kockázatokat jelentő beállítások komolyan gyengítik a rendszerek védelmét.

Hogy ezeket elkerülhessük, ajánlott egy a feljebb már említett Security Operations Center (SOC) kiépítése vagy pedig egy MSSP (Managed Security Service Provider) szolgáltatás igénybevétele.

3.1. Kiberbiztonsági képességek érettségének meghatározása

Az alábbi rendszert az oxfordi Global Cyber Security Capacity Center dolgozta ki azzal a céllal, hogy egy jól meghatározható formában lehessen besorolni a cégeket és országokat az alapján hogy a lehetőségeikhez képest milyen szinten állnak kiberbiztonsági képességek és kapacitások szempontjából. Öt dimenzió alapján mérik a képességeket, minden egyes dimenzión belül számos további faktor található.

A kiberbiztonság öt dimenziója, ami ma meghatározza a képességeket és kapacitásokat:

1. Kiberpolicyk és stratégiák szintje
2. A társadalmon belüli felelős kiberkultúra színvonala
3. A kibertudatosság az egyszerű dolgozótól a vezetőkig

4. Jogi szabályozás hatékonysága
5. A kockázatok korlátozása szabályozással, standardizálással és technológiával

Ezek alapján besorolható az ország egy úgynevezett cyber security capability maturity modellbe, ahol a legalacsonyabb szint azt jelenti, hogy gyakorlatilag nincsenek kiberbiztonsági kapacitások, a legmagasabb pedig, hogy minden elképzelhető eszköz és tudás rendelkezésre áll.

3.1.1 Az egyes szintek:

- Start-up: ezen a szinten nagyjából semmi nem létezik még, vagy még csak embrionális állapotban, esetleg tervek szintjén.
- Formálódó: néhány dolog már elkezdett kialakulni, de gyakran ad-hoc, rosszul definiált és szervezetlen.
- Kialakult: a védelem elemei a helyükön vannak és működik is, de még kiegyensúlyozatlan, esetleges az erőforrások eloszlása.
- Stratégiai: már eldöntött, hogy mi mennyire fontos, mire mekkora erőforrásokat allokálnak.
- Dinamikus: tisztán látható stratégia van arra, hogy az erőforrásokat bizonyos helyzetekben hogyan csoportosítsák át, a döntéshozás gyors, és folyamatos a környezet megfigyelése.

3.1.2.Kategóriák, ami alapján a szervezet besorolható:

1. Dimenzió
   a) Nemzeti kiberbiztonsági stratégia: milyen szinten és milyen mélységben került kidolgozásra, milyen forrásokkal rendelkezik, mennyire rugalmas.
   b) Incidens válasz: hogyan, milyen gyorsan, milyen eszközökkel történik.
   c) Kritikus nemzeti infrastruktúra védelem: mit, milyen erővel és hogyan védenek.
   d) Krízis menedzsment: mik az akciótervek, hogyan mérik fel a krízis nagyságát, hogyan reagálnak.
   e) Kibervédelmi megfontolások.
   f) Digitális redundancia: mennyire optimalizált a rendszer, vannak-e olyan részei amik ugyanazt a feladatot végzik.

2. Dimenzió
   a) Kiberbiztonsági mind-set: milyen az emberek hozzáállása a kiberfenyegetésekhez.
   b) Tudatosság: mennyire vannak az emberek tisztában a fenyegetéssel.
   c) Bizalom az internetben: mennyire bíznak az emberek az online szolgáltatásokban.
   d) Online magánélet: mennyire fontos, és mit tesznek a megőrzése érdekében.

3. Dimenzió
   a) Nemzetileg elérhető kiberoktatás: mit tesz az állam, hogy a polgárai ismerjék a veszélyeket
   b) A kiberoktatás központi fejlesztése: van-e elég szakértő oktató, ha nincs, tervezik-e orvosolni a hiányt, tanterv fejlesztése.
   c) Céges képzések, a cégek bevonása az oktatásba: vannak-e ilyen tervek vagy már folyamatban lévő programok.
   d) Vezetők hozzáértése: mennyire vannak tisztában a cégek döntéshozói a kiberfenyegetésekkel.

4. Dimenzó
   a) Kiberbiztonság jogi keretei: jogi környezet kialakítása, ennek a színvonala.
   b) Törvényes vizsgálatok: vannak-e a rendfenntartó szerveknek emberei arra hogy fellépjenek a kiberbűnözők ellen és betartassák a szabályokat, a bíróságok értenek-e a témához annyira, hogy releváns döntést hozzanak.
   c) Felelősségteljes közzététel: hogyan szabályozott az adatok, sérülékenységek kiadása, kezelése.

5. Dimenzió
   a) Ragaszkodás a standardekhez: a kötelező folyamatok lefektetése, betartása.
   b) A nemzeti infrastruktúra rugalmassága: új technológiák beszerzése és integrálása a már meglévő rendszerekbe lehetséges-e.

c) Kiberbiztonsági piac: milyen forrásból szerzik be a biztonsági technológiákat, milyen időnként frissítik azokat, esetleg adnak-e el másnak technológiákat.

3.2. Kiberbiztonság Struktúrája és működése

A kiberhadviselés mára bevált módja annak, ha egy országot vagy céget akar valaki „büntetlenül" támadni. A kibertámadások többségükben lekövethetetlenek, maximum következtetni lehet a károkozó kódjának mintázatából és stílusából, hogy vajon ki lehetett a támadó és mi lehetett a célja. A komolyabb támadásokban használt eszközök újfajta elnevezése APT (Advanced Persistent Threat), olyan megoldások ezek, amelyek általában sokáig észrevétlenül dolgoznak egy-egy rendszerben, adatokat szivárogtatnak egy távoli megfigyelőhöz, esetleg később komoly károkat okoznak közvetlenül az adott rendszernek.

Az APT-k célja gyakran „csak" adatlopás, ipari kémkedés, szabotázs, néha viszont a hagyományos hadviselés kiegészítőjeként tekintenek rá. Például a továbbra is tartó orosz-ukrán konfliktus során, a történelem során először ismerte el az USA kormánya dokumentáltan, hogy véleménye szerint valakinek sikerült egy másik ország energiaellátását kizárólag kibertámadásokkal összeomlasztani. (www.reuters.com, 2016). A feltételezhetően orosz támadás következtében 2015. december 23-án 225.000 fogyasztó maradt áram nélkül Nyugat-Ukrajnában. A támadók távolról átkapcsolták a biztosítékokat egy malware segítségével, majd az ügyfélszolgálatokat telefonhívásspammel blokkolták, elmélyítve a krízist.

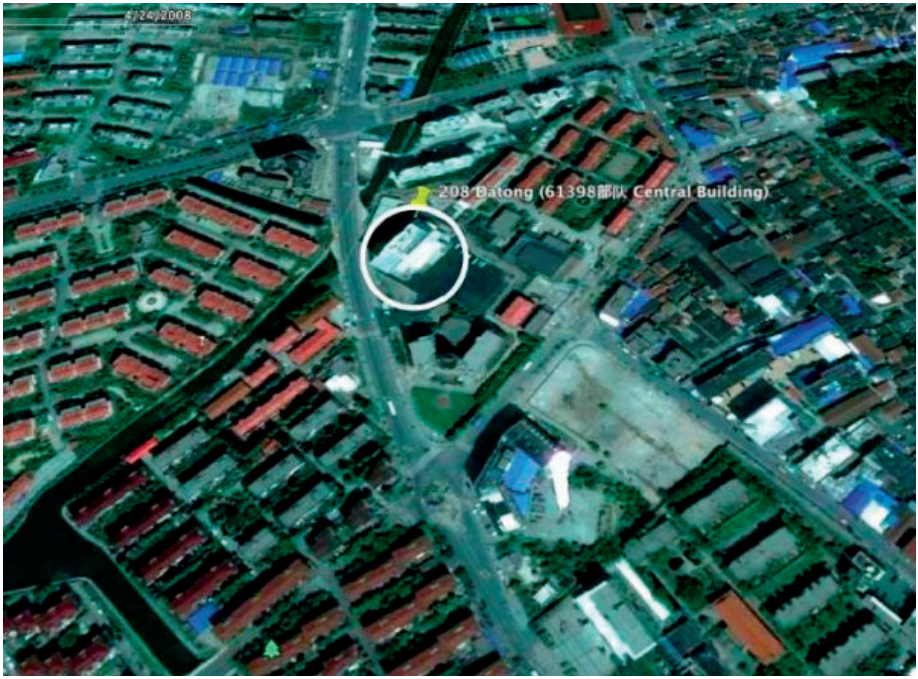
A kiberhadviselésben talán az a legszörnyűbb, hogy csak nagyon körülményesen köthetőek nemzetközi határozatokhoz, általános világelvekhez, ezért sokszor a hackerek és a megbízóik „lelkiismerete" szabhat határt, amely egy hadviselésben nehezen kezelhető elem. „Ma nem létezik olyan nemzetközi álláspont vagy keretrendszer, amely kötelező érvényű lenne bármelyik nemzetállam számára az offenzív kiberbiztonsági műveletek tekintetében." („There is no international standing or framework that is binding over any one nation-state in terms of offensive cyber operations,") – Bradley P. Moss nemzetbiztonsági ügyvéd nyilatkozta a Tech Insidernek májusban. „Bármilyen szabály,

amit magunknak határozunk meg." („It's whatever rules we put in place for ourselves.") (www.techinsider.io, 2016)

Bár az USA és Kína elviekben kötött egy megállapodást (www.nytimes.com, 2015), nevezhetjük kölcsönös kiber megnem támadási szerződésnek, ezt azóta is mindkét fél felrúgja (www.engadget.com, 2015), éppen azért mert rendkívül nehéz – ha nem lehetetlen – 100%-os bizonyossággal megállapítani a támadó személyét/országát. A nagy kiberbiztonsági vállalatok, mint a FireEye-Mandiant, Crowdstrike, Kaspersky Lab, vagy a Symantec gyakran ki tudnak deríteni mélyebb információkat, neveket, csoportokat és hogy valószínűleg ki áll a támadás hátterében, de ez messze nem elég a nemzetközi politikában.

Kik a kiberháború fő játékosai?

Egyértelműen **Kína** áll a kiberhadviselés élén. A kínaiaknak van a világon a legjobban szabályozott internete, fizetett cenzorok szabályozzák a lakos-



(http://edition.cnn.com, 2014)

ságot és a Kínai Néphadsereg kötelékében több tízezer hivatásos hacker szolgál. Nehéz felbecsülni a pontos számukat a fenti képen látható épületben; vélhetően legalább 1000 szerver szolgál ki 2000 hackert, ezt a csoportot úgy ismeri a világ hogy PLA unit 61398, más neveken „UglyGorilla," „KandyGoo", „WinXYHappy". Ez a hatékonyan működő csoport 2014 nyaráig több száz terabyte-nyi adatot lopott el legalább 141 szervezettől (pl. Coca-Cola, RSA Security és az USA kritikus infrastuktúrái) 20 iparágból 2006 óta. (edition.cnn.com, 2014)

Becslések szerint legalább 20 (BBC CIKK LD FELJEBB), de akár 50 ilyen csoport (www.techinsider.io, 2016) is működhet az országban. Pontos azonosításukat nehezíti, hogy vannak a katonaság szervezetén belül működő csoportok, katonai felhatalmazással működő kormányzati szerveknek dolgozó csoportok és vannak nem kormányzati csoportok, akik az épp aktuális érdekeik szerint cselekszenek.

Fontos játékos még **Oroszország** is. A putyini Oroszországban szintén erős az internet irányításának vágya, és az agresszív külpolitikai lépéseket gyakran támogatják meg például a fentebb említett kibertámadásokkal. Az ismételten nagyhatalmi ambíciókat dédelgető Oroszország egyre aktívabban vesz részt a világpolitikában, például aktívan befolyásolja az amerikai elnökválasztást (www.theguardian.com, 2016). Trump pedig beszédben szólította fel az oroszokat, hogy találjanak meg politikai ellenfele, Hillary Clinton által letörölt emaileket (www.nytimes.com, 2016). Az elmondottakat később úgy finomította, hogy csak szarkasztikus szeretett volna lenni, de észlelhető, hogy Trump politikája alapvetően összhangban áll az orosz törekvésekkel.

Az **USA** jelentősen lemaradt a kiberfegyverkezési versenyben. Egy, a Business Insidernek adott riport során John McAfee, az extravaganciája miatt sokat bírált, de tagadhatatlanul professzionális biztonságtechnikai szakértő azt nyilatkozta, hogy „Kínának, Oroszországnak, sőt még Iránnak is megvan a képessége arra, hogy szó szerint visszaküldjön minket a kőkorszakba".

„Egy kiberháború közepén vagyunk, ami nem közelít, nem feldereng a horizonton, hanem már itt van. És úgy tűnik, a kormányzatunkból ezt senki nem érti meg. Ha megértenék, akkor a kínaiak nem lettek volna képesek ellopni 21 millió adatot mindenkiről, aki az amerikai kormánynak dolgozott az elmúlt 50 évben."

McAfee szerint az oroszok és a kínaiak abban járnak Amerika előtt, hogy míg az USA-ban a hackereket ellenségként kezelik, addig Kínában és Oroszországban kormányzati állást ajánlanak nekik. Ezek az emberek kiemelkedően jók a saját területükön, és okosabbak mint az átlag kibervédelmi szakember.

„Olyan sokáig voltunk a világ vezető hatalma, hogy elképzelhetetlennek tartjuk, hogy Amerika csúnyán le legyen maradva a világ mögött egy olyan tudományágban, ami végtelenszer erősebb, mint az összes atombombánk és csatahajónk együttvéve. Elvakítanak a történelmi sikereink."

Természetesen az USA is hatalmas forrásokat csoportosít át kibervédelmi feladatokra, de bizonyos részei a katonai számítástechnikai struktúrának megbocsájthatatlanul elavultak (szokatlan, de érdekes példája ennek, hogy még mindig floppy diszkek vezérelik a nukleáris kilövő rendszert) (www.bbc.com, 2016).

Fontos tényezők még a kiberhadviselésben **Észak- és Dél-Korea**. Észak-Koreának nagyjából 6000 katonája teljesít szolgálatot a kiberfronton és az ország általános számítástechnikai fejletlenségéhez képest kiemelkedően jól teljesítenek (a Sony Pictures 2014-es feltörését, amely állítólag 100 terrabyte mennyiségű adat ellopásával járt is hozzájuk kötik) (www.businessinsider.com, 2014). Továbbá megvan az az előnyük mindenki mással szemben, hogy míg a támadó képességeik a legjobbak közé tartoznak, maga az ország közel sebezhetetlen, mivel az infrastruktúrájuk nincs központosítva és általánosan is nagyon alacsony az internethozzáférés.

Dél-Korea ennek nagyjából az ellentette; az ország technológiailag az egyik legfejlettebb a világon, minden központilag vezérelt, ergo erősen sérülékeny a kibertámadásokkal szemben. Hogy ezt problémát kezeljék a dél-koreaiak azt a módszert választották, hogy az amúgy is kötelező sorkatonaságot az állampolgárok letölthetik katonai kiberszakemberként is, ami egy vonzó életpálya, mert a hazafias érzelmek mellett a techorientált országban a karrierépítést is elősegíti. Az északiaknál kicsit kevesebb, kb. 5500 fős kibervédelmi hadsereg szolgálja az országot, de az ösztöndíjakkal támogatott képzésnek hála a szakembergárda magasabb színvonalat képvisel.

Irán az amerikai-izraeli Stuxnet vírus támadása után 20 millió dollárt költött el a saját kiberhadserege felállítására, ami mostanra a negyedik legnagyobbra nőtte ki magát a világon. Az USA pénzügyi szektorán kívül támad-

ták még a Saudi Aramco olajvállalatot is körülbelül 35.000 számítógép működését megállítva és több hónap folyamatos fennakadást és működési pauzát okozva ezzel a vállalatóriásnak, aki csak méretének köszönhette, hogy gazdaságilag túl tudta élni a kibertámadás okozta megpróbáltatásokat.

„Nagyon gyorsan és nagyon jelentőssé nőtték ki magukat az elmúlt néhány év alatt". („They've grown up very fast and very significant over the past few years,") David Kennedy, a TrustedSec kiberbiztonsági vállalat CEO-ja nyilatkozta ezt a Tech Insidernek. „Ráébredtek, hogy nem lehet légi vagy hasonló erőfölényük, különösen ha az Amerikai Egyesült Államokat nézzük. Tehát nagyon sokat fektetnek be a kibertér részébe." („They realize they can't have any type of superiority around air, or anything like that, especially when it comes to the United States. So they're investing a lot of it into the cyber piece.")

De hol vannak az oroszok? Már bizony ott, ahol az 1965-ös híres magyar vígjáték mondja: a spájzban. Vagyis veszélyesen közel ellenségeik számára. Természetesen a katonaság és a hírszerzés is rendelkezik kibervédelmi kapacitásokkal (ahogy azt az amerikai demokraták szerverei elleni 2016-os támadás is jól példázta), de az orosz kiberbiztonsági kapacitások egyik gerincét a nagy mennyiségű hacker adja és az a módszer, ahogy Oroszország kezeli őket. Vagyis aktívan kommunikál velük és a „munkájukért" cserébe elnézi az egyéni akciókat, ahogy Michael V. Hayden tábornok, az NSA és a CIA egykori igazgatója mondta egy 2016-os kiberhírszerzéssel foglalkozó konferencián.

Izrael jelentős erőt képvisel a kiberpolitikában. Nem elsősorban mérete, hanem inkább geopolitikai és szakmai környezete predesztinálja erre. Az ország zaklatott múltja és konfliktusokkal teli kapcsolata a szomszédjaival hamar arra az útra terelte az országot, hogy minden téren erős védelmet építsen ki. Az USA-val való együttműködés stratégiai eleme a katonai fejlesztéseknek, de Izrael jóval hamarabb felismerte a kiberfenyegetésekkel kapcsolatos veszélyeket, mint például az olyan amerikai háttérrel rendelkező piaci óriások, mint a Cisco. Az ország létrehozta a saját kibervédelmi divízióit. Az USA-t nem számolva mostanra Izrael több kiberbiztonsági eszközt és szolgáltatást exportál, mint bárki más a világon. 2015-ös jelentések szerint a kibertermékek piacából 10%-ban részesült, a befektetések tekintetében pedig ez az arány 20% globálisan (Computerweekly.com, 2016). Szám szerint csak szoftver tekintetében 60 milliárd dollárt jelentett 2014-ben (Fortune.com, 2015).

Az izraeli kiberipart a hadseregből kikerülő (a kötelező katonai szolgálatot kibervédelmi szakemberként is leszolgálhatják az állampolgárok) nagy részben tehetséges szakemberek által alapított startupok adják. Ezek elindításában, támogatásában a hadsereg is aktív részt vállal. A nagy amerikai kibervállalatok jelentős összegeket fektetnek be az itt induló izraeli startupokba, például a Cisco legalább 10 izraeli startupot vásárolt fel, többek közt az Intucellt 213-ban 475 millió dollárért. Szintén 2013-ban a Google vásárolta meg a népszerű Waze-t 1 milliárd dollárért (Techrepublic.com, 2016). És vannak a mai napig izraeli tulajdonban lévő, olyan világszinten jelentős kiberbiztonsági vállalkozások, mint a Checkpoint.

Az **Egyesült Királyság** a GCHQ (Government Communications Headquarters, amely a titkosszolgálat egy kiberbiztonságra szakosodott ágát is működteti) kiberbiztonsági területének létrehozásával és a 2011-ben bejelentett 750 millió font átcsoportosításával a klasszikus katonai kiadásokról a kiberbiztonságra alapozta a helyzetét. 2013-ban létrehozott egy keretrendszert a kiberbiztonsági információk megosztására a civil és katonai szféra közt (Cybersecurity Information Sharing Partnership), ami segítette az ország megerősödését a kiberharctéren. 2016-ban az Egyesült Királyság növelte a területre koncentrált kiadásait, 1,9 milliárd fonttal többet kívánnak elkölteni 2020-ig. Ez 1900 új szakember hadrendbe állítását jelenti 3 hírszerző ügynökség keretein belül, és létrehozzák a nemzeti kibervédelmi központot is (NCSC – National Cyber Security Centre), ami otthont ad majd az ország első kiberhaderejének (gov.uk, 2016). A szervezet létrehozásával Anglia reméli, hogy egy olyan dinamikus, a modern piaci viszonyoknak megfelelően működő szervezetet hoz létre, ami vállaltan strukturáltan kommunikál a kormányzat szándékairól, őszinte és együttműködő párbeszédet kezdeményezve a piaci szereplőkkel. (gov.uk, 2016)

3.3. SOC-megoldások

A SOC alapvetően a cég azon részlege, amelyik a rendszer kiberbiztonságáért felel. Az itt dolgozó szakemberek, a hardverek, szoftverek és know-how összessége. A már meglevő kibervédelmi rendszer ernyője alatt dolgozó csapat, akinek a feladata az illegális hozzáférések, malwarek megkeresése, azonosítása, majd kezelése. A SOC feladatkörébe tartozik a már meglévő fenyegetések analizálása,

„kriminalisztikai" elemzése, esetleg az adatok bizonyítékként való felhasználásra való felkészítése és a bekövetkező incidensekről jelentések készítése.

3.3.1. Nemzeti SOC-ok

A SOC-októl megszokott rendszerben működő nemzeti eseménykezelő központ a CERT (Computer Emergency Response Team) vagy CSIRT (Computer Securitiy Incident Response Teamnek). A jelentősebb, informatikai értelemben fejlettebb országok majdnem mind rendelkeznek saját CERT-csapattal (a teljes lista itt megtekinthető: www.cert.org, 2016), amiknek a fő feladata hogy az ország kibervédelmét ellássa vagy legalább figyelmeztetni tudjon a veszélyre. Sokszor kommunikációs és tájékoztatási feladatokat is ellát. Mint sok állami szervnek, a nemzeti CERT-eknek is kérdéses az értéke és az is, hogy milyen mértékben támaszkodhatnak rá az államok a kibervédelmük megszervezésében; a legnagyobb szereplők a nemzetközi kiberszíntéren magáncégeket is megbíznak.

Egy CERT feladata szinte teljes mértékben megegyezik a SOC-al, a legjelentősebb különbség talán a rá háruló felelősség és a feladatkör nagysága. Egy nemzeti CERT/CSIRT a teljes ország infrastruktúrájáért felel, a kormányzati szerverek, honlapok biztonságáért, esetleg kritikus infrastruktúrák kiberbiztonságáért vagy a kommunikációs biztonságért. Míg a SOC-ok általában egy területre vagy vállalatra koncentrálnak. Ugyanakkor ebből a szempontból egy csendes átrendeződés jelei bontakoznak ki az elmúlt pár év változásaiból, amely a CERT-ek feladataiból egyre többet enged át a privát vagy nemzetileg üzemeltetett SOC központoknak.

A különböző országok kiberbiztonságért felelős hivatalai között létezik szakmai együttműködés, például a NATO-tagállamok külső támadás esetén segítenek egymásnak, vagy például a kínai-orosz kiberpaktum, melynek célja az USA dominanciájának csökkentése a kibertérben. Ez persze nem azt jelenti, hogy ezek az országok nem támadják egymást, időről-időre kipattannak kisebb-nagyobb botrányok, de ahogy a kibervilágban mondják: aki nem ellensége az embernek, az szinte a barátja…

A magyar kibervédelem, mely a 2010-es évek elején a világ élmezőnyébe tartozott, ma már nincs ebben az állapotban. „Az információbiztonsági törvényt inkább átírták, hogy új szervezeti felépítést hozhassanak létre. Sokáig

azonban nem történt semmi, a régi intézmények megszűntek, elvesztették szerepüket, az újak pedig nem jöttek létre. A védelem biztosítása ideiglenesen a titkosszolgálatokhoz került, amelyeknek a támadás is feladatuk, így feloldhatatlan dilemma elé kerültek." Írja az Index egy 2015 végi cikke. Több országban végigmentek ezen a folyamaton (például Thaiföld), először a titkosszolgálatok kezelték a nemzeti kiberbiztonságot aztán „liberalizálták" éppen az információmegosztás érdekében. A jelenlegi magyar modellnek, noha az információmegosztás korlátai miatt vannak hátrányai, de komoly előnyei is jelentkeznek. A titkosszolgálatok eleve rendelkeznek operatív felhatalmazással, ezért komoly kiberbiztonsági incidens esetén nagyobb eséllyel tudnak gyorsan és hatékonyan beavatkozni a nemzet biztonságának érdekében.

3.3.2. A SOC-ot specifikusan az alábbi célokra tervezték:

- Központi helyet biztosít a cég forgalmának vizsgálatára, a fenyegetések elkülönítésére és kezelésére.
- Felkészül arra, hogy válaszoljon a kiber-incidensekre.
- Lehetővé teszi az üzleti tevékenység folytatását és a hatékonyság visszanyerését. A Ponemon tanulmányban vizsgálta, hogy a külső költségeken belül az üzleti tevékenység megzavarása (szerver-leállás ideje, belső rendszer összeomlasztása, kommunikáció ellehetetlenítése) volt a legmagasabb. (Ponemon, 2015, 16. oldal)
- Megakadályozza, hogy az üzleti infrastruktúrát károsítsák a kiberfenyegetések.
- Részletes szakértői jelentésekkel járul hozzá a vállalat működéséhez.
- Biztosítja, hogy azok a csoportok, akik a kritikus védelmi rendszereket figyelik (tűzfalak, behatolás-védők, jogosultságkezelők, naplóelemzők, hálózati infrastruktúra routerek) potenciális fenyegetés esetén hamar tudjanak reagálni.

3.3.3. A SOC feladatai még specifikusabban:

- Megfigyelés, analizálás, korrelációk észrevétele és a behatolási események feltárása.
- Mintázatok feltárása a fenyegetésekben és a potenciális hatásuk elemzése az üzleti tevékenységre.

- Megfelelő védelmi eljárások kifejlesztése védekezésre, elhárításra és válaszra.
- Incidenselemzés lefolytatása és a behatolás bűnügyi elemzése.
- A krízishelyzeti eljárásokban és kommunikációban való részvétel.

3.3.4. Mi az MSSP, és SOC-ra vagy MSSP-re van-e szükség?

Az MSSP tulajdonképpen egy külsős szolgáltató cég, a SOC-ok működtetésére specializálódik. Specializálódásuk okán sokkal hatékonyabban tudják ellátni ezt a feladatot, mint azok a hagyományos IT cégek akiknek házon belül kell ezt megoldani. Egy MSSP szolgáltató lényegében plusz kapacitást jelent anélkül, hogy a cégnek foglalkoznia kelljen egy teljes rendszer kiépítésével és működtetésével.

Hogy melyik megoldást kell választani, sok tényezőtől függ, ezért egymagában a CEO, CTO, CIO vagy a biztonságért felelős CISO és CSO nehezen tudják eldönteni. Jellemzően nincs egyértelmű válasz arra, hogy az olyan globális kiberbiztonsági kérdésekben, mint a kiberbiztonsági kapacitás kiépítése, pontosan kinek kell a döntéseket meghozni, az IT szakembereknek vagy pedig az üzleti vezetőknek. Nagyon ritka, hogy egy vezető átlátja a cég „globális" működését üzleti, adatvédelmi és kiberbiztonsági aspektusból is, és minden szempontból kompetens. Mind a SOC, mind az MSSP megoldás jár előnyökkel és hátrányokkal, ezeket fogjuk a következőkben taglalni.

3.3.5. Belső SOC előnyei

- Specifikus belsős csapat, magasan képzett szakemberek értékes tudással (egy tanfolyam ára akár 5-6 ezer dollárra is rúghat) (sans.org, 2016), akik mindig elérhetőek.
- Jobban ismeri a cég belső működési mechanikáit, mint egy third-party partner (ez egyébként az egyik legnagyobb előnye a belső SOC-nak, nem véletlenül szoktak nagyobb szervezetek a saját erőforrásból felépített SOC mellett dönteni).
- A megoldások sokkal személyre szabhatóbbak.
- Nagy valószínűséggel hamarabb észreveszi az összefüggéseket a belső csoportok között, például ha az egyik divízió működése potenciálisan kiszolgáltat egy másikat, támadhatóvá teszi azt.

- A logokat helyileg tárolja, az adatok kiszolgáltatása sok esetben lehet törvényellenes (nemzetbiztonság), vagy ütközhet a cég belső adatkezelési szabályaival. A logok kezeléséről bővebben: csrc.nist.gov, 2006.

3.3.6. A belső SOC hátrányai

- Sokkal nagyobb egyszeri befektetés (a fizikai berendezések, a szoftverek, a képzések ára könnyedén elérheti a félmillió dollárt is).
- Nagyobb a nyomás, hogy jobb befektetés-arányos megtérülést mutasson.
- Nagyobb az esély, hogy az elemző közvetlen találkozik a támadóval.
- Valószínűtlenebb, hogy a finom mintázatokat észreveszik a nagyméretű rendszerekben.
- Nehéz jó szakembert találni, képezni és megtartani.

3.3.7. Kérdések, amiket érdemes feltenni

- A csapatunknak megvan a képessége (tehetsége és tudása) arra, hogy egy SOC-ot hatékonyan tudjon üzemeltetni?
- Ha megvannak ezek a képességek, hogyan akarjuk ezeket kiaknázni?
- Hajlandóak vagyunk az időt és energiát fektetni a SOC összes folyamatának és módszerének dokumentálásába?
- Ki fogja a képzési programot elkészíteni?
- Ki fogja a fizikai berendezéseket összeállítani?
- Képesek vagyunk arra, hogy elég embert felvegyünk és egy hatékony csapatot fenntartsunk?
- Ha ezek az összetevők hiányoznak, nem érdemes belevágni, mivel jelentős források árán hamis biztonságérzetet teremtenénk, ami később valószínűleg visszaütne.

3.3.8. A siker összetevői

- Profi csapat.
- Jó SOC menedzsment.
- Elégséges büdzsé.
- Hatékony folyamatok.
- Az incidenskezelésbe való bevonás.

3.3.9. Az MSSP előnyei

- A nagy kiadások elkerülése – a hardver- és a szoftver-megoldás egyben.
- Potenciális új ügyfelekkel való megismerkedés.
- Gyakran olcsóbb, mint házon belül megoldani.
- Kisebb az esély arra, hogy a támadó és az elemző összeütköznek.
- Nem részrehajló.
- Potenciálisan rugalmas és skálázható
- Nagy tapasztalat megfigyelésben és SIM (Security Intelligence Management) eszközök terén.
- SLA – Service Level Agreement (szolgáltatási szint biztosítása).

3.3.10. MSSP hátrányai

- Szerződéses partner soha nem fogja olyan jól ismerni a rendszert, mint egy belsős csapat.
- A munkák kiszervezése csökkentheti a belső morált.
- A dedikált belső csapat hiánya.
- Az adatok hanyag kezelésének veszélye (ezt auditokkal karban lehet tartani).
- A logok nem elérhetőek bármikor.
- Rugalmatlan szerkezet, az MSSP-k standard módszereket alkalmaznak a minél nagyobb kliensbázis lefedése érdekében.

3.3.11. Általános kérdések a potenciális MSSP felé

- Milyen a reputációja?
- Kik az ügyfelei?
- Vannak-e már ügyfelei az iparágunkban (ez akár állami vagy nemzeti is lehet)?
- Skálázható-e a cégünk / feladat méretéhez?
- Milyen régóta partnerei a jelenlegi ügyfelei?
- Milyen arányú közöttük a szerződésbontás, szerződésmegújítás elmaradása?
- Hogyan védik meg az adatokat, milyen szintű a biztonság az ő SOC-üknél?

3.3.12. Az MSSP belső csapata felé releváns kérdések

- Mennyire tapasztalt a csapat? Felfogadnak-e etikus hackereket?
- Ellenőrzik-e az új alkalmazottak hátterét?
- Kiszervezik-e bármelyik munkafolyamatukat?
- Az alkalmazottak elég szigorú titoktartási szerződést írnak-e alá?
- Milyen a tapasztalt mérnökök aránya a kliensekhez képest?
- Milyen képesítésekkel rendelkeznek a senior/junior alkalmazottak?
- Milyen az alkalmazotti felmondási arány?

Tekintettel arra, hogy az eseményszám nagyobb szervezetnél elérheti akár a 20 milliós nagyságrendet is (nextgov.com, 2013), ezért a kapacitás tervezése kulcsfontosságú, amikor kiberbiztonsági eseményeket akarunk kezelni. A probléma súlyát érezhetjük, ha egy pillantást vetünk két professzor Doug Altner és Les Servi matematikai mélységű tanulmányára (A Two-Stage Stochastic Shift Scheduling Model for Cybersecurity Workforce Optimization with On Call Options), amelyben a kiberbiztonsági erőforrások időbeli optimalizálására dolgoztak ki modelleket ismeretlen és bizonytalan munkaterhelés mellett (Doug Altner és Les Servi, 2016).

Költségek lebontása	Naplóelemző megoldás (SIEM)	Távfelügyelet (MSSP)	Megtakarítás	%
Eszközök (Termék ár) SOC infrastruktúra (a termék vásárláshoz)	$400,000			
MSSP (távfelügyeleti) díjak / induló költségek	$100,000	$30,600		
Teljes / Kezdeti	$500,000	$30,600	$469,400	94%
Éves / Folyamatos kiadások				
Erőforrások (2FTE azaz 2 db teljes munkaidős munkatárs)	$212,500			
Vezetői költségek	$106,250			
Biztonsági szakmérnöki költségek	$78,750			
Oktatás	$11,250			
Eszközök és karbantartás	$90,000			
SOC működtetési költségek	$9,200			
Értékcsökkenés és Amortizáció	$166,667			
Folyamatos tanácsadói költségek	$12,500			
Hálózati behatolásvédő (IDS / IPS)	$10,000			
MSSP (Távfelügyeleti) díjjak		$511,240		
Teljes (folyamatos, megújuló)	$697,117	$511,240	$185,877	27%

(Forrás: Wyndham Worldwide, 2012)

3.3.13. Ha úgy döntünk szükségünk van egy SOC-ra

A cégnek muszáj megterveznie a kiépítés folyamatát. Ez a tervezési fázis gyakran csak az emberekre, folyamatokra, technológiára terjed ki, míg az alapvető motivációk feltérképezését – hogy miért hozzuk létre pontosan a SOC-ot és mire fogjuk használni – kihagyja. A sikeres munkához a fentiek nélkülözhetetlenek. A kezdeti, tervezéssel töltött idő hosszú távon megtérül. Mielőtt a cég kiépítene egy SOC-ot, fontos hogy megválaszolja tehát a következő kérdéseket:

- A szervezet milyen szükségleteit elégíti ki majd a SOC?
- Pontosan milyen feladatok tartoznak majd a SOC-hoz?
- Kik dolgozzák majd fel a SOC által gyűjtött információt? Mit várnak ők el a SOC-tól?
- Ki képzi majd ki és milyen anyagok mentén a SOC használatára a cég többi részlegét?
- Ki lesz az, aki a döntéshozóknak bemutatja a költségeket, megtérülést és a várható előnyöket?
- Milyen jellegű biztonsági eseményekkel foglalkozik majd a SOC?

A HP Building a successful SOC Business Whitepaper-ében (HP, 2013) részletesen ír a SOC rendszer kiépítésekor szükséges összetevőkről. Az építés során a kiadási- és megtérülési tervet is el kell készíteni.

Az alábbi lista jó kiinduló pontot adhat ezek elkészítéséhez:

Felszerelés

Bútorok, számítógépek, speciális fizikai biztonsági rendszerek, telekommunikációs rendszerek, áram, fűtés, légkondicionálás.

SOC-munkaerő

Biztonsági elemzők, műszakvezetők, SOC menedzserek.

Támogató munkaerő

Hálózati támogatás, rendszertámogatás, adatbázistámogatás, telekommunikációs támogatás, biztonságieszköz-menedzsment.

Oktatás és képzés
Tanórák, konferenciák, folyamatos képzés. Az összköltség jelentős százalékát adja (lásd a táblázatban).

Threat Intelligence előfizetések
Mindig up-to-the-minute információkkal kell rendelkezni a legújabb fenyegetésekről. Megfigyelési technológiák: hardver, szoftver, tárhely és megvalósítási szolgáltatások.

További technológiák
Probléma- és változásmenedzsment, e-mailek, tudásmegosztás. Ezeken nehéz spórolni, az alábbi pontokban a költségek csökkenthetőségével, ROI-val foglalkozunk:

Költségelkerülés
Egy SOC kiépítése valószínűleg kisebb költségvonzattal jár, mint nem észlelni és nem megakadályozni a kibertámadásokat.

Költséghatékonyság
Nagy rá az esély hogy a SOC-folyamatok és technológiák segíthetnek automatizálni és hatékonyabbá tenni már meglévő funkciókat a vállalaton belül. Bizonyos fenyegetéstípusokban az új adatfolyam befogadásával, az ebből nyert adatok elemzésével, valamint az automata jelentési rendszer felállításával, a manuális feladatok csökkentésén keresztül a SOC költséget takaríthat meg a vállalatnak.

Javított biztonsági ROI
A legtöbb cég számos különböző biztonsággal kapcsolatos technológiába fektet (DLP, AV, IDPS stb.). A maximális hatékonyság elérése érdekében az összegyűjtött adatok feldolgozása és analizálása kulcsfontosságú. A korreláló adatok a technológiák közt tovább növelik a befektetés értékét és hatékonyságát.

Költségmegosztás
Néha már létező csoportok végeznek olyan tevékenységet, melyet később a SOC lát majd el. Ezek a csoportok kihelyezhetik ezeket a feladatokat a SOC-hoz. Esetleg egy partner céggel együttműködve csökkenthetők a kiadások.

Kereskedelmi előnyök
Az információbiztonság talán még soha nem volt olyan fontos kérdés, mint manapság. Egy jó SOC jelenléte a cégen belül segítheti az ügyfelek vagy állampolgárok bizalmának elnyerését, bizonyos piacokra való belépést és a konkurenciával szembeni előny megszerzését.

A csapat
Amint az eddigiekben taglalt alapokat lefektettük, a SOC kiépítése folytatódhat a hagyományos IT projekthez szükséges eszközök (emberi erőforrás, folyamat-szervezés, technológia) előteremtésével. Ezek egyenlő fontosságúak; a cégek leggyakrabban a megfelelő munkaerő alkalmazása és megtartása során vétenek hibát.

Kiválasztás
Belső SOC kiépítésekor a leggyakoribb hiba a nem megfelelő munkaerő alkalmazása. A vállalatok gyakran túl alacsonyra teszik a mércét az elemzők kiválasztásakor. Egy SOC elemző az információbiztonsági közösség gyalogosa, az az egyén, aki napi szinten száll harcba egy kemény és kreatív ellenséggel. Ez az ellenség pontosan ismeri az elemző munkájának nehézségeit, azt, hogy milyen nehéz egy monitor előtt ülve ezernyi jelentésből kiemelni a valóban fontos rosszindulatú támadásokat. A hatékony SOC elemzőinek végtelen türelemre van szüksége, és arra, hogy képes legyen észrevenni a problémákat és nyugodtan kommunikálni stresszes időkben is. Ez több, mint amit egy belépő szintű IT alkalmazottól várhatunk.

Az elemző pozícióba érkezhet akár korábban help-desk operátorként dolgozó munkatárs is, de jobb kiindulópont lehet, ha a rendszeradminisztrátorok vagy rendszerüzemeltetők közül választunk. Az ideális személy tapasztalatot szerzett rendszerüzemeltetésben, szerverekben és támogatásban, általában rendelkezik a szükséges problémamegoldó képességgel, és jól

működik elemző feladatkörben, melynek része a TCP/IP protokollok kezelése és a különböző behatolásra utaló jelek felfedése. A fenti kvalitások mentén összeállított csapat létrehozása önmagában is problémát jelenthet (bérköltség, kulturális konfliktusok stb.). Ezt sok cég úgy oldja meg, hogy a kezdő SOC-csapatot később folyamatos képzés során juttatják el a minimálisan elvárt tudásszintre.

4. A Threat Intelligence

4.1. Mi az a Threat Intelligence?

A Threat Intelligence-nek nehéz pontos magyar fordítást találni, talán a fenyegetettségi hírszerzés áll a legközelebb hozzá. Kiberbiztonsági cégek által nyújtott szolgáltatásról beszélünk, amelynek elsődleges feladata, hogy előrelátóan számolni tudjon a kockázatokkal (threat actors) és a lehetséges támadásokat időben észlelje, illetve együttműködve a biztonsági központokkal esetleg megállítsa azokat.

Ezek szolgáltatásaikkal a SOC és MSSP csapatokat támogatják, tájékoztatják őket a fennálló veszélyek és a jövőben várható támadások természetéről, ismerhető paramétereiről. Mindemellett hálózatvédelmi tanácsadást is nyújtanak, hogy a már felfedezett hibákat a lehető leghatékonyabban orvosolni tudják.

Miután a hálózatot fenyegető veszélyekről sikerült reális képet kialakítani, már könnyebb eldönteni, hogy pontosan milyen védelemre lesz szükség és mekkora anyagi forrást érdemes a hálózatvédelemre fordítani. Biztonsági cég alkalmazása és a „threat actor"-ok (fenyegető felek) felfedése ma elengedhetetlen, máskülönben az esetleges támadásokból származó veszteségek bizonytalanná tehetik a cég pénzügyi jövőjét, veszélyeztetik az üzleti és gazdasági növekedést vagy kiszolgáltatottá tesznek egy államot a kibertámadásokkal szemben. Noha a védelmi rendszer felállítása és folyamatos frissítése költséges lehet, még mindig kevesebbe kerül mint a kiszivárgott adatok és az ebből adódó problémák megoldása.

Ahogy a jelenlegi állapot áttekintésében is láthattuk, ma mindent az informatika segítségével irányítunk, így informatikai eszközeink védelme meg-

kerülhetetlen, kritikus ponttá vált. A kockázat és veszélyek szintje egyre nő, ahogy a világ halad a digitalizáció útján. Gondoljunk csak egy állam olyan kritikus infrastruktúráira, mint a vízellátás, közlekedés és bankrendszerek, hogy csak néhányat említsünk. Ha ezeket éri komolyabb támadás (ahogy az például 2016 elején Ukrajnában történt), az könnyen megbéníthatná egész régiók, az ország normális működését.

4.2. Mivel dolgozik a Threat Intel?

A fejlesztők elsősorban esettanulmányok alapján dolgozzák ki a threat intelt, az eddigi támadások technikái alapján próbálnak megfelelő védelmi rendszert kiépíteni. Emellett kalkulálnak a hackerek támadásainak eddigi gyakoriságával és a használt módszerek változásaiból próbálják megjósolni, hogy a jövőben milyen irányba fejlődnek tovább az alkalmazott technikák. Ismert módszerekre készülnek fel, ugyanakkor próbálnak rugalmasak maradni, hogy látókörük minél szélesebb legyen, ezzel is növelve az elemzők hatékonyságát.

A hálózat védelme érdekében a Threat Intelligence által szállított információnak relevánsnak kell lennie a jelenlegi működő struktúrára. Ha a cégnél Threat Intelligence-t állítanak szolgálatba, előzetesen képben kell lenniük, hogy milyen veszélyeztetett rendszereik vannak és meg kell, hogy ismerkedjenek a saját hálózatukkal, annak pontos felépítésével, működésével és mindennapos műveleteivel. Ezek után van lehetőség a Threat Feed-ek megfelelő fogadására. A biztonsági programok analizálják a hálózat működését, és olyan művelet esetén, mely még nem fordult elő vagy szokatlan, a megszokottól eltér, riasztják a SOC üzemeltetőit. Ezzel jelentősen növelik a fejlett eszközöket használó adatlopásra vagy információszerzésre szakosodott hacker csoportok lebukási esélyeit. A Threat Intel táplálkozhat Big Data állományokból vagy naplóelemző rendszerek adataiból.

4.3. A Threat Intelligence fejlesztése, finomítása és alkalmazása

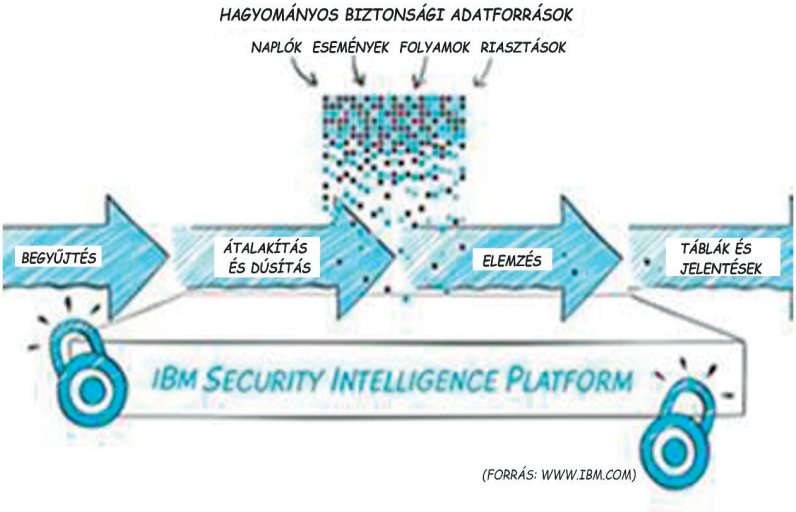
A Threat Intelligence központjában az észlelt támadások és egyéb információk kielemzését követően a Threat Intelt használó munkatársaknak lehetőségük nyílik az esetleges új módszerek, újfajta kémprogramok megismerésére, megértésére. Ezáltal fogást lehet találni azokon és a „betörési" módszerek fejlődési

sebességére is lehet következtetni abból, ahogy az előző támadáskor alkalmazott módszerekhez képest miben térnek el az új események során tapasztaltak, illetve milyen új alkalmazásokat használtak. A folyamatos biztonsági tesztelések szintén lehetővé teszik, hogy a Threat Intel mindig napra kész legyen és a lehető legjobb információt szállítsa a hálózatok számára.

Ahogy a kiberbiztonsági rendszerek egyre több támadást lepleznek le, a biztonsági cégek egyre többféle hackerek által használt alkalmazással és módszerrel találkoznak. Ezek segítségével a későbbiekben a már leleplezett támadásokat azonosítani tudják, felhasználva a már ismert kódrendszereket egyfajta „ujjlenyomatként". Hogy hatékonyabban tudjunk védekezni a támadások ellen, sokat segít, ha tudjuk, hogy támadóink mit keresnek, mi a motivációjuk és egyáltalán kikkel állunk szemben. A legtöbb esetben lekövethetetlenek a támadások, viszont ha ismert alkalmazásokat, módszereket és kódrészleteket fedezünk fel valamely esemény során, következtethetünk a támadóra és céljaira.

Ez az információ hozzásegíthet minket ahhoz, hogy a veszélyforrásokat hamarabb észleljük és az esetlegesen okozott károkat hamarabb helyreállítsuk, illetve ezek segítségével kaphatunk teljesebb képet akár a saját hálózati környezetünk sérülékenységeiről és fenyegetettségi szintünkről is.

A Threat Feedek megbízhatóságától és pontosságától függően a Threat Intelligence három fontos tényezőre ad rálátást: a múltra, a jelenre és a jövőre. A részletes jelentés egy észlelt támadásról új réseket fedhet fel a hálózatot védő kiberbiztonsági rendszeren, melyek javításával egy „ütésállóbb" rendszert hozhatunk létre. Riasztást is ad az aktuális támadásokról és fenyegetettségről, hogy azonnal le lehessen reagálni azokat. Ha szerencsénk van és megfelelően fejlett kiberbiztonsági architektúrával és csapattal rendelkezünk, akkor a megszerzett információt felhasználva megelőzhetjük, hogy akár egy szélesebb, akár egy célzott adatlopási kampánnyal a cégünket vagy hivatalunkat is sikeresen találják meg a Threat Intel által jelentett aktív hacker csoportok. Segít abban is, hogy a jövőben olyan infrastruktúrát és védelmi rendszert lehessen kiépíteni a hálózathoz, mely a lehető legnagyobb kihívást biztosítja a hackerek számára.



(Forrás: www.ibm.com)

4.4. A Threat Intelligence rendszer felhasználási lehetőségei

Érdemes arról szólnunk, hogy mi igen és mi nem a Threat Intel, mivel viszonylag új területként sok megoldással és módszerrel rendelkező szolgáltatókkal akadhat dolgunk.

A Threat Intel nem összekeverendő a Threat Feeddel. Ez utóbbit a legtöbb kiberbiztonsággal foglalkozó cég szolgáltatni tudja és tulajdonképpen arra szolgál, hogy táplálja az informatikai biztonsági rendszereket aktuális, friss információkkal, amelyek segítik a biztonsági rendszerek üzemeltetőit, hogy – lehetőleg automatikusan – elkerüljenek komolyabb hacker támadásokat. Ezek a feed-ek segíthetik a munkát és az észlelést, például nem megbízható IP címek, osztályozások, geográfiai jellemzők átadásával, de nem árulnak el sokat a fenyegetések motivációjáról, a támadók profiljáró célpontjairól és módszereiről. Az olyan Threat Intel megoldások vagy szolgáltatások tudnak nagyságrendekkel jobb minőségű segítséget nyújtani, amelyek

- képesek azonosítani a fenyegetést jelentő hacker csoportot (vagy ehhez elegendő információt szállítanak),
- körberajzolják a támadók lehetséges motivációit,
- iparágakra vagy állami szektorokra jellemző információkat adnak a hackerek tevékenységéről,

- információt adnak a használt malware-ekről, azok felépítéséről, használatuk jellemzőiről,
- meghatározzák a hacker csoportok elsődleges célpontjait,
- megmutatják az adott fenyegető csoportok támadási és cselekvési képességeit (pl. milyen anyagi vagy támogatási háttérrel rendelkeznek),
- rendelkeznek adatokkal sikeresen végrehajtott támadások elemzéssel megtámogatott részleteiről
- adatokkal rendelkeznek a csoportok által megcélzott sérülékenységek természetéről,
- tudnak historikus információkat biztosítani a csoportok tevékenységéről vagy a felhasznált malware-kről.

Egy komplex Threat Intel platformtól elvárható, hogy támogatja az együttműködést az alábbi rendszerekkel (FireEye – iSight, 2016):
- Threat Intelligence Platform (TIP): fenyegetettségi információk átadása;
- Végponti védelem: védelmi profilok meghatározása;
- Naplóelemzők (SIEM): esemény priorizációk, riasztások validálása;
- Hálózati védelem: riasztások validálása;
- Elemzési megoldások (GRC): események elemzése, mi, miért és ki követte el;
- Nyomrögzítés és nyomozás: háttérinformációk szállítása.

Amennyiben sikerül megfelelő elemző csapatot összeállítani a Threat Intel feldolgozására, és be tudjuk kötni a lehetséges információforrásokat a lehető legtöbb biztonsági eszközbe, akkor joggal remélhetjük, hogy hatékonyabb védelmi rendszert tudunk kialakítani, és jóval az események bekövetkezte előtt esélyünk lesz az elhárításra vagy a védelem megerősítésére.

4.5. Szakértői gondolatok a kiberbiztonsági cégek szolgáltatásairól

A jelenlegi megoldásokban nagyon nagy mértékben keverednek a biztonsági védelmi funkciók és a Threat Intelligence. Ezért nehéz általános véleményt adni arról, hogy mely megoldással érdemes egy vállalatnak vagy állami szervezetnek kezdenie. A megfelelő szolgáltatás vagy termék kiválasztása attól is nagy mértékben függ, hogy rendelkezik-e már az adott szervezet működő

SOC-al és fejlett védelmi technológiákkal amelyek a Threat Intel-től érkező információkat sikerrel be tudják fogadni és fel is tudják dolgozni.

Ed Tittel szakértő véleménye szerint kiberbiztonság téren a Cyveillance Cyber Threat Center és a FireEye képes a legnaprakészebb szolgáltatást nyújtani. Ezek a megoldások magas hatékonysággal védekeznek a legújabb támadási és behatolási módszerekkel szemben is, illetve a fenyegetési források leleplezése terén is kiemelkedően teljesítenek, különösen azért, mert rendszeresen hívják segítségül őket kiberbiztonsági incidensek felderítéséhez és utólagos nyomozásához. A FireEye Mandiant csapatát például a Sony Pictures elleni 2014-es támadás körülményekire felderítéséhez használták sikerrel.

Az ActiveTrust egy más típusú szolgáltatást nyújt. A legújabb fenyegetésforrások technikai hátteréről gyűjt össze adatot és tapasztalatot, majd az illetéktelen behatolás megelőzése érdekében hatékony és effektív tanácsokkal és információval szolgál. Ezzel az információval ezután segítségére lehet a klienseinek, akik tovább tudják bővíteni saját Threath Intelligence védőhálójukat.

A LogRhythm Security Intelligence egyszerűbb, felhasználóbarát felületével igyekszik különbözni társaitól. A platform hardware bázisú, integrált szoftverrel dolgozik. A felhasználónak lehetősége van választani több eszköz és kialakítás közül, a védeni kívánt hálózat mérete és infrastruktúrája függvényében (searchsecurity.techtarget.com, 2015).

Természetesen sok cégnek van még hatékony megoldása: az Intel Security, a Cisco, az RSA, a Trend Micro, a Checkpoint, a Fortinet és sokan mások kínálnak még Threat Intelt, de abban már eltérnek, hogy milyen elemző háttérrel rendelkeznek, és valójában milyen mélységig és sebességgel képesek információkat szolgáltatni.

5. Rövid kitekintés a viselkedés alapú megfigyelési technikákra

5.1. Behavior Base Cyber Security

A Behavior Base Cyber Security forradalmian új irány a kiberbiztonság területén. Ez az új technológia, ahelyett, hogy falakkal próbálná megakadályozni

a hackerek bejutását a hálózatba, azon dolgozik, hogy azonosítsa és felismerje őket akár már a támadás első perceiben is.

A viselkedés megfigyelésének több szintjét értelmezhetjük:

- biztonsági rendszerekben összegyűlt adatok elemzésével az egyes rendszerek és felhasználók viselkedési furcsaságainak jelzése,
- az üzleti és irodai alkalmazásokban fellelhető logikai inkonzisztenciák és szokatlan felhasználói viselkedések kimutatása,
- a hálózatokon, operációs rendszerekben vagy adatbázisokban zajló tevékenységben előforduló nem jellemző viselkedések észlelése,
- a felhasználók számítógépén vagy mobiltelefonján végzett tevékenységében fellelhető anomáliák, a megszokottól eltérő viselkedések kimutatása.

A kinyert adatok feldolgozására új technológiájú a Big Data elemzési módszereket és gyakran már mesterséges intelligenciát is felhasználó keresőmotorokat dolgoznak ki, elsősorban az erre a piacra belépő új cégek.

A fenti felsorolás valamennyi kategóriájában komoly fejlesztések zajlanak. Az utóbbi szinttel, vagyis a felhasználók kliens gépeken történő viselkedését elemző megoldással foglalkozik egy új startup vállalat programja a BioCatch, amely eddig már több mint 11 millió dollár támogatást kapott.

A BioCatch programja úgy dolgozik, hogy létrehoz egy mintát a számítógép felhasználójának „viselkedése" és számítógéphasználati paraméterei alapján, majd a későbbi bejelentkezések folyamán ehhez viszonyítva ellenőrzi a műveletek lefolyását a számítógépen.

Ha bejelentkezés történik a számítógépbe, a program elkezdi figyelni a kurzor mozgásának tulajdonságait és a gépelésünk sebességét, a mi saját paramétereinket. A BioCatch képes lesz meghatározni, hogy valóban az account tulajdonosa használja-e a profilt vagy esetleg egy külső behatoló. Ez a program attól függetlenül is tudja a jogosulatlan használatot azonosítani, ha a felhasználó saját belépési adataival léptek be a rendszerbe. Egy felhasználó viselkedését sokkal nehezebb utánozni, lemásolni, mint meghackelni egy védelmi rendszert. Ebben rejlik a módszer hatékonysága.

Hasonló elven működik, mint a bankkártyakezelés. A bank látja, hogy ha szokatlan helyen használjuk a kártyát, például külföldön, és ilyen esetekben

felveszi velünk a kapcsolatot, hogy igazolja a kártyahasználat jogosultságát és beazonosítsa a tranzakció indítóját. A BioCatch technológiája is így működik, kivéve, hogy ebben az esetben a felhasználó számítógépkezelési mintájától eltérő viselkedés esetében jelez. Ilyen indikátor lehet a gépelés, az egérmozgatás, kattintások sűrűsége vagy éppen a megnyitott dokumentumok száma. Ez a program pár belépés után megtanulja, megjegyzi a felhasználó stílusát, és a továbbiakban ez alapján ellenőrzi a műveleteket.

A rendszerben hatalmas potenciál rejlik, globális alkalmazása esetén a biztonság megsokszorozódna és a kibervédelem jelenlegi szintjét is komolyan növelhetné. Paradox módon épp ez gáncsolja az új technológia terjedését. Az általánosan elfogadott privacy policy alkalmazási gyakorlat miatt jelenleg egy szervnek sincs lehetősége legálisan felülvizsgálni globális szinten a számítógépeket és felhasználóikat. Noha a Gartner a kiberbiztonság jövőjét vizsgáló elemzése (Gartner, 2013) szerint 2020-ra már létrejöhetnek olyan iparspecifikus kiberdomainek (pl. pénzintézeti), amelyek akár jogosultságokat is szerezhetnek hasonló tevékenységekre a védelmi szint növelése érdekében. Jelenleg mindenki csak a saját területén mozoghat, szigorúan csak a saját rendszerének felhasználóit tudja figyelemmel kísérni. Szintén kérdés az információ megosztásának lehetősége is. Az összefogás nagyobb cégek és szervezetek között elengedhetetlen lenne ahhoz, hogy a viselkedés megfigyeléséből származó információk „összeérjenek". Viszont tisztában kell lennünk azzal, hogy ez jelenleg még nagyrészt csak elméletben működik. Az információ megosztására vannak jó gyakorlatok is, mint például az amerikai CitiBank kezdeményezései (CitiBank, 2014). Azonban a különböző országok titkosszolgálatai közül senki sem akarná megosztani az információit másokkal, mindenki lépéselőnyben kíván maradni a többiekkel szemben.

6. Összefoglalás

Összegezve láthatjuk, hogy a világban az egyik legfontosabb tényező jelenleg a kiberbiztonság. A hiánya évente több mint 400 milliárd dollár kárt okoz és sok milliárd dollárt költenek rá világszinten, hogy ezt a kárt enyhítsék. Még mindig sok probléma van a biztonsági rendszerekkel, sok rés található rajtuk,

melyeket a szakemberek próbálnak beazonosítani és befoltozni, illetve újfajta technikákkal igyekeznek a lehető legnehezebb feladat elé állítani a hackereket. Ez egyelőre a nemzetek és a vállalatok szintjén is strukturált szélmalomharc, mert ahogy létrejön egy új típusú védelem, azonnal megjelenik mellé egy új módszer, mely megtalálja a sebezhetőséget, és kezdődik minden előröl. A védelmi rendszerek általában csak néhány hónap előnyben vannak támadóikkal szemben, már persze, amikor épp nem néhány hónap hátrányból indulnak.

Éppen a megnövekedett tempó és adatmennyiség – valamint az informatikai rendszerek vitális feladata a létfontosságú rendszerek irányításában elkerülhetetlenné teszi a kiberbiztonsági szakemberek csapatokba és központokba történő szervezését és a SOC létrehozását nemzeti és vállalati szinten is. Az ilyen központ minden szervezetnél létfontosságú, létrehozásához és működtetéséhez nagy mennyiségű technológia és emberierőforrás-beruházásra van szükség. A hatékonyság érdekében működését szükséges megtámogatni Threat Intelligence-szel is, melynek naprakész és használható adatbázissal kell rendelkeznie, hogy a szervezet a legfejlettebb, legújabb behatolási technikákat is képes legyen felismerni, hatékonyan reagálni rá és megfelelő Threat Intel csapat felállításával akár a megelőzésben is eredményeket elérni. Ehhez épülhet hozzá a védelmi technológiák oldalán a Behavior Based Cyber Security, hogy a saját ellenőrzésünk alatt tartott számítógépek és azok felhasználói aktivitásából és tevékenységéből következtethessünk a veszélyekre, fenyegetésekre és időben megelőzhessük azokat. A technológia lehetőséget kínálna arra is, hogy nemzeti szinten ráláthassunk a nemzetbiztonságot veszélyeztető gyanús kiberbiztonsági eseményekre is, azonban ehhez még fejlődnünk szükséges az információmegosztás jogi és gyakorlati alkalmazásának területén.

Ha ezekben előre tudunk lépni, talán képessé válhatunk megvédeni magunkat 2016-ban a kibertérben.

Felhasznált irodalmak jegyzéke

Bhaskar Chakravorti, Christopher Tunnard, Ravi Shankar Chaturvedi: Bhaskar Chakravorti, Digital Planet: Readying for the Rise of the e-Consumer http://fletcher.tufts.edu/eBiz/Digital-Planet, 2014.09 (Utolsó letöltés: 2016. 07.22.)

2017 DOD budget calls for 15 percent increase in military cyber security spending. http://www.militaryaerospace.com/articles/2016/02/cyber-security-dod-budget.html, 2016. (Utolsó letöltés 2016.07. 31.)

Zoe Li What we know about the Chinese army's alleged cyber spying unit http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/, 2014. (Utolsó letöltés 2016.06.20.)

Paul Szoldra: These are the most-feared hacker groups in the world http://www.techinsider.io/advanced-persistent-threats-2016-7, 2016 (Utolsó letöltés 2016.07.02.)

Cyber threats prompt Estonia to set up UK data centre, http://www.ft.com/cms/s/0/be26fbd2-5005-11e6-88c5-db83e98a590a.html#axzz4FzcB9cuM, 2016.07.22 (Utolsó letöltés 2016.07.31.)

Sam Thielman: DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach, https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2, 2016 (Utolsó letöltés 2016.07.02.)

Ashley David E. Sanger arker Donald Trump Calls on Russia to Find Hillary Clinton's Missing Emails, http://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html?_r=1, 2016. (Utolsó letöltés 2016.07.31.)

Adam Butler: US nuclear force still uses floppy disks, http://www.bbc.com/news/world-us-canada-36385839, 2016. (Utolsó letöltés 206.07.07.)

David E. Sanger: U.S. and China Seek Arms Deal for Cyberspace, http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?_r=1, 2015.09.19 (Utolsó letöltés: 2016. 07.31.)

Nincs szerző: List of National CSIRTs, https://www.cert.org/incident-management/national-csirts/national-csirts.cfm, 2016. (Utolsó letöltés 2016.07.31.)

Karen Kent -Murugiah Souppaya Guide to Computer Security Log Management, http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf, 2006. (Utolsó letöltés 2016. 07.02.)

Nincs szerző: What it means to have cybersecurity capacity, https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/capacity_dimensions, 2014. (Utolsó letöltés 2016.06.20.)

Antal Lajos: Tudtán kívül bárki segítheti a kibertámadások elkövetőit, http://www2.deloitte.com/hu/hu/pages/risk/articles/barki-segithet-a-kibertamadoknak-sajtokozlemeny.html, 2016.05.02 (Utolsó letöltés: 2016.07.02.)

Daniel Cooper: China accused of hacking US firms even after cyber-peace treaty https://www.engadget.com/2015/10/19/china-accused-hacking/, 2015. 10 19. (Utolsó letöltés:2016.07.02.)

Larry Alton Next-Gen Cybersecurity Is All About Behavior Recognition, https://techcrunch.com/2015/08/23/next-gen-cybersecurity-is-all-about-behavior-recognition/, 2015. (Utolsó letöltés: 2016.07.02.)

Ed Tittel: Security threat intelligence services: A buyer's guide (2015.), http://searchsecurity.techtarget.com/buyersguide/Threat-intelligence-services-A-buyers-guide, 2015. (Utolsó letöltés: 2016.07.31.)

Dustin Volz: U.S. government concludes cyber attack caused Ukraine power outage, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K, 2016.02.25 (Utolsó letöltés : 2016.06.20.)

IBM Security Intelligence with Big Data, http://www-03.ibm.com/security/solution/intelligence-big-data/, 2013. (Utolsó letöltés: 2016.07.28.)

Paul Szoldra: Here's how the US military is beating hackers at their own game, http://www.techinsider.io/us-military-cyberwar-2016-5, 2016. (Utolsó letöltés: 2016.07.31.)

JANOBI 65 Million Tumblr Passwords for Sale on TheRealDeal, https://www.deepdotweb.com/2016/05/31/65-million-tumblr-passwords-sale-therealdeal-market/, 2016. (Utolsó letöltés: 2016.07.20.)

Stan Schroeder: Someone is selling 33 million Twitter passwords on the dark web, http://mashable.com/2016/06/09/twitter-password-leak/#c73Vk3DcP5q7, 2016.(Utolsó letöltés: 2016.07.31.)

Microsoft Secure Blog Staff Microsoft Secure Blog Staff, https://blogs.microsoft.com/microsoftsecure/2016/02/29/anatomy-of-a-breach-how-hackers-break-in/, 2016. 02.29. (Utolsó letöltés: 2016. 07.31.)

Global Cyber Security Capacity Centre, University of Oxford Cyber Security Capability Maturity Model (CMM) v1., https://www.sbs.ox.ac.uk/cyber-

security-capacity/system/files/CMM%20Version%201_2_0.pdf, 2014. (Utolsó letöltés: 2016. 05.28.)

The Institute of World Politics Cyber Security: Why Is This (Still) So Hard?, https://youtu.be/47zJPU0VHSQ, 2016.05.27. (Utolsó letöltés: 2016.07.31.)

Nincs Szerző Security Operations Center Summit, https://www.sans.org/event/security-operations-center-summit-2016/courses/, 2016. (Utolsó letöltés: 2016.07.30.)

Brian Fung How Many Cyberattacks Hit the United States Last Year?, http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/, 2013. (Utolsó letöltés: 2016.07.20.)

Waqas Anonymous Hacks Philippines Election Commission, Leaks 55 Million Voter Data, https://www.hackread.com/anonymous-philippines-hacks-leaks-voters-data/, 2016.04.09. (Utolsó letöltés: 2016.07.31.)

Jon Fingas The US and China want to set ground rules for cyberwarfare, https://www.engadget.com/2015/09/19/us-china-cyberwarfare-treaty-talks/, 2015.(Utolsó letöltés: 2016.05.22.)

Samantha White Global cyber-attacks up 48% in 2014, http://www.cgma.org/magazine/news/pages/201411089.aspx?TestCookiesEnabled=redirect, 2014. (Utolsó letöltés: 2016. 07.20.)

Global Cyber Security Capacity Centre, University of Oxford Cyber Security Capability Maturity Model (CMM) v1.2, https://www.sbs.ox.ac.uk/cyber-security-capacity/system/files/CMM%20Version%201_2_0.pdf, 2014. (Utolsó letöltés: 2016.07.31.)

Steve Morgan Cybersecurity job market to suffer severe workforce shortage, http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-, 2015. 07.28. (Utolsó letöltés: 2016. 07.31.)

James Cook Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far, http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12, 2014.12.16 (Utolsó letöltés: 2016.07.30.)

Doug Altner Les Servi A Two-Stage Stochastic Shift Scheduling Model for Cybersecurity Workforce Optimization with On Call Options, 2016.04.10 (Utolsó letöltés: 2016.06.20.)

HP: A HP Building a successful SOC Business Whitepaper, 2013. (Utolsó letöltés: 2016.07.31.)
FireEye: iSIGHT Partners Introduction, 2016. (Utolsó letöltés: 2016.06.20)
Gartner Gartner: 2020 study on cyber security, 2013. (Utolsó letöltés: 2016. 06.20.)
CitiBank: Fighting cyber-crime together, https://www.citibank.com/tts/about_us/articles/docs/2014/article_fighting_cybercrime.pdf, 2014.12.01. (Utolsó letöltés: 2016.07.31.)