Molnár Dóra

Kiberbiztonsági alapvetések – a 2016-os kitekintéssel[1]

Nem túlzás azt állítani, hogy manapság „a csapból is a kiberbiztonság folyik". Hol százmilliók adatait lopják el, máskor választásokat manipulálnak, vagy szigorúan titkos hírszerzési anyagok kerülnek a nyilvánosság elé. De kik az elkövetők? És miként képzelhető el működési területük? Jelen tanulmány célja, hogy röviden bemutassa a kiberbiztonsággal összefüggő legfontosabb alapfogalmakat, majd felvázolja azokat a folyamatokat, amelyek elvezettek e speciális biztonsági terület gyors kiemelkedéséhez. A tanulmány második felében néhány, 2016-ban elkövetett és/vagy nyilvánosságra hozott nagy horderejű kibertámadást ismertetek röviden, amelyek az Egyesült Államokat és a Közel-Kelet térségét érintették. Választásom azért esett a múlt év eseményeire, mert tavalyra vált igazán érzékelhető néhány olyan, a kibertámadásokat jellemző tendencia, amelyekből távolabbi következtetések vonhatók le.

Kulcsszavak: *kiberbiztonság, kibertér, zsarolóvírus, Yahoo*

Molnár Dóra: Basic Theories of Cyber Security – With an Outlook on 2016

It is no exaggeration to say that today cybersecurity is all over the news. Once data of hundreds of millions are stolen, at other times elections are manipulated or top secret intelligence materials are made accessible to the general public. But who are the perpetrators? And how to imagine their area of operation? The aim of the study is to briefly present the most important basic concepts related to cyber security and also to outline the processes that led to the rapid emergence of this special security area. In the second half of the study, some high-profile cyber-attacks committed and/or published in 2016 are described; ones that affected either the United States or the Middle East. I have decided to choose the events of last year because some trends characterizing cyber-attacks have become so obvious by 2016 that further conclusions can be drawn.

Keywords: *cyber security, cyber space, ransomware, Yahoo*

Bevezetés

A biztonság területeinek köre az utóbbi időben igen látványosan kibővült egy új szektorral: az informatikai – vagy egyre elterjedtebb nevén – kiberbiztonsággal. A szakirodalom szerint az információbiztonság „az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt

[1] A tanulmány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Egyed István Posztdoktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos".[2] Napjainkban azonban ezt a törékeny rendszert egyre többször, egyre több ponton és egyre keményebb támadások érik, amelyeket kezelni kell egyéni, állami és nemzetközi szinten egyaránt. Bár a kibertérből érkező fenyegetésekkel és támadásokkal szemben leghatékonyabban nemzetközi keretek között lehetne reagálni, mégis azt láthatjuk, hogy a nemzetállami – vagy még alsóbb szintű – kezdeményezések kerülnek túlsúlyba. Az utóbbi években az államok sorra fogadták el kiberbiztonsági stratégiájukat és állították fel az állami kibervédelmi szerveiket annak következtében, hogy évről évre emelkedik a kibertámadások száma és az érintett államok köre is folyamatosan bővül. Bár az élen még mindig a legfejlettebb államok járnak, de számos példa van már arra vonatkozóan is, hogy egy kis ország a biztonsága szempontjából olyan fontosnak értékeli a kibervédelmet, hogy speciális és fejlett kiberképességek fejlesztése mellett dönt.[3] Ugyanakkor az egyes vállalatok is igyekeznek magukat a lehető legteljesebben megvédeni a hackerekkel szemben – többkevesebb sikerrel. Jelen tanulmányban felvázolom a kiberbiztonság néhány alapvető jellemzőjét, majd néhány konkrét példával szemléltetem, hogy milyen nehéz felvenni a harcot a támadásokat elkövető profi hackerekkel szemben.

A kiberbiztonság alapvető jellemzői

Képzeljünk el egy folyót, amelyben hömpölyög a víz, és a halászok úgy próbálják meg kifogni a halakat, hogy ketten keresztbefeszítenek egy 1 méter magas és a víz színe alatt 1 méter mélyen húzódó hálót. A halak fennakadnak rajta, de amint egyre több hal érkezik a folyón, a háló gyorsan megtelik velük, és az újonnan (és igen gyorsan) érkező halak előbb megpróbálnak átugrani a hálón, majd amikor elérik a kritikus tömeget, egyszerűen magukkal sodorják azt – a halászokkal együtt. Ez a jelenet tökéletesen illusztrálja az államok kibervédelmének jelenlegi állapotát. A halak a kibertérben jelentkező fenyegetések megfelelői, amelyek dömpingszerűen érkeznek, és amelyekkel az állami szerveknek és vállalatoknak folyamatosan számolniuk kell. A halászokkal pedig a kiberbiztonsági egységek feleltethetők meg, amelyek még kevesen vannak a fenyegetésekhez képest, és amelyeken jelenleg még idővel felülkerekednek a fenyegetések. Ez az a pillanatnyi állapot, amelyben valamennyi szereplő próbál sikeresen küzdeni, más és más megoldási sémákkal.

A kiberbiztonsághoz köthető egyik alapfogalom a kibertér kifejezés.[4] A kibertér egy olyan virtuális közeg, amely sokkal kevésbé megfogható, mint a föld-víz-levegő-világűr jól ismert négyes közege, de amely körülöleli mind a négyet. A kibertér könnyebb megér-

[2] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, *Bolyai Szemle,* 17. évf., 2008/4, 137–156. o.

[3] Tipikusan ilyen Észtország, ahol a 2007-es orosz támadást követően építettek ki egy egyedülálló állami kibervédelmi struktúrát.

[4] A fogalomnak egységes definíciója a mai napig nem létezik, az államok az egyes szervezeteken belül sem tudnak közös nevezőre jutni (mint például a NATO-ban).

téséhez a rétegre osztás technikáját alkalmazzák. A szakirodalom a kibertér három rétegét[5] különbözteti meg: a fizikai, a szintaktikai és a szemantikai réteget.[6]

A legalsó szint (amelyet nevezhetünk a hardverszintnek is) a fizikai réteg, amelyet a távközlési rendszerek, számítógépek és kábelek sokasága alkot. Ha ez megsérül, az kihat a többi rétegre is, ha pedig megsemmisül, az a rendszer összeomlásához vezet. A középső réteg azokat az instrukciókat foglalja magában, amelyeket a felhasználók adnak a gépeknek, valamint azokat a protokollokat, amelyek segítségével a gépek egymással összekapcsolódnak. Ez lényegében az alkalmazások, azaz a szoftverek és operációs rendszerek szintje (ezért ezt a réteget nevezhetjük a szoftverszintnek is), ahol a hackerek tevékenysége (és ezáltal az emberi tényező) a leglátványosabban jelenik meg. A legfelső réteg a szemantikai réteg, amely magát a kibertérben tárolt információt tartalmazza. Ezeket az információkat szeretnék a támadók manipulálni, megsemmisíteni vagy további információval bővíteni, ezért az információs műveletek túlnyomó többsége ebben a rétegben zajlik. A három réteg egymásra épül, ezért valamely alsóbb réteg sérelme vagy megsemmisülése ugyanilyen hatást vált ki a magasabb rétegekben is.

A kiberbiztonság területének felértékelődése számos, az elmúlt évtizedben bekövetkezett változásnak köszönhető. Ezek közül az egyik az aktorok körének kiszélesedése lefelé, ugyanis a biztonságnak ezen a területén kifejezetten hangsúlyosan jelenik meg az állam alatti szint, azon belül is az egyéni szint. A kibertér jelen lévő elkövetői csoportok között természetesen megtaláljuk a nemzetállamokat is, de mellettük igen hangsúlyosan vannak jelen a terrorista elkövetők, a kiberbűnözők vagy a hacktivisták.[7]

Másik fontos tényező az aktorok akciói mögött meghúzódó motivációkon belüli különbség. Míg a nemzetállamok a legszofisztikáltabb módszereket elsősorban hírszerzési, szabotázs vagy pusztán más állam zaklatásának céljával alkalmazzák, addig például a kiberbűnözők főként haszonszerzési céllal végzik jogellenes tevékenységüket. Kiemelendő továbbá a kibertámadással érintett célterületek változatossága is. Egy támadás elvezethet például az ellenőrzés vagy az információba vetett bizalom elveszítéséhez, a nemzetbiztonsági rendszer sérelméhez, vagy a kritikus infrastruktúra valamely elemének működésképtelenségéhez. Mindezek pedig az állampolgárok részéről az állami rendszerbe vetett bizalom elveszítését eredményezhetik. Végül a kiberbiztonság felértékelődésének okai között nem szabad megfeledkezni arról sem, hogy ezen tevékenységek költségigénye minimális, és a terület jogi szabályozása még annyira gyermekcipőben jár, hogy az elkövetők elleni eredményes fellépés gyakran lehetetlen.

Mára a kiberbiztonság jelentősége annyira megnőtt, hogy az a biztonság más területeinek alakulására is közvetlen hatással és befolyással van. Bár a területet gyakran a katonai biztonsággal összefüggésben vizsgálják, azonban mégsem valamely kizárólagos katonai kérdésről van szó, amelyet az államok védelmi minisztériumain keresztül kell megoldani,

---

[5] A kibertér felosztása más szakirodalmi források alapján némiképp módosulhat. Így például az Egyesült Államok mind a négy haderejére kötelező kiberműveleti doktrína alapján a hármas felosztás a kibertér fizikai hálózati rétegét, logikai hálózati rétegét és a kiberszemélyek rétegét foglalja magában. Lásd: Cyberspace Operations, [online], Joint Chief of Staff, US, 2013. 02. 05. Forrás: Dtic.mil [2017. 02. 02.].

[6] Martin C. Libicki: *Cyberdeterrence and cyber war,* [online], (Prepared for the US Air Force) Rand Corporation, 2009, 12. Forrás: Rand.org [2017. 02. 02.].

[7] Az aktorok közötti határok gyakran összemosódnak, ezért nehéz őket egyértelműen bekategorizálni.

hanem olyan összkormányzati megközelítésre van szükség, amelyben valamennyi ágazat és szereplő a maga szaktudásával képviselteti magát. Ezért a kiberfenyegetések és -támadások elleni küzdelem csapatjáték, ráadásul olyan, amelyet nemcsak nemzetállami szinten kell folytatni, hanem nemzetközi szereplők bevonásával is, köztük kormányzati szervezetekkel, rendőri egységekkel, kereskedelmi csoportokkal, a pénzügyi és az energiaszektor részvételével, nem megfeledkezve a közösségi média adta lehetőségek kihasználásáról sem. Mindennek előfeltétele egy olyan bizalmi viszony kialakulása az érintett szereplők között, amely lehetővé teszi az érzékeny információk egymással való megosztását – bár ez még valószínűleg hosszú ideig a szűk keresztmetszet marad. Arról azonban nem szabad megfeledkezni, hogy az ellenség ugyanolyan sérülékeny, mint mi vagyunk, és ezt ki is kell használni.

A 2000-es évek vége felé, amikor a kiberbiztonság kezdett egyre inkább felértékelődni az állami biztonság garantálása szempontjából, az egyes nemzetállamok arra helyezték a hangsúlyt, hogy hogyan tudják állampolgáraikat, az állami szervezetrendszert és a kritikus infrastruktúrát megvédeni a kibertámadásokkal és -fenyegetésekkel szemben. Ez egyértelműen defenzív megközelítést jelentett, amely bár kezdetben még elegendőnek bizonyult, az elmúlt évek (alább röviden bemutatott) eseményei azonban rávilágítottak arra, hogy szemléletváltásra van szükség. Mára már egyre több állam hangsúlyozza, hogy olyan támadó kiberképességekre kell szert tenniük, amelyek segítségével sikeresen el tudnak hárítani olyan nagy erejű támadásokat, mint amellyel az elmúlt évben – többek között – az Egyesült Államoknak is szembe kellett néznie.[8] Ennek előfeltétele a jogi szabályozás megalkotása, amely még a kezdeti fázisában jár, és minden bizonnyal majd a precedensértékű támadások nyomán sikerül kialakítani az egységes kiberszabályozás kereteit. Mindehhez pedig arra van szükség, hogy az állami döntéshozók képesek legyenek úgy gondolkodni, ahogyan azt az ellenség is teszi: előbb a célt kell felderíteni, utána meg kell keresni és azonosítani annak gyenge pontjait, végül ki kell küszöbölni a sérülékenységünket.

Kibertámadások 2016-ban

A 2016-os esztendőben történt kiberesemények ismét rávilágítottak arra, hogy a világban a kiberbűnözés növekszik, és ezzel a növekvő veszéllyel valamennyi államnak szembe kell néznie. A tavalyi év a zsarolóvírusok és a makrók visszatérésének éve volt.[9] Csak 2016-ban 62 új zsarolóvírus-család tűnt fel a „piacon". Míg az év elején még „csak" minden 20. másodpercben ért valakit zsarolóvírussal végrehajtott támadás, addig az év végére már minden 10. másodpercben,[10] ugyanis az Office-fenyegetések 99%-a közvetlenül függ makrók használatától. Emellett a kis- és középvállalkozások 42%-át érte zsarolóvírussal végrehajtott támadás 2016-ban, 32%-uk pedig – engedve a nyomásnak – kifizette a kért árat azért, hogy adatait vagy az azokhoz való hozzáférést visszakapja.

---

[8] 2016 októberében, oroszországi látogatása alkalmával a brit külügyminiszter már úgy fogalmazott, hogy az Iszlám Állam ellen kiberműveletek megindítása szükséges. A miniszter kijelentése már egyértelműen az offenzív megközelítést tükrözi. Ugyanakkor a nemzetközi szervezeteknél egyelőre még nagy az ellenállás a támadó kiberképességekkel való rendelkezéssel szemben. A NATO például kizárólag védelmi kiberképességekkel rendelkezik és engedélyez, támadó képességeket nem.

[9] Kaspersky Security Bulletin 2016, [online], 2016, 5. Forrás: Kasperskycontenthub.com [2017. 02. 10.].

[10] Uo., 23.

A továbbiakban röviden bemutatok néhány, az Egyesült Államokban és a Közel-Keleten 2016-ban végrehajtott vagy nyilvánosságra hozott nagy horderejű támadást, amelyek másmás szempontból ugyan, de kiemelkedő jelentőséggel bírnak: egy részében az állami infrastruktúra volt a kiszemelt célpont, a másiknál nagyvállalatoktól loptak el nagy mennyiségben érzékeny adatokat. Választásom azért erre a két régióra esett, mert míg az Egyesült Államokban a legnagyobbak az adatlopás elleni küzdelem indirekt költségei, addig az arab térség a direkt költségek terén listavezető.[11]

Bár az Egyesült Államok elleni kibertámadások közül – politikai hatása miatt – kétségkívül az elnökválasztás manipulálása tekinthető az első számúnak, azonban az ezzel hivatalos retorika még csak formálódik, ezért most azt a kibertámadást mutatom be elsőként, amelynek sajtóvisszhangja „minden idők legnagyobb hackeléséről" szól. Mivel azonban gyakran hosszú időbe telik, míg bizonyos kibertámadások nyilvánosságra kerülnek, azért – még ha ez a támadás nem is minden idők legtöbb adat ellopását megvalósító támadásaként marad majd meg a köztudatban – az vitathatatlan, hogy egy igen jelentős gazdasági visszaélésre okot adó kibereesemény történt.

Maga a támadás még 2014-ben történt a Yahoo-nál, de a cég azt csak 2016. szeptember 22-én jelentette be. Felmerülhet a kérdés, hogy miért vártak a bejelentéssel több mint két évet. A történteket először egy Peace[12] nevű hacker hozta a nagyvilág tudomására oly módon, hogy 2016 augusztusában 200 millió Yahoo-felhasználói adatot kezdett el értékesíteni a feketepiacon. Ezek az adatok a hacker állítása szerint a Yahoo-t ért támadásból származtak.[13] Ezt követően a cégnél azonnali vizsgálatot rendeltek el. Két hónapos nyomozás után kiderült, hogy a helyzet sokkal rosszabb annál, mint ahogyan azt gondolták. A támadás eredményeként ugyanis 500 millió felhasználó adatait lopták el, köztük e-mail-címeket, biztonsági kérdésekre adott válaszokat, jelszavakat, születési dátumokat és telefonszámokat. (Összehasonlításképp az alább közölt ábra azt mutatja, hogy a más vállalatok ellen elkövetett támadások hány millió adatot érintettek, kiemelve azokat, amelyek szintén a 2016-os évhez köthetők.) Amellett, hogy ez hatalmas mennyiségű adat, azok jellege is egyedi. Mégpedig azért, mert az internetkor hajnalán a Yahoo volt a piac vezető e-mail-szolgáltatója, s nála vélhetőleg olyan adatok gyűltek fel az évtizedek alatt, amelyeket a felhasználók más portálokon is használnak. Az pedig tény, hogy a hackerek az egyszer megszerzett adatokat máshol is felhasználják.[14] A hacker által kiadott adatok megvizsgálást követően tovább bonyolódott a Yahoo körüli botrány, ugyanis a biztonsági mentések és az adatbázis egybevetéséből kiderült, hogy a 2014-es adatokhoz képest még korábbi adatokról

[11] Direkt költség alatt értjük például az igazságügyi szakértők, jogi cég alkalmazását, vagy az áldozatok biztonságának és személyes adataik védelmének biztosítását. Indirekt költségek közé tartozik mindaz az idő- és energiaráfordítás és egyéb szervezeti források allokálása, amelyeket az adatlopás következményeinek kezelésére kell fordítani. Lásd: 2016 Cost of Data Breach Study: Global Analysis, [online], Ponemon Institute – Research Report, 2016, 4. o. Forrás: Public.dhe.ibm.com [2017. 02. 10.].

[12] Korábban ugyancsak ő árulta a MySpace-től és a LinkedIntől ellopott fiókokat a feketepiacon.

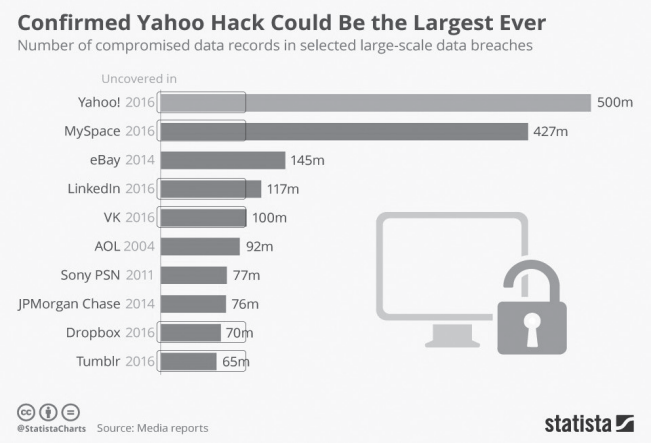
[13] Seth Fiegerman: Yahoo says 500 million accounts stolen, [online], 2016. 09. 23. Forrás: Money.cnn.com [2017. 02. 06.].

[14] Teszik ezt azért, mert a felhasználók is hatalmas hibát követnek el egyrészt azzal, hogy ugyanazt a jelszót több holnapon is használják, másrészt pedig azzal, hogy előszeretettel használnak olyan jelszavakat, mint például az „123456". (A hackerek éppen ezt használták ki a LinkedIn elleni támadásnál is, ugyanis az ellopott jelszavak közül több mint 1 millió esetben ez a számsor volt a jelszó.) Lásd: Kaspersky Security Bulletin 2016… *i. m.,* 75.

is szó van. Ez a korábbi támadás még 2013-ban történhetett, és még több, 1 milliárd felhasználó adatait érinthette. Ezt a vállalat 2016 decemberében jelentette be.[15]

Az elkövető vagy elkövetők személyét illetően még biztosat nem lehet tudni, bár a Yahoo határozottan azt állítja, hogy egy külföldi állam pénzelte és támogatta őket. A szálak – az amerikai álláspont szerint – Oroszország irányába vezetnek. Az amerikai vállalat egyébként már évek óta küzdött a talpon maradásért, míg végül az online részleg eladásáról döntöttek. 2016 júliusában bejelentették, hogy a Verizon telekommunikációs mamutvállalat fogja felvásárolni a Yahoo online piacát közel 5 milliárd dollárért. Érdekes, hogy a bejelentés nagyjából egybeesett azzal, amikor a cég tudomást szerzett rendszerének két évvel korábbi meghackeléséről. Az kérdéses, hogy a megállapodás megkötésekor a Yahoo-nál már ténylegesen tudtak-e az adatlopásról, mert ha igen, akkor ennek súlyos jogi következményei lehetnek.[16] A vállalat ellen egyéb jogi lépések megtételére viszont már sor került: Ronald Schwartz New York-i lakos valamennyi olyan amerikai ügyfél nevében beperelte a céget, aki az adatlopásban érintett. Állítása szerint, ha a vállalat gondosan jár el, a kibertámadás elkerülhető lett volna, de emellett azt is sérelmezte, hogy a Yahoo igen lassan észlelte a lopást – a többi meghackelt vállalathoz képest mintegy háromszor annyi idő elteltével.[17] A jogi szabályozás egyébiránt elég kaotikus az Egyesült Államokban. Elvileg a megtámadott vállalatoknak azonnali jelentéstételi kötelezettségük van, de erre vonatkozó szabályok csak állami szinten léteznek, szövetségi szinten nem. S bár vannak kísérletek egy egységes szövetségi szabályozás megalkotására, az még a mai napig nem létezik – ellentétben az Európai Unióval, ahol 2016-ban elfogadták azt az adatvédelmi rendeletet, amely rendelkezéseinek 2018 májusától valamennyi tagállami szabályozásnak és gyakorlatnak meg kell felelnie.

1. ábra: A 10 legtöbb felhasználót érintő adatlopás (millió fő)



Forrás: www.statista.com/chart/5983/data-breaches/ [2017. 02. 06.]

[15] Vindu Goel – Nicole Perlroth: Yahoo Says 1 Billion User Accounts Were Hacked, [online], 2016. 12. 14. Forrás: Nytimes.com [2017. 02. 06.].

[16] Érdekességképp megemlítem, hogy kísértetiesen hasonló folyamatok zajlottak a LinkedInnél is: a cég szintén 2016 nyarán jelentette be, hogy évekkel ezelőtt meghackelték, de ettől függetlenül a Microsoft hatalmas összegért felvásárolta.

[17] New York man sues Yahoo over 500 million account breach, [online], 2016. 09. 23. Forrás: Nydailynews.com [2017. 02. 06.].

Végül az Egyesült Államokkal összefüggésben aktualitása okán röviden utalnék arra a 2017. január 17-én történt támadásra, amely a Gmail-fiókokat támadta és támadja.[18] A támadás egy megbízható, ismerős forrástól érkezik, ezért még a gyanú árnyéka sem merül fel a felhasználókban, hogy kibertámadás áldozatai lennének. A csatolmány gyanútlan megnyitását követően azonban, ha a felhasználó eleget tesz a rendszer ismételt bejelentkezésre irányuló kérésének, máris áldozattá válik. Ez a támadási mód hasonló a Facebook elleni phishing-támadáshoz, ám ez kifinomultsága miatt sokkal veszélyesebb.

Az első IoT (*Internet of Things* – a dolgok internete) botnet támadást 2016. október 21-én élte át az amerikai lakosság, amikor a keleti parton (és Európa egyes részein) arra ébredtek, hogy számos kedvelt oldal (köztük a Twitter, az Amazon) elérhetetlen az interneten vagy akadozik (mint a CNN vagy a The New York Times). A kibertámadás a Dyn amerikai vállalat szervereit érintette, és volumenét tekintve elérte az 1,2 Tbps-t (terabájt per szekundumot).[19] A támadás különlegességét az adta, hogy ez volt az első alkalom, amikor a támadók a lakosság által használt internetre csatlakoztatott okoseszközökből építették fel azt a hálózatot, amellyel a támadást végrehajtották.[20] Az elkövetők kihasználták a dolgok internetének egyre szélesebb körű elterjedését és azt, hogy a háztartási okoseszközök igen könnyen feltörhetők, ezáltal egy ilyen támadás során a lakosság tudta nélkül használhatók. Az októberi támadás a Mirai nevet kapta az ezen a néven elterjedt olyan rosszindulatú szoftver *(malware)* után, amely forráskódja 2016 szeptembere óta szabadon hozzáférhető a világhálón, és jellemzője, hogy a gyári jelszóval védett okoseszközöket állítja a kiberbűnözők szolgálatába.

A Közel-Kelet térségét illetően 2016-ban két jelentős kibertámadás is történt. Az első 2016 májusában Szaúd-Arábiából indult,[21] de hamarosan érintetté vált az Egyesült Államok, Izrael, Katar és Törökország is. Az országok egymással fennálló szoros pénzügyi érdekeltsége okán „Fúrótorony-támadássorozat" néven kezdett terjedni ez az eseménysorozat. A támadás szaúdi pénzügyi intézményeket és technológiai szervezeteket célzott meg, majd utána a védelmi szektort és a high-tech ipari létesítményeket is. A kampány öt hónapja alatt négy különböző rosszindulatú szoftverrel támadtak az elkövetők: kezdetben a közösségi médián keresztül fertőzött hibaelhárító programokat kínáltak, majd ugyanott hamis álláshirdetéseket adtak fel. Trójai vírust használva hátulról hatoltak be a rendszerekbe, két különböző megoldással: az egyiket VBScriptben és PowerShellben írták, amelyeket makrók segítségével juttattak Excel-táblázatokba (ezt az „agyagcsúszda" névvel illették), a másik egyszerűen Windowsban futtatható (ez volt a „bélféreg").[22] Augusztusban például 15 millió iráni Telegram-fiókjának belépési adataihoz jutottak hozzá, majd fértek hozzá a levelezésükhöz. A kiválasztottak elsősorban újságírók, aktivisták és más prominens személyek voltak.[23] Ezt követően egy újabb hullámban az Oxfordi Egyetem nevében hoztak

[18] Sulleyman Aatif: Gmail Phishing: latest cyber attack infects users by mimicking past emails, [online], 2017. 01. 17. Forrás: Independent.co.uk [2017. 02. 02.].

[19] Nicky Woolf: DDoS attack that disrupted internet was largest of its kind in history, experts say, [online], 2016. Forrás: TheGuardian.com [2017. 02. 02.].

[20] A támadás csúcsán 760 000 eszköz szolgálta ki az elkövetőket.

[21] Bár a kibertámadást 2016 tavaszára teszik, ennek már 2015 őszén voltak látható előzményei.

[22] Robert Falcone – Bryan Lee: Organizations Deliver Helminth Backdoor, [online], 2016. 05. 26. Forrás: Researchcenter.paloaltonetworks.com [2017. 02. 05.].

[23] Pierluigi Paganini: OilRig Campaign – Iran-linked Hackers Target US Govenment & Energy Grid, [online], 2016. 10. 08. Forrás: Securityaffairs.co [2017. 02. 05.].

létre hamis VPN-holnapot, amelyen konferenciára és állásajánlatokra lehetett jelentkezni, és a gyanútlan jelentkezők természetesen rögtön a támadás áldozatává váltak.[24]

A közel-keleti térséget 2016 novemberében érte a másik nagy támadás. Az elkövetők két hullámban, előbb november 17-én, majd 29-én csaptak le szaúdi szervezetekre, érintve olyan kritikus ágazatokat is, mint például a közlekedési szektor. Ezúttal nem adatlopás volt a céljuk, hanem szolgáltatások leállítása úgy, hogy a szerverek összeomlását érjék el a rosszindulatú szoftverek számítógépes rendszerekbe történő telepítését követően. A támadáshoz annak a Shamoon nevű vírusnak az egyik verzióját használták, amely 2012-ben a közel-keleti energiavállalatok számítógépeinek százezreit – köztük az Aramco állami olajtársaság gépeit – bénította meg. A párhuzam okán ez a támadás a Shamoon 2 nevet kapta, ugyanis míg 2012-ben a merevlemezre egy égő amerikai zászló képét tették a hackerek, addig 2016-ban Alan Kurdi 3 éves szíriai kurd kisfiú holttestéről készült kép került a fertőzött számítógépekre. Az akciót valószínűleg külföldről irányították, és egy szaúdi hackercsoportot sejtenek mögötte. Az események egy szervezett támadássorozatra engednek következtetni, amit az is alátámaszt, hogy 2017. január végén újabb informatikai támadás történt az országban: mintegy 30 000 szaúdi magáncég és közintézmény gépeit – köztük a Munkaügyi Minisztériumét és a polgári repülésügyi szervezetét is – ismét a Shamoon 2 vírussal fertőzték meg.[25] Mindezek pedig rávilágítanak arra, hogy Szaúd-Arábia kiberbiztonsági rendszerei mennyire sebezhetők – a Shamoon számítógépes vírussal szemben mindenképp. Ezt már a szaúdi belügyminisztérium Nemzeti Kiberbiztonsági Centruma is hivatalosan megerősítette.[26]

Összegzés

A 2016-os év igen eseménydús volt kiberbiztonsági szempontból. Az események rávilágítottak arra, hogy még a világ legnagyobb vállalatainak is milyen nehéz hatékony informatikai védelmi rendszert kiépíteniük a hackerekkel szemben, akik mindig egy lépéssel előrébb járnak. Kérdés, hogy ilyen történések után merre tart a világ? Minden bizonnyal afelé, hogy már nemcsak kis és nagy vállalatok lesznek kibertámadások kiszemelt célpontjai, hanem egyre gyakrabban állami információs rendszerek is. Ezt sajnálatos módon a 2017-es év első hónapjának események is igazolták: a norvég kormányzati és hírszerzési levelezőrendszerek orosz hackerek általi feltörése,[27] vagy a cseh külügy levelezőrendszere elleni két támadás (amelyből az egyik olyannyira sikeres volt, hogy 7000 dokumentumot loptak el a támadók).[28] A hollandok pedig a közelgő márciusi választások alkalmával vissza kívánnak térni a régi papíralapú szavazási rendszerhez, mert attól tartanak, hogy orosz hackerek feltörik és ezáltal manipulálják az elektronikus választási rendszerben tárolt eredményeket. A holland lépés már azt mutatja, hogy a politikai vezetés próbál előre gondolkodni

[24] Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford, [online], 2017. 01. 05. Forrás: Clearskysec.com [2017. 02. 05.].

[25] Tara Seals: Saudi Arabia Issues Shamoon 2 Alert, [online], 2017. 01. 26. Forrás: Infosecurity-magazine.com [2017. 02. 05.].

[26] Saudi Arabia still on cyber alert over Shamoon 2., [online], 2017. 02. 01. Forrás: English.alarabiya.net [2017. 02. 05.].

[27] Greg Price: Russia Hacked Norway like US? Cyberattack Similar to Trump Election in 2016, [online], 2017. 02. 03. Forrás: Ibtimes.com [2017. 02. 06.].

[28] Hackers steal 7,000 documents from Czech diplomacy, [online], 2017. 02. 02. Forrás: Praguemonitor.com [2017. 02. 06.].

és kivédeni egy esetleges kibertámadást, amely az állam politikai biztonságát alááshatná. A kibertérben jelentkező fenyegetések tehát olyannyira valósak és nagy horderejűek, hogy a biztonság már olyan más szektoraiban is komoly fennakadást okoztak, mint a politikai, a katonai vagy a gazdasági szektor. Európa vezető nemzete, Németország már most kifejezte aggodalmát azzal kapcsolatban, hogy a bő fél év múlva esedékes szövetségi parlamenti választások kampányát manipulálni fogják.[29] A fenyegetés tehát reális, a félelem jogos, de a megoldás még várat magára.

FELHASZNÁLT IRODALOM

2016 Cost of Data Breach Study: Global Analysis, [online], Ponemon Institute – Research Report, 2016. Forrás: Public.dhe.ibm.com [2017. 02. 10.]

Aatif, Sulleyman: Gmail Phising: latest cyber attack infects users by mimicking past emails, [online], 2017. 01. 17. Forrás: Independent.co.uk [2017. 02. 02.]

Annyira tartanak az orosz hackerektől, hogy inkább kézzel számolják a szavazatokat a hollandok, [online], 2017. 01. 01. Forrás: Hvg.hu [2017. 02. 05.]

Cyberspace Operations, Joint Chief of Staff, [online], 2013. 02. 05. Forrás: Dtic.mil [2017. 02. 02.]

Falcone, Robert – Lee, Bryan: Organizations Deliver Helminth Backdoor, [online], 2016. 05. 26. Forrás: Researchcenter.paloaltonetworks.com [2017. 02. 05.]

Fiegerman, Seth: Yahoo says 500 million accounts stolen, [online], 2016. 09. 23. Forrás: Money.CNN.com [2017. 02. 06.]

Goel, Vindu – Perlroth, Nicole: Yahoo Says 1 Billion User Accounts Were Hacked, [online], 2016. 12. 14. Forrás: Nytimes.com [2017. 02. 06.]

Hackers steal 7,000 documents from Czech diplomacy, [online], 2017. 02. 02. Forrás: Praguemonitor.com [2017. 02. 06.]

Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford, [online], 2017. 01. 05. Forrás: Clearskysec.com [2017. 02. 05.]

Kaspersky Security Bulletin 2016, [online], 2016. Forrás: Kasperskycontenthub.com [2017. 02. 10.]

Libicki, Martin C.: Cyberdeterrence and cyber war. (Prepared for the US Air Force) Rand Corporation, [online], 2009. Forrás: Rand.org [2017. 02. 02.]

Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, *Bolyai Szemle,* 17. évf., 2008/4, 137–156. o.

New York man sues Yahoo over 500 million account breach, [online], 2016. 09. 23. Forrás: Nydailynews.com [2017. 02. 06.]

Paganini, Pierluigi: OilRig Campaign –Iran-linked Hackers Target US Govenment & Energy Grid, [online], 2016. 10. 08. Forrás: Securityaffairs.co [2017. 02. 05.]

Price, Greg: Russia Hacked Norway like US? Cyberattack Similar to Trump Election in 2016, [online], 2017. 02. 03. Forrás: Ibtimes.com [2017. 02. 06.]

Saudi Arabia still on cyber alert over Shamoon 2., [online], 2017. 02. 01. Forrás: English.alarabiya.net [2017. 02. 05.]

Seals, Tara: Saudi Arabia Issues Shamoon 2 Alert, [online], 2017. 01. 26. Forrás: Infosecurity-magazine.com [2017. 02. 05.]

Woolf, Nicky: DDoS attack that disrupted internet was largest of its kind in history, experts say, [online], 2016. Forrás: TheGuardian.com [2017. 02. 02.]

[29] Annyira tartanak az orosz hackerektől, hogy inkább kézzel számolják a szavazatokat a hollandok, [online], 2017. 02. 01. Forrás: Hvg.hu [2017. 02. 05.].