HADTUDOMÁNYI SZEMLE
13. évfolyam (2020) 1. szám 113–130. • DOI: 10.32563/hsz.2020.1.9

Koczka Ferenc[1] – Négyesi Imre[2]

Az információbiztonság fejlesztésének lehetőségei az akadémiai szférában

Improving Information Security in the Academic Sphere

Absztrakt

A magyar akadémiai szférában az oktatási, kutatási források és eredmények, valamint az adminisztratív folyamatok ellátása során nagy mennyiségű szenzitív adat kezelése történik. Ezek az intézmények nem tartoznak az állami és önkormányzati szervek körébe, így nem tartoznak a működésüket meghatározó jogszabályok hatálya alá sem. Az informatikai rendszerek védelmének módszerei és eszközparkja így sokkal változatosabb, ugyanakkor a rendelkezésre álló erőforrások korlátozottak. A tanulmány megvizsgálja az aktuális támadási motivációkat, a védelmi rendszerek éves jelentései alapján prognosztizálja az elkövetkező időszak fő védendő területeit és ezek alkalmazását a védelmi stratégia kialakításában. A bemutatott eredmények nem akadémiaspecifikusak, így azok nemcsak ott, hanem más területeken is hasznosíthatók.

Kulcsszavak: *információbiztonság, penetrációs teszt, kiberbűnözés, kiberbűnözés eszközei, felsőoktatási információs rendszerek*

[1] Eszterházy Károly Egyetem, informatikai igazgató – Eszterhazy Karoly University, Director of IT, e-mail: koczka.ferenc@uni-eszterhazy.hu, ORCID: https://orcid.org/0000-0002-7541-6495

[2] Nemzeti Közszolgálati Egyetem, tanszékvezető – National University of Public Service, Department of Informatics, Head of Department, Associate Professor, e-mail: negyesi.imre@uni-nke.hu, ORCID: https://orcid.org/0000-0003-1144-1912

Abstract

In the Hungarian academic sphere, a large amount of sensitive data is processed in the course of education, research resources and results, as well as administrative processes. These institutions do not belong to state and municipal bodies and are therefore not subject to the legislation governing their operation. Methods and tools for protecting IT systems are thus more diverse, but the resources available are limited. The study examines the current motivation for attackers, predicts which key areas should be protected in the near future based on the annual reports of defence systems, and their application to the defence strategy. The results presented are not academic-specific, so they can be used not only in that field, but also in other organisations.

Keywords: *information security, penetration test, cybercrime, cybercrime tools, higher education information systems*

Bevezetés

Ma szinte minden szervezet rendelkezik olyan adatvagyonnal, amely biztonságának megőrzése a szervezet elemi érdeke. A biztonság megvalósítása sokrétű és számos aspektusból tárgyalható, de szinte minden összetevője besorolható az információbiztonság alapelemeinek valamelyikébe; ezek a bizalmasság, sértetlenség és a rendelkezésre állás. A biztonság adott szintjének elérésére igénybe vehetők technikai eszközök és szolgáltatások, ezek azonban folyamatosan változnak, miközben egyre magasabb szinten látják el a feladataikat.

A nemzeti adatvagyon védelme minden ország elemi érdeke, amelynek kereteit jogszabályok határozzák meg. Magyarországon az állami és önkormányzati szervek információbiztonságáról a 2013. évi L. törvény rendelkezik,[3] a 41/2015-ös BM rendelet konkrét gyakorlati útmutatót ad a biztonsági osztályokba sorolásról és a védelem kialakításának konkrét teendőiről.[4] A létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről a 2012. évi CLXVI. törvény rendelkezik.[5] Ezeknek a jogszabályoknak a hatályuk alá tartozó intézményi kör egésze ma biztosan nem felel meg, ennek elsődleges oka a szakemberek és a szükséges anyagi erőforrások hiánya.

Jelen cikk célja annak bemutatása, hogy az akadémiai szféra rendelkezik-e védendő adatvagyonnal, és megvizsgálja a védelem fejlesztésének néhány nem általános aspektusát.

[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[4] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

[5] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

Az akadémiai szféra adatvagyona

A felsőoktatásban működő informatikai rendszerek három fő területen látják el a feladataikat, ezek az oktatás, kutatás és az adminisztráció. Az intézmények ezen feladataik ellátása érdekében nagy tömegű személyes adatot kezelnek. A személyi állomány adatait kezelő célszoftverek, valamint a hallgatók személyes adatait tartalmazó tanulmányi rendszerek minden intézmény esetében olyan érzékeny adatokat jelentenek, amelyek elvesztése komoly kárt, illetéktelenek hozzáférése esetén a GDPR-ban foglaltak szerinti komoly büntetést és az intézménnyel szembeni komoly bizalomvesztést eredményezne. Az elektronikus rendszerek biztonsági osztályba sorolását, azaz a védelmének elvárt erősségét a 2013. évi L. törvény öt osztályba sorolja, de a törvény hatálya nem terjed ki felsőoktatási intézményekre. A besorolási rendszer alapján az említett rendszereket a kezelt adatok mennyiségétől függően 4-es biztonsági osztályba kellene sorolni. A biztonsági besorolást maguk az érintett szervezetek végzik el, a besorolás fő kritériumai ebben az osztályban a nagy mennyiségű személyes adat sérülése, jogszabályok betartásának vagy végrehajtásának elmaradása, valamint a szervezettel szembeni bizalomvesztés bekövetkezése lehetnek.[6]

Az egyes felsőoktatási intézmények tevékenységi körük és képzési területeik alapján további informatikai rendszerekhez férnek hozzá, vagy kezelik azok adatait. Egy érzékletes példa az egészségügyi adatok kezelése. Magyarországon ma négy egyetemen folyik orvosképzés, a gyakorlati képzés az egyetemek gyakorló kórházaiban is zajlik.[7] A betegek személyes adatait kezelő rendszerek egészségügyi (ideértve a gyógyszeres kezeléseket is) adatok tömegét tartalmazzák, amelyhez az egyetemi hallgatók szűkebb, az oktatók, rezidensek és PhD-hallgatók viszont sokkal szélesebb körben rendelkeznek hozzáféréssel, így különleges védelmet kell biztosítani azoknak. Más egyetemek esetében is vannak hasonlók, az Eszterházy Károly Egyetembe olvadt Károly Róbert Főiskola egyik kutatócsoportja a 2010. október 4-én bekövetkezett vörösiszap-katasztrófa során végzett mérései során is minősített adatok keletkeztek. Az akadémiai szféra egészében kezelt rendszer a tanulmányi rendszer, amely a jelenlegi képzésben részt vevők mellett a már végzett hallgatók adatait is tartalmazza.

Az adminisztrációs terület minden intézmény esetében tartalmaz érzékeny adatokat. Az iktatórendszerek alkalmazási szintjüktől függően legalább részleges vagy akár a teljes iratkezelést megvalósítják. A konkrét beszerzési dokumentációk kikerülése a potenciális beszállítók számára jelenthet konkrét gazdasági előnyt, így a verseny tisztaságának fenntartása érdekében ezek is védendők.

A szellemi adatvagyon (intellectual property) védelme szintén alapvető fontosságú feladat a felsőoktatási informatikai rendszereket üzemeltetők számára. A magyar egyetemek egy része általános kutatási feladatokat lát el, és nem lehet megjósolni, hogy melyik és mikor jelent majd olyan értéket, amely megtérülővé tehet egy támadást az adott intézmény ellen.

[6] 41/2015. (VII. 15.) BM rendelet 2.5 §.

[7] A Semmelweis Egyetem Általános Orvostudományi Karának gyakorló kórházainak listája, http://semmelweis.hu/aok/files/2018/11/Gyakorló-Kórház-lista-2018.pdf (Letöltve: 2019. 03. 10.)

A fentiek alapján elmondható, hogy az akadémiai szférában végzett kutatások során keletkezett adatvagyon biztonsága akár nemzetbiztonsági érdek is lehet, ennek ellenére ezek azonosítása, kijelölése és védelmének törvényi szabályozása e cikk írásáig nem történt meg.

Nemzetközi gyakorlat

A felsőoktatási rendszerek tekintetében a nemzetközi gyakorlat nem sokban különbözik a magyartól. Számos ország esetében fogalmaznak meg ajánlásokat a kritikus infrastruktúrák számára, amelyet más szervezetek is alkalmazhatnak a saját működésük biztonságossá tételére. Ez a lehetőség érhető el (és ajánlott) az akadémiai szféra számára is. Az egyik figyelmet érdemlő ajánlást az amerikai Nemzeti Szabványügyi és Technológiai Intézet (NIST) adta ki *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* címmel,[8] amelynek fő célja a költséghatékonyság szem előtt tartásával a köz- és magánszféra, valamint a társadalmi, gazdasági és iparági szereplők számítógépes kockázatainak csökkentésére irányuló védelmi célú szabványok, iránymutatások, módszerek és jó gyakorlatok biztosítása. Az ajánlás három részből épül fel: a keretrendszerből, a végrehajtási szintekből és a keretprofilokból. A végrehajtási szintek tulajdonképpen a szervezet érettségét írják le, vagy annak elérését tűzik ki célul a kockázatkezelési folyamat, az integrált kockázatkezelési program és a külső szervezetek részvétele szempontjából, a részlegestől az adaptív szintig. A keretrendszer segítségével felépíthető a szervezeti profil, amely tartalmazza, hogy melyek az adott szervezetre vonatkozó kockázati területek, azonosítja azok követelményeit, valamint rögzíti a kockázatviselési tolerancia szintjét. Ebben rejlik a NIST Framework rugalmassága: a védendő informatikai rendszer függvényében minden szervezet egyénileg szabhatja testre a védelmi stratégiáját.

A keretrendszer felépítése és az ajánlott metodika alkalmazása esetén a szervezet információs rendszerének és adatvagyonának védelmi rendszere a szervezet szükségleteinek és a vállalható anyagi kondícióknak megfelelően építhető fel, az ajánlás rendszeres frissítésének és aktualizálásának követése biztosítja annak érvényességét a jövőben is.

A felsőoktatási rendszerek védelme

A fenti jogszabályok egyike sem vonatkozik a felsőoktatásban üzemeltetett informatikai rendszerekre, így azok tervezése, kivitelezése és fenntartása során nem kötelező az ezekben foglaltak betartása. Ez nem jelenti azok védtelenségét, de a védelem szempontrendszerének definiálása, a védelmi infrastruktúra meghatározása és működésének

[8] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Letöltve: 2019. 05. 13.)

szabályozása jelenleg az intézményi autonómia keretein belül történik. Ugyanakkor elmondható, hogy az üzemeltető szervezetek egy része ismeri és a kötelezettség hiánya ellenére is alkalmazza azokat a saját szervezetében. Több magyar egyetem informatikai biztonsági szabályzata a 2013. évi L. törvény és az ISO 27001 szellemében készült, tartalmazza az informatikai rendszerek és szervezeti egységek biztonsági osztályba sorolását. A megvalósítás azonban komoly problémákba ütközik: a jelenlegi munkaerő és piaci viszonyok mellett a felsőoktatási intézmények vezetésének komoly nehézséget jelent a megfelelő tapasztalattal bíró új informatikai szakemberek alkalmazása, illetve a meglevők megtartása. Az évek óta érzékelhető szoftverkrízis[9] hatására az erős gazdasági szereplők felszívják a szakma legjobban képzett embereit, így azok az állami, katonai és oktatási szektorban csak kis számban dolgoznak. Tovább rontja a szakemberek megtartását a külföldi munkavállalás lehetőségének leegyszerűsödése, az informatika esetében ráadásul ennek ma már nem feltétlenül kell a mobilitással együtt járnia.

Fontos kérdés, hogy milyen mértékben kell számolnunk az akadémiai szféra elleni kibertámadásokkal, hiszen a költségarányos védekezést ez alapján lehet megvalósítani. A magyar felsőoktatási rendszerek elleni támadásokról nem találtunk nyilvános adatokat. Külföldi források nagyobb számban számolnak be ilyen esetekről, azok motivációiról,[10] így a kibertér globális jellege miatt érdemes ezeket is megvizsgálni. A hackmageddon.com internetes oldal évről évre közzéteszi az adott év kibertámadási statisztikáit, ezek tartalma jó kiindulási alapot szolgáltathat a magyar fenyegetettség mértékének megállapításához is.[11] Ezekből a statisztikákból az alábbi táblázatban foglaltam össze az oktatási rendszerek egésze elleni kibertámadások alakulását 2012 és 2018 között (a 2013. és 2012. évi adatok egy-egy kiválasztott hónapra vonatkoznak). Az elmúlt hét év átlaga alapján az összes támadás 5,98%-a irányult oktatási intézmények ellen, ugyanakkor intenzitásuk nem homogén: az egyes évek közt nagyobb eltérések mutatkoznak.

Érdekes probléma lehet annak megállapítása, hogy 2016-ban (és csak abban az évben) miért esett felére a detektált támadások száma. A lehetséges okokat egyrészt a társadalmi vagy gazdasági környezetben kereshetjük, ugyanakkor egy másik lehetséges ok a detektálás hibás mérése például azért, mert azok jellege ebben az évben megváltozott.

[9] A szoftverkrízis a szoftverek fejlesztésének és naprakészen tartásának válságát jelenti, azt az állapotot, amelyben nem lehetséges az igényeknek megfelelő mennyiségben szoftvereket előállítani, működőképességüket fenntartani, működésüket az aktuális igényeknek megfelelően aktualizálni.

[10] Cyber attacks on colleges and universities: who, when and why? www.jisc.ac.uk/blog/cyber-attacks-on-colleges-and-universities-who-when-and-why-14-sep-2018 (Letöltve: 2019. 03. 26.)

[11] 2018 master table, www.hackmageddon.com/2018-master-table/ (Letöltve: 2019. 02. 28.); 2017 Cyber Attacks Statistics, 2018, www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2016 Cyber Attacks Statistics, 2017, www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.); 2015 Cyber Attacks Statistics, 2016, www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2014 Cyber Attacks Statistics (Aggregated), 2015, www.hackmageddon.com/2015/01/13/2014-cyber-attacks-statistics-aggregated/ (Letöltve: 2019. 03. 09.); 2013 Cyber Attacks Statistics, www.hackmageddon.com/2013-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.); 2012 Cyber Attacks Statistics, www.hackmageddon.com/2012-cyber-attacks-statistics-master-index/ (Letöltve: 2019. 03. 09.)

1. táblázat: *Az oktatási szféra elleni kibertámadások eloszlása az elmúlt években.*

Év	%
2018	5,5
2017	6,6
2016	3,4
2015	6,9
2014	5,5
2013	6,7
2012	7,3

Forrás: 2018 master table. www.hackmageddon.com/2018-master-table/ (Letöltve: 2019. 02. 28.); 2017 Cyber Attacks Statistics, 2018, www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2016 Cyber Attacks Statistics, 2017, www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.); 2015 Cyber Attacks Statistics., 2016, www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2014 Cyber Attacks Statistics (Aggregated)., 2015, www.hackmageddon.com/2015/01/13/2014-cyber-attacks-statistics-aggregated/ (Letöltve: 2019. 03. 09.); 2013 Cyber Attacks Statistics, www.hackmageddon.com/2013-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.); 2012 Cyber Attacks Statistics, www.hackmageddon.com/2012-cyber-attacks-statistics-master-index/ (Letöltve: 2019. 03. 09.)

A motiváció

Egy informatikai rendszer elleni támadások megértésének egyik elsődleges alapja lehet a támadók motivációinak feltérképezése és megértése. A lehetséges motivációk kategorizálására több forrás is vállalkozik. A hackmageddon.com a motivációkat nagyobb csoportokba sorolja úgy, hogy elsősorban a külső okokra koncentrál, amelyek a következők:[12]

- A kiberhadviselés, azaz olyan politikai indíttatású konfliktus, amelyet ellenséges számítógépes és információs rendszerre irányuló támadásként kezdeményeztek. Céljuk az adott helyzetben más és más lehet, a létfontosságú számítógépes rendszerek működésének megzavarásától a minősített adatok ellopásán vagy megváltoztatásán át a psyops[13] műveletekig.
- A hacktivizmus, azaz az interneten folytatott politikai aktivizmus, amelynek célja szólásszabadság, az információszabadság és az emberi jogok kivívása

[12] 2018 master table, www.hackmageddon.com/2018-master-table/ (Letöltve: 2019. 02. 28.); 2017 Cyber Attacks Statistics, 2018, www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2016 Cyber Attacks Statistics, 2017, www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.); 2015 Cyber Attacks Statistics, 2016, www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2014 Cyber Attacks Statistics (Aggregated), 2015, www.hackmageddon.com/2015/01/13/2014-cyber-attacks-statistics-aggregated/ (Letöltve: 2019. 03. 09.); 2013 Cyber Attacks Statistics, www.hackmageddon.com/2013-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.); 2012 Cyber Attacks Statistics, www.hackmageddon.com/2012-cyber-attacks-statistics-master-index/ (Letöltve: 2019. 03. 09.)

[13] Psyops: psychological operations, lélektani műveletek. A NATO szerinti értelmezésben „olyan tervezett lélektani […] tevékenység, amely a béke válság és háború időszakában az ellenséges és a semleges közegekre irányul, amelynek célja, hogy hatást gyakoroljon a politikai és katonai célkitűzések elérését befolyásoló célcsoport(ok) szellemi beállítottságára, magatartására és viselkedésére." Pix Gábor: A lélektani műveletek jellemzőinek vizsgálata, Doktori értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2005.

vagy szabadságának megőrzése. Főbb eszköztárába a médiahack, a túlterheléses támadások, a defacement és a különféle információszivárogtatási módszerek tartoznak.[14]
- A kiberkémkedés számítógépes rendszerekben tárolt adatok kifürkészésére irányul, célja a legtöbb esetben személyes, gazdasági, politikai vagy katonai előny megszerzése.
- A kiberbűnözés, amelyben a bűncselekmény elkövetése a kibertérben történik függetlenül attól, hogy a bűncselekmény célja a számítógépekre vagy az azokban tárolt adatokra irányul, esetleg a kibertér csak a bűnelkövetés eszköze vagy tere.

Az elmúlt évek statisztikái alapján a fő motivációs tényezők is megváltoztak. Az alábbi táblázat tanúsága szerint a hacktivizmus évről évre gyengül, ugyanakkor nagyban megerősödött a kiberkémkedés.

2. táblázat: *Az elmúlt négy év kibertámadásainak motivációja*

Év	Kiberbűnözés	Hacktivizmus	Kémkedés	Hadviselés
2018	79,2%	2,8%	16%	1,9%
2017	84,6%	4,4%	9,9%	1,1%
2016	72,1%	14,2%	9,2%	4,3%
2015	67%	20,8%	9,8%	2,4%

Forrás: 2018 master table. www.hackmageddon.com/2018-master-table/ (Letöltve: 2019. 02. 28.); 2017 Cyber Attacks Statistics, 2018, www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2016 Cyber Attacks Statistics., 2017, www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.); 2015 Cyber Attacks Statistics, 2016, www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.)

A tendencia alapján 2019-ben a védelmi rendszerek üzemeltetése során célszerű a kiberbűnözés és a kiberkémkedés kivédésére helyezni a hangsúlyt.

A fenti felosztás elsősorban a külső motivációs okokra koncentrál, és kevésbé veszi figyelembe a lehetséges belső motivációkat. Az Intel vizsgálatai eredményeként egy részletesebb, tízelemű felosztást alkalmaz, amely lényegesen szélesebb körben határozza meg az egyes motivációkat,[15] és utal az egyes motivációk közötti lehetséges összefüggésekre is. Eszerint a motivációk fő területei:
- *Véletlen támadások (accidental),* amelyek a támadást elkövető akaratán kívül jönnek létre. Ezek körébe leginkább azok az események tartoznak, amelyek kiváltó oka a munkatárs inkomptenciája az elvégzendő feladattal kapcsolatban.

[14] Hacktivizmus, https://occupy.fandom.com/hu/wiki/Hacktivizmus (Letöltve: 2019. 03. 11.)
[15] Understanding Cyberthreat Motivations to Improve Defense, White Paper, Intel Security and Privacy Office, 2015, www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf (Letöltve: 2019. 03. 03.)

- *A kényszerítés (coercion)* során a támadó egy munkatársat zsarolás vagy egyéb fenyegetés, kényszerítés útján vesz rá egy olyan cselekmény elvégzésére, amely az információs rendszert a támadó céljainak elérése érdekében módosítja.
- Az *elégedetlenség (disgrunlement)* a munkahelyen kialakult helyzetből adódó sértettség által motivált bosszú. Ezt a motivációt nemcsak az alkalmazásban levő, hanem a távozott munkatársak esetében is figyelembe kell venni.
- *Fölény (dominance)* elérése a legváltozatosabb területeken. Ez a motiváció nemcsak a kibertérre, hanem a valós világra is kiterjed.
- *Ideológiai okok (ideology)*. A vallási és politikai okok mellett számos más ideológiai (erkölcsi, igazságérzet stb.) ok jelenthet motivációt a támadók számára.
- A *hírhedtség (notoriety)* elérése a kibertámadások legkorábbi indítékainak egyike volt, és még mindig megtalálható a motivációk közt.
- A *szervezeti haszon (organization gain)* megszerzése a legtöbb szervezet számára elsődleges célt jelent. Ez és a személyes haszon elérése a kibertámadások egyik legfőbb motivációja, amelyet a kiber alvilág szolgáltatásként kínál *(CaaS – Cybercrime as Service, EaaS – Espionage as a Service),* és amelyet tételesen beárazva terjeszt.[16] A támadások céljai közt egyaránt megtalálhatók az ellenfél tudásbázisának megszerzése és ezzel a saját célok elérésének megerősítése, valamint az ellenfelek rendszerének meggyengítése, hírbe hozása, jogellenes tevékenységének nyilvánosságra hozása.
- *Személyes üzleti/pénzügyi haszon (personal financial gain)* megszerzése.
- *Személyes elégedettség (personal satisfaction)* megszerzése. Ebbe a körbe elsősorban olyan információk megszerzése tartozik, amelyek birtoklása nem jelent realizálható hasznot, ugyanakkor növelik a támadó személyes mentális elégedettségét. Tipikus példái a híresség egészségügyi, tanulmányi vagy más személyes adatainak megszerzése, de sok esetben csupán a tiltások különösebb ok nélküli áthágása is.
- *Egyéb (unpredictable)* előre nem látható motivációk. Ebbe a körbe a teljesen kiszámíthatatlanul bekövetkező események tartoznak, például egy korábban teljesen ismeretlen anarchista csoport motivációi.

[16] Rapp, Nicolas – Hackett, Robert: A Hacker's Tool Kit, 2017, http://fortune.com/2017/10/25/cybercrime-spyware-marketplace/?xid=gn_editorspicks (Letöltve: 2019.03. 11.)

1. ábra: *A kibertámadások motivációs okai*

Forrás: Frumento, E. et al.: The role of Social Engineering in evolution of attacks, 2016, www.dogana-project.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf (Letöltve: 2019. 07. 07.)
Az ábrát fordították a szerzők.

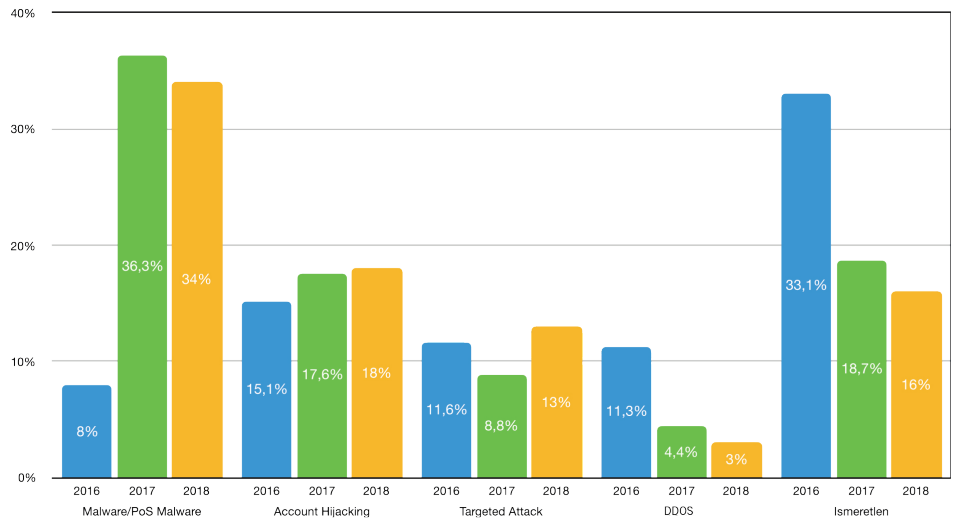
A lehetséges kibertámadások motivációinak felismerése és rendszerezése lehet a védekezési stratégia egyik alapja. A motivációk alapján azonosíthatók a fenyegetett rendszerek, a kockázatkezelés elvégzése után megtervezhető és felépíthető lehet a védelmi stratégia és az ahhoz szükséges eszközrendszer.

Az akadémiai rendszerek elleni támadások alacsony arányát a kiberbűnözést motiváló okok vizsgálatával lehet magyarázni. Ugyanakkor nem zárható ki, hogy a fenti motivációk valamelyike a felsőoktatás célpontszerepét magasabb szintre fogja emelni.

A támadás eszközei

A védelem tervezéséhez a támadók eszközkészletének analizálása és a célok azonosítása adhat kiváló támpontot. Érdemes a szervezet védelmi rendszerét az ismert támadási módszereknek megfelelően alakítani és az intenzíven támadott pontokat megerősíteni. Ezen támadások forrásaként a már hivatkozott hackmageddon.com

statisztikái mellett az erre szakosodott cégek és szervezetek éves jelentéseit és előrejelzéseit érdemes alapul venni.



2. ábra: *A fő támadástípusok változása 2016–2018 között*

Forrás: 2018 master table. www.hackmageddon.com/2018-master-table/ (Letöltve: 2019. 02. 28.); 2017 Cyber Attacks Statistics, 2018, www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2016 Cyber Attacks Statistics, 2017, www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.); 2015 Cyber Attacks Statistics, 2016, www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.); 2014 Cyber Attacks Statistics (Aggregated), 2015, www.hackmageddon.com/2015/01/13/2014-cyber-attacks-statistics-aggregated/ (Letöltve: 2019. 03. 09.)

A diagram alapján megállapítható, hogy az elmúlt évek támadási területein megváltozott a hangsúly. A 2016-ban még nem igazán hangsúlyos malware támadások felerősödtek, az ezt követő két évben taroltak a zsarolóvírusok. 2018-ban csak minimálisan csökkent a számuk, így valószínűsíthető, hogy ezek a támadások hangsúlyosak lesznek a 2019-es évben is.

Az account hijacking[17] előfordulásában nem tapasztalható jelentős eltérés az elmúlt három évben, a célzott támadások száma a 2017-es visszaesés után 2018-ban ismét megemelkedett. A DDOS[18]-támadások száma visszaesőben van, ez jó jel a kritikus szolgáltatásokat működtető szervezetek számára. Szintén ígéretes, hogy az ismeretlen támadások száma is jelentősen csökkent, ez valószínűsítheti a támadási módszerek megismerését, de az új módszerek megjelenésének elmaradását is.

[17] Olyan számítógépes tevékenység, amelynek során a támadó célja valamilyen rendszer hozzáféréséhez szükséges azonosító, tipikusan bejelentkezési név és jelszó megszerzése.

[18] Distributed Denial of Service. Olyan számítógépes támadási forma, amelyben a célszámítógéphez rengeteg kérést küldenek, amelyet az képtelen kiszolgálni, vagy a keletkezett forgalom a rendelkezésre álló hálózati kapcsolatának teljes kapacitását meghaladja.

A Panda Lab a Panda Security kártevőellenes laboratóriuma, amely minden évben kiadja a veszélyforrásokról szóló éves riportját, amelyet az érzékelő hálózatára és a végpontvédelmi szoftverek statisztikáira alapoz. A cég 2018-as jelentése szerint mára megváltozott az internetes támadások szerkezete.[19] A védelmi megoldások 2018-ban hozzávetőleg 9 millió kártékony webhelyet blokkoltak, és egymillió végpontonként 2,4 millió támadást akadályoztak meg. A malware támadások száma folyamatosan emelkedik, ez a tendencia az elmúlt évben sem sokat változott. A trend szerint a fájlalapú támadások visszaesőben lesznek, ezek felismerése (a központi védelmi központok kiépülésével) megoldottá válik, ezért amennyiben a kiberbűnözők elérik a célrendszert, a meglevő szolgáltatásokban keresik a továbblépés lehetőségét – a jelentés konkrétan az RDP-re[20] alapozott támadások számának brutális emelkedését emeli ki.[21] Méréseik szerint a közepes és nagy ügyfeleik 70%-a minden hónapban ki van téve egy ilyen támadásnak.

Ugyanakkor a cél ismerete nélkül, tömegesen szétküldött megtévesztő levelek (phising, scam) számának csökkentését jósolja a jelentés. Az ilyen támadások hatékonysága nehezen becsülhető, de szinte biztosan nem lehet több néhány tized százaléknál, mert ez a támadási forma a felhasználók jó része számára azonnal felismerhető. A gépi fordítású és rossz helyesírású szövegek sokak számára egyértelmű jelzést jelentenek a csaló tartalomra, és részben a levél feladóját és címzettjét is ellenőrizni tudják. Ehhez hozzájárul a levelező rendszerek hatékonyságának növekedése, így várhatóan ezekből a korábbi időszakban jellemző mértéknél kevesebb jut el a végpontig, illetve nagyobb hatékonysággal kerülnek a kéretlen leveleket gyűjtő mappába.

2018-ban a kriptovaluták bányászatával kapcsolatos támadások száma 3,5-szeresére nőtt. A támadások ilyen mértékű növekedésére egy rosszul elsült kísérlet adta meg a táptalajt: a Coinhive-projekt egy weboldalba illeszthető bányászszoftver kifejlesztését tűzte ki célul, amit a weboldalak tulajdonosai a saját weboldalaik kódjában helyezhettek el. A szoftver az oldalt meglátogató kliensek gépein futott, és azok erőforrásait kriptovaluta bányászatára használta fel. Az így kibányászott kriptovaluta az üzemeltető tárcájába került, ennélfogva ezzel az üzleti modellel lehetett volna az oldal működtetésének pénzügyi forrását biztosítani. Az ilyen weboldalak viszont mágnesként vonzották a kiberbűnözőket, akik ezeket a weblapokat feltörve módosították a szoftver paramétereit, és a kibányászott kriptovalutát a saját tárcájukba utalták.[22]

[19] PandaLabs Annual Report 2018, https://partnernews.pandasecurity.com/uk/src/uploads/2018/12/PandaLabs-2018_Annual_Report-uk.pdf (Letöltve: 2019. 03. 09.)

[20] Az RDP (Remote Desktop Protocol) a Microsoft által tervezett protokoll, amely lehetővé teszi egy Windows rendszerű számítógépre a távoli bejelentkezést. A protokollban több alkalommal is fedeztek fel sérülékenységet, és a hibás konfigurációk, valamint a bekapcsolva hagyott konfigurálatlan rendszerek következtében számos alkalommal szolgált a kiberbűnözők bejutási pontjaként. Az RDP-n támadható publikus szerverek elérhetősége az interneten sokáig megvásárolható volt, a 2014-től működő xDedic csoport site-ján, ahol egy hozzáférést földrésztől és Windows verziótól függően 3 és 9 $ közötti áron lehetett megvásárolni. Az oldalt a hatóságok végül 2019-ben zárták be, az üzemeltetők valószínűleg a szolgáltatást más néven újra fogják indítani.

[21] Schwartz, Mathew J.: Stolen RDP Credentials Live On After xDedic Takedown, 2019, www.bankinfosecurity.com/stolen-rdp-credentials-live-on-after-xdedic-takedown-a-11987. (Letöltve: 2019. 03. 11.)

[22] Bezár a Coinhive: nem éri meg, 2019, https://kriptoakademia.com/2019/03/02/bezar-a-coinhive-nem-eri-meg (Letöltve: 2019. 03. 11.)

A ransomware támadások száma 2018-ban jelentősen nőtt. Míg 2017-ben a malware-eknek csak 1%-a volt ransomware, 2018-ra ez 7%-ra emelkedett, ezért ezek kivédésére továbbra is nagy hangsúlyt kell helyezni.[23]

Célzott támadások

A felsőoktatási rendszerek adataihoz történő hozzáférés valószínűleg inkább célzott támadások útján valósulhat meg. A hivatkozott előrejelzések a cél véletlenszerű kiválasztása helyett a spear phising[24] jelentőségének, ennélfogva azok számának növekedését prognosztizálják, és kiemelik a támadások előtérbe kerülését.

A korábban említett motivációk által generált célok eléréséhez a támadók számára az akadémiai szférában a célzott támadások biztosíthatnak nagyobb lehetőséget. Annak ellenére, hogy a felsőoktatási rendszerek a rendelkezésre álló anyagi erőforrások hiánya miatt a legtöbb esetben nem élvonalbeli technikai védelmi eszközöket használnak, a támadások jelentős része továbbra is a humán oldal megtévesztésével indítható el egyszerűen. Ezt a kiberbűnöző csoportok is felismerték, így a pszichológiai manipuláció eszköztárát is megújították. A cél elérése érdekében a támadók mára felhasználják a korszerű tudományos eredményeket, és az adatgyűjtési technikák is jelentősen megújultak.

A tudományos eredmények felhasználása

Bár sokak számára a számítógépes rendszerek sérülékenységeinek feltérképezése és kihasználása tisztán technikai kérdésnek tűnik, ez már a kezdetekben sem volt így. A korai social engineering leginkább hype-olt celebje, Kevin Mitnick eszköztára is humán módszereken alapult.[25] A humán megtévesztésben az ő sikereit inkább a megérzései és meggyőző stílusa biztosította, tudományos eredményeket ezen a téren nem használt. A mai professzionális támadók számára viszont ezek az eredmények kiváló lehetőséget jelentenek az áldozat bizalmának elnyerésében és a támadó akaratának elérésében. Ezen a téren a legfontosabb tudományos területek a szociológia-, pszichológia-, marketing- és kommunikációs tudományok mellett a mesterséges intelligencia[26] és a véleménybányászat (sentinel analisys) az, amelyeket a támadói kör elitje ismer és alkalmaz is.

[23] NTT Security 2018 Global Threat Intelligence Report Executive Guide, www.dimensiondata.com/insights/-/media/dd/corporate/pdfs/gtir-executive-guide-2018.pdf (Letöltve: 2019. 03. 11.)

[24] Meghatározott személy, szervezet vagy vállalkozás ellen indított e-mail, esetleg más megtévesztő elektronikus kommunikáció útján történő támadás. Tipikus példái a személyre szabott hamisított levelek, amelyek célja a támadó akaratának megfelelő reakció kiváltása, például internetes fizetés elérése.

[25] Mitnick, Kevin D. – Simon William L. – Wozniak Steve: The Art of Deception: Controlling the Human Element of Security, Indianapolis, John Wiley & Sons, 2001.

[26] Az MI a védekezésben is hasznos fegyver lehet, egy érdekes alkalmazást kínál a https://www.rescam.org weboldal projektje. A me@rescam.org címre továbbított adathalász levelekre egy MI robot fog válaszolni a feladóknak, így adva felesleges munkát a nigériai csalók számára.

Az OSINT

A social engineering (SE) korai fázisában az adatok gyűjtése kimerült a klasszikus módszerek alkalmazásában.[27] Az OSINT (Open Source Intelligence) egy új út ebben, nyilvánosan elérhető forrásokból történő információgyűjtést jelent. Személyes és céges adatok gyűjtésében a nyilvánosság nagyban segíti a támadók munkáját. A Facebook, Instagram, LinkedIn és hasonló közösségi site-ok, a személyes és céges weblapok, hírek, iparági folyóiratok, szabadalmi listák, valamint egyéb információs rendszerek értékes források, és sok esetben már önmagukban is nagy jelentőségű információt adnak közre. Az összekapcsolásukkal azonban új összefüggések állapíthatók meg például kulcspozícióban levő vezetők magánéletéről, szokásaikról, érdeklődési körükről, amely a modern SE következő fázisát, a bizalom elnyerésének lépését alapozza meg. Ezeket összerakva tehát a támadó számára komplex kép alakítható ki, amely nagyban megkönnyíti a célirányos akció megtervezését és végrehajtását.[28] A nyilvános adatszolgáltatási kötelezettségekből adódó adatközlések, az átlátható működést biztosító előírások így az OSINT aranybányáivá váltak, egy célzott támadás előkészítésének folyamatában az első lépést jelentik.

Az adatgyűjtés automatizálására jelenleg csak részleges módszerek ismertek, de a feladatra nagyon egyszerűen használható, publikusan is elérhető eszköztár áll már rendelkezésre, amelyek elsősorban kész szoftverek vagy webalapú szolgáltatások. Néhány tipikus példa:

- Egy rendszerben elérhető adatok megkeresésére a Google-hackingtechnikák alkalmazását szokás bevetni. A Google keresőmotorja a webes tartalmak teljes áttekintésével olyan elemeket is felindexel, amelyeket a rendszerek tervezői nem akartak közzétenni, akár teljes adatbázismentéseket, forráskódokat tölthet le a támadó egy hibás konfiguráció eredményeként,[29] de számos más publikus alkalmazás segíti az adatgyűjtők munkáját.[30]
- Szintén webes alapú szolgáltatás a checkusernames.com, amely egy megadott felhasználónevet keres 160 webes szolgáltatásban, így egy felhasználói hozzáférés megszerzése után segít megkeresni további lehetséges oldalakat, amelyek esetében ugyanezzel a hozzáférést használja a tulajdonos.
- A searchcode.com a GitHub és hasonló kódmegosztó weboldalakon közzétett szoftverek forráskódjában keres, amellyel egy ismert sérülékenységet tartalmazó webhely könnyen megkereshető és felhasználható.
- A felderítő munkára célszoftverek vehetők igénybe, amelyek megnevezésükben szinte minden esetben penetrációs tesztek elvégzésére létrehozott terméket sugallnak, használóit azonban semmi sem akadályozza meg abban, hogy ezeket támadási céllal alkalmazzák. Az ingyenes Kali Linux e sorok

[27] Tipikus példák voltak a telefonos megtévesztések, az irodai szemét átvizsgálása, feljegyzett jelszó keresése, de a Whois adatbázisok, esetleg teljes zónák adatainak lekérése is a DNS-szerverektől.

[28] Az interneten közzétett személyes adatokat digital footprint néven említik. Ezek azonban egy másodlagos információs forrásként is szolgálhatnak, tipikus példa erre a képekben szereplő GPS-információ, amely lehetővé teszi a pontos helyszín meghatározását. Az ilyen, rendszerint akaratlanul közzétett információk gyűjtőneve digital shadow.

[29] Long, Johnny: Google Hacking for Penetration Testers, Syngress Publishing, Rockland, 2014.

[30] Passi, Harpreet: Top 10 Popular Open Source Intelligence (OSINT) Tools, 2018, www.greycampus.com/blog/information-security/top-open-source-intelligence-tools (Letöltve: 2019. 03. 12.)

írásakor több mint 600 ilyen eszközt tartalmaz.[31] Ezek jó része azonban nem teljes értékű szoftver, az ingyenes változatok több esetben csak korlátozottan használhatók, a teljes értékű változatok beszerzése pedig komoly költséget jelent.

A védekezés lehetőségei

A védekezés lehetőségeit alapjában véve két területen érdemes megvizsgálni, a technikai és a humán oldalról.

Az informatikai rendszerek üzemeltetését végző szervezeti egységnek ismernie kell az aktuális támadási motivációkat, a potenciális célokat és a támadók eszköztárát. A rendszer biztonságának felmérésében ezeket a szoftvereket a saját rendszerén is futtatnia kell, így felmérve, hogy milyen információkat gyűjthet be róla egy támadó. Ezzel biztosítható, hogy csak a szükséges mértékben kerüljenek ki olyan információk, amelyek az információs infrastruktúra felépítésére, a használt rendszerekre, illetve azok verziószámára utalnak. Ebben az eljárásban a támadók által használt eszközök valóban védelmi célokat szolgálnak majd.

A támadók eszközkészletének ismeretében potenciális lehetőség a támadó megtévesztése, amelyben a megtámadott rendszer a támadás tényét érzékeli, és nem a valóságnak megfelelő válaszokat ad, így megelőzve a sérülékenységet kihasználó szoftverek sikeres futtatását[32] vagy akár a támadó megtévesztését.

Az üzemeltetésnek nyomon kell követnie azokat az adatforrásokat, amelyek az aktuális kibertámadásokról adnak jelentéseket, ezek a különböző számítógépes eseménykezelési központok (CSIRT-ek vagy CERT-ek). A Govcert e sorok írásakor az egyetlen általánosan elérhető forrás, amelyet a Nemzeti Kibervédelmi Intézet[33] tart fenn. A CERT-ek tájékoztatást adnak a napi szintű sérülékenységek mellett az SE-módszerekről is, egy ilyen esetben a felhasználók azonnali tájékoztatása nagyban rontja a támadók esélyeit.[34]

A Magyarországon nem túl elterjedt Twitter szintén hasznos információforrást jelent az intézményi kiberbiztonsági felelős személy számára. Több szakember és csoport küld tweeteket kiberbiztonsági figyelmeztetésekről és eseményekről, valamint tájékoztatást ad a témával kapcsolatos források elérhetőségéről.

A felhasználók információbiztonsággal kapcsolatos ismereteinek hiánya a fentieken túl súlyos problémát jelenthet az őket alkalmazó szervezet számára. Az adatkezeléssel kapcsolatos folyamatoktól való eltérés, a szabályzatok ismeretének hiánya vagy be nem tartása forrása lehet a szervezeti adatvagyon elvesztésének vagy nyilvánosságra kerülésének. Amennyiben ők kibertámadás áldozatává válnak, jogosultságaik révén

[31] A legismertebb elemei a Maltego, Harvester, Metagoofil, Recon-ng.

[32] Az egyik elterjedt MTA, az Exim esetében a távoli kapcsolat felvételekor megjelenő szöveg az smtp_banner változóban adható meg, és egyszerűen módosítható akár egy más gyártó SMTP-szerverének adataira.

[33] A szolgáltatás a https://govcert.hu oldalon érhető el.

[34] Egy példa: a 2019-es év adóbevallási időszakára időzített támadás adóvisszatérítést ígérve próbált Ügyfélkapu hozzáféréseket gyűjteni. A támadás részletes leírása a https://govcert.hu/figyelmeztetesek/tajekoztatas/ado-visszateritesre-hivatkozik-a-nav-nevevel-visszaelo-uj-adathalasz-kampany/ oldalon jelent meg.

a szervezetük informatikai rendszerén kisebb-nagyobb mértékben ők maguk fognak biztonsági réseket nyitni.

Éppen ezért a felhasználók képzésének és ismereteik szinten tartása a szervezetek egyik kiemelt feladata kell hogy legyen. Egy-egy témában készültek tananyagok, és jó minőségű összefoglaló művek is rendelkezésre állnak.[35] Az általánosan elterjedt képzési módszereket, amelyek egy általános tananyag átadásán nem lépnek túl, valamint a felhasználói tudatosság mérésének hagyományos módszereit már nem tartom elégségesnek. Utóbbi esetben gyakran kérdőívet használnak, ennek hatékonysága véleményem szerint erősen megkérdőjelezhető, a felhasználók viselkedése a gyakorlatban eltér az elvárttól, annak ellenére, hogy legalább részben ismerik a lehetséges kockázatokat.

Javaslatom szerint a megoldást a folyamatos oktatás, tesztelés és visszacsatolás körforgása jelenti, ahol a tesztelésben szerepet kell kapnia az intézmény saját magán végrehajtott penetrációs tesztjeinek is. Az a tény, hogy a felhasználók tudatában vannak annak, hogy rendszeres időközönként meg kell felelniük ezeken, fenn fogják tartani a figyelmüket, és ez visszatartó erőként működik a kritikus helyzetben adott reakcióik során.

Ezeket a teszteket az utóbbi időben több szervezetben is alkalmazták. A NATO saját katonáit tesztelte egy ilyen vizsgálattal,[36] de Magyarországon az Innovációs és Technológiai Minisztérium dolgozói is találkozhattak már hasonlóval egy nyereményjáték keretében. Ilyen, 1750 főre kiterjedő vizsgálat történt az Eszterházy Károly Egyetemen, amelynek célközönsége az egyetemi oktatók és egyéb munkakörben dolgozók köre volt.[37] Ezek a tesztek sajnos a legtöbb esetben rossz állapotot tükröznek, sem az elvégzésük, sem az eredményeik nem nyilvánosak, ami nagyban megnehezíti a téma kutatását.

Szót kell ejteni a felelősség kérdéséről is. Az üzemeltetésben dolgozók feladatai és az elvárt munkafolyamatok rendszerint a munkaköri leírásokban, illetve egyéb intézményi dokumentumokban tisztázottak. A felhasználói oldal esetében ez a kérdés sokkal nehezebb, mivel a kifinomult támadások felismerése és az arra adott helyes reakció a mai magyar munkavállalók esetében nem feltétlenül várható el. Az észszerű határ kijelölése szubjektív, ennek pontos meghatározása nehézkes lenne, így azt a szervezetek nem vállalják. Ezért ma túlnyomórészt nincsenek valódi következményei annak, ha egy munkavállaló kibertámadás áldozatává válva okoz kárt. Mivel a tájékozatlanság még a vezetők körében is általános, ők is megtéveszthetők, ezért a felelősségre vonás a kifinomultabb támadási metodikák esetében erkölcsi szempontból sem vihető végig, így a legtöbb esetben az legfeljebb a formalitás szintjét éri el. A felelősségre vonás elmaradása viszont negatívan hat az információbiztonságra, mivel annak betartási kényszeréből egy elem kiesik.

[35] A Neumann János Számítógéptudományi Társaság kiadványa egy nagy területet lefedő és egyszerűen megfogalmazott, ingyenesen letölthető kiadvány. IT biztonság közérthetően, 2019, http://njszt.hu/de/it-biztonsag-kozerthetoen (Letöltve: 2020. 02.10.)

[36] Lapowsky, Issie: NATO Group Catfished Soldiers to Prove a Point about Privacy, 2019, www.wired.com/story/nato-stratcom-catfished-soldiers-social-media (Letöltve: 2019. 03. 21.)

[37] Koczka Ferenc: Információbiztonsági teszt az Eszterházy Károly Egyetemen, Networkshop 2018 konferenciakiadvány, HUNGARNET Egyesület, Budapest, 2018.

Következtetések

A felsőoktatási információs rendszerek védelmének fenntartásában a technikai védelmen túl a humán oldalra is nagy hangsúlyt kell fektetni. Az előrejelzések szerint a hagyományos technikákat újak váltják fel, és erősödni fog az új megvilágításba került pszichológiai manipuláció is. A social media szerepe kiemelkedő információs forrássá vált a támadók számára, így a jövőben a megtévesztéses támadások felismerése is egyre nehezebb feladatot jelent majd.

Az akadémiai szféra informatikai környezete általános, néhány speciális adminisztratív és kutatási célú rendszer kivételével általánosan használt elemekből épül fel. Ennek következtében az informatikai rendszereit érő támadások jó része nem kifejezetten a felsőoktatásra specializált. Az általános támadási módszerek nagy része a felsőoktatási rendszerekben is megjelenik, így az informatikai üzemeltető szervezeti egységek számára fontos feltétel az aktuális támadási technikák ismerete, az általuk használt szoftverek, főként az információk begyűjtésére és analizálására szolgáló, a támadást előkészítő szoftverek és a malware-eket célba juttató eszközök ismerete.

A támadók motivációinak, módszereinek és az ehhez használt eszközök ismeretében a védekezési módszerek nem csak technikai téren tökéletesíthetők, a felhasználók tájékoztatása és információbiztonsági tudatossági szintjének emelése a social engineering technikák hatékonyságát nagymértékben képes csökkenteni.

A felhasználók éberségének fenntartásához a rendszeres penetrációs tesztek végrehajtását tartom a legjobb módszernek. A felhasználók támadása a jövőben sokkal kifinomultabbá válik, ezért a jól működő és fenntartható módszertan alapján történő oktatás minden szervezet számára elengedhetetlen.

Felhasznált irodalom

Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2018, DOI: https://doi.org/10.6028/NIST.CSWP.04162018

Koczka Ferenc: Információbiztonsági teszt az Eszterházy Károly Egyetemen, Networkshop 2018 konferenciakiadvány, HUNGARNET Egyesület, Budapest, 2018, DOI: https://doi.org/10.31915/NWS.2018.1

Lapowsky, Issie: NATO Group Catfished Soldiers to Prove a Point about Privacy, 2019, www.wired.com/story/nato-stratcom-catfished-soldiers-social-media (Letöltve: 2019. 03. 21.)

Long, Johnny: Google Hacking for Penetration Testers, Syngress Publishing, Rockland, 2014.

Mitnick, Kevin D. – Simon, William L. – Wozniak, Steve: The Art of Deception: Controlling the Human Element of Security, Indianapolis, John Wiley & Sons, 2001.

PandaLabs Annual Report 2018, https://partnernews.pandasecurity.com/uk/src/uploads/2018/12/PandaLabs-2018_Annual_Report-uk.pdf. (Letöltve: 2019. 03. 09.)

Passi, Harpreet: Top 10 Popular Open Source Intelligence (OSINT) Tools, 2018, www.greycampus.com/blog/information-security/top-open-source-intelligence-tools (Letöltve: 2019. 03. 12.)
Pix Gábor: A lélektani műveletek jellemzőinek vizsgálata, Doktori értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2005.
Understanding Cyberthreat Motivations to Improve Defense, White Paper, Intel Security and Privacy Office, 2015, www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf (Letöltve: 2019. 03. 03.)
Rapp, Nicolas – Hackett, Robert: A Hacker's Tool Kit, 2017, http://fortune.com/2017/10/25/cybercrime-spyware-marketplace/?xid=gn_editorspicks (Letöltve: 2019. 03. 11.)
Schwartz, Mathew J.: Stolen RDP Credentials Live On After xDedic Takedown, 2019, www.bankinfosecurity.com/stolen-rdp-credentials-live-on-after-xdedic-takedown-a-11987 (Letöltve: 2019. 03. 11.)
Frumento, E. –Puricelli, R. –Freschi, F. –Ariu, D. –Weiss, N. –Dambra, C. –Cotoi, I. – Roccetti, P. –Rodriguez, M. –Adrei, L. –Marinelli, G. –Kandela, G. –Pachego, B.: The role of Social Engineering in evolution of attacks, 2016, www.dogana-project.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf (Letöltve: 2019. 07. 07.)

Jogi források

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

Internetes források

2012 Cyber Attacks Statistics, www.hackmageddon.com/2012-cyber-attacks-statistics-master-index/ (Letöltve: 2019. 03. 09.)
2013 Cyber Attacks Statistics, www.hackmageddon.com/2013-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.)
2014 Cyber Attacks Statistics (Aggregated), 2015, www.hackmageddon.com/2015/01/13/2014-cyber-attacks-statistics-aggregated/ (Letöltve: 2019. 03. 09.)
2015 Cyber Attacks Statistics, 2016, www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.)
2016 Cyber Attacks Statistics, 2017, www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/ (Letöltve: 2019. 03. 09.)

2017 Cyber Attacks Statistics, 2018, www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/ (Letöltve: 2019. 03. 21.)
2018 master table, www.hackmageddon.com/2018-master-table/ (Letöltve: 2019. 02. 28.)
Bezár a Coinhive: nem éri meg, 2019, https://kriptoakademia.com/2019/03/02/bezar-a-coinhive-nem-eri-meg (Letöltve: 2019. 03. 11.)
Cyber attacks on colleges and universities: who, when and why? www.jisc.ac.uk/blog/cyber-attacks-on-colleges-and-universities-who-when-and-why-14-sep-2018 (Letöltve: 2019. 03. 26.)
Hacktivizmus, https://occupy.fandom.com/hu/wiki/Hacktivizmus (Letöltve: 2019. 03. 11.)
IT biztonság közérthetően, 2019, http://njszt.hu/de/it-biztonsag-kozerthetoen (Letöltve: 2020. 02. 10.)
NTT Security 2018 Global Threat Intelligence Report Executive Guide, www.dimensiondata.com/insights/-/media/dd/corporate/pdfs/gtir-executive-guide-2018.pdf (Letöltve: 2019. 03. 11.)
A Semmelweis Egyetem Általános Orvostudományi Karának gyakorló kórházainak listája, http://semmelweis.hu/aok/files/2018/11/Gyakorló-Kórház-lista-2018.pdf (Letöltve: 2019. 03. 10.)