INFORMÁCIÓBIZTONSÁGI TESZT AZ ESZTERHÁZY KÁROLY EGYETEMEN

Koczka Ferenc
Eszterházy Károly Egyetem
koczka.ferenc@uni-eszterhazy.hu

DOI: 10.31915/NWS.2018.1

APT test at Eszterhazy Karoly University Most Hungarian organizations are not informed on the level of information security of their employees. The increasing number of threats requires surveying and taking appropriate measures. Technical based defense isn't enough to guarantee the necessary security, if human information security consciousness remains low. There is no general method to measure the level of information security consciousness, as a result in most cases questionnaires are used. However for several reasons their validity is considered unreliable, therefore a five step APT test was performed in Eszterhazy Karoly University. In three of the steps the IT staff was tested, in the remaining two all other employees. The results of the tests were worse than the anticipated. This publication describes the APT test, its results and presents some possible solutions.
Keywords: cybersecurity, APT test, phishing, information security consciousness

Bevezetés

Az informatikai rendszerek védelmére az üzemeltetők évről évre egyre nagyobb összegeket költenek, a védelmi eszközök egyre bonyolultabbak, és az üzemeltetésük is egyre nagyobb terhet jelent a tulajdonosuk számára. Ugyanakkor a védelmi eljárásokra fordított összegek 2017-ben nem feltétlenül értek célt, sok esetben azokat rossz védelmi technológiákra költötték. Eközben a sikeres támadások száma a szóban forgó évben összességében 27%-kal nőtt, ezen belül a ransomware támadások több mint a duplájára emelkedtek[1]. A média gyakran hangsúlyozza, hogy Magyarország jelenleg nem célpont, mégis, 2013-ban Magyarország volt a kibertámadások kiindulásának listáján a hatodik helyen[2]. Ha csak a lehetséges támadási formák egyikét, a számítógépes vírusokat vizsgáljuk, a 2017-es évben egyes források szerint 3,2 másodpercenként jelent meg egy új példány, ennek következtében a növekedés ilyen üteme mellett a jelenlegi vírusvédelmi megoldásokat időről időre újra kell gondolni, melyre több szakmai hivatkozást találunk[3]. Bár a támadástípusok jó része a szolgáltatási körrel párhuzamosan változik, nagy számban vannak nyitva azok a lehetőségek is, amelyekre a technikai oldal már rég megoldást adott: a súlyos károkat okozó, 2017-ben megjelent Petya ransomware annak ellenére ki tudott használni egy olyan SMB sebezhetőséget, melyet a WannaCry már korábban alkalmazott, hogy gyártó már javítást adott ki rá. A WannaCry és másolatai – bár a WannaCry maga is másolat – olyan mértékű kárt okoztak,

1 Accenture, Cost of cyber crime study insights on the security investments that make a difference. Hozzáférés: 2018. 07. 05. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

2 Angelyn flowers, Sherali Zeadally. Cyberwar: The What, When, Why, and How. IEEE Technology and Society Magazine. Fall 2014. Hozzáférés: 2018. 07. 01. https://doi.org/ 10.1109/MTS.2014.2345196

3 Danny Yedron. Symantec Develops New Attack on Cyberhacking. 2014. 05. 04. Hozzáférés: 2018. 07. 05. https://www.wsj.com/articles/symantec-develops-new-attack-on-cyberhacking-1399249948

hogy a Microsoft a már nem támogatott Windows XP-re is kiadta a javítást. Ugyanakkor számos olyan sebezhetőség is ismert, amelyet a gyártók sosem javítottak ki, a nulladik napi sebezhetőségek kezelése pedig a szakma egyik máig megoldatlan problémáját jelentik[4].

A műszaki oldal sajnos nem elég a biztonsági problémák megoldására, ezért a védelmet adminisztratív megoldásokkal is ki kell egészíteni. A mai gyakorlatban az emberi oldal jelenti a leggyengébb láncszemet, amit a támadók előszeretettel használnak ki: az ún. lándzsás adathalászat, bár nagyon egyszerű módszer, még mindig elég hatékony ahhoz, hogy folyamatosan a támadók első lépcsőfokként használják. Ennek lényege a nagy tömegben szétküldött becsapós levél, amely változatos módokon megpróbálja rávenni a címzettet valamilyen – rá nézve nem kívánatos – tevékenységre a kártékony szoftver telepítésétől az adatainak megadásán át a hamis számlák kifizetéséig.

Az informatikai üzemeltetés nem tud teljes körű védelmet nyújtani abban az esetben sem, ha jelentős anyagi kondíciók állnak a rendelkezésére. A technikai finomhangolások és az adott helyzetre adott műszaki válaszok mellett elengedhetetlen a felhasználók képzése, nélküle nem várható el az adott helyzetben helyes válaszreakciók adása. Annak ellenére, hogy a témában számos, jó minőségű képzési anyag készült[5], a munkahelyek jelentős részében nem történik ilyen oktatás. Az információbiztonsági tudatosságfejlesztési folyamat sikerességének mérése sem kidolgozott, az információbiztonság mérési szempontból nehezen definiálható, számszerűsítésére jelenleg nincs általánosan elfogadott módszertan sem. A legtöbb mérés kérdőíven alapul, a tényszerűségük vitatható, mivel annak során a vizsgált személyek tisztában vannak a mérés tényével, a figyelmük erre irányul, a gyakorlati munka során fellépő zavaró tényezők (pl. az idő hiánya) nincsenek jelen. Ezért felmerül a kétség, mely szerint a kérdőíven alapuló, az információbiztonság állapotát célzó mérések során kapott kép a valós helyzetnél pozitívabb lesz, mivel a válaszok sokkal inkább az elvárthoz fognak közelíteni.

Amennyiben más mérési eljárás keresése a cél, egy lehetséges irány a gyakorlatban lefolytatott teszt, mely során a felhasználók valódi élethelyzetekben adott valódi reakciói mérhetők. Az Eszterházy Károly Egyetem Informatikai Igazgatóságán a fentiekben vázolt célok és elvek alapján mérést végeztünk, melynek végeredménye azt tükrözi, hogy az információbiztonság javításának terén még komoly feladatok állnak előttünk.

1. Módszer

Az egyetem munkatársai változatos informatikai képzettséggel és képességekkel rendelkeznek. Az üzemeltetésben az a benyomásunk, hogy a számítógépes veszélyforrásokat részben ismerik, tisztában vannak az ártalmas programok létével, a ransomware-ek hatásmechanizmusával, de nincsenek mélyebb

4 Robert O' Harrow, Jr. Zero Day The Threat in Cyberspace. New York, Diversion Books, E-Book, 2013.

5 Erdősi Péter Máté, Solymos Ákos. IT biztonság közérthetően. Neumann János Számítógéptudományi Társaság. Hozzáférés: 2018.04.21. http://njszt.hu/sites/default/files/IT_biztonsag_kozerthetoen_V2.pdf

ismereteik pl. a jelszavak használatának szabályairól. Ennek legfőbb oka a rendszerezett szakmai anyagok és az oktatás hiánya. Az információbiztonság tudatosságának tesztelésére létrehozott környezet ezért nem a lándzsás adathalász módszerek mentén épült fel, inkább egy célzott támadás és szándékos zavarkeltés lehetőségének megvalósítása volt a cél. A támadási módszert többen ismertették és alkalmazták[6], egy Excel táblázat ismeretlen forrásból történő letöltése és annak megnyitása volt, mely egy makrovírust is tartalmazhatott volna. A kialakított döntési helyzet tehát egyáltalán nem volt nyilvánvaló a felhasználók számára, de minden esetben tartalmazott olyan elemet, amely az elvárttól eltérő reakciót sugallt.

Egy valódi támadás szimulálásának érdekében semmilyen olyan adatot nem használtunk fel, amelyhez belső információforrásból jutottunk, kizárólag az intézmény publikus forrásait vettük igénybe.

Az Eszterházy Károly Egyetem, hasonlóan a legtöbb magyar egyetemhez, a tájékoztatási feladatainak ellátása érdekében a munkatársainak elérhetőségeit – ideértve a hivatali e-mail címét és telefonszámát – egy webalapú tudakozóban teszi elérhetővé. Ez a felület bárki számára elérhető és pár órás munkával a teljes tartalma kinyerhető.

A tesztet két területre csoportosítottuk. Az általános felhasználók tesztje mellett a rendszer üzemeltetőit is igyekeztünk megtéveszteni, ennek érdekében az alábbi eseteket dolgoztuk ki és hajtottuk végre:

1. Az informatikai személyzet megtévesztése és annak elérése, hogy a rendszerbe új felhasználót vegyenek fel.
2. Excel táblázat letöltését felkínáló e-mail kiküldése minden felhasználó számára, és annak mérése, hogy hányan töltik le ezt.
3. Jelszóellenőrzésre történő felszólítás e-mailben, és annak ellenőrzése, hogy hányan adják meg hozzáférésüket egy hamis weboldalon.
4. Amennyiben az 1-es eset megvalósul, az így létrejött fiktív személy számára egy virtuális szerver létrehozásának elérése az egyetem infrastruktúráján.
5. A szerverrel kapcsolatos megszorítások, tűzfalszabályok fellazításának kísérlete, külső hozzáférési csatornák (portok) megnyitása.

A fentiek mellett további tesztek is rendelkezésre álltak, de a teszt során kialakult helyzet miatt azok végrehajtásától eltekintettünk.

6 Deris Stiawan, Mohd. Yazid Idris, Abdul Hanan Abdullah, Fahad Aljaber, Rahmat Budiarto. Cyber-Attack Penetration Test and Vulnerability Analysis. Hozzáférés: 2018. 07. 01. http://www.online-journals.org/index.php/i-joe/article/view/6407/4243

A tesztelés alapja egy valódinak tűnő domainről beküldött hamis e-mail volt, amelyhez domain név regisztrációjára volt szükség. Az eszterhazy.hu domain nem az egyetem birtokában levő név, de a megtévesztésre kiválóan alkalmas. Emellett egy másik név is bejegyzésre került, amely az egyetem hivatalos domain nevétől csak egyetlen karakterben különbözött, így az szintén nehezen volt felismerhető, ez az *uni-esztehazy.hu* domain volt. A mai magyarországi gyakorlat szerinti regisztrációs folyamat nem tartalmaz olyan elemet, amely az ilyen módon megtévesztő neveket a regisztrációból kizárná.

Egy domain név anonim módon történő regisztrálása nem egyszerű, de végigvihető folyamat, az anonimitást csak a fizetés lebonyolítása nehezíti meg. A korábbi magyar gyakorlattól eltérően a domain nevek ma a bejegyzési kérelem benyújtását követően szinte azonnal használatba vehetők, így alkalmas regisztrátort választva egy valódi támadás a megfelelő előkészítés után szinte azonnal elindítható.
A phishing levelek tömeges küldéséhez kész szoftverek is elérhetők, ehhez még a Darknetet sem kell igénybe venni. A GoPhish kifejezetten jó alap lehet erre, de a távlati célok elérése érdekében esetünkben minden elem saját megvalósításban épült fel.

A levelek küldéséhez egy teljesen jól konfigurált Linux operációs rendszerű szerver készült. Ez a hamis domainhez DNS szervert, a levelek küldéséhez és az esetleges válaszlevelek fogadásához és olvashatóságához SMTP illetve IMAP szervert tartalmazott. A webszerver funkcióját az Apache-PHP páros biztosította, rájuk a jelszóellenőrzést végző szoftver futtatásáért volt szükség. A LetsEncrypt tanúsítványszolgáltatóra alapozva minden szolgáltatást titkosított protokollon, a lehetséges pontokon korrekt tanúsítványokkal ellátva lehetett létrehozni.

A szerver felépítése során teszteket kellett végezni, mivel hiba esetén a megtévesztő levelek nem, vagy hibásan jutottak volna el a felhasználókhoz. Utóbbi esetben a teljes vizsgálat meghiúsulhatott volna, hiszen nyilvánvalóvá vált volna a megtévesztő szándék. A kiküldött leveleknek át kell menniük az intézményi spamszűrési eljáráson, ehhez az egyedileg generált, különböző tartalmú levelek, a tartalmi ellenőrzés[7], a DKIM és SPF rekordok megléte az EKE rendszere esetében elégséges volt.

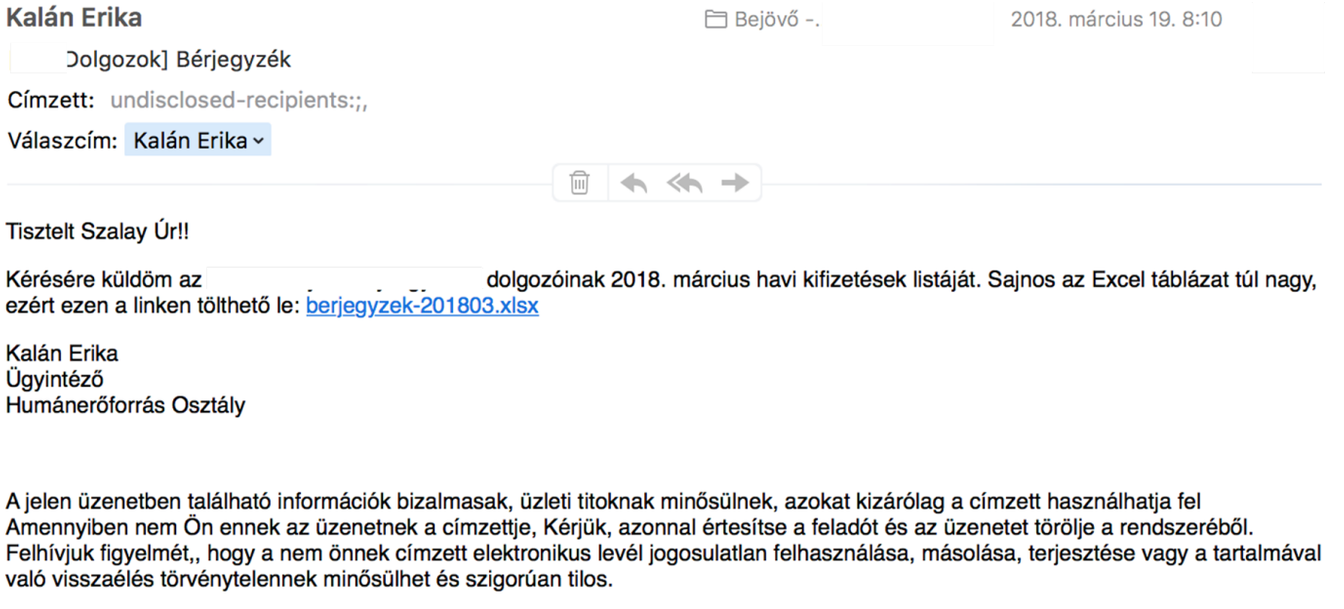
Az első teszt az egyetem Informatikai Igazgatóságán dolgozó informatikus munkatársat célozta. A kiválasztása a forgatókönyv szerint csak nyilvános információk alapján történt, a munkatársak tájékoztatása érdekében ezek elérhetők voltak a megfelelő weblapon. Őt egy hamis, uni-esztehazy.hu domainből küldött e-maillel sikerült rávenni arra, hogy egy nem létező munkatárs számára e-mail címet hozzon létre. Az egyetem weboldalán az informatikai munkatársak elérhetősége is rendelkezésre állt, ezért nem okozott nehézséget a feladatot ellátni képes informatikus munkatárs kiválasztása. A megtévesztésben nagy segítséget nyújtott az, hogy a feladóként feltüntetett egyetemi vezető neve és e-mail címe nyilvános volt, így a küldő személy valósnak tűnt. Emellett a kérést az egyik hosszú hétvégét megelőző nap délutánján, sürgető hangnemben megfogalmazott levél tartalmazta. Az informatikus

7 Egy jó eszköz erre a http://www.mail-checker.com oldal, ami sajnos mára már csak korlátozott számú tesztelést tesz ingyenesen lehetővé.

kolléga igyekezett ellátni a feladatát, ezért eltért a normál ügyintézési folyamattól, és nem tűnt fel számára a megtévesztő (hiányos) domain név sem.

A valós e-mail cím birtokában a következő lépés a szerver adminisztrátorok felé irányult. Egy olyan virtuális szerver létrehozása volt a cél, melyhez a támadó teljes felügyeleti jogkört kap. A levél tartalmában szereplő indoklás szerint a szerver kutatási feladatok ellátására szolgál, és az üzemeltetés ellátására a kutató önállóan is képes. Ezt egy hosszas levelezésből álló huzavona árán, a szakmai kompetencia bizonyítása után hozzávetőleg egy hónap alatt sikerült elérni. A gyanakvás eloszlása után, kis idő elteltével egy másik adminisztrátort célozva a tűzfalszabályok részleges feloldásának kérése is sikerrel járt, így az egyetem belső infrastruktúráján az általános szerverekkel egy hálózatban működő szervert teljes hozzáférés mellett sikerült birtokolni.

A felhasználók tesztjének lebonyolításához az intézményi tudakozóból kigyűjtött nevek és e-mail címek szolgáltak alapul. Mivel az egyetem esetében a munkakörök is elérhetők voltak, ezért az informatikai munkatársakat könnyen ki lehetett szűrni, ők az adathalász leveleket nem kapták meg. A címlista birtokában egy munkanap reggelén, 7:30-kor a már előkészített szerver 1750 levelet küldött szét az intézmény dolgozóinak. A levél címzettje nem az adott dolgozó volt, hanem látszólag az egyetem egyik levelezési listája (az egyetemi levelezési listák egy alkalmas Google keresőkérdéssel pillanatok alatt kideríthetők). A megszólításból egyértelmű volt, hogy a levelet nem a listára szánták, a feladó a Humánerőforrás Osztály nem létező munkatársa volt, a levél szövege egy jogi záradék mellett egy aktuális havi bérlistát tartalmazó Excel fájlra mutató linket tartalmazott.



Kalán Erika Bejövő -. 2018. március 19. 8:10

Dolgozok] Bérjegyzék

Címzett: undisclosed-recipients:;,

Válaszcím: Kalán Erika

Tisztelt Szalay Úr!!

Kérésére küldöm az dolgozóinak 2018. március havi kifizetések listáját. Sajnos az Excel táblázat túl nagy, ezért ezen a linken tölthető le: berjegyzek-201803.xlsx

Kalán Erika
Ügyintéző
Humánerőforrás Osztály

A jelen üzenetben található információk bizalmasak, üzleti titoknak minősülnek, azokat kizárólag a címzett használhatja fel Amennyiben nem Ön ennek az üzenetnek a címzettje, Kérjük, azonnal értesítse a feladót és az üzenetet törölje a rendszeréből. Felhívjuk figyelmét,, hogy a nem önnek címzett elektronikus levél jogosulatlan felhasználása, másolása, terjesztése vagy a tartalmával való visszaélés törvénytelennek minősülhet és szigorúan tilos.

1. ábra A megtévesztő levél szövege

A link valójában minden levél esetében más, az e-mail címmel egyértelmű megfeleltetésben álló paramétert tartalmazott, így minden letöltő személye azonosítható volt. A fájl forrásaként a már előkészített uni-esztehazy.hu domain állt, a táblázat tartalma pedig az intézményi tudakozóból letöltött névsor, valamint egy, az Excel Rand függvényével generált, így minden betöltéskor megváltozó összegeket mutató táblázat volt.

A második tesztlevél kiküldése 10:00-kor indult. Ebben a hamis levélben, mely szintén az uni-esztehazy.hu domainből indult, a felhasználókat az egyik, a tudakozóból kiválasztott hibásan aláírt üzemeltetési vezető a reggeli eseményekre hivatkozva egy jelszóellenőrzési weboldal felkeresésére, illetve a jelszó ellenőrzésére kérte. Az oldal LetsEncrypt tanúsítvánnyal ellátott webszerveren, de a hamis domain név alatt működött, ennek ténye a címsorban jól látható volt.

2. ábra A https://jelszoellenorzes.uni-esztehazy.hu oldal

A jelszó helyességének ellenőrzését egy script végezte, amely a megadott hozzáférési adatokkal bejelentkezett az intézményi IMAP szerverbe, ezzel képes volt eldönteni a munkatárs által megadott adatok érvényességét. Az oldalon használt e-mail címeket és a helyes jelszó megadásának tényét (tehát a jelszót nem) a preparált weboldal szoftvere rögzítette, így biztosítva a későbbi azonosítást és a statisztikák alapadatait.

2. Eredmények

A két teszt végrehajtása a szervezetben olyan zavart okozott, amely következtében a tervezett továbbiak lefolytatása már nem tűnt vállalhatónak. A levelezési rendszerbe vetett bizalom megrendülni látszott és több váratlan esemény merült fel. A nyilvános tudakozóból címlistát generáló program hibájából adódóan pl. néhány munkatárs nem szerepelt a táblázatban, róluk megindult a szóbeszéd, hogy az intézmény vezetése már nem számít a munkájukra.

Súlyos problémát jelentett, hogy az Informatikai Igazgatóság munkatársait az első levél kiküldése után 106 perccel értesítették arról, hogy adatszivárgás történt. Az egyetem szerverüzemeltetői ettől az időponttól képesek lettek volna a megtévesztő levelek eltávolítására a postafiókokból, ez volt az a pillanat, amikor a teszt tényét előttük fel kellett fedni. Egy valódi támadás esetén, egy ransomware aktiválódásával ennyi idő alatt már óriási károk keletkezhettek volna.

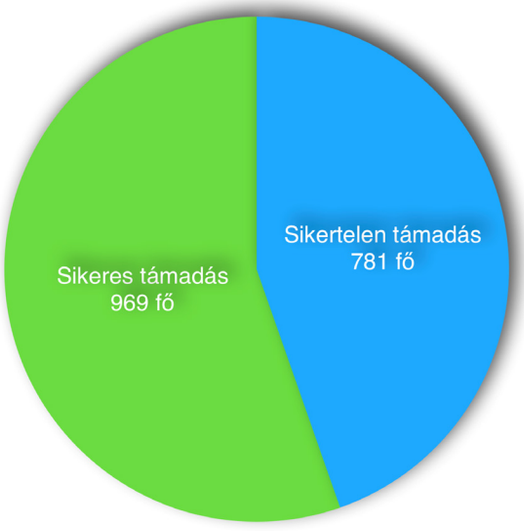
A teszt lefutása ezért eltért az éles helyzetben várhatótól, az üzemeltetés figyelmeztetést adott volna ki, a hamis leveleket törölte volna a postafiókokból és tiltotta volna a jelszóellenőrzést végző űrlap elérését az intézmény hálózatából, ezzel nagyban csökkentette volna a támadó sikerességét. Az a tény, hogy a felhasználók csak jelentős késéssel jelezték az informatikai üzemeltetők számára a célzott tartalmú, hamis levelek beérkezését, a védekezés lehetőségét is nagyban rontotta.

A teljességhez hozzátartozik, hogy sok felhasználó azért nem reagált a levelekre, mert a vizsgált időszakban nem olvasta a levelezését, így megítélésem szerint a valós kép a mért eredménynél valójában rosszabb. Annak ellenére, hogy a teszt összefoglalását kora délután kiküldtük, még egy héttel később is történtek új felhasználói válaszreakciók.

De az elvárt válaszra is számos példa akadt: volt olyan munkatárs, aki már az első levél során felismerte a támadás tényét és a szervezeti egységében minden munkatársát személyesen figyelmeztette, ismertetve a hamis domain felismerésének módját is.

2.1 Táblázat letöltése

Az első levél esetében, mely az Excel táblázat letöltését célozta, 969 letöltést regisztrált a rendszer, ez 532 különböző link mentén történt. Ebből következően a fájlokat többször is letöltötték, illetve a linkeket mások számára továbbküldték.

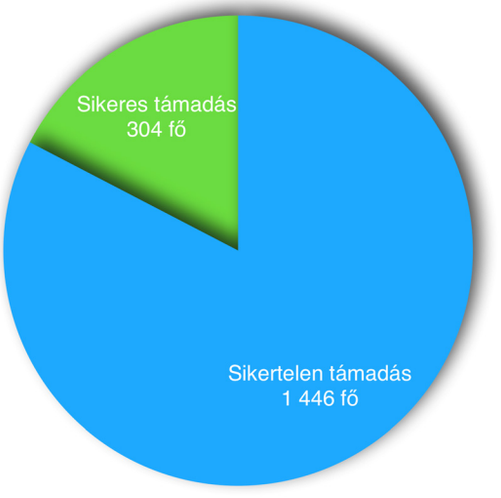


3. ábra Letöltések aránya az adathalász e-mail alapján

A felhasználók szempontjából komoly hiba volt, hogy a többszörös figyelmeztető jelek ellenére a támadó szándéka szerinti reakciót adták. A fizetéseket tartalmazó levél számos ilyet tartalmazott: nem a címzettnek szólt, külső linket tartalmazott, az Excel fájl az egyik kedvelt támadási forma alapja, és sokan a levélben olvasható jogi záradékot is semmibe vették. A fájl letöltése során csak kevesen vették észre, hogy az adatok véletlenszerűek, így hamisak. A figyelmeztető jelek miatt a domain név hiányzó karakterének feltűnése reális elvárás lehetett volna, ami nyilvánvalóvá tette volna, hogy a levél valódi célja a megtévesztés. Sajnos az általánosságban használt levelezőprogram alapértelmezés szerint a feladó e-mail címét nem jelenítette meg, így a hamis domain beavatkozás nélkül nem volt látható. Az ellenőrzéshez további műveleteket kellett volna végezniük, amire a bérlista megismerésének lehetősége mellett nem fordítottak időt.

2.2 Jelszó megadása

A teszt során 1750 felhasználóból 304-en adták meg a jelszavukat, ez 17,3%-os arányt jelent.



4. ábra Jelszavak megadásának aránya az adathalász weboldalon

Az ellenőrzésének kérése a reggeli események fényében reálisnak tűnhetett, bár a weboldal túlságosan kidolgozott volt ahhoz, hogy azt az üzemeltetés a reggeli támadás utáni két órában elkészítse. Az oldal kérése szintén gyanakvásra kellett volna, hogy okot adjon, a címsorban pedig egyértelműen ellenőrizhető volt a hamis domain név.

2.3 Az üzemeltetés

Az üzemeltetés részéről már komolyabb hibaként értékelhető a felhasználó felvétele a HR Osztály visszaigazolása nélkül, csupán egy e-mail alapján. A vélt vészhelyzet miatt be nem tartott eljárásrend kiindulópontja lehet egy támadó bejutásának az intézmény informatikai rendszerébe. Egyetemünk gyakorlatában az e-mail cím nemcsak levelezésre szolgál, több alrendszerünk hozzáférésének alapja az e-mail cím és jelszó páros, ennek birtokában, a nyilvános technikai útmutatók alapján így további szolgáltatások is igénybe vehetők. A szerverigénylés és annak egyedi adminisztrációja, bár nem gyakori, mégsem teljesen szokatlan eset egy egyetem életében. A kockázatokat nagyban növeli a szervezet nagy méretéből következően az a tény, hogy a munkatársak személyesen nem ismerik egymást.

2.4 Egyéb megállapítások

A teszt utolsó lépése egy összefoglaló üzenet küldése volt, amelyet minden, abban részt vevő munkatárs megkapott. Ebben tájékoztatást kaptak a teszt tényéről és annak rövid, számszerű eredményéről. Az egyéni reakciókról semmilyen visszajelzést nem adtunk és a teszt során nem is használtuk fel ezeket.

A munkatársak válaszai a két szélsőség köré csoportosultak. Azok esetében, akiknél a megtévesztő levelek elérték a céljukat, a tanulságok levonása leginkább a nem oktatói munkakörben dolgozók részéről volt érzékelhető. Mivel az intézmény szempontjából kritikus adatok (tanulmányi rendszer, gazdasági rendszer, iktatás) jó részét ők kezelik, és a teszt rávilágított arra, hogy a hibás reakciójuk a szervezetre nézve komolyabb következményekkel járhat, így hosszabb távon ők a teszt nyertesei lettek.

Az oktatói és kutatói kör sokkal rosszabbul élte meg, hogy a teszt során nem az elvárt reakciót adták, bár ezzel személyesen nem szembesültek. A freudi énvédő mechanizmusok tiszta példáit hozták, volt, aki személyes támadásként tekintett erre, és az intézmény felsővezetői elé vitte a kérdést.

Jelen cikk írásakor a teszt végrehajtása óta négy hónap telt el. Ezalatt számos visszajelzést kaptunk adathalász levelek érkezéséről, melyek közt látszólag az egyetem rektora által írt, célzott támadás is volt. Gyakran teszik fel a kérdést az üzemeltetés felé, hogy az adott levél egy újabb teszt eleme-e. Emellett az üzemeltetés is sokkal alaposabban figyeli a saját levelezését, hogy nehogy áldozatul essen egy újabb tesznek, esetleg az informatikai tanszékek revansának.

Mindkét kör esetében pozitív elem volt annak demonstrálása, hogy az e-mail nem jelent hiteles forrást, és hogy a hamisításuk nem bonyolult feladat.

2.5 Jogszerűség

Több forrásból is felmerült a jogszerűség kérdése. Ezen a területen alapvető szempont, hogy egy ilyen teszt csak abban az esetben törvényes, amennyiben az az intézmény felsővezetői által támogatott és engedélyezett tevékenység. A GDPR életbe lépésével fokozott mértékben merül fel a dolgozók nevének, beosztásának és e-mail címének felhasználásával kapcsolatos jogszerűség kérdése, hiszen személyes adatok tömeges felhasználása történik[8]. Ennek biztonsági ellenőrzési folyamatok során történő felhasználhatóságát célszerű a munkaköri leírásokban illetve az intézményi IBSZ-ben rögzíteni. A leginkább kritizált pont a hamis béradatokat tartalmazó Excel táblázat készítése és terjesztése volt. Jogi szakember véleménye alapján ez nem törvénytelen, de a hamis adatok előállítását és terjesztését több forrás sem tartotta kívánatos tevékenységnek.

3. Konklúzió

Az első és legnagyobb problémát az jelentheti, ha az egyetemek, amelyek nem tartoznak a 2013. évi L. törvény hatálya alá, nem fordítanak figyelmet az információbiztonság kérdéseire. Tapasztalatom szerint ez egy részük esetén nem áll fenn, az több egyetem IBSZ-ében jól érzékelhető az említett törvény mellett a 41/2015-ös BM szellemének alkalmazása. Az egyetemeknek nem kell rendelkezniük információbiztonsági vezetővel, ezt a feladatkört formálisan az informatikai vezetők látják el, így az információbiztonság terén nincs kontrolljuk. (Az L. törvény hatálya alá tartozó szervezetek esetében felmerülne az összeférhetetlenség kérdése.) Célszerű ezeket a törvényeket illetve az alapjukként szolgáló ajánlásokat, szabványokat a felsőoktatási intézmények üzemeltetésért felelős szakembereinek megismerni, illetve a működési folyamataikban felhasználni.

3.1 Adminisztratív intézkedések

Az informatikai rendszerek és a szolgáltatási kör módosítása elengedhetetlen feladat. Biztonsági szempontból komoly hiba, hogy a munkatársak e-mail címei, beosztásai és egyéb elérhetőségi adatai nyilvánosan, nagy tömegben elérhetők. Érdemes ezt a szolgáltatást úgy átalakítani, hogy csak néhány, a külkapcsolat szempontjából releváns elérhetőségi adat legyen nyilvánosan hozzáférhető, a teljes belső telefonkönyv csak az arra feljogosítottak számára, a teljes letölthetőséget minél inkább megnehezítve álljon rendelkezésre.

A helyzet általánosságának ellenőrzésére 32 magyarországi egyetem weblapjait tekintettem át hasonló lehetőségek után kutatva. Jelen cikk írásakor 25 egyetem valamilyen formában szintén elérhetővé tette a munkatársai elérhetőségét, így munkatársaik e-mail címei begyűjthetők, és az EKE-n lefolytatott vizsgálat esetükben megismételhetőnek tűnik.

8 Eur-Lex. Hozzáférés: 2018. 07. 05. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679

3.2 Műszaki intézkedések

Az adathalász levelekben használt, az eredetire hasonlító és így megtévesztő domain nevek kiszűrésére több, az egyetemen használt SMTP szerver is lehetőséget ad: az intézmény által birtokolt domain nevek és a feladó domainje nagyfokú egyezése esetén a levél tárgyába beszúrt figyelmeztető üzenet direkt figyelmeztetést nyújthat a címzettnek arról, hogy valószínűleg megtévesztő tartalommal van dolga. Érdemes megfontolni a levelezésben az elektronikus aláírás bevezetését minden dolgozó számára.

Az ismert megtévesztő domain nevek kiszűrése több ezer munkaállomás esetében már nehezebb feladat, a US-CERT ajánlásában szereplő TAXII™–STIX™–CybOX™ hármas de facto szabványt jelenthet a megoldására[9], ha a kérdést nem lehet a központi szervereken megoldani.

3.3 Oktatás

Az oktatási anyagok elkészítése és az oktatási folyamat megvalósítása minden munkatárs számára kötelező kell, hogy legyen. Jelen sorok írásakor az EKE oktatási anyaga részleges készültségben van, egy távoktatási rendszerre alapozva tervezzük a tananyag közzétételét és a tesztek elvégzését. A tananyagot időről időre aktualizálni kell, ezzel biztosítva a megjelent újabb veszélyforrások megismertetését.

Az oktatási anyagok célközönsége elsősorban a felhasználók köre, az üzemeltetést végzők számára az egyes rendszerek működtetésének szabályainak aktualizálása, az abban foglaltak betartása illetve az IBSZ rendszeres frissítése az elsődleges cél.

Az információbiztonsági teszt szoftverének továbbfejlesztése során tervezem annak automatizálását úgy, hogy kiterjesztett tesztesetekkel minden új belépő munkatárs esetében automatikusan lefusson, és a nem elvárt reakciókról jelentést adjon. Emellett ritkább tesztelési periódusidőkkel, de kiterjesztett tesztesetekkel el kell látnia a folyamatos tesztelést is a teljes foglalkoztatotti körre kiterjedően. Meggyőződésem, hogy a megfelelő visszacsatolás mellett ezzel a módszerrel az informatikai biztonságra fordított figyelem magasabb szintre emelhető úgy, hogy a szervezet „sokkolása”, mely jelen vizsgálat nem várt következménye volt, elkerülhető legyen.

Az így kialakított rendszer mérési adatokat szolgáltathat majd, amely biztosíthatja a szervezet információbiztonsági szintjének számszerűsítését is.

9 United States Computer Emergency Readiness Team. Hozzáférés: 2018. 07. 05. https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity