How did Social Engineering change 21st century cybersecurity?

Hogyan változtatta meg a XXI-ik századi kibervédelmet a Social Engineering?[1]

KRASNYÁNSZKI Brúnó[2]

Abstract

My goal with this research is to find the non-informatic attack vectors with which the today's information security experts has the need to face. According to the hypothesis that established before the research, nowadays information security experts don't take appropriate actions to prevent non informatic threats. Due to this reason the non-informatic security infrastructures haven't been established. During my research my next goal was to inspect and compare the differences between the public sector and the market sector. On the top of that I would like to give good practices to SMEs for whom it has now become necessary to deal with cyber security. For my primer research I tried to fill out surveys with IT head of departments and after that I made deep interviews with IT leaders, auditors, cybersecurity researchers and university professors. As my secondary research, I had analysed the available literature!

Keywords

Social Engineering, Information Security, Cyber Security, Security Awareness

Absztrakt

Kutatásom célja, felmérni milyen nem csak informatikai támadásokkal kell szembenéznie napjaink információbiztonsági szakembereinek.

Kutatásom előtt felállított hipotéziseim szerint a jelenlegi informatikai biztonsági szakértők nem foglalkoznak megfelelően a nem informatikai irányultságú támadásokkal és ennek köszönhetően nem épültek ki megfelelő nem informatikai védelmi megoldások sem. Kutatásom során célom továbbá összehasonlítani az állami szektor intézményeit a piaci intézményekkel és jó gyakorlatokat javaslatként megfogalmazni az olyan KKV-k számára, akiknek most vált szükségessé a kiberbiztonsággal foglalkozni. Primer kutatásként kérdőíveket töltettem ki cégek informatikai osztályvezetőivel és ezek után mélyinterjúkat készítettem felső vezetőkkel, auditorokkal, kiberbiztonsági kutatókkal és egyetemi professzorokkal. Szekunder kutatásként pedig a fennálló szakirodalmat elemeztem!

Kulcsszavak

Social Engineering, információbiztonság, kiberbiztonság, biztonságtudatosság

[1] A tanulmány kutatási hátterének alapját a Kutató Dákok Mozgalmában végzett kutatásom adta, amivel 2022-ben a Tudományos Diákkörök XXII. Kárpát-medencei Konferenciáján Harmadik, a XX. KutDiák Tudományos Esszépályázaton második helyezést értem el Műszaki és reáltudományi szekcióban.

[2] brunokrasnyanszki@gmail.com | ORCID: 0000-0002-5672-4919 | university student, Óbuda University John Von Neumann Faculty of Informatics | egyetemi hallgató, Óbudai Egyetem Neumann János Informatika Kar

BEVEZETÉS

Motiváció és a kutatásom felépítése

Mindig is érdekeltek azok a területek, amivel kevesebben foglalkoznak. Nem volt ez másként a biztonsággal sem. Biztonságtudatos felhasználóként láttam magam körül, hogy minden második ismerősömet valamilyen kibertámadás érte. Tízből kettő vette észre ennek következményeit és csupán tízből 1 volt az, akinek az informatikai védelmi megoldásai megakadályozták ezt.

Testközelből láttam amikor 2 multinacionális céget, ahol barátaim gyakornokként dolgoznak teljesen működésképtelenné tett a WannaCry és a NOPetya és a családom majdnem minden tagját is érte már valamilyen támadás. Célom lenne felhívni a vállalatok, állami intézmények és felhasználók figyelmét arra, hogy a XXI-ik században már nem csak informatikai támadás érhet minket és ez ellen szükséges védekeznünk!

Célom továbbá bemutatni a védekezés lehetséges formáit melyben górcső alá veszem az informatikai és nem informatikai védelmi metódusokat összehasonlítva ezek hatékonyságát, integrálhatóságát és költségeit, bemutatva ezeket az opciókat az állami szférára és a piaci cégekre.

Célom továbbá bemutatni a közepesen reprezentatív kutatásomat, melyben azt vizsgáltam, hogy mennyire foglalkozik az állami szektor és a piaci cégek a biztonsági megoldásokkal és a kiberbiztonsági tudatosítással. Primer kutatásként kérdőíveket töltettem ki cégek informatikai osztályvezetőivel és ezek után mély interjúkat készítettem felső vezetőkkel, auditorokkal, kiberbiztonsági kutatókkal és egyetemi professzorokkal. Szekunder kutatásomként pedig a fenn álló szakirodalmat elemeztem.

Ez után szeretném megmutatni azt is, hogy a humán faktor sérülékenysége fuzzy logika segítségével matematikailag mérhető, de nem csak a humán faktor sérülékenysége, hanem a szervezeti biztonságtudatossági kultúra és a biztonságtudatossági oktatások hatékonysága is.

Végül javaslatokat fogalmazok meg arra vonatkozóan mikortól érdemes egy vállalatnál foglalkozni a kiberbiztonsággal és hogy a konvencionális informatikai megoldásokkal vagy inkább az un-konvencionális védelmi kontrollokkal foglalkozzon.

Hipotézis

A hipotézisem az volt, hogy a jelenlegi informatikai biztonsági szakértők nem foglalkoznak megfelelően a nem informatikai jellegű támadásokkal (például a Social Engineeringel) és mind az állami intézmények, mind a piaci cégek estében ez egy komoly probléma, aminek a leghatékonyabb kezelése az lenne, ha megpróbálnánk a dolgozóinkat tudatosítani és a védelmi kiadásokat a hagyományos vírusirtó[3] + tűzfal helyett biztonságtudato-

[3] Hagyományos vírusirtó alatt a reaktív védelmet nyújtó vírusírtókat értem, melyek vírusdefiníciós adatbázis alapján találják meg a kártékony kódokat rendszereinken. A mesterséges intelligencia alapú úgynevezett heurisztikus vírusvédelmet nyújtó szolgáltatást azért nem értem alatta, mivel ez általában nem a vírusírtó szoftver része, hanem egy komplex informatikai biztonsági megoldásnak amely általában a következő elemeket tartalmazza: Adatbázis alapú vírus védelem, viselkedés alapú vírusvédelem, valós idejű védelem (heurisztikus védelem ami az operációs rendszer kritikus részein történő változásokat kiséri figyelemmel), dinamikus tűzfal szolgáltatás, szolgáltatás/applikáció engedély kontroll.

sító képzésekbe, adminisztratív és logikai preventív védelmi kontrollokra próbálnánk fordítani a detektív védelmi mechanizmust tartalmazó vírusirtók helyett, mivel ezeket egy belső, zárt nagyvállalati környezetben nem gondolom hatékonynak a nem tisztán informatikai támadásokkal szemben. Ezen hipotézisemet arra alapozom, hogy a támadások nem csak informatikai eredetűek lehetnek. Ezáltal a vírusírtók egy fizikai térben vagy akár telefonhíváson keresztül történő támadáskor semmilyen védelmet nem tudnak nyújtani.

Ezzel szemben a biztonságtudatosító képzésekkel elérhető, hogy a dolgozók felkészültek legyenek a nem nulla kattintás-os sérülékenységekkel[4] szemben szinte passzív kivédésére és ezen felül a nem informatikai támadásokkal szemben is felkészültek lesznek. További fontos nemzeti kiberbiztonsági szempont az is, hogy a munkahelyen tanult tudást és tapasztalatot haza is vihetik. Ezáltal nem csak a munkahelyük lesz biztonságosabb, hanem a dolgozók családja is biztonságtudatosabb lesz!

MI IS A SOCIAL ENGINEERING?

A fő nem informatikai támadási lehetőség a Social Engineering[5]. „A Social Engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a Social Engineer tényleg az, akinek mondja magát. Ennek eredményeként a Social Engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni” [2]. A Social Engineering (továbbiakban SE) a leggyakoribb nem informatikán alapuló támadási forma, ahol az emberen, a leggyengébb láncszemen van a hangsúly. Ez azért fontos, mert a legtöbb cég életében már evidensé vált, hogy amennyiben nem költ informatikai védelmi megoldásokra akkor a teljes internetet támadó automata bot net-ek könnyedén átveszik a cégük teljes informatikai irányítási rendszerét, mely nélkül a legtöbb cég nem, vagy akiknek van erre alkalmas BCP-je[6] csökkentett üzemmódban képes csak működni, termelni. De azokkal a támadásokkal, amiket a kiberbiztonsági szakemberek nem észlelnek, a cég vezetésnek pedig rövid távon fel sem tűnik nagyon nehéz foglalkozni. De hogyan is érzékelhetne az a biztonsági elemző egy támadást, aki csak a kibertérből[7] érkező támadásokat vizsgálja? A kérdés egyszerű ahogy a válasz is. Sehogy! Amire a cégek többségének sikerült 2022-re eljutnia az az, hogy megértsék a fizikai és az informatikai biztonság fogalmát (Informatikai biztonság alatt minden olyan védelmi megoldást értünk, ami informatikai eszközökön fut és a fizikai térbe semmilyen módon nem terjed ki. Pl.: vírusirtó és tűzfal informatikai biztonsági megoldás, míg a dolgozóink munkaidő monitorozása adminisztratív biztonsági kontroll), de az olyan veszélyek, amik nem tartoznak bele a fent említett kategóriákba sajnos nem kerülnek detektálásra sem. Sajnos, mivel ahány szakember, annyi definíció. Így a későbbiek folyamán én Krasznay Csaba definícióját fogom használni, mivel véleményem szerint az Ő összefoglalása nyújtja

[4] Nulla kattintás-os sérülékenység alatt minden olyan sérülékenységet értek melynek kihasználásához nem kell humán interakciót igénybe venni. Ezeket a sérülékenységeket nyilvános felfedezésükig nulladik napi sérülékenységnek is nevezzük.[1]

[5] A magyar szakzsargonban nem terjedt még el megfelelő fordítás. Ezért az angol kifejezést fogom használni.

[6] (Business Continuity Plan – üzletmenet folytonosság) [3]

[7] „A kibertér egy számítógépekkel és kommunikációs kapcsolatokkal kialakított, globális hálózatra alapozott, többdimenziós, mesterségesen létrehozott virtuális valóság.” [4]

a legszélesebb körű definíciót. „Az információbiztonság az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és kockázatokkal arányos”. [5]
Míg ezzel szemben „a kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.” [5]
Miért fontos a humán tényező és miért kell vele foglalkoznunk?
Már akkor a humán tényező volt a leggyengébb tényező a kiberbiztonsági képletünkben amikor elkezdtünk jelszavakat használni. Ezeknek bonyolultnak kell lennie és az sem árt, ha az ember megjegyzi őket. Ma már viszont, ha felhívunk egy titkárnőt vagy egy középvezetőt a rendszergazda nevében, hogy behatolás történt és szükségünk lenne a jelszavára annak érdekében, hogy megakadályozzuk az egész céget érintő kibertámadást gondolkodás nélkül hangosan lediktálják!
Ezekre a szituációkra a dolgozókat fel lehet (és az Információ Biztonsági Törvény [továbbiakban IBTV] hatálya alá eső intézményeknek kötelező is!) készíteni biztonságtudatosító képzésekkel.

Ezen képzések elsődleges célja, hogy a dolgozók vegyék észre, ha valami nem stimmel az adott szituációban és amennyiben ezt észrevették kérdéseket tegyenek fel annak megállapítására, hogy ez jelenthet-e kockázatot vagy sem. Az ilyen képzések azért is fontosak, mert az olyan jellegű támadásokat, ahol a dolgozókat felhívják a saját telefonjukon és így próbálják rávenni őket különböző SE technikákkal hozzáférések vagy információk átadására jelenleg nem kivédhető semmilyen műszaki és informatikai megoldással! Ezért az egyetlen megoldás az, ha ilyen képzésekkel felkészítjük a dolgozóinkat, hogy gyanakodjanak, amikor olyat kérnek tőlük, amit a szervezet szabálya szerint tilos vagy valamilyen csalásra adhat okot.

A SOCIAL ENGINEERING TÁMADÁSOK FAJTÁI

Ebben a szekcióban szeretném röviden bemutatni milyen SE támadási formák léteznek, azért, hogy az olvasó jobban el tudja képzelni mi is ez valójában. Ehhez Tóth Tamás az egyes Social Engineering módszerek elhatárolása és rendszerezése című publikációját és Hadnagy Cristopher (2011): Social Engineering The Art of Human Hacking című könyvében leírt példákat fogom bemutatni a leggyakoribb SE támadások típusait és rendszerezéseit! A SE támadásokat két típusra oszthatjuk. A tisztán humán módszerrel elkövetett SE támadások, illetve az IT-alapú módszerek. Amennyiben a támadás hatékonyságát növelni szeretnénk, kombinálhatjuk is a két típust. A két típus alkalmazásának célja a támadó legendájának megerősítése, így az áldozat egy hamis biztonságérzetet kaphat, a „másik forrásból” ezáltál nőni fog a bizalom a támadó felé. [6, p. 87]

Humán alapú támadások típusai:

1. Idegen identitás felhasználása

Mint a nevéből is kiderül valaki másnak a személyazonosságát használja fel a támadó arra, hogy információhoz jusson egy természetes személy megtestesítésével. Nagy cégek esetében felső vezetőként mutatkozik be egy alkalmazottnak akkor nagy rá az esély, hogy az alkalmazott jóhiszeműen megteszi, amit a „felsővezetője" kér tőle. A személyazonosság lopás egy másik formája az úgynevezett „tombstone theft" – sírkőlopás amikor egy nemrég eltűnt vagy elhunyt ember személyazonosságát „felhasználva" rendelkezik az elhunyt jogosultságaival. Ezért használhatja a közösségi felületeit, a bankkártyáját, de akár még a munkahelyi belépőjét is! Amivel jogosulatlanul visszaélve nem csak egy cég üzletmenet folytonosságát veszélyezteti, hanem adott esetben egy kritikus infrastruktúrát is megbéníthat, mivel az adatait nem törlik a rendszerből közvetlen a halála után.
Az is előfordulhat, hogy egy fiktív személy legendáját („Előre kidolgozott, a valóság elemire épülő, nagyrészt ellenőrizhető, dokumentumokkal is alátámasztott fedőtörténet, magyarázat…") [7] alkalmazzák [6, p. 89] a támadásra, mely módszer jól alkalmazható eseti jelleggel amikor rögtönözni kell, de akár hosszú távon is, amikor tetszőleges karakterre van szüksége a támadónak. Ennek hatékony módja lehet, hogyha valaki auditornak adja ki magát, ezáltal beleláthat minden kényes adatba. További nagyon hatékony módszer amikor valaki rendőrtisztnek adja ki magát és egy folyamatban lévő nyomozásban kér segítséget, gyakran olyan emberektől, akik a célponttal rossz kapcsolatot ápolnak. A rendőri legendát erősítheti, ha rendelkezik hamis okmányokkal, egyenruhával, kényszerítő eszközökkel és akár többen is vannak. További kreatív módszer lehet az objektum feltérképezésére amikor karácsony tájékán valaki mikulásjelmezben csokoládét, cukrot osztogatva jelenik meg. Ennek alkalmával körbe „kell" mennie az egész épületben, mely során dokumentálhat és megfigyelhet mindent. [6, p. 88] Ugyanakkor egy egyszerű ételfutár vagy kézbesítő is elég lehet ahhoz, hogy valaki bejusson egy őrzött épületbe. De bármilyen formát is ölt a támadó a legfontosabb teendője az előzetes információgyűjtés, amit ma leggyakrabban nyílt forrású hírszerzéssel (továbbiakban: OSINT – Open Source Intelligence) [8]. Ennek segítségével minden nyilvánosan elérhető (közösségi oldalak [9], munkahely weboldala stb..) adatot összegyűjt annak érdekében, hogy az előzetes információt kihasználva előnyre tegyen szert bizonyos szituációkban.

2. A második gyakori módszer a segítség kérése. Ebben az esetben az emberek jóhiszeműségét és segítőkészségét használja ki a támadó. Ilyen támadási formák lehetnek az ügyfélszolgálat kihasználása. Általában vezetőt megszemélyesítve „felejtik el jelszavukat" amire nagyon gyorsan szükségük van egy határidős feladathoz, mivel ezen a cég pénzügyi helyzete múlik és az sem lenne jó, ha amiatt, hogy nem teljesíti a nagyon sürgős feladatát és a cégét rossz pénzügyi helyzetbe sodorja emiatt le kellene építeni az ügyfélszolgálatot. De működőképes forgatókönyv lehet az is amikor egy „rendszerhiba" miatt egy lehetetlen munkaidő utáni pillanatban hívják fel a dolgozót, hogy remek lenne, amennyiben be tudna fáradni és bejelentkezni egy adatmentésre, mert különben holnapra elvesznek az adatai. A dolgozó, aki nem tud bemenni megkéri, hogy találjanak ki valami megoldást erre, de a „rendszergazda" azt mondja, hogy ez csak akkor lenne lehetséges, ha megadná a jelszavát, ami pedig szigorúan tilos, de a dolgozó csak, hogy ne kelljen bemennie szívesen megadja a jelszavát, ezzel céges szabályzatot szegve [6, pp. 89-90]. Támadási forma lehet még az úgynevezett harmadik fél felhatalmazása, ahol vezetőre hivatkozva kikapcsoltatja a biztonságtechnikai eszközöket, hogy a „szerelők" hozzáférjenek a rendszerhez [6, p. 91].

További támadási módszer az úgynevezett piggybacking (más jogosultságának kihasználása), célja bejutni egy objektumba más személyazonosságának felhasználásával. Például otthon hagyta a belépőkártyáját ezért megkéri az őrszemélyzetet, hogy engedjék be őt [6, p. 91].
Ehhez hasonló módszer az úgynevezett „tailgating" [6, p. 92] – azaz magyarul a szoros követés. Biztonsági intézkedések hiányosak, mivel az alkalmazottak közlekedhetnek csoportosan, a támadó is „csatlakozhat egy csoporthoz". Az utolsó ezen kategóriába tartozó támadási forma a hamis bizalomkeltés. Hamis bizalomkeltés során nem feltétlenül kell más személyazonosságot felvenni. A cél az, hogy pozitív vélemény alakuljon ki róla. Remek technika lehet, ha egy ellenkező nemű dekoratívan öltözött nő vagy férfi leköti az ellenkező nemű őrt/alkalmazottat míg társai bejutnak az objektumba.

3. A következő nagyobb támadási kategória a segítség nyújtás [6, p. 92] módszere, melynek során egy mesterségesen előidézett szituációt alakít ki a támadó. Ez a szituáció úgy van kialakítva, hogy csak a támadó tudjon segíteni. Ez azért hatékony, mert legtöbbször az áldozat keresi fel támadót és ennek okán teljesen más függési lánc alakul ki, amit a támadó ki tud használni.

4. Egy érdekes módszer a fordított Social Engineering [6, p. 93] ahol el kell hitetni a célponttal, hogy egy áldozat. Erre egy tökéletes konspirált megoldás lehet egy telefonhívás, ahol a támadó egy banki alkalmazottnak kiadva magát felhívja, hogy gyanús pénzmozgást észleltek vagy túllépte a hitelkeretét és 2 napja van rendezni különben a bank zárolja a számláját. Ettől az áldozat megijed és bármit hajlandó lenne megtenni, hogy megoldódjon a probléma. A banki ügyintéző felajánlhatja, hogy újra ellenőrzi vagy visszaélést jelent be, amennyiben hitelt érdemlően igazolja magát. A támadó így megszerezhet minden adatot, amit személyazonosság lopáshoz. De akár nagy segítség lehet egy informatikai probléma a nem ismert jelszó beállításában is, mivel rengetegen adják meg vagy építik a születésnapjuk vagy tajszámuk köré a jelszavukat.

5. Ennek a technikának a fejlettebb hosszú távú módja a VALAMIT VALAMIÉRT MÓDSZER [6, p. 93], ahol egy hosszú bizalmas kapcsolatra alapoz a támadó a biztos siker érdekében. Ekkor a támadó küld egy kártékony kódot tartalmazó emailt [10] [11]. A támadást követően az áldozat rögtön a támadóhoz rohan „javításért". A támadó így nem csak a felhasználónév/jelszó párosokat szerezheti meg, hanem minden adatot a laptopról! Illetve viszonzást is várhat ezért cserébe, amit a későbbiekben ki fog tudni használni. Azzal a jócselekedettel, hogy megoldotta a számítógépes „problémáját" még tovább fokozza a legendáját, mint kiváló szakember képét.

6. Két nagyon hasonló támadás a shoulder surfing [6, p. 94] (váll fölött átnézés tükörfordítás szerint, viszont valójában a képernyő jogosulatlan megtekintését jelenti) és a dumpster diving [6, p. 94] (az információ felkutatása a hulladékban). Első esetben a célpont mögött, hogy rálássunk a képernyőjére (kamera is elhelyezhető). Míg a másik esetben elég átkutatni a céges szemetet, ami tartalmazhat kényes adatokat is, de abban az esetben sem jobb a hely-

zet amikor az audit előtt gyorsan kidobott jelszófecnit a kukába való kidobással „semmisítjük meg". Persze gondolhatnánk, hogy „kinek van kedve a szemetemben turkálni???", de „van az a pénz…" (jelen esetben információ)!

IT alapú támadások típusai

A másik nagy csoport az IT alapú támadások [6, p. 94], melynek előnye, hogy nem kell személyesen ellátogatni a helyszínre. Emiatt a támadó személyazonossága is rejtve marad. A kiberteret kihasználva csak annyit kell elhitetni a célponttal, hogy a rendszer, amivel kommunikál valós. Ennek köszönhetően nagyon kevésszer veszik észre azonnal, hogy támadás áldozativá váltak!
Egyik ilyen támadási forma az álweboldalak készítése [6, p.94], sokszor nem is az számít, hogy kik a célpontok, hanem hogy mennyien vannak. Ezek a weboldalak valamilyen szolgáltatást vagy terméket hirdetnek meg, ehhez viszont a felhasználónak regisztrálnia kell! Ezzel a regisztrációval viszont olyan adatokat kényszerül megadni, amivel a célpontunk sebezhetővé válik. Email cím és jelszó mindenhol kötelező, viszont abba kevesen gondolnak bele, hogy ma átlagosan 50-200 helyre vagyunk beregisztrálva ugyanazzal az email/jelszó párossal.

Az egyik, hanem a leghatékonyabb és legflexibilisebb módszer az adathalászat [6, p. 95]. Ennél lesarkítva nem kell mást csinálnunk csak lemásolni egy weboldalt, ahol található bejelentkező panel. Erre az álweboldalra kell eljuttatni a célpontot és megvárni ameddig jóhiszeműen bejelentkezik. Ezzel lényegében bármilyen adatot megszerezhetünk a felhasználótól. Leggyakoribb közösségi oldalak vagy email fiókok esetén mivel ezekbe gyakran kell belépnünk, de az általam végzett kísérletek alapján remekül hasznosítható az egyébként nehezen törhető WPA2[8] -es Wifi jelszavak megszerzésére is. Ennek a támadásnak az a sajátossága, hogy rá kell vennünk egy felhasználót, hogy újra beírja a wifi jelszavát, csak most a mi rogue access pointunk [9] által létrehozott hálózatba.

De nézzük is meg az általános támadás fajtáit:
1. Phising (email alapú adathalász módszer) [6, p. 95]
Ennek a módszernek a segítségével egy hamisított emailt küld a támadó az áldozatnak egy olyan indokkal, hogy sürgősen változtasson jelszót, mert a céget támadás érte, vagy egyszerűen csak tartozása van, amiben egy hivatkozás található egy olyan weboldalra (pl.: bankok, közösségi oldalak, kormányzat által kezelt létfontosságú oldalak például ügyfélkapu) ahol a bejelentkezési panel valójában a támadónak továbbítja az adatokat. Amennyiben nem „körlevélként" kiküldjük százezreknek, hanem csak egy vagy pár kiválasztott személyt támadunk, ahol fontos, hogy ki a célszemély úgy ez a támadási forma részletes felderítést igényel a célpontokról, amit általában OSINT segítségével valósítanak meg és így állítják össze az emailt is, ott ezt a támadási formát spear fishing-nek hívják, mivel csak konkrét célpontokat „akarunk kifogni".

[8] WPA2 (Wi-Fi Protected Access – Wi-Fi védett hozzáférés): A vezeték nélküli kapcsolat titkosítására szolgáló technológia és szabvány
[9] Gonosz hozzáférési pont – Gyakran használják az olyan eszközök elnevezésére, amelyeket a támadó úgy állít be, mint ha valódi hozzáférési pont lenne.

2. Whailing (vezető IT-eszközöket célzó támadás)
Ez a phising vagy spear phising egy olyan formája, ahol kifejezetten az IT vezetőket, magas állami tisztviselőket és egyéb magas rangú, befolyásos embereket céloz meg a támadó.

3. Smishing (SMS alapú adathalászat) [6, p. 98]
Az SMS alapó támadási módszerrel lehetőségünk van nagyobb bizalmat kialakítani, mivel nem közvetlen SMS-ben várunk el cselekedeteket az áldozattól, hanem hogy egy életszerű példát hozzak az áldozat kap egy SMS-t miszerint zárolták a bankszámláját gyanús pénzmozgás miatt. Leírják, hogy bemehet egy bankfiókba vagy felhívhatja az „ügyfélszolgálat" telefonszámát (péntek délután az utóbbit fogja választani). Ekkor az „ügyfélszolgálat" egy készséges adategyeztetés után sűrűn elnézést kér a probléma miatt és feloldja a célszemély számláját.

4. További SE támadás lehet még egy trójai program [6, p. 103] vagy dokumentum, ami ugyan egy hasznos és jóindulatú programnak adja ki magát, de valójában kártékony kódot tartalmaz. Nem kell akkor sem megnyugodni, hogyha „mi sosem töltünk le az internetről semmit", mert elég nagy valószínűséggel nyitottunk meg olyan Word dokumentumot vagy Excel táblát, amit a kollégánktól kaptunk és esetenként még makró is volt benne. Ez ugyan olyan kockázat, mint az internetről letöltött programok. Sosem tudhatjuk, hogy valójában ki küldte az az emailt, amit a főnökünk írt alá!

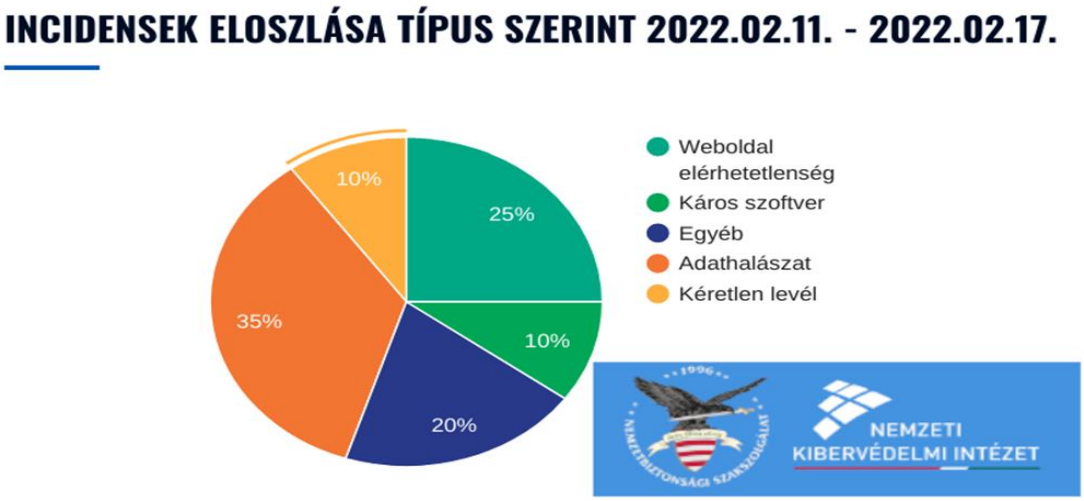
5. Baiting – adathordozó szétszórása [6, p. 104]
Az adathalászat után talán a legnagyobb hatékonysággal végrehajtható támadási forma a baiting során adathordozókat (régebben CD-t, ma már inkább pendrive-okat) hagyunk szándékosan a célobjektum közelében, vagy amennyiben fizikai biztonságot nem implementáltak a célobjektumban akár valamilyen ürügy folyamán be is mehetünk. Remek példa lehet erre amikor egy IT osztályvezetőt megkér egy kedves diák, hogy legyen a konzulense a tárgyévi Tudományos Diákköri Konferencián! Ennek okán könnyedén (és úgymond legálisan) bejut az épületbe, ahonnan, ha nem kísérik ki „szétnézhet", elhozhat iratokat (akár laptopokat is [10]), de elejthet 1-2 pendrive-ot is, amelyet más dolgozók megtalálnak és annak érdekében, hogy „kiderüljön kié" (vagy, hogy már rögtön használatba is vegyék) bedugják a munkahelyi számítógépükbe. Ekkor még nem tudják, de abban a pillanatban fertőzték meg a teljes céges hálózatot!

VIZSGÁLATOK ÉS EREDMÉNYEK

Az informatika fejlődésével együtt fejlődött a hacker kultúra és az államok érdeke is ezen a téren. Míg a kor mérnökeinek leginkább a CD-n terjedő vírusokkal kellett megbirkózniuk, a jelen kor biztonsági szakembereinek már egészen más helyzetük van. Nem elég pusztán jó informatikai vagy műszaki szakembernek lenniük. A kiberbiztonság ma már 95%-ban stratégia (soft defense) és csak 5%-ban technikai védelem (hard defense). [5, s. 4] Minden szakembernek, aki ma foglalkozik védelmi (vagy támadó) megoldásokkal

[10] Konzultáción elhangzott mondat: „Úgy a legkönnyebb laptopot lopni egy cégtől, hogy ebédidőben egy üres laptoptáskával besétálunk az épületbe, majd, amikor már mindenki elment enni csak „megkeressük a sajátunkat" és kisétálunk az épületből!"

el kell gondolkoznia miért alakult ez így? Az információ biztonság sosem volt még ennyire fontos, mint napjainkban, de nem védhetünk mindent technikával [13], mert a támadások sem csak informatikai jellegűek! A támadások 2022-ben akár 75%-ban11 is tartalmazhatnak olyan támadási vektort, ami nem informatikán, hanem pszichológián alapszik.



1. ábra: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Incidensek eloszlása 2022.02.11-17 Szerző által módosított diagram

Ennek oka az, hogy az ember nem tudatos, amikor információbiztonságról van szó, mivel a kibertér még csak pár éve létezik és nem alakultak ki azok a védekezési mechanizmusok, amik a fizikai dimenzióban már kialakultak [14] (pl.: Őseink megtanulták, hogy az éhes oroszlán elől el kell futni, de az adathalász e-mailekre való kattintás ellen még nem alakult az üss vagy fuss reakcióhoz hasonló védekezési mechanizmus). Erre rájöttek a támadók (támadók alatt innentől olyan szakembereket értek, akik vagy törvényi felhatalmazással [állam által támogatott hackerek pl.: Kiber katonák, kiber hírszerzők (CYBINT[12]), kiber nyomozók vagy egyéb az ország törvényei alapján felhatalmazott és jogos bűnüldözési vagy nemzetbiztonsági cél érdekében cselekvő személyek], vagy törvényi felhatalmazás nélküli kiberbűnözők[13] , köznapi értelemben vett szürke vagy fekete kalapos hackerek [16], kiber terroristák[14] [15] és ipari kémek [17] is) is. Ezen felül az informatika rohamos fejlődésével az informatikai biztonság is fejlődött, ennek okán bonyolultabbá és erőforrás igényesebbé váltak ezen támadási vektorok. Ennek köszönhetően csökkentek a technológiai sérülékenységek és emiatt a támadások is [6, p. 87]. Ez egészen pontosan azt jelenti, hogy

[11] 1. ábra adatai alapján
[12] Cyber Intelligence – Kiberhírszerzés [18]
[13] „A kiberbűnözés (…) az informatikai eszközök segítségével olyan illegális cselekmények elkövetése, amely a támadóknak anyagi haszonnal kecsegtet.” [15]
[14] Olyan terroristák, akik nem a fizikai dimenzióban, hanem a kibertérben akarnak kárt okozni. pl.: Kritikus infrastruktúrákat elérhetetlenné tenni
[15] A témával, mint terrorizmus elleni védekezés lásd: [19]

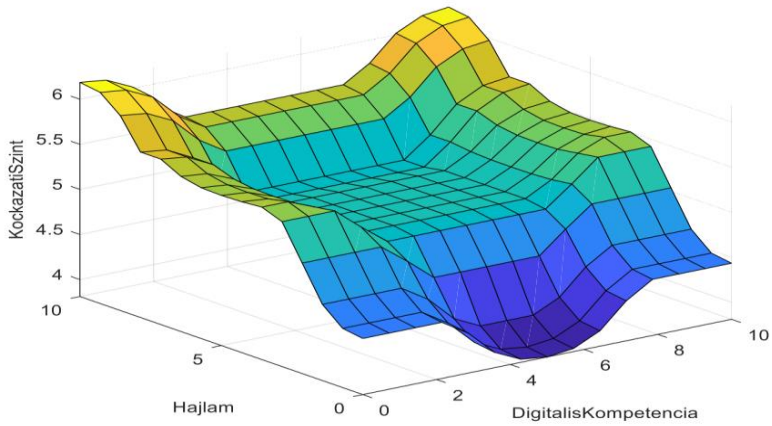
hatékonyabbnak találták, ha nem kattintás nélküli sérülékenységeket[16] keresnek, hanem csak a kártékony kódot juttatják el a célpont rendszerére és azt a felhasználó saját elgondolásból (igaz pszichológiai manipuláció hatására) fogja futtatni! Vagy kártékony kód helyett csupán nemes egyszerűséggel megkérik a felhasználót, hogy jelentkezzenek be a felhasználói profiljukba (ezt leggyakrabban egy úgynevezett phising-gel[17] vagy Smishingel[18] hajtják végre). Csak, hogy ebben az esetben nem a profiljukba jelentkeznek be (amennyiben profi támadóval van dolgunk a fiókunkba is bejelentkezünk és észre sem fogjuk venni, hogy bármi is történt), hanem a támadóknak adták meg az adataikat.
A SE típusú támadások különösen veszélyesek olyan célpontok ellen, akik nem tudatosan (itt csak a hagyományos tudatosságot értem, nem a biztonságtudatosságot) használják az informatikai eszközöket, például kisgyermekek vagy nyugdíjasok. A támadók gyakran ezen csoportokat célozzák meg botnetek építése céljából, mivel szinte garantált a siker! A botneteket pedig a támadó típusától függően pénzért a Dark Net-en eladásra bocsájthatják, vagy az adott állam kiberhadseregébe [21] [22] integrálódva indíthatnak kiberműveleteket ellenérdekelt országok infrastruktúrája ellen. [23] Az ilyen jellegű támadások közül a leggyakoribb a DDOS[19] támadás, melynek hatására az interneten keresztül elérhető szolgáltatások nem lesznek elérhetőek. Ezzel nagymértékű anyagi kárt okoz a cégeknek, mindazonáltal a civil lakosság körében kitörő pánik is hatalmas tud lenni, ami eseteként nagyobb kárt okoz. [24] [25]A SE támadásoknak az erőfölénye abban rejlik, hogy nem csak informatikai támadási vektorokat alkalmaznak, hanem pszichológiákat is, aminek kezelésére a cégek alapvetően informatikai biztonsággal foglalkozó szakemberei nem állnak készen! [20] Az informatikai támadások is mindig egy lépéssel a védelmi megoldások előtt járnak ebben a macska – egér játékban, de az emberi sérülékenységgel egy olyan tényezőt viszünk be az egyenletbe, ami konvencionális védelmi megoldásokkal nem, vagy csak részlegesen detektálható, kivédése pedig csak alacsony %-os arányban történik meg. Az egyedüli védelmi megoldás, amit kutatásom alatt találtam és képes érzékelni a már megtörtént SE támadásokat az a mesterséges intelligencia alapú felhasználói viselkedés elemzés (AI assisted User Behavior Analytics).[26] Ezen megoldások viszont jelenleg csak kezdeti fázisban vannak. Idő kell ameddig „megtanulják" a felhasználói szokásokat és védelmet nem nyújt a támadások ellen, csupán detektálja azokat.

Amennyiben az emberi tényező által okozott kockázatot matematikailag szeretnénk modellezni és mérni, már erre is megvan a lehetőségünk. Váczi Dániel egy cikke az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának Kiberbiztonsági tanulmány kötetében (ISBN: 978-963-449-131-6) jelent meg „A kiberbiztonsági kockázatelemzés lehetséges új iránya. Az emberi tényező kockázatainak valós modellezésének lehetősége Fuzzy logikával a vasútnál, mint kritikus infrastruktúrában" címmel, amelyben felvázolta miért érdemes

[16] Olyan sérülékenység, ami nem igényel semmilyen humán interakciót ahhoz, hogy le tudjon futni a céleszközön
[17] A támadó egy legitimnek tűnő e-mailt küld a célpontnak, amely egy olyan felületre irányítja őt, ami megszólalásig hasonlít az eredeti bejelentkezési oldalra (Ennek az az oka, hogy a nyilvánosan elérhető, a böngészőnkbe letöltött úgy nevezett „Front End" részt másolja le a támadó. Ezáltal az oldal 100%-ban ugyan úgy fog kinézni). Magyar fordítása: „Adathalászat". Az adathalászat kifejezést fogom a későbbiekben használni. [20]
[18] SMS phising
[19] Distributed Denial Of Service attack – Elosztott Szolgáltatásmegtagadással járó támadás
[20] Konzultációk eredményei alapján

mérni a humán faktort, mint biztonsági tényezőt. Miért nem alkalmas ennek felmérésére a BOOLE algebra és miért lehet jobb megoldás a fuzzy logika? Ezen cikke szerint a következő szempontok az alapvetőek amennyiben meg akarjuk állapítani, hogy a dolgozóink jelenthetnek-e veszélyt cégünk kiberbiztonságára:

1. Életkor
2. Generációs jellemzők
3. Alaptermészet
4. Szociális helyzet
5. Családi helyzet
6. Anyagi helyzet[21]
7. Saját, egyéni érdek
8. Vallási háttér és etnikai háttér
9. Függőségek (itt nem csak az illegális kábítószerre kell gondolni, ugyanúgy veszélyes lehet a szerencsejáték függőség vagy egyéb káros hóbort)
10. Zsarolhatóság
11. Céges pozíció
12. A társadalomban betöltött hely
13. A szociális hálóban betöltött hely
14. Technológiai kompetenciák
15. Biztonságtudatosság
16. A dolgozót körülvevő informatikai eszközök és ezek használata
17. Online jelenlét és annak minősége (minél több szabadon elérhető információ érhető el valakiről annál könnyebb lesz zsarolási alapot találni)
18. A privát-magánszféra közötti helyzete



A Hajlam és a Digitális Kompetencia hatása a kimenetre

2. ábra [30]

[21] 2-es diagram egyszerű szemléltető példaként szolgál, hogy miért lehet a fuzzy-val ábrázolt érték pontosabban ábrázolható.

Állami intézmények esetében gyakran nincs szükség a fent említett módszertanra, mivel bizonyos pozíciók betöltéséhez nemzetbiztonsági ellenőrzés szükséges. A piaci cégek viszont nagyban profitálhatnának abból hogyha valamilyen módon ellenőrizhetnék a humán faktort, hasonlóan az állami szférához. A konzultációk és az interjúk tapasztalata alapján megérné a területtel foglalkozni, ezért a kutatásom jövője ebbe az irányba fog menni. Egy olyan automatizált keretrendszert szeretnék készíteni, mellyel mérhető lenne a humán faktor kockázata, mindazonáltal kitöltése nem eredményezhetne munkahelyi diszkriminációt a felhasznált kényes adatok jellege miatt.
Amennyiben már úgy gondoljuk, hogy megfelelő a biztonságtudatosság szervezetünkben érdemes lehet ezt is matematikailag mérni. Ennek alapjait Tarján Gábor fektette le „AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI SZINTJÉNEK MÉRÉSE SZERVEZETEKBEN" című PhD dolgozatában melyben olyan minden szervezet számára hasznosítható következtetésre jutott, amit ma minden információbiztonsággal foglalkozó szakembernek érdemes fontolóra vennie. Többek között érdemes lehet ezeket a méréseket Magyarországon is a Spitzner, L. (2012): „Security Awareness Maturity Model" (SANS Institute) modellje alapján végezni, mivel ez jól adaptálható a magyar környezetbe is. Ezen felül remekül használható az ITIL érettségi modellje mely 6 szintet különböztet meg:
0. Szint – Káosz/Teljes hiány szintje
1. Szint – Kezdeti/reaktív folyamatok
2. Szint – Megismételhető és vagy aktív folyamatok
3. Szint – Meghatározott és proaktív tevékenységek
4. Szint – A folyamatok szilárdak és általában jól teljesítenek
5. Szint – Minden tevékenység jól kontrollált, menedzselt, irányított és optimalizált

A fent említett PhD dolgozat statisztikai adataiból, 2 cég Információbiztonsági menedzsment belső eljárásainak dokumentációjából, konklúziókból, továbbá a szakirodalomban mások által gyűjtött információból megállapítottam, hogy hatékonyabbá tehetőek a biztonsági irányú céges fejlődések amennyiben a modelleket és szabványokat követve folyamatosan monitorozva van cégünk biztonsági felkészültsége! Továbbá növelhető a képzések hatékonysága, hogyha először az érdeklődést teremtjük meg gyakorlati példákkal! [27]

Az oktatásnál viszont az is fontos szempont, hogy ne csak a munkahelyen legyünk tudatosak, hanem a közösségi médián is! [28] Ugyanis OSINT segítségével nagyon sok kritikus információ gyűjthető valakiről csak a nyílt források felhasználásával, amiket a támadó minden esetben ki fog használni. De ugyanolyan fontos, hogy a marketinges szakember megértsék, hogy a kiberbiztonságot is biztonságosan kell reklámozni. Erre az egyik példa a sok közül a Gloster Infokommunikációs Nyrt. esettanulmánya az Óbudai Egyetemről [29] amelyben pontosan megnevezik, hogy 2 darab Cisco Firepower 2130-as tűzfalat üzemeltek be az egyetemen. Ez első sorban azért lehet problémás mert olyan oldalakon mint például az exploit-db.com könnyen lehet eszköz típus alapján sérülékenységeket találni. [22,23]

[22] 3-as számú melléklet
[23] 4-es számú melléklet

Közintézményként az Óbudai Egyetem arra kötelezett, hogy a Digitális Kormányzati Ügynökség portálján keresztül bonyolítsa le a kiemelt beszerzéseit. Az IT eszközök megvásárlása is annak bizonyul. Az egyetemen hagyománya van a Cisco eszközök használatának, így az intézmény eleve Cisco megoldásban gondolkodott.

Az intézmény a legjobb ár-érték arányt képviselő megoldást kereste, ahol a termék árazása mellett fontos volt az is, hogy a kiválasztott vállalat milyen minőségű technikai támogatást nyújt. A Digitális Kormányzati Ügynökség portálon a Gloster ajánlata volt a legjobb ár-érték arányú.

Az egyetemnek a Cisco Magyarország képviselőivel is van közvetlen kapcsolatuk. A gyártó képviselői is kiemelten ajánlották a Gloster, megerősítették, hogy mint szállító, alkalmas feladatai ellátására. Erről tanúskodnak a **Gloster Cisco tanúsítványai is**: a cég a **Cisco Premier Partnere**, 2020 decemberében megkapta negyedik Advanced minősítését, data center területen, de security, collaboration és enterprise területeken is Advanced Partner.

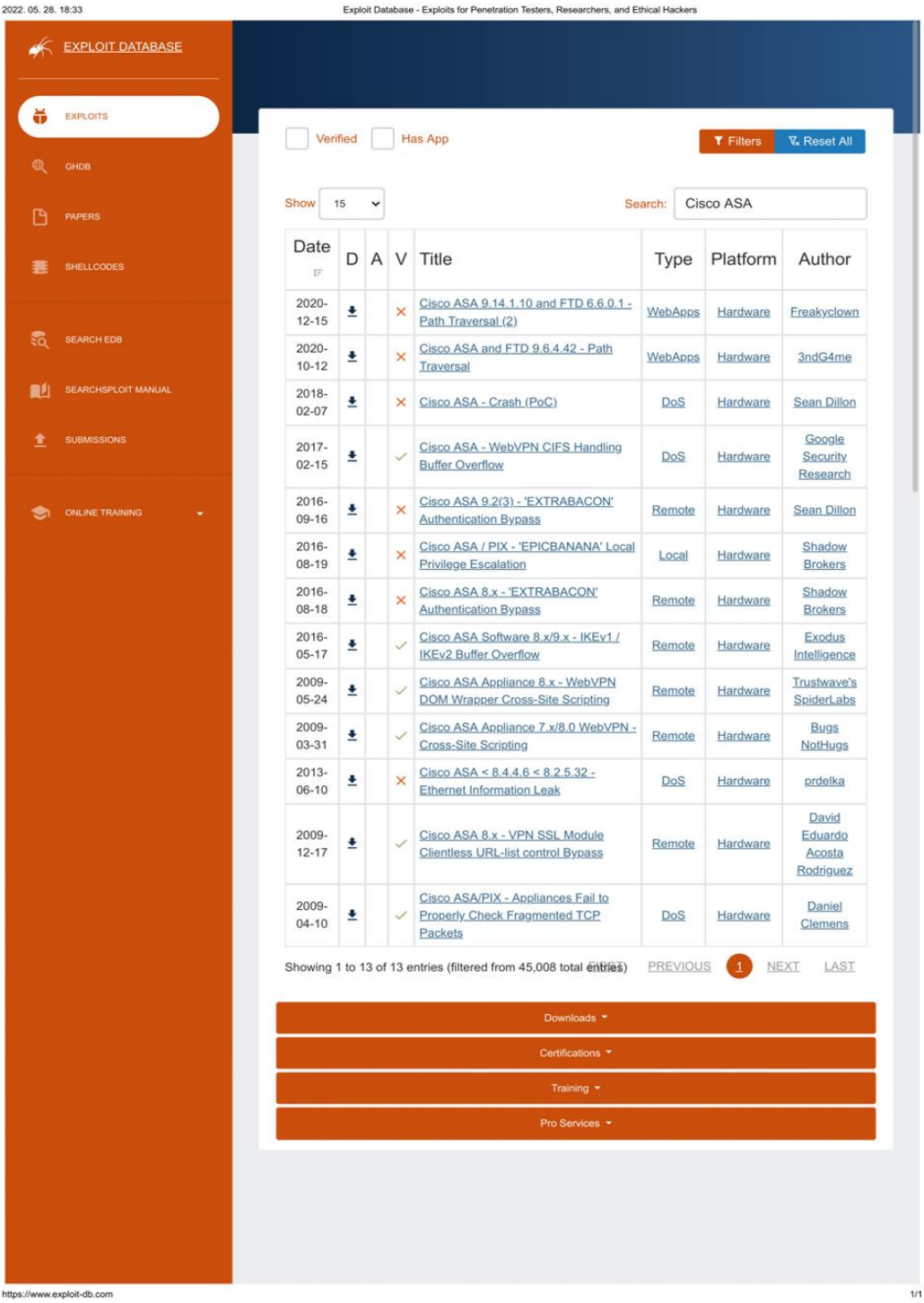
Korábbi közös IT projektek kapcsán az Óbudai Egyetem és a Gloster között már megvolt a kapcsolat, így már egy kipróbált vállalatra bízták a feladat megoldását.

A választás 2 darab redundáns, központi **Cisco Firepower 2130-as tűzfalra** esett.

A Gloster és az Óbudai Egyetem szakemberei első körben közösen beszélték meg, hogy pontosan milyen megoldás lenne ideális az intézmény számára. A tervezés, műszaki egyeztetés és beszerzés tekintetében egyaránt részt vettek a megbeszélésen és segítettek az egyetemnek a megfelelő eszközt kiválasztani. A műszaki paraméterezés során figyeltek a maximális terhelésre és a jövőbeli tervezett fejlesztésekre egyaránt.

A megoldás előnyei

3. számú melléklet



4. számú melléklet

Oroszi Eszter Diána előadásait hallgatva [30] és kutatásait olvasva elkezdett az foglalkoztatni, hogyan lehetne ezeket a biztonságtudatosító képzéseket hatékonyabbá tenni. Az auditorokkal folytatott konzultációim során megállapíthatóvá vált, hogy a képzések színvonala általában a management motivációját tükrözi a téma iránt. Amennyiben követelmény miatt (pl.: egy pályázat elnyeréséhez a cégnek rendelkeznie kell ISO 27001-es szabvánnyal) kell tartani ilyen képzéseket a színvonala a mindig rendkívül érdekes munka, baleset és tűzvédelmi előadásokhoz fogható. Vagyis a poroltó helyét vissza tudja mondani a dolgozó és valószínűleg ez után azt is, hogy hogyan néz ki egy erős jelszó, viszont amennyiben „éles helyzet állna elő" ezzel a tudással sajnos nem menne sokra. A management számára fontos szempont, hogy a dolgozók kevés időre vagy ne essenek ki a termelékeny munkafolyamatokból egy ilyen képzés miatt. Ezért ezeknek a képzéseknek az időpontját úgy kell megválasztani, hogy vagy az összes ilyen képzést egy napra kell időzíteni, ami eddigi tapasztalatok alapján kevésbé hatékony! Vagy céges ünnepségekhez, rendezvényekhez. Egy céges születésnap első programja vagy a karácsonyi vacsorát megelőző „biztonságtudatossági verseny" a dolgozók között motivációt adhat azoknak, akik fogékonyak lennének a téma iránt és jó élményekkel is összeköthetik az amúgy unalmas képzéseket!

KONKLÚZIÓ

- A humán faktor sérülékenysége matematikailag mérhető. Fuzzy logika alapú rendszerrel a pár fős cégektől a multinacionális vállalatokig korlátlanul skálázható.
- A dolgozók nem biztonságtudatos magatartása a rendszerünk legsérülékenyebb pontja.
- Biztonságtudatosító képzésekkel hatékonyan fel lehet készíteni a dolgozókat a Social Engineering támadásokra.
- Jelenleg (2022.05) nincs olyan informatikai védelmi megoldás, ami megakadályozná a Social Engineering támadásokat!
- Mesterséges intelligencia alapú valós idejű felhasználói viselkedés elemzéssel érzékelhető, ha a dolgozó digitális adatot juttat ki a cégből.
- Zero Trust módszer bevezetésével nagyban csökkenthetőek a károk egy támadás esetén
- Állami intézményeknek megalapításuktól, piaci cégeknek az első kockázat elemzésüktől érdemes információ biztonsággal foglalkozni.
- A vállalatok védekezését megkönnyítheti az ISO 27000-es szabványcsalád implementálása.
- A támadások döntő többsége már tartalmaz Social Engineeringet a hatékonysága miatt.
- Az állami szektor 2013 óta foglalkozik biztonságtudatosító képzésekkel!
- Érdemesebb a drága konvencionális védelmi megoldások előtt bevezetni azokat az adminisztratív és logikai biztonsági kontrollokat, amik nem kerülnek dologi kiadásba a cég számára.

JAVASLATOK

- Az IBTV hatálya alá tartozó intézményeknek megalakulásuktól törekedniük kell a számukra szükséges és elégséges információbiztonság megvalósítására

- A piaci szereplőknek az első kockázatelemzésüktől érdemes az információbiztonsággal foglalkozni, az abban megállapított kockázatokat kezelni, de alternatíva lehet a kockázat a biztosító felé történő áthárítása is.
- Nem célszerű nagyobb összeget költeni a védelemi megoldásokra, mint amekkora összeget vesztenénk a kockázat bekövetkeztével.
- Nem minden esetben célszerű a kockázatokat teljesen eliminálni költségességüknél fogva, mindazonáltal a menedzsmentnek törekednie kell arra, hogy számukra vállalható szinten mozogjanak!
- Amennyiben érzékeny adatokkal dolgozunk vagy olyan adatokkal (például szellemi termékkel) amiket ellopva anyagi ellentételezésben részesülne az adatok eltulajdonítója érdemes nem csak az üzletmenet folytonosságot védeni, hanem a cég belső információit, értékeit!
- Amennyiben a fent említett adatokat meg kell védenünk, érdemes nem csak a konvencionális védelmi megoldásokat beszereznünk, mivel ezek drágák és csak az informatikai kockázatok ellen nyújtanak bizonyos fokú védelmet. Emellett célszerű lenne biztonságtudatosító képzéseket tartani és a fizikai, logikai és adminisztratív védelmi kontrollokat erősíteni. Ezek preventív védelmi intézkedések, ezzel megelőzhetővé vállnak a támadások, míg a konvencionális védelmi megoldások (pl.: reaktív vírusírtók) detektív és korrektív védelmi kontrollokat nyújtanak. Próbáljuk meg megelőzni a támadásokat!
- Érdemes lehet vállalatirányítási szabványokat bevezetni (ISO 9001 és 27001).

FELHASZNÁLT IRODALOM

[1] Krasznay Csaba és Bányász Péter: Kiberbiztonsági incidensek a magyar közigazgatásba (https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/13172/A_Jo_Allam_merhetos-ege_III_2019.pdf?sequence=1#page=250 Hozzáférés ideje: 2022.05.21 21:05:13) p. 264

[2] Christopher Hadnagy „The Art of Human Hacking” ISBN: 978-1-118-02801-8 Wiley Publishing, Inc. (2011) p.23 szerző által fordított

[3] Katonai Nemzetbiztonsági Szolgálat Felderítő Szemle XIV. évfolyam 4. szám 2015. november HU ISSN 1588-242X Az Informatikai Üzemeltetés Általános Kérdései Holtai András, Magyar Sándor, Puskás Béla p. 91

[4] Haig Zsolt Információs Műveletek A Kibertérben Dialóg Campus Kiadó, 2018 p.220 4.1.1

[5] Információbiztonság vs. kiberbiztonság – az okos város szempontjából Krasznay Csaba NKE Kiberbiztonsági Akadémia https://www.hte.hu/documents/10180/4588545/2.4-Krasznay_Csaba.pdf hozzáférés ideje: 2022.05.21 21:05:13)

[6] Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle XVIII. évfolyam 1. szám 2020. március HU ISSN 1785-1181 Tóth Tamás Az Egyes Social Engeneering Módszerek Elhatárolása És Rendszerezése

[7] Dezső András Fedősztori 2021 ISBN: 978 963 568 115 0 – p. 423

[8] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban (https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/14723/01_Banyasz_Bota_Csaba_A_social_engineering.pdf?sequence=22 utolsó elérés ideje: 2022.05.21 21:05:13) p. 16
[9] . Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola Bányász Péter Doktori (PhD) Értekezés A közösségi média lehetőségei és kihívásai a védelmi szférában Budapest, 2018p. 84
[10] Katonai Nemzetbiztonsági Szolgálat XV. évfolyam 3. szám 2017. november Szakmai Szemle HU ISSN 1785-1181 60-76 Deák Veronika Biztonságtudatosság Az Információs Környezetben p. 64
[11] Dunakavics 2015. III. évfolyam VIII. szám Oroszi Eszter Diána: Kártékony programok terjedése social engineer szemmel p. 14
[12] ISO Consulting Kuwait https://isoconsultantkuwait.com/2019/12/08/iso-270012013-a-7-human-resource-security/ hozzáférés: 2022.05.21 21:05:13)
[13] Ludovika Szabadegyetem 2022. április 19. 18.00 Krasznay Csaba: A kiberbűnözés fajtái, kiberbűncselekmények és a dark web
[14] Nemzetbiztonsági Szemle HU ISSN 2064-3756 VI. évfolyam, 1. szám, 2018. Social engineering and social media 1 Bányász Péter p. 60
[15] Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet: Az információbiztonság lélektana (Psychology of Information Security) KÖFOP-2.2.2-VEKOP-16-2016-00001 pp. 6-7
[16] Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Kar
Katonai Műszaki Doktori Iskola Krasznay Csaba PhD Értekezés A Magyar Elektronikus Közigazgatási Alkalmazások Információbiztonsági Megoldásai Budapest, 2011 p. 119
[17] Katonai Nemzetbiztonsági Szolgálat Felderítő Szemle XIV. évfolyam 2. szám 2015. június HU ISSN 1588-242X Vida Csaba p. 197
[18] Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola Pix Gábor Alezredes A Lélektani Műveletek Jellemzőinek Vizsgálata Doktori (Phd-) Értekezés Budapest, 2005 3.1.1 A terrorizmus kezelésének lehetősége – A lélektani műveletek szemszögéből pp. 77 – 80
[19] Cisco Networking Academy CCNA: Enterprise Networking, Security, and Automation (v7.02) 3. szemeszter online tananyag - 3-as fejezet Network Security Concepts - 3.5.6 alfejezet Social Engineering Attacks – szerző fordítása | elérhető: https://www.netacad.com/courses/networking/ccna-enterprise-networking-security-automation
[20] Haig Zsolt - Várhegyi István A cybertér és a cyberhadviselés értelmezése p. 6
[21] Ludovika Szabadegyetem Kovács László dandártábornok: Kiberbiztonság és kiberhadviselés 2022-. 03. 8 18:00
[22] Nemzet És Biztonság 2010. február Kovács László dandártábornok – Krasznay Csaba: Digitális Mohács Egy kibertámadási forgatókönyv Magyarország ellen p. 2
[23] Nemzet És Biztonság 2010. február Kovács László dandártábornok – Krasznay Csaba: Digitális Mohács Egy kibertámadási forgatókönyv Magyarország ellen p. 6

[24] Óbudai Egyetem Biztonságtudományi Doktori Iskola Váczi Dániel PhD értekezés Kiberbiztonsági humán kockázati matematikai modell szenzitív digitális információszivárgás potenciáljának mérésére Budapest, 2021. 09. hónap 27. nap p. 31
[25] https://www.splunk.com/en_us/data-insider/user-behavior-analytics-ueba.html utolsó hozzáférés: 2022. május 22. 00:08:01
[26] Dub Máté: A social engineering támadások megelőzésének lehetőségei (https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/5476/4721 : 2022.05.21 21:05:13)
[27] Deák Veronika A Social Engineering humán alapú támadási technikái p. 8
[28] https://www.gloster.hu/eroforrasok/esettanulmany/obudai-egyetem-esettanulmany-cisco-tuzfal-vedi-az-online-egyetemi-oktatast hozzáférés: 2022. május 27. 20:48:27
[29] CodingClub - Oroszi Eszter: Social Engineering (https://www.youtube.com/watch?v=ikcuLV4HUvY&t=489s 2022.05.21 21:05:13)
[30] Bánki Közlemények 4.Évfolyam 1.Szám
Az emberi tényező fuzzy alapú kiberbiztonsági kockázatelemzése a minősített információszivárgás szempontjából Váczi Dániel, Tóth-Laufer Edit, Szádeczky Tamás 10. ábra: A pénzügyi helyzetet leíró tagsági függvény
[31] Konzultációk:
- Hack Zoltán (ISO 27001 auditor és oktató) – állandó konzulensem
- Krasznay Csaba (Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpont-Kiberbiztonsági Kutatóközpont vezető) 2022.03.23
- Kollár Csaba (Óbudai Egyetem Mesterséges Intelligencia Műhely vezető) 2022.04.05