Az információbiztonság lélektana

(Psychology of Information Security)

A tanulmány a KÖFOP-2.2.2-VEKOP-16-2016-00001

„KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése”

című projekt keretében készült.

Tartalomjegyzék

Absztrakt

A megfelelő szintű kiberbiztonság megteremtése komoly kihívásként jelentkezik napjainkban a kibertámadások számának folyamatos növekedésének és az egyre újabb támadási alternatívák, technikák megjelenésének következtében. A támadók sokkal kifinomultabban használják ki a különféle információs rendszerek, valamint az emberi tényező sebezhetőségeit, illetve egyre komplexebb támadások jelennek meg. Ezen okokból kifolyólag létfontosságú az információbiztonság folyamatos fejlesztése és erősítése. Megvalósításának alapeleme a megfelelő szintű biztonságtudatosság kialakítása, melynek eléréshez elengedhetetlen az információbiztonság lélektanának, illetve az emberi tényező szerepének mélyebb vizsgálata.

Abstract

Due to the continuous increase in number of cyber attacks and the emergence of ever renewing offense alternatives and techniques, the appropriate level of cyber security to ensure calls for special attention, nowadays. Attackers deploy the vulnerability of information systems in a more sophisticated and complex way than ever. For these reasons it is of crucial importence to develop and strengthen information security, which entails raising awareness in the field of information security. The latter can only be attained by the deeper analysis of the human factors and psychology of information security.

Kulcsszavak: információbiztonság, tudatosság, emberi tényező

1. Bevezetés

Az információbiztonság nélkülözhetetlen eleme életünknek, hiszen információs társadalomban élünk. Ez azt jelenti, hogy napjainkban az információ meghatározó társadalmi értékké válik, és a társadalom, illetve a gazdaság maga is információs értékeket termel és használ fel. Az információ előállítása, elosztása, terjesztése, használata és kezelése jelentős gazdasági, politikai és kulturális tevékenység. Az információs társadalom működésének alapja az információs infrastruktúra (információs közműhálózat).[1] Az információ egyre fontosabb szerepet tölt be mindennapjainkban, a társadalom egyik alappillérévé vált. Jelen van a kommunikációban, a döntéshozatalokban, valamint a különféle folyamatok, eljárások lebonyolításában is. Az információ értékének növekedésével együtt jár a különböző információk megszerzésére irányuló támadások megjelenése is, függetlenül attól, hogy az adott információ bizalmasnak tekinthető-e vagy sem. A számítástechnikai és elektronikai eszközök tárháza szinte végtelen, és az idő előrehaladtával folyamatosan jelennek meg új és új eszközök, amelyek azonban számos veszélyt rejthetnek magukban. Az új eszközök megjelenése új támadási alternatívát, felületet is jelenthet, éppen ezért kiemelt jelentőségű, hogy megvédjük a ránk bízott információkat a jogtalan hozzáféréstől, az információk esetleges kiszivárgásától, módosításától vagy akár megsemmisítésétől. Ahhoz, hogy a védelem sikeres lehessen, nem elég csupán a támadási és védekezési módszereket ismerni, minden esetben ki kell térni a támadást végrehajtó személyek, a felhasználók, valamint a vezetők szerepére is, hiszen a védelem sikeres kialakításával sok esetben megelőzhetők a bizalmas információk megszerzésére irányuló támadások.

A jelen tanulmány célja az emberi tényező információbiztonságban betöltött szerepének bemutatása, különösen az információ kezelésével, védelmével és megszerzésével kapcsolatba hozható személyek, mint például a felhasználók, vezetők vagy akár a támadók információbiztonsági vonatkozásának ismertetése.

[1] Haig Zsolt: *Információ – társadalom – biztonság.* NKE Szolgáltató Kft., Budapest, 2015. pp. 29–39.

2. Az emberi tényező az információbiztonságban

Az emberi tényező információbiztonságban betöltött szerepét vizsgálva megállapítható, hogy a bizalmas információk védelmében és megszerzésében egyaránt kiemelt jelentőségű a humán tényező információval kapcsolatos tevékenysége, ennek során tanúsított magatartása, valamint a szervezetben betöltött munkaköre és meghatározott jogosultságai. Különbséget kell tenni az információbiztonság és az információk elleni támadások megvalósításában résztvevők között, funkciójuk, szerepük és az információkkal kapcsolatos tevékenységük, felelősségeik alapján. Ezek alapján három szereplőt mutatunk be:

- a támadót,
- a felhasználót és
- a vezetőt.

2.1. A támadó lélektana

A támadó lélektanának vizsgálata elengedhetetlen az információk ellen irányuló támadásokkal szembeni hatékony és eredményes védelem kialakítása érdekében. A megfelelő védelem kialakítása pedig csak úgy valósulhat meg, ha megismerjük a támadás módjait, eszközeit és a támadások során tanúsított magatartásokat is. Fontos: ahhoz, hogy igazán jól védekezzünk, meg kell értenünk a támadások végrehajtása mögött álló motivációkat, pszichológiai tényezőket. A következőkben a támadók típusai, indítékai és célpontjai, valamint az általuk alkalmazott lélektani módszereket tárgyaljuk.

2.1.1. A támadók típusai

Ahhoz, hogy a támadók viselkedését és a támadások motivációit feltárhassuk, mindenképpen szükséges tisztázni a kibertámadások végrehajtásáért felelős személyek típusait. A támadók kategorizálásának alapjául a támadások megvalósításának eszközei, céljai és motivációi szolgálnak, tehát a különféle támadótípusok megkülönböztetésének szempontjai: az adott támadónak mi a célja a támadás végrehajtásával, milyen előnyre, haszonra kíván szert tenni, és milyen eszközök segítségével valósítja meg a támadást.

Az első nagy csoportot a *hackerek* alkotják.

A hacker olyan személy, aki az internet segítségével képes hozzáférni védett, illetve belső és bizalmas információkhoz a számítógépeken és egyéb infokommunikációs eszközökön.

A hackereknek kezdetben két nagy típusuk volt: a fehérkalaposok („white hat") és a feketekalaposok („black hat"), akik alapvetően ugyanazokat az eszközöket és módszereket használták, de eltérő célok érdekében. A *white hat hackerek* vagy más néven etikus hackerek célja a különféle informatikai, információs rendszerek gyenge pontjainak, sebezhetőségeinek feltárása annak érdekében, hogy az azt kezelők számára feltérképezzék és bizonyítsák a hiányosságokat, illetve hibákat. A sérülékeny pontok és biztonsági hibák felfedése, továbbá kijavítása érdekében különböző programokat, rendszereket, weboldalakat törnek fel, hogy ezáltal elkerülhetővé váljanak a black hat hackerek betörési kísérletei. Ezzel szemben a *fekete kalapos* (black hat) *hackerek*, akik valamilyen haszonszerzés (pl. gazdasági, politikai stb.), károkozás céljából vagy szimplán rosszindulatból, illetve kíváncsiságból hatolnak be jogosulatlanul számítógépekbe vagy számítógép-hálózatokba.[2] Motivációjuk sokfélék lehet, többek

[2] Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* 2012, p. 135.

https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf (2018. 10. 08.)

között pénzszerzés, erőfitogtatás, károkozás, de ezen indítékokat a következő (2.1.2.) alpontban mutatjuk be részletesebben. Megjelent a két hacker típus közötti átmenetet jelentő szürkekalapos („grey hat") hacker elnevezés is: a támadó az adott biztonsági rés feltárása közben kihasználja azt, majd a sebezhetőségről értesíti a rendszer üzemeltetőjét, valamint előfordulhat, hogy segítségét is felajánlja a hiba elhárítása érdekében.[3]

A kibertámadásokat végrehajtó személyek következő nagy típusát a *hacktivisták* alkotják, akik a hackerek és az aktivisták jellemzőit és céljait közösen birtoklók társasága.

A hacktivisták számítógépes hálózatokon speciális eszközökkel proaktív politikai aktivizmust hajtanak végre, a legtöbb esetben a szólásszabadság, az emberi jogok és az információszabadság jegyében.[4] Kisebb csoportokban valósítanak meg informatikai bűncselekményeket, és fő céljuk médiafigyelem elérése, hogy ezáltal minél többen láthassák saját ideológiai véleményüket.

Rendszerint politikai motivációval rendelkeznek, és ezen célok elérése érdekében olyan akciókat hajtanak végre, amelyek során egy számukra fontos ügy érdekében internetes oldalakat törnek fel, módosítják, átalakítják azokat, megakadályozzák ezen oldalak rendeltetésszerű használatát és működését, valamint adatokat is lophatnak ezen webhelyekről. Hacktivistának tekinthető például a napjainkban működő Anonymus csoport, amely leginkább a különféle kormányok, kormányzati szervek, vállalatok vagy akár a Szcientológiai Egyház támadásairól vált széles körben ismertté.[5]

A *számítógépes bűnözők* magas szintű hálózati és számítógépes ismeretekkel rendelkező elkövetők.

A számítógépes bűnözők elsődleges tevékenysége a különböző információtechnológiai eszközök, rendszerek, illetve rendszerelemek ellen irányulnak, vagy információ-technológiai eszközöket, rendszereket használnak a bűncselekmény elkövetésének eszközeként. A számítógépes bűnözők elsődleges célja a pénzszerzés.

Akcióikat rosszindulatú szoftverek (mint például a vírusok, férgek, trójai programok, backdoor programok, rootkitek stb.), illetve eljárások alkalmazásával (például phishing) hajtják végre. Az elmúlt években jelentősen nőtt a számítógépes bűnözők által elkövetett bűncselekmények száma, illetve az ezekkel okozott károk nagysága.[6]

A támadók következő nagy csoportját az *ipari kémek* alkotják. Az ipari kémek célja továbbra is az iparban elkövetett illegális információszerzés, azonban ma már új módszerek, eszközök segítségével hajtják végre ezen információk megszerzését. A napjainkban használt új technológiák, a számítógépes tervezés, irányítás és rendszerfelügyelet már lehetővé teszi, hogy a különféle infokommunikációs eszközökön tárolt, illetve a hálózatokon áramoltatott adatokat, információkat illetéktelenek szerzik meg, jelen esetben az ipari kémek, mint például a konkurens cégek, vállalatok alkalmazottai vagy az előbb említett számítógépes bűnözők, akik a megszerzett információkat, üzleti titkokat eladják a piacon, például a konkurens vállalatnak. A technológia fejlődésével az illegális adatszerzők tevékenységét az elektronikus csatorna segíti, amelyen keresztül hatalmas mennyiségű információ szerezhető meg viszonylag rövid idő alatt, költséghatékonyan.

[3] Papp Zoltán István: *A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái.* 2018. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/Papp_Zoltan_PhD_ertekezes_tervezete.pdf (2018. 10. 07.)
[4] Carabott, Emmanuel: *Hacking Motivations – Hactivism.* 2011. http://www.gfi.com/blog/hacking-motivations-hacktivism/ (2018. 10. 08.)
[5] Haig et al., i. m. pp. 135–136.
[6] Haig et al., i. m. p. 136.

Az ipari kémek célja, hogy az ellenérdekelt fél ne szerezzen tudomást arról, hogy információs rendszerét támadás érte, és bizalmas információk kerültek illetéktelen kezekbe, mivel így az esetlegesen bevezetett intézkedések következtében a megszerzett adatok értéktelenné válhatnak.[7]

A támadók típusainak feltárásakor mindenképpen ki kell térni a *munkatársakra*, valamint a *belső és külső szakértőkre*, ugyanis komoly veszélyforrást jelenthetnek a bizalmas információkra nézve. Az informatikai biztonságot vizsgáló cégek statisztikái szerint a betörések nyolcvan százalékát a szervezetek saját alkalmazottai követik el.

A sértődött vagy elbocsátott emberek a rendszerről meglévő ismereteiket kihasználva hatalmas károkat okozhatnak mind a szervezet informatikai, információs rendszerében, mind a bizalmas információk illetéktelen kezekbe jutásának tekintetében. Az okok általában irigység, sértettség, bosszú, vandál pusztítási vágy, rosszindulat, hirtelen felindulás, hírszerzés és ipari kémkedés támogatása, anyagi vagy egyéb előnyök szerzése, de előfordulhat, hogy befolyásolás vagy zsarolás következtében szolgáltatnak bizalmas információkat illetékteleneknek.

A külső szakértők kiemelése azért fontos, mert a különféle szervezetek, vállalatok életében rendkívül fontos szerepet játszanak. Az információs infrastruktúrák tulajdonosai sok esetben külső, erre a feladatra specializált szakértőkre bízzák információs hálózatuk kialakítását, valamint üzemeltetési feladataikat.

Ennek hátránya, hogy a szervezet kiszolgáltatottá válik, mert a külső szakértők az üzemeltetés, hibaelhárítás során magas szintű hálózati hozzáféréssel, belépési jogosultságokkal rendelkeznek, így olyan érzékeny információkhoz férhetnek hozzá az érintett rendszerekről, az ezekben tárolt adatokról, valamint a szervezet működéséről, struktúrájáról, illetve a munkatársakról, amelyekkel visszaélve súlyos és visszafordíthatatlan károkat okozhatnak a szervezet számára.[8]

A kibertámadások végrehajtásáért felelős személyek esetében meg kell említeni a *terroristákat* is, hiszen ők is aktívan alkalmazzák a nyílt forrású információszerzés, az infokommunikációs technológiák és az internet nyújtotta lehetőségeket, eszközöket.

A terroristák az információs infrastruktúrákra és szolgáltatásaikra már nemcsak célpontként tekintenek, hanem eszközként is felhasználhatják őket.[9]

Összességében megállapítható, hogy a támadók – típusuktól függően – céljaik elérése érdekében számtalan módszert alkalmazhatnak. Miután megismertük a támadók kategorizálásának alapjait, ezt követően kerülhet sor a motivációk és célok ismertetésére.

2.1.2. A támadók motivációi, céljai

Ahhoz, hogy megérthessük a támadók viselkedésmódját, eszközeit és a lehetséges behatolási pontokat, tisztázni szükséges a támadás céljait és az ezek mögött álló motivációkat. Ha tudjuk, hogy mire irányulhat a támadás, akkor sokkal hatékonyabb és eredményesebb védelem alakítható ki. A támadók motivációját mindig a támadás végrehajtásával elérni kívánt cél határozza meg, hisz a motiváció az az ok (pl. az információ hiánya, érdekellentét, anyagi nehézségek stb.), amely cselekvésre készteti a támadót. A motiváció tehát az az indíttatás, amely a támadásra ösztönzi a támadót, így a következőkben a támadók egyes céljai, motivációi kerülnek bemutatásra, a teljesség igénye nélkül.

[7] Papp 2018, i. m. pp. 53–54.
[8] Papp 2018, i. m. pp. 54–55.
[9] Uo., p. 55.

2.1.2.1. Információszerzés

Az információszerzés mint cél értelmezésekor elsőként azt szükséges tisztázni, hogy mire irányulnak ezen információszerzések, tehát mi a tárgya ennek a tevékenységnek. Az információszerző támadások mögötti motiváció maga az információ hiánya. Ebben az esetben a tevékenység központi célja az adatok, információk gyűjtése, majd pedig saját célra történő felhasználása.

Az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.[10]

Az információ értelmezésére számtalan definíció létezik, nincs egységes meghatározása. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerint az információ bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott tapasztalat, megfigyelés vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét átalakítja, megváltoztatja, illetve befolyásolja, továbbá bizonytalanságát csökkenti vagy megszünteti.[11]

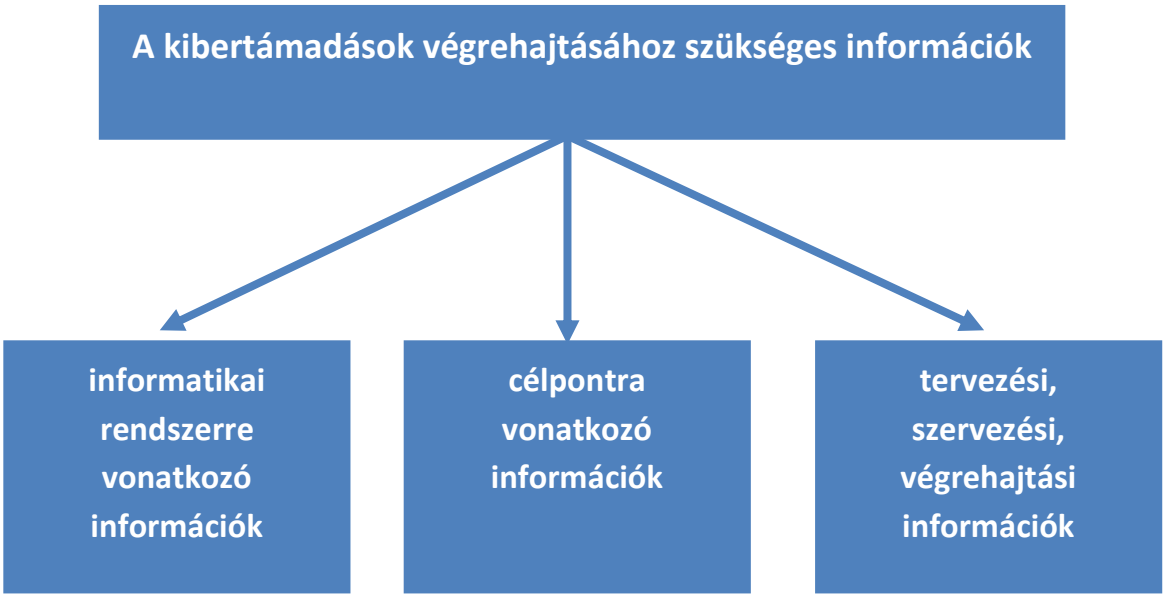
Egy másik definíció szerint az információ olyan új ismeret, adat, tény, amelynek megismerésekor olyan plusz tudásra teszünk szert, amely addig nem volt a birtokunkban.[12]

A kibertámadások jelentős részének elsődleges célja a belső és/vagy bizalmas információk megszerzése. Ezek az információk sokfélék lehetnek, az információszerzés irányulhat többek között személyes adatokra, jelszavakra, bankkártyaadatokra vagy üzleti titkokra is. A belső és bizalmas információkat érdemes különválasztani egymástól, hiszen a belső információk nem minden esetben tekinthetők bizalmas információknak. A belső információk nem titkosnak minősített információk, ennek ellenére mégis az adott szervezet dolgozóira vonatkoznak, éppen ezért nem javasolt megosztani idegenekkel, hiszen az adott közösségre érzékeny információk birtokában egy támadó könnyen megszemélyesíthet egy kitalált személyt, aki az adott szervezet egy új tagja.[13] A megszerzett információkkal a támadó további támadásokat is megvalósíthat, illetve előkészíthet, hisz az információszerzés nemcsak a támadás közvetlen célja lehet, hanem annak részcélja, első lépése is.

Az információszerzés mint részcél

A kibertámadások nélkülözhetetlen elemeként értelmezhető az információszerzés, hiszen minden támadás alapja a támadás sikeres végrehajtásához szükséges információk megszerzése. Az, hogy pontosan milyen információk megszerzése a cél, az attól is függhet, hogy mi a konkrét támadás motivációja. A kibertámadások során az információszerzés célja olyan információk gyűjtése, amelyek a támadás céljától függően biztosítják a sebezhetőségek, kockázatok és sérülékenységek feltárását. Egy kibertámadás alapjául szolgáló információszerzés alapvetően az alábbi ábrán látható információkat célozza. Az információszerzés irányulhat az informatikai rendszerre vonatkozó jellemzőkre és a célpontra vonatkozó információkra, amelyek kapcsán elsődlegesen a sebezhetőségek, gyenge pontok feltárása a cél, majd ezek alapján következhet a tervezési, szervezési és végrehajtási információk összegyűjtése, rendszerezése.

[10] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 1. § (1)
[11] Uo.
[12] Krasznay Csaba: *Az információbiztonság alapjai.* 2007. http://krasznay.hu/presentation/elte_01.ppt (2018. 10. 12.)
[13] Deák Veronika: *A social engineering humán alapú támadási technikái.* 2017. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (2018. 10. 12.)



1. ábra: A kibertámadások végrehajtásához szükséges információk
(Saját szerkesztés)

Az *informatikai rendszerre vonatkozó információk* tartalmazzák az adott rendszer felépítésére, működésére vonatkozó adatokat és a rendszerhez csatlakozó eszközök jellemzőit. Nem létezik tökéletes biztonság, naponta jelennek meg újabb és újabb támadási módszerek, biztonsági rések, ennek következtében minden kockázatra kiterjedő védelemről sem beszélhetünk. Éppen ezért a technológiai sérülékenységek feltárása minden esetben kulcsfontosságú, hiszen ezek segítségével azonosíthatók az információs rendszerek vagy azok elemeinek gyenge pontjai. Egy informatikai rendszer esetében kockázatnak tekinthetők többek között a különféle biztonsági rések, lehetséges szoftverhibák, hibás beállítások, gyenge jelszavak, a különböző szintű jogosultságok beállításának a hiánya, illetve hibás hozzáférési szintek megállapítása, a titkosítás hiánya vagy hibája, alkalmazás szintű hibák, mint például a hitelesítési, logikai hibák vagy akár az alkalmazások frissítéseinek elmulasztása.[14] A *célpontra vonatkozó információknak* két típusát különböztethetjük meg: Az egyik csoportba tartoznak azok az adatok, amelyek egy *szervezetre jellemzőek*, míg a másik csoportot a *személyre utaló* információk alkotják. A szervezettel kapcsolatos adatok magukban foglalják a szervezet tevékenységével, munkavállalóival, fizikai jellemzőivel, védelmével, struktúrájával, illetve elérhetőségeivel kapcsolatos adatokat. A *személyre utaló információk* megszerzése elősegíti a tökéletes célpont kiválasztását, aki a későbbiekben a támadó segítségére lesz a támadás megvalósításában. Ezen információk megszerzése során kerül sor a felhasználók biztonságtudatosságának felmérése, vagyis annak vizsgálatára, hogy mely alkalmazott nem rendelkezik megfelelő szintű információbiztonsági tudással, és ezáltal mely munkavállaló segítségével szerezhetők meg a szervezetre vagy az informatikai rendszerre vonatkozó adatok, vagy mely célszemély alkalmas például egy kártékony program aktiválására, működésbe hozatalára.[15]

[14] Dolánszky György: *Informatikai rendszerek sérülékenységvizsgálata.* 2013. http://users.nik.uni-obuda.hu/poserne/ibst/Frissitett_anyagok_2013/20130508_Serulekenysegvizsgalat_eSec_KURT_DGY.pdf (2018. 10. 12.)

[15] Deák Veronika: *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során.* 2018. http://www.hadmernok.hu/183_29_deak.pdf (2018. 11. 03.)

A célinformációk harmadik nagy csoportját a *tervezési, szervezési, végrehajtási információk* alkotják. Ezen információk magukban foglalják a konkrét támadás kivitelezéséhez szükséges technikai, személyi, tárgyi és pénzügyi feltételeire vonatkozó ismereteket. Ezek egy része külön információszerző tevékenységet igényel, míg másik részét a már korábban megszerzett másik két célinformáció-csoport alapján határozzák meg. A támadás végrehajtásához szükséges technikai feltételek tartalmazzák az infrastruktúra meglétét, többek között a különféle hálózati eszközöket (router, tűzfal), vezeték nélküli hálózatokat, VPN-t és az energiát is. A személyi feltétel magában foglalja a támadás megvalósításának egyik elengedhetetlen feltételét, vagyis azt a személyt, aki magas szintű technikai tudásának köszönhetően képes végrehajtani az adott támadást. A tárgyi feltételek a támadás kivitelezéséhez szükséges eszközöket, berendezéseket, szervereket és szoftvereket jelentik. A pénzügyi feltételek az előbb említettek beszerzéséhez, megszervezéséhez szükséges anyagi forrásokat jelölik. Ezen információk megszerzését követően lehet összeállítani a támadás konkrét végrehajtási tervét, amely az előbbiek alapján tartalmazza a támadást kivitelezők körét, az ehhez szükséges technikai, infrastrukturális, tárgyi, pénzügyi feltételeket, a támadás konkrét időpontját, helyét, cselekvési tervét és a támadás konkrét célját.[16]

Összességében megállapítható, hogy az információszerző támadások segítségével megvalósuló sebezhetőségek, sérülékenységek feltárása azért kiemelkedő jelentőségű, mert ennek tudatában a támadó fel tudja mérni, hogy egy további támadást pontosan hol kell végrehajtani. Abban az esetben, ha az információszerzés során sikerül feltárni a célpont sebezhetőségét, például informatikai rendszerében vagy akár a szervezet egy alkalmazottjában, akkor a támadó egy sokkal személyre/szervezetre szabottabb támadást tud megvalósítani.

2.1.2.2. Információ végrehajtott egyéb művelet

Egy kibertámadás számos információn végrehajtott műveletre irányulhat, többek között az információk megváltoztatására, továbbítására, nyilvánosságra hozatalára, zárolására, törlésére, valamint új információk rögzítésére az adott rendszerben. Ezen támadások motivációja a végrehajtás céljától függ. Például, ha a támadó célja a nyilvánosságra hozatal, akkor motiváció lehet, hogy a szervezet eltitkolt valamilyen (pl. kényes, a szervezet megítélését negatívan befolyásoló stb.) információt, vagy saját érdekeinek érvényesítése érdekében félre akarja vezetni a nyilvánosságot. Az információk törlése esetén a támadó motivációja lehet, hogy eltitkoljon egy számára kényes információt, míg zárolás esetében egyaránt motivációnak tekinthető a félrevezetés és a hátráltatás is.

2.1.2.3. Hátráltatás, működéskorlátozás

A kibertámadások további célja lehet a hátráltatás, illetve valamely szolgáltatás, infrastruktúra, szervezet működésének korlátozása. Sok esetben a támadó elsődleges célja a szervezeten belüli rendszerek, programok rendeltetésszerű működésének, használatának a korlátozása. A támadó motivációja, hogy hátráltassa az adott szervezetet a hatáskörébe tartozó tevékenysége elvégzésében, valamint korlátozza a szervezet által nyújtott szolgáltatás használatát, amely további károkat okozhat a szervezetnek.

A támadás irányulhat valamely kritikus infrastruktúra vagy kritikus információs infrastruktúra működésének korlátozására is, amely rendkívül veszélyes, hisz ennek következtében a társadalom működéséhez alapvetően szükséges állami és közintézmények, illetve a létfontosságú rendszerelemek leállhatnak, a szolgáltatások pedig akadozhatnak. A korábbi 2080/2008. (VI. 30.) kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról a következőképp definiálta a kritikus infrastruktúra fogalmát: „*Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó,* interaktív *és*

[16] Uo.

egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában." [17] A 2012. évi CLXVI. törvény már létfontosságú rendszerelemként definiálja a korábbi kritikus infrastruktúrákat. A törvény szerint létfontosságú rendszerelemnek tekinthetők azok a rendszerek, illetve rendszerelemek, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához (például az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális szolgáltatások biztosításához), és amelynek kiesése jelentős következménnyel járna.[18] Ezzel kapcsolatosan szükséges kitérni a kritikus információs infrastruktúrák fogalmára is: *„Az információs társadalom működéséhez szükséges információk előállítására, szállítására és felhasználására különböző rendeltetésű, funkciójú és típusú infrastruktúrarendszerek, hálózatok állnak rendelkezésre. Ezek összessége képezi az információs társadalom komplex információs infrastruktúráját."*[19]

A kritikus infrastruktúrák működésének korlátozására irányuló támadások egyik legismertebb példája a STUXNET. Ez olyan káros szoftver, amelyet célzottan ipari vezérlőrendszerek megfertőzésére, manipulálására és rombolására fejlesztettek ki. Alkalmazásának elsődleges célja Irán atomprogramjának lassítása volt, úgy, hogy meghibásodásokat idézett elő azáltal, hogy leégette az urándúsító centrifugák egy részét (kb. 20%-át), amelynek következtében Irán 2010 novemberében le is állította az urándúsító működését.[20]

A támadók célja lehet továbbá a különféle infokommunikációs megoldások (pl. internetes fizetés, bankkártya-használat) széles körű elterjedésének, alkalmazásának hátráltatása, korlátozása is. Ez a módszer azonban az adott pénzintézetre, illetve a szolgáltatás üzemeltetőjére nézve különösen hátrányos, hiszen ebben az esetben nemcsak a szolgáltatás akadályozása okozhat problémát, hanem az ügyfelek bizalma is megrendülhet.

A fentebb említett eseteken kívül a támadás a döntéshozatali folyamatok hátráltatását is célozhatja, például úgy, hogy a támadó a döntéshez szükséges információkhoz való hozzáférést ellehetetleníti, hamis információkat szolgáltat a döntéshozó számára, vagy módosítja a már meglévő információkat.

2.1.2.4. Érdekérvényesítés – befolyásolás

Előfordulhat, hogy a támadó célja az áldozat befolyásolása, hiszen a befolyásolhatóság egy olyan emberi tulajdonságunk, amelynek kihasználásával a másik fél számtalan előnyhöz juthat. Ezen módszernek többféle eszköze lehet: a meggyőzéstől kezdve a megfélemlítésen át a megvesztegetéssel bezárólag.

Például sokkal könnyebb befolyásolni egy olyan embert, aki valamilyen családi problémával küzd, vagy éppen a munkahelyi környezet kellemetlen számára. A megfélemlítés esetében, ha a támadó megtud valamilyen bizalmas információt a másik félről, ezzel próbálja rávenni az együttműködésre vagy befolyásolni egy konkrét döntés meghozatalában.

[17] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
[18] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, 1. § f)
[19] Várhegyi István – Makkay Imre: *Információs korszak, információs háború, biztonságkultúra.* OMIKK, Budapest, 2000.
[20] Gyebrovszki Tamás: *Stuxnet – mint az első alkalmazott kiberfegyver – A Tallini Kézikönyv szabályrendszere szempontjából.* 2014. http://hadmernok.hu/141_16_gyebrovszkyt.pdf (2018. 11. 04.)

A befolyásolás eszközével pedig akár olyan dolgokra is rávehető az áldozat, amit korábban saját gondolatai alapján nem tett volna meg, így például bizalmas információk szolgáltatására, illetve egyéb információkon végrehajtott műveletek elvégzésére, kártékony programok működésbe hozatalára, szolgáltatások, rendszerek leállítására, károkozásra vagy akár álhírek terjesztésére is. Ezenkívül a befolyásolás irányulhat a szemben álló fél információs eszközeire is, hogy ezáltal a támadó nyomást gyakorolhasson, valamint manipulálhassa az ellenfél információs rendszereit.

Érdekérvényesítés esetén a támadók célja sok esetben a kormányzat és a lakosság befolyásolása a saját társadalmi, politikai, vallási vagy akár ideológiai céljuk érdekében.

Ezen támadások esetén a támadó motivációja a kormányzat, a lakosság döntéseinek befolyásolása, valamint egy esetlegesen fennálló érdekellentét, illetve együttműködés hiányának megszüntetése.

2.1.2.5. Erőfitogtatás, figyelemfelhívás

A támadás célja lehet erőfitogtatás és figyelemfelhívás is, a támadást végrehajtók támadóképességeinek és -kapacitásainak szemléltetése a szemben álló fél számára. Ennek segítségével a támadó egyfajta betekintést nyújt a szemben álló fél számára arról, hogy milyen eszközök, források állnak a rendelkezésére egy további támadás megvalósítására, és célja, hogy ezáltal egyfajta fölényt tudjon kialakítani.

2.1.2.6. Szándékos károkozás

A támadás célja lehet szándékos károkozás is, melynek során a támadó a szemben álló fél információs rendszereit vagy például valamely információs infrastruktúra elemét célozva azok szándékos tönkretételére, megsemmisítésére törekszik. Ez történhet többek között az adott infokommunikációs eszköz, illetve információs rendszer fizikai károsításával, leállításával vagy akár kártékony programmal való megfertőzésével. A támadás motivációja lehet az előző pontokban említett erőfitogtatás és a szervezet egésze, illetve az általa nyújtott szolgáltatások működésének korlátozása is.

2.1.2.7. A sebezhetőségek, gyenge pontok feltárása

A támadás irányulhat a szervezet sebezhetőségeinek, gyenge pontjainak feltárására, amely történhet például betörési vagy más néven behatolási teszt segítségével.[21] A teszt során a „támadók" szimulált támadást, betörési tesztet hajtanak végre ellenőrzött környezetben, előre meghatározott célrendszerrel vagy programmal szemben. Ezen támadás célja a biztonsági kockázatok, az esetleges szabályozási hiányosság, valamint a felhasználói mulasztások feltárása. Ez a teszt a munkatársak számára is rendkívül hatékony, hiszen így a gyakorlatban, valós élethelyzeteken keresztül tanulhatják meg, hogyan reagáljanak a különböző támadásokra. A támadás végrehajtását követően a megvalósítás minden elemére kiterjedő jelentés készül, amely tartalmazza a támadás kivitelezésért felelős személy nevét, a támadás típusát, módszereit, az ehhez felhasznált eszközöket, a konkrét időtartamot és a szimuláció során feltárt biztonsági kockázatokat. A támadás mögött rejlő motiváció a hatékony és megfelelő szintű védelem kialakítása.

2.1.2.8. Oktatás, kutatás

A kibertámadások felismeréséhez és kivédéséhez szükséges, hogy a fejlesztőmérnökök, rendszergazdák megismerjék ezeket a támadásokat. Csak akkor lehet hatékonyan felkészülni esetleges támadásokra, ha tudjuk, mivel állunk szemben. Ezért célszerű nemcsak a klasszikus, de a legújabb módszereket is kipróbálni.

[21] Oroszi Eszter: *Social Engineering.* 2008, pp. 63–64. http://krasznay.hu/presentation/diploma_oroszi.pdf (2018. 10. 17.)

Klasszikus támadási technikák ellen (pl. SQL Injection, DDos) már kialakult védekezési mechanizmusok vannak, amelyeknek használata mára annyira evidens, hogy sokszor nem is emlékszünk arra, miért használjuk őket. Ezért fontos, hogy az oktatásban ismétlés gyanánt mindig előkerüljenek. Ne csak a megoldást adjuk a mérnökök kezébe, hanem a problémát is át kell adni, amire megoldást adunk. Ezáltal elkerülhető, hogy az elmúlt években megismert támadásokra újra lehetőséget adjunk a támadóknak.

A legújabb módszerek esetében gyakran nincs még biztos védekezési megoldás. Itt a kutatócsoportok jelentősége kerül előtérbe. Nem elég egy-egy probléma esetén befoltozni a megtalált támadási felületet: olyan megoldást kell találni, amely precízen bizonyított védelmet ad. Ezt csak mindenki által elfogadott bizonyítással lehet elérni, amelyet leggyakrabban akadémia publikációkban szokás közölni a nagyvilággal.

A legmodernebb malware-ek számítógépeink olyan alsóbb rétegeinek hibáira épülnek, amelyek megértése és megtalálása nem várható el egy egyszerű informatikustól (processzorüzenetek, memóriacímzések),[22] főleg nem olyan szakemberektől, akik más témakörben végezték tanulmányaikat. Komoly kutatási tevékenység egy-egy támadás végrehajtása, elemzése és annak feltérképezése, hogy milyen hibát használ ki a támadó. Továbbá egy-egy ilyen támadás végrehajtása kontrollált környezetben további zero-day[23] jellegű hibára deríthet fényt, melyek minél előbbi publikálása további támadásokat előzhet meg.

A támadás mögöttes motivációja az új eljárások, módszerek kidolgozása és gyakorlatban történő tesztelése, valamint a védekezési alternatívák, lehetőségek gyakorlása.

2.1.2.9. Anyagi haszonszerzés

A támadások jelentős részének célja a vagyoni haszonszerzés, amely számos social engineering[24] technikával megvalósítható. Ennek egyik módja az adathalászat, más néven phishing, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra.[25] A támadó motivációja ebben az esetben, hogy anyagi nehézségeit valamilyen módon enyhítse.

Összegezve: a támadók céljai igen sokrétűek lehetnek attól függően, hogy milyen motivációval rendelkeznek. Így jelen alfejezetben áttekintettük a különféle motivációkat és célokat, amelyek nagyban befolyásolják a támadás végrehajtásának eszközeit, módszereit, továbbá a támadás során alkalmazott lélektani módszereket, stratégiákat. Ezeket a következőkben mutatjuk be.

Elengedhetetlen, hogy mindennapjaink során megvédjük különféle információs, informatikai rendszereinket, alkalmazásainkat, eszközeinket és információinkat a jogtalan hozzáféréstől, illetve további káros műveletektől, támadásoktól. Ahhoz pedig, hogy ez a védelem sikeres lehessen, úgy gondolom, fontos, hogy mindenki megismerje a különböző támadási módszereket és az ezek mögött rejlő viselkedési stratégiákat, hiszen csak ezek tudatában lehet meghatározni, hogyan tudjuk megelőzni, megakadályozni a bizalmas információinkhoz való jogosulatlan hozzáférést, illetve hogyan

[22] Erre példaként szolgálhat a következő eset: https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw

[23] Nulladik napi támadás.

[24] Az ember manipulálásán, befolyásolásán alapuló támadási technika.

[25] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Nke Szolgáltató Kft., 2014, p. 51.

kell reagálnunk a már bekövetkezett eseményekre. A következőkben a támadók által leggyakrabban alkalmazott lélektani módszereket, viselkedési stratégiákat mutatjuk be.

2.1.3. A támadók lélektani módszerei, stratégiái

A támadók típusainak, motivációinak és céljainak ismertetését követően kerül sor az általuk gyakran alkalmazott lélektani módszerekre, beleértve a különféle emberi tulajdonságokat, amelyeket a támadó aktívan alkalmaz annak érdekében, hogy manipulálja, befolyásolja és megtévessze a célszemélyeket.

A különféle támadási technikák manapság már sokrétűek, egyik jellemző formájuk az emberi tényező és az infokommunikációs eszközök gyengeségeit, illetve sérülékenységeit együttesen kihasználó támadási módszer, a social engineering. A social engineering meghatározására számos definíció létezik.

Douglas P. Twitchell egyetemi professzor szerint a social engineering a csalás vagy rábeszélés gyakorlati alkalmazása bizonyos információk vagy ingóságok megszerzése érdekében.[26]
Kevin D. Mitnick az egyik leghíresebb hacker, a social engineering nagymestere. A legendás hacker című könyvében így határozza meg a social engineering fogalmát:

„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."[27]

Összességében elmondható, hogy a social engineer ugyanazokat a meggyőző technikákat alkalmazza, mint amelyeket mindannyian használunk a mindennapok során. Szerepeket veszünk fel, szívességeket teszünk másoknak. A támadó azonban manipulálja és megtéveszti az embereket, illetve etikátlan módon alkalmazza e technikákat, amelyekkel gyakran elsöprő sikert ér el. Így tehát felmerülhet a kérdés bennünk, hogy mitől lesz ő más, mitől dőlnek be neki az emberek, milyen stratégiát alkalmaz a megtévesztés sikeressége érdekében.[28]

Fontos megjegyezni, hogy a biztonságtudatosság nemcsak abból áll, hogy meghallgatjuk a különböző biztonságtudatossági tréningeket, oktatásokat, hanem ahhoz, hogy megértsük, az emberek miért sebezhetők a támadásokkal szemben, az első fontos lépés, hogy felismerjük, a támadó miért tud minket manipulálni, melyek azok a támadó által alkalmazott pszichológiai tényezők, tulajdonságok, amelyek miatt a támadása sikeres lesz.

A következőkben az ilyen típusú támadások során alkalmazott pszichológiai tényezőket, stratégiákat, viselkedési jellemzőket mutatjuk be, hiszen ha ezeket megértjük, könnyebben felismerünk egy esetleges befolyásolási, manipulálási kísérletet.

2.1.3.1. Szerepcsapdázás

Az első ilyen taktika a szerepcsapdázás. Lényege: a támadó feltárja az álcázás során választott szerepének viselkedési jellemzőit, hogy azonosulni tudjon a szereppel, illetve, hogy sikeres lehessen a támadás, ám a megtévesztés során az áldozat ebből csak néhányat lát, így a többit hozzáképzeli. Például, ha látunk egy férfit öltönyben, aki felsővezetőnek adja ki magát, automatikusan azt feltételezzük, hogy biztosan okos, megbízható, elfoglalt stb. A támadó szinte minden megtévesztésnél, illetve támadásnál szerepcsapdázást használt annak érdekében, hogy az áldozat a szerep további

[26] Twitchell, Douglas P.: *Social Engineering and Its Countermeasures. Handbook of Research on Social and Organizational Liabilities in Information Security.* Kennesaw, Georgia, USA, 2006, p. 228–242.
[27] Mitnick, Kevin D.: *A legendás hacker – A megtévesztés művészete.* Perfact-Pro, Budapest, 2003, borító.
[28] Mitnick, Kevin D.: *A legendás hacker – A behatolás művészete.* Perfact-Pro, Budapest, 2006, p. 280.

jellemzőire következtessen, és azoknak megfelelően cselekedjen. Gyakori csapdázási technikának minősül például a célpont főnöke vagy más munkatársak nevének említése, illetve az adott szervezetre/cégre jellemző szakmai nyelv használata, de ide tartozik még a támadó által megtestesíteni kívánt szerepre jellemző öltözet vagy egyéb kiegészítők (pl. céges toll) is. Ezek a módszerek mind a támadó által felvett szerep hitelességét sugallják, és ha a támadó hatékonyan alkalmazza őket, akkor az áldozat elfogadja a szerepét (vezető), és következtetni fog a többi jellemvonásra (megbízható, szavahihető, okos, gazdag stb.).[29] A szerepcsapdázás megelőzhető, ha például kérdések feltevésével pontosan megbizonyosodunk többek között a másik fél személyéről, beosztásáról, munkahelyéről, az információkérés okáról és az ehhez szükséges jogosultság meglétéről.

2.1.3.2. A szavahihetőség megteremtése

A következő stratégia, amelyet a támadók használnak, a szavahihetőség megteremtése, amely azért fontos, mert ez számít a legtöbb social engineering támadás első lépésének, illetve a bizalom kialakítása, hiszen minden további lépés erre épül. Dr. Brad Sagarin társadalompszichológus három olyan módszert nevez meg, amely a szavahihetőség megteremtésére alkalmas.[30] Az első ilyen technika szerint a támadó olyasvalamit mond, amely látszólag ellenkezik a saját érdekeivel. Ezt nagyon jól tükrözi az a példa, amikor a támadó felhívja az alkalmazottat, hogy kijavítsa a számítógépén lévő problémát, lefuttat néhány tesztet. Azzal kezdi, hogy látja azokat a billentyűket, amelyeket az áldozat lenyom. A támadó megkéri az áldozatát, hogy lépjen be a gépbe, a felhasználónév beírásakor pedig kéri, hogy mondja hangosan mit ír, ő pedig ellenőrzi, hogy tényleg azokat látja-e. Később, mikor az áldozatnak a jelszavát kell beütnie, azt mondja, hogy nem látja a betűket, csak csillagokat, a jelszava teljesen védve van, illetve megkéri, hogy ne mondja ki, milyen billentyűket nyomott le. Hozzáteszi, hogy soha ne mondja meg a jelszavát senkinek, még a rendszergazdának sem. Ezzel az utolsó mondattal hiteti el az áldozattal, hogy ő megbízható, tőle nem kell félni, miközben a támadó már meg is szerezte a jelszavát.[31] A másik, a szavahihetőség megteremtésére alkalmas módszer, amikor a támadó olyan esemény bekövetkezésére figyelmezteti a leendő áldozatot, amelyet a támadó fog okozni. Ilyen például, mikor a támadó figyelmezteti a munkatársat, hogy a hálózati kapcsolat leállhat. Ezt követően pedig el is követ valamit, hogy ez ténylegesen megtörténjen, az áldozat hálózati kapcsolata leáll, ez pedig megteremti a támadó hitelességét az áldozat szemében. A harmadik módszert az előzővel gyakran együtt használják: a támadó előre szól a bekövetkezendő problémáról, majd pedig segít megoldani, ezzel bizalmat és hálát keltve az áldozatban. Ezen módszerek megakadályozhatók, ha a bizalmas információk kezelésére szolgáló rendszerekben fellépő problémák orvoslására a szervezet valamely alkalmazottját kérjük meg, így elkerülhető, hogy szervezeten kívüli személy birtokába kerülhessenek belső vagy bizalmas információk.

2.1.3.3. Szerep ráerőltetése a célpontra

A social engineer egy alternatív szerep felvételére veszi rá a célszemélyt. Erre példa lehet egy zsarolás, mikor a támadó agresszív viselkedéssel kierőszakolja az áldozat engedelmességét. A legtöbb esetben azonban a segítőkész szerepbe kényszerítik az áldozatot, és ha valaki egyszer elfogadta ezt a szerepet, akkor általában kényelmetlennek vagy nehéznek találja, hogy visszakozzon belőle. Éppen ezért az előrelátó támadó megpróbálja kitalálni, hogy a célpont milyen szerepben érezné magát kényelmesen,

[29] Mitnick 2006, i. m. pp. 280–281.
[30] Uo., pp. 281–282.
[31] Mitnick 2003, i. m. pp. 118–120.

ezt követően pedig úgy irányítja a beszélgetést, hogy az áldozatot abba a szerepbe kényszerítse. Az emberek könnyebben vesznek fel pozitív hatású szerepeket, mint például a segítőkészség.[32]

2.1.3.4. A szisztematikus gondolkodástól való elterelés

Az ember kétféleképpen, szisztematikusan és heurisztikusan dolgozza fel a kívülről érkező információkat. Szisztematikus feldolgozás esetén a felénk érkező kérést alaposan, logikusan és racionálisan átgondoljuk, mielőtt meghoznánk a döntést. Amikor heurisztikusan gondolkodunk, akkor rövidített szellemi úton hozzuk meg a döntéseket, tehát például az alapján teljesítünk egy kérést, hogy ki kéri az adott információt tőlünk, kinek adja ki magát, és nem gondolunk abba bele, hogy a kért információ mennyire tekinthető bizalmasnak. Alapvetően szisztematikus módon próbálunk gondolkodni és döntést hozni olyan esetekben, amikor számunkra fontos vagy bizalmas információ iránti igényről van szó, ugyanakkor az idő nyomása, a sürgetés, a nyugtalanság, illetve az erős érzelmek a heurisztikus mód irányába vezethetnek minket. A támadók ezt úgy használják ki, hogy a manipuláció és a befolyásolás eszközeivel úgymond kiléptetik az áldozatot a szisztematikus módból, hiszen tudják, hogy heurisztikus gondolkodás esetén sokkal kevésbé valószínű, hogy gyanút fog, összezavaró, összefüggéseket ellenőrző kérdéseket tesz fel, vagy megakadályozza az információszerzést.

A támadók többféleképpen is képesek elérni a heurisztikus döntéshozatalt. Ennek egyik módja, mikor a támadó közvetlenül a munkaidőidő lejárta előtt hívja fel az áldozatot. Ebben a módszerben a támadó arra épít, hogy a munkahely időben történő elhagyása, esetleg egy további programról való elkésés miatti félelem és aggodalom következtében olyan kérés teljesítésére ösztönzi a célpontot, amit normális esetben nem tenne meg.[33] Ezen módszerek elkerülése érdekében fontos, ha valamely feladat elvégzésére vagy információ szolgáltatására kérnek minket, mindig alaposan, racionálisan és logikusan gondoljuk át, hogy ki az, akitől a kérés érkezik, rendelkezik-e a megfelelő jogosultságokkal akár az információ megszerzésére, akár pedig a feladat kiosztására, majd pedig ezen információk átgondolását követően hozzuk meg a megfelelő döntést.

2.1.3.5. Az engedékenység megalapozása

2.1.3.5.1. Ártalmatlan kérdések

A támadók kérések és kérdések sorát intézik az áldozathoz, kiemelten ügyelve arra, hogy ártalmatlan kérdésekkel kezdjék, ezzel alapozva meg az engedékenységet. Mivel az első kérdések ártalmatlannak tűnnek, olyan légkört teremt a támadó, amelyben az áldozat hajlamos bizalmasabb információit is ártalmatlanként kezelni.[34] Fontos, hogy minden kérdést alaposan gondoljunk át, különös figyelmet fordítva a személyes és bizalmas információk iránti kérdésekre, minden esetben mérlegeljük, hogy az adott információ kiadható-e harmadik fél részére, illetve hogy a másik félnek milyen célból van szüksége az adott információra.

2.1.3.5.2. A segítségnyújtás iránti vágy

A támadók sok esetben alapoznak a célszemélyek segítségnyújtás iránti vágyára, hiszen a legtöbb ember segítőkész. Szinte minden ember szívesen segít a nehéz helyzetben lévőknek, és együtt is érez velük. Továbbá az emberek nagy része megbízik a másikban, nem is sejtené, hogy az, aki például felhívja telefonon, megemlít pár belső információt, és használja a szervezeten belüli szakzsargont, esetleg egy támadó lehet, és éppen bizalmas információt próbál meg kicsalni belőle.[35] A

[32] Mouton, Francois et al.: *Socal engineering attack examples, templates and scenarios.* Computers and Security, 2016, pp. 186–209.
[33] Mitnick 2006, i. m. p. 283.
[34] Uo., p. 284.
[35] Oroszi 2008, i. m. pp. 31–33.

segítségnyújtás utáni pozitív érzések is nagyban hozzájárulnak ahhoz, hogy az emberek szívesen segítenek másokon. Ilyen például, ha segítséget adunk, erősnek érezhetjük magunkat, és jó érzéssel tölt el minket. Éppen ezért minden esetben alaposan át kell gondolni, hogy miben kérik a segítségünket, esetleg milyen információ szolgáltatására próbálnak rávenni minket.

2.1.3.6. Társított tulajdonságok

A társított tulajdonságok arra utalnak, ahogy az emberek saját és mások viselkedését magyarázzák. A támadó célja, hogy az áldozat bizonyos tulajdonságokat társítson hozzá, például szakértelmet, szavahihetőséget, őszinteséget, rokonszervet, megbízhatóságot vagy akár hitelességet. Erre tökéletes példa, mikor a támadó odasétál a recepcióshoz, letesz némi pénzt a pultra, és arra utal, hogy útközben találta, biztos valaki elveszítette. Ezt követően a recepciós olyan tulajdonságokat fog társítani a támadó személyéhez, mint az őszinteség, megbízhatóság és becsületesség. További példa, ha egy férfi idős hölgynek tartja az ajtót, esetleg segít cipelni a csomagjait, akkor könnyedén arra következtethetünk, hogy ez a férfi milyen udvarias és tisztelettudó. [36]

2.1.3.6.1. Rokonszenv

A támadók gyakran kihasználják, hogy nagyobb valószínűséggel segítünk, teljesítünk egy kérést olyan ember számára, akit kedvelünk, illetve aki iránt rokonszenvet érzünk. Ennek oka, hogy az emberek általában szeretik a hozzájuk hasonlókat, akikkel nagyrészt egyező érdeklődési körük, tanulmányi hátterük vagy akár hobbijuk van. Éppen ezért a támadó a célszemély felkeresése előtt utánanéz a hátterének, egyrészt azért, hogy felkészüljön, és érdeklődést tanúsítson a célszemély által kedvelt dolgok iránt, másrészt pedig, hogy ezen információk segítségével könnyedén kapcsolatba léphet, beszélgetést kezdeményezhet az áldozattal. A támadók gyakran használják az udvarlást, udvariasságot, megjelenésüket a rokonszenv kialakítására és fokozására. Ezenkívül a támadó azzal is kiválthatja a célszemély rokonszenvét, ha megemlíti egy a célszemély által ismert és kedvelt ember nevét, hiszen ez esetben a támadóra ismerősként tekint a célszemély.[37] Fontos: ha egy számunkra idegen személy kér tőlünk információt vagy segítséget, ne az alapján teljesítsük kérését, hogy milyen véleménnyel vagyunk az illetőről, mindig ellenőrizzük a kérés valódiságát, a kérő jogosultságát, hitelességét.

2.1.3.7. A félelem kihasználása

Ennél a módszernél a támadó elhiteti a célszeméllyel, hogy valamilyen szörnyű dolog fog történni, ami azonban elkerülhető, ha azt teszi, amit a támadó javasol. A támadó így használja ki, hogy áldozata fél a probléma bekövetkezésétől. Ilyen eset például, ha a támadó egy azonnal ellátandó feladattal bízza meg az alkalmazottat, és mindeközben hangsúlyozza a feladat elvégzésének fontosságát, a sürgős jelleget, illetve azt, hogy ha nem végzi el a feladatot, illetve nem osztja meg vele a szükséges információt, akkor bajba kerül, még akár ki is rúghatják.[38] Éppen ezért, ha valamilyen problémát jeleznek felénk, mindig bizonyosodjunk meg annak valódiságáról, és a szervezet szakemberétől kérjünk segítséget a probléma biztonságos megoldása érdekében.

2.1.3.8. Ellenállás

A pszichológiai ellenállás olyan negatív reakció, amelyet akkor tapasztalunk, ha úgy érezzük, hogy korlátozzák vagy elveszik választási lehetőségünket, esetleg szabadságunkat. Ez automatikusan negatív érzéseket vált ki belőlünk, és ennek következtében csökken a valós helyzetértékelési képességünk, mivel az elveszített dolog utáni vágy minden egyéb dolgot elhomályosít. Ilyen eset, mikor a támadó azt

[36] Mitnick 2006, i. m. p. 285.
[37] Mitnick 2006, i. m. pp. 285–286.
[38] Uo., p. 286.

mondja az áldozatnak, hogy a számítógépes fájlokhoz való hozzáférés nem fog működni meghatározott ideig, például két héten keresztül nem tud majd hozzáférni a fájljaihoz. Amikor a célszemélyből érzelmeket vált ki ez a jelenség, és érintetté válik, akkor a támadó felajánlja, hogy rövidebb idő alatt is képes helyreállítani a fájlokat abban az esetben, ha megadja a hozzáférési adatait, felhasználónevét és jelszavát. Az áldozatok jelentős része ilyenkor együttműködik a támadóval, és megadja belépési azonosítóit, annak reményében, hogy így jelentősen lecsökkenthető az akadályoztatás időtartama.[39]

Az ellenállás másik módszere, amikor a támadó valamilyen beígért előnnyel, haszonnal próbálja megtéveszteni áldozatát. Erre tökéletes példa a különböző nyereményjátékokat vagy ingyenes ajánlatokat hirdető áloldalak. Elméletileg mindenki tudja, hogy ingyen nem kaphatunk semmit, ennek ellenére az, ha valamit úgy ajánlanak fel, hogy ingyen van, mégis mindig csalogató. A legtöbben annyira vágynak az ingyen kapott dologra, hogy még csak bele sem gondolnak, hogy valójában miről szól az adott ajánlat.[40] Sok esetben az ilyen oldalak nyereményjátékot hirdetnek számtalan ajándékért cserébe, amiért ők csak azt kérik tőlünk, hogy regisztráljunk. Egyszerűnek tűnik, ám ha jobban megnézzük, milyen adatokat kér tőlünk az adott oldal, rögtön rájövünk, hogy ez már nem a felhasználónak kedvező ajánlatokról szól, hanem az adatainkról. Sajnos az emberek többsége nem látja be, ha valamilyen ingyen szolgáltatást ingyen kapunk, ez esetben mindig mi vagyunk a termék.

2.1.3.9. Az emberi természet hajlamai[41]

Ezek azok a hajlamok, amelyeket a támadók manipulálási kísérleteikben szándékosan kihasználnak. Ilyen például a *hatalom*, hiszen az emberek hajlanak eleget tenni a felettesüktől érkező kéréseknek, például sokkal könnyebb rávenni őket egy kérés teljesítésére, ha azt hiszik, hogy a kérés egy felettestől vagy egy ilyen kérés feltevésére jogosult személytől érkezik, tehát ha a támadó például egy másik osztály vezetőjeként mutatkozik be, inkább eleget tesznek kérésének, mintha például egy új munkatársként kérné ugyanezt.

Ilyen hajlam a *szeretet* is, hiszen az emberek könnyebben tesznek eleget az olyan kéréseknek, amelyek olyan emberektől érkeznek, akik képesek magukról kedvező, szeretetreméltó képet kialakítani, vagy akiknek látszólag közös az érdeklődésük, véleményük, erkölcs- és emberképük, mint az áldozatnak. Ezért a támadók sok esetben eljátszák, hogy az áldozattal azonos hobbijuk, érdeklődési körük vagy céljaik vannak az életben, illetve sok esetben a támadók megpróbálják a célpont viselkedését, tulajdonságait is utánozni, hogy a köztük lévő hasonlóság még nagyobb legyen.

A *kölcsönösség* szintén fontos a támadó számára, hiszen hajlamosak vagyunk automatikusan teljesíteni egy kérést, ha valami értékeset kapunk vagy ígérnek számunkra. Amikor valaki tesz értünk valamit, azt érezzük, hogy viszonoznunk kell azt, függetlenül attól, hogy kértük-e azt vagy sem. Éppen ezért az emberek befolyásolásának egyik legegyszerűbb eszköze, ha valamilyen ajándékot vagy segítséget adunk a leendő áldozatnak, amellyel viszonzásra kényszerítjük őt. Az ajándék lehet akár egy jó tanács, segítség, de akár tárgyi jellegű is, illetve ide sorolhatók például a korábban már említett hamis áloldalak, amelyeken valamilyen ingyen ajándékot ígérnek a regisztrációnkért vagyis az adatainkért cserébe. De tökéletes példa erre, ha egy magát rendszergazdának kiadó támadó felhívja az alkalmazottat, hogy a számítógépét vírus fertőzte meg, amelyre nem hatnak a gépén lévő antivírus szoftverek, ráadásul az összes fájt el is pusztíthatja. Az informatikus felajánlja segítségét, majd miután elmagyarázta a vírus eltávolításához szükséges lépéseket, megkéri, hogy próbáljon ki egy nemrég frissített szoftvert, amellyel a felhasználók megváltoztathatják a jelszót. Az alkalmazott nem akarja

[39] Mitnick 2006, i. m. pp. 286–287.
[40] Mitnick 2003, i. m. pp. 93–105.
[41] Uo., pp. 250–253.

majd visszautasítani a támadót, mert éppen most segített neki, és a segítségének hála nem vesztek el a gépen lévő fájljai, ezért azzal köszöni meg, hogy teljesíti a hívó kérését.

Egy másik fontos hajlam a *következetesség*, hiszen az emberek hajlanak a korábban nyilvánosan tett ígéreteik vagy vállalt kötelezettségeik teljesítésére. Ha megígértük, hogy megteszünk valamit, azt az állításunknak és ígéretünknek megfelelően be is tartjuk, mert nem akarunk megbízhatatlannak vagy esetleg felelőtlennek tűnni. Például a támadó felvilágosítja az új munkatársat, hogy a szervezet információs rendszerének használatához tiszteletben kell tartani a biztonságpolitikai irányelveket. A támadó közöl vele néhány biztonsági gyakorlatot, majd ellenőrzésképp megkérdezi az alkalmazott jelszavát, hogy az megfelel-e az előírásoknak, majd mikor az áldozat felfedte jelszavát, javaslatot tesz neki, hogy milyen módon alakítsa ki a jövőben a jelszavát, hogy ő azt könnyen kitalálhassa. Az áldozat engedelmeskedik, hiszen korábban beleegyezett, elfogadta a szervezeti biztonságpolitika szabályait (ezzel együtt a jelszó kialakítására vonatkozó irányelveket is).

Kiemelt jelentőségű a *társadalmi megerősítés*[42] hajlama is, hiszen az emberek hajlanak az olyan dolgok végrehajtására, amelyek összhangban vannak a többi ember cselekedeteivel. Mások tettei pedig megerősítik abban az áldozatot, hogy amit kértek tőle, azt nyugodtan megteheti, mert amit cselekszik, az helyes, hiszen a többi ember is hasonlóan jár el. Sok esetben előfordult már, hogy a támadó felhívta az alkalmazottat, hogy kutatást végez, és megnevez néhány alkalmazottat az osztályról, akik már szintén válaszoltak a kérdéseire. Így az áldozat azt gondolja, hogy mivel a többiek is ugyanígy cselekedtek, ezért ő is így tehet, a többiek közreműködése pedig megerősíti a kérés jogszerűségében. Az alkalmazott beleegyezik, a támadó pedig a sor kérdés közé belecsempész néhány olyan kérdést is, amelyre neki van szüksége.

A *szűkösség* hajlama azt jelenti, hogy az emberek könnyebben tesznek eleget olyan kéréseknek, amelyek valamilyen előnyhöz juttatják. Ilyen például, ha a támadó küld egy olyan e-mailt az alkalmazottnak, amelyben közli, hogy a cég új weboldalán az első 100 regisztráló ingyen jegyeket kap egy sikerfilmre. Amikor a felhasználó regisztrál az oldalra, és megadja a céges e-mail címét, a jelszóválasztás során sokan hajlamosak ugyanazt a jelszót megadni több helyre is. Így a támadó ezzel a megadott jelszóval megpróbálja feltörni az áldozat felhasználói fiókjait.[43]

A támadók által alkalmazott stratégiák bemutatása nélkülözhetetlen a támadó viselkedésének megértése és az ilyen típusú támadások elkerülése érdekében, hiszen a fentebb említett pszichológiai tényezők feltárásával könnyebben felismerjük ezeket valós, éles helyzetekben.

2.1.4. Social engineering technikák

A támadók által alkalmazott, az áldozatok megtévesztésére, befolyásolására és manipulálására alkalmas stratégiák ismertetését követően a következőkben néhány, ezen lélektani módszereket felhasználó social engineering technikát mutatunk be.

Fontos, hogy elhatároljuk a humán, vagyis az emberi megtévesztésen alapuló informatikai eszközök nélkül cselekvő technikákat és az IT, vagyis a számítógép alapú támadásokat. Az IT, vagyis az informatikai eszközök segítségével cselekvő technikák esetében a támadó valamilyen informatikai szoftver, program segítségével próbálja megtéveszteni és átejteni az alkalmazottat. Ez különösen kedvező a támadónak, hiszen nincs személyes kontaktus, ezáltal a lebukás veszélye is sokkal kisebb.

[42] Mitnick 2003, i. m. pp. 250–253.
[43] Mitnick 2003, i. m. pp. 250–253.

Ezen módszerek jellemzője, hogy a social engineer azt hiteti el az áldozatokkal, hogy valódi rendszerrel kommunikálnak, ezáltal pedig nem veszik észre, hogy csalás áldozataivá válnak.[44]

A humán alapú social engineering módszerek esetében a támadó nem a technológiai sérülékenységeket használja ki, hanem a felhasználó különböző tulajdonságait használja megtévesztésre. Ez ellen a módszer ellen nagyon nehéz védekezni, azonban ebben az esetben a támadónak is nehezebb dolga van, hiszen a támadást személyesen, szemtől szemben kell végrehajtania, ezáltal pedig a lebukás veszélye is sokkal nagyobb. A megtévesztésnek számos technikája létezik, a következőkben ezeket a módszereket ismertetem.

2.1.4.1. Segítségkérés

Számos bonyolult, hosszas tervezéssel járó social engineering támadás létezik, azonban sok esetben elég, ha csak megkérdezzük a kért információt az adott alkalmazottól, vagy éppen segítséget kérünk. A segítségkérés technikáját két csoportra lehet osztani: a rutin munkát végző alkalmazottaktól való segítségkérésre és a munkatársak segítőkészségének, naivságának, jóhiszeműségének kihasználására.

Rutin munkát végzőktől való segítségkérés

A segítségkérést eljátszó támadások funkciójukból fakadóan leginkább a help desk-en, titkárságon, ügyfélszolgálaton, recepción dolgozókat veszik célba, hiszen ők azok, akik napról-napra ugyanazt a típusú munkát végzik, emberekkel foglalkoznak, és általában hasonló megkeresésekkel találkoznak nap mint nap. Éppen ezért nem biztos, hogy ki tudják szűrni a valótlan megkeresést, vagy esetleg figyelmetlenségből nem veszik észre a napi rutin feladataik és a támadó kérése között különbségeket, ezáltal segítve a támadót. Sok esetben például úgy próbálják becsapni a dolgozót, hogy szándékosan megemlíti egy-két kollégájának a nevét, vagy az adott szervezeten belül gyakran használt szakkifejezéseket használja, ezáltal biztosítva, hogy ismeri a szervezetet, az abban lezajló folyamatokat és az embereket. Nyilván ez még nem jogosítja fel az alkalmazottat a belső információ kiadására, de azt sejteti, hogy a támadó valóban az, akinek mondja magát.[45]

A munkatársak segítőkészségének, naivságának, jóhiszeműségének kihasználása

A social engineerek sok esetben választják ezt a technikát, hiszen a legtöbb ember segítőkész. Szinte minden ember szívesen segít a nehéz helyzetben lévőknek, és együtt is érez velük. Továbbá itt kell megemlíteni azt is, hogy az emberek nagy része megbízik a másikban, nem is sejtené, hogy az, aki például felhívja telefonon, és megemlít pár belső információt, használja a szervezeten belüli szakzsargont, esetleg egy támadó lehet, és éppen bizalmas információt próbál meg kicsalni belőle.[46] Az alkalmazottak sok esetben jóhiszeműek és naivak, nem gondolják, hogy ez velük is megtörténhet.

2.1.4.2. Segítség nyújtása („fordított social engineering")

Sokszor előfordul ez a technika is, amikor a támadó kihasználja, hogy éppen egy problémával küszködünk, segítségre szorulunk, és ebben az esetben pont ő lesz az, aki tudja a megoldást, illetve akinek megvan a szükséges tudása, képessége és hajlandó is rá, hogy elhárítsa a problémát. Az esetek döntő többségében a támadó okozza, generálja a problémánkat, hogy ezt megoldva hálánkat kifejezve mi is segítsünk neki. Ezt a technikát fordított social engineeringnek is szokás nevezni, hiszen amikor az

[44] Deák Veronika: *Biztonságtudatosság az információs környezetben.* 2017, p. 62. http://www.knbsz.gov.hu/hu/letoltes/szsz/2017_3_szam.pdf (2018. 10. 21.)
[45] Sörös Tamás et al.: *Social engineering a biztonságtechnika tükrében.* 2013, p. 14. http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/Inform%C3%A1ci%C3%B3biztons%C3%A1g/TDK-Social_Engineering-Soros-Vaci_orszagos.pdf (2018. 10. 21.)
[46] Oroszi 2008, i. m. pp. 31–33.

alkalmazott a támadó segítségét kéri, már nem kell bebizonyítania hitelességét, szimplán csak meg kell oldania a felmerült problémát.[47]

Ennek a technikának a speciális esete a „*valamit valamiért*". Ilyenkor az előidézett hiba megoldása után a támadó kér egy szívességet, melyről tudja, hogy normál esetben nemleges választ kapna. Az ilyen fajtájú támadások sokkal jobban kihasználhatók különböző információtechnológiai megoldásokkal együtt. Például, ha hamis e-mailben vagy weboldalon keresztül valamilyen vonzó ingyenes tartalmat, például filmet, zenét vagy jellemzően valamilyen szexuális témájú képet vagy videót kínálnak regisztráció ellenében, akkor a kíváncsi felhasználó önként megadja e-mail címét, jelszavát. Abban az esetben vagy ha több oldalon is ugyanazt a jelszót használja, máris megszerezték a hozzáférést a többi az oldalhoz is.[48]

2.1.4.3. Identitáslopás

A humán alapú módszerek nagy többsége arra irányul, hogy a támadó egy másik személynek adja ki magát. Ez lehet valós vagy kitalált személy is, a lényeg, hogy a támadó azonosulni tudjon az adott szerephez.

Ennek a technikának több fajtája is van:

- *Álruhába bújás:* ebben az esetben a támadó egy másik személy (például rendszergazda, karbantartó, takarító, futár) bőrébe bújik, ezzel tévesztve meg az alkalmazottat. Ez több szempontból is előnyös a támadó számára, hiszen a kiválasztott személy szerepköre teljesen ideális számára, mivel ő választja ki a hozzá legtesthezállóbb „szerepet".[49] Másrészt az alkalmazott nem feltétlenül ismeri ezeket a típusú személyeket, vegyük például a karbantartót, a takarítót vagy éppen a futárt, ha azelőtt még nem volt dolga velük. Ennek a módszernek az egyik szélsőséges esete, ha a támadó egyenruhát visel, ugyanis ilyenkor nem ellenőrizzük, hiszen az egyenruha bizalomkeltő, egyfajta biztosítékot és megnyugvást ad számunkra.
- *Szervezeten belüli alkalmazottnak adja ki magát:* a szervezet nagyságától függően nem ismerhetünk minden kollégát, de az, hogy a támadó ugyanabban a szervezetben dolgozik, egyfajta bizalmat teremt, így könnyen adunk át bizonyos információkat.
- *Új munkatársnak adja ki magát:* ebben az esetben is a támadók arra helyezik a hangsúlyt, hogy egy nagy szervezet esetében nem ismerhetjük az összes dolgozót, főleg nem az új munkatársakat.
- *Fontos embernek adja ki magát:* ennek a technikának két fajtája van. Az egyik, mikor a támadó egy a szervezeten belüli személy bőrébe bújuk, mint például egy másik részleg, osztály vezetőjéébe. A másik esetben egy szervezeten kívüli személy lesz az álca, amikor is például egy hatósági személyt, külső auditort vagy ellenőrt személyesít meg a támadó.
- *Rendszergazdának/IT szakembernek adja ki magát:* ez a módszer nagyon hatásos lehet, hiszen az emberek nagy része csak felhasználói szinten ért a számítógépekhez és elektronikai eszközökhöz, így ha a támadó csak egy kicsit is ért az informatikához, és ismeri a különböző szakkifejezéseket, könnyen megtéveszthetí az alkalmazottakat.
- *„Sírkő lopás" – Tombstone theft:* ez egy ritka, de létező támadási módszer. A támadó egy már elhunyt ember bőrébe bújuk. Ez úgy történhet meg, hogy a halál beállta után nem azonnal és

[47] Mitnick 2003, i. m. pp. 55–75.
[48] Oroszi 2008, i. m. pp. 34–35.
[49] Sörös et al. 2013, i. m. p. 9.

nem automatikusan törlődik a különböző rendszerekből. Így például benne maradhat számos adatbázisban, illetve maradhat még akár bankszámlája is.[50]

- *Felhatalmazás:* ebben az esetben nem konkrét megszemélyesítés történik, hanem a támadó egy harmadik személyre hivatkozik. Ilyen például, ha egy szabadságon lévő alkalmazott hatalmazza fel a támadót, hogy határidőre készítsen el egy jelentést, amelyhez szükségesek bizonyos belső információk.[51]

2.1.4.4. A jelszavak kitalálása

A jelszavak kitalálásának és megszerzésének számtalan módja van. Ezek egy részét egy informatikai szoftver segítségével szerzik meg, míg másik részüket pedig az emberi figyelmetlenség, illetve hanyagság segítségével találják ki.

Fontos kitérni rá, hogy annak ellenére, hogy a felhasználói utasítások és biztonsági ajánlások/szabályzók kifejezetten hangsúlyozzák, sokan mégsem változtatják meg a kapott alapértelmezett jelszavukat. Ez komoly problémát okozhat, hiszen az ilyen alapértelmezett jelszavak – mint például a password, admin, 0000, 1234, 123456 – könnyen kitalálhatóak. Ez akkor is veszélyes lehet, amikor az adott szervezet egy új informatikai eszköz telepítését követően nem állít be új felhasználónevet és jelszót, hanem meghagyja az alapértelmezettet. Ez azért különösen veszélyes, mert a különböző internetes fórumokon ezekre az alapértelmezett, úgynevezett „default" jelszavakra egyszerűen rá is lehet keresni.[52]

Idetartoznak még a túl egyszerű vagy túl bonyolult jelszavak. Egyrészt ezek vagy könnyen kitalálhatók, vagy éppen nehézségük miatt általában valahova feljegyzik őket, így egy esetleges látogatás az irodában akár a jelszó rossz kezekbe kerüléséhez is vezethet.

Ezenkívül a jelszavak további fajtájába tartoznak a személyre utaló jelszavak. Ebbe a csoportba sorolhatók a személyünkhöz kötődő szavak, mint például a születési időpontunk, a szerelmünk, a gyermekünk neve, a kedvenc háziállatunk vagy éppen a hobbink neve. Ez azért veszélyes, mert a támadónak elég egy kicsit megismernie bennünket ahhoz, hogy megtudja ezek az információinkat.[53]

2.1.4.5. Baráti üdvözlet

Lehet, hogy odafigyelünk számos veszélyesnek tűnő jelre, és az ismeretlen címről érkező e-mailekkel nem törődünk, ám ha egy kedves barát küld nekünk üzenetet, azt automatikusan megnyitjuk, hiszen nem hisszük, hogy bármi veszélyt is rejthet. Azért nagyon veszélyes ez a technika, mert eszünkbe sem jut, hogy ez veszélyforrás, hiszen megbízható személytől kaptuk az üzenetet. Ahhoz pedig, hogy a támadó hiteles legyen, elég csak megnézni az alkalmazott közösségi oldalát, és rögtön talál számtalan barátot, akiket alapul véve elküldheti a vírust. Ha pedig nem is egy baráttól jön az üzenet, de például valamilyen ünnepi jókívánságot tartalmaz, akkor azt is automatikusan megnyitjuk a kíváncsiság jegyében, hogy vajon ki kedveskedhetett nekünk és mivel. Mindkét esetben megnyitjuk a csatolt mellékletet, és máris rákerült egy kártékony program az eszközünkre.[54]

2.1.4.6. Bejutás az épületbe

Ez a módszer kiemelten fontos biztonságtechnikai szempontból, hiszen ilyenkor a támadó észrevétlenül, a különféle beléptetőrendszerek kikerülésével jut be az épületbe.

---

[50] Sörös et al. 2013, i. m. p. 12.
[51] Uo., pp. 9–12.
[52] Uo., pp. 13–14.
[53] Sörös et al. 2013, i .m. p. 14.
[54] Mitnick 2003, i. m. pp. 96–98.

2.1.4.6.1. Tailgating – szoros követés

Ebben az esetben a támadó a bejutáskor egy csoporthoz kapcsolódik szorosan, és úgy tesz, mintha annak tagja lenne. Ehhez a technikához némi előkészület szükséges, meg kell érdeklődni, hogy mikor jön az adott társaság, és hogy maga a csoport milyen típusú. Hiszen nem mindegy, hogy egy takarítóbrigádhoz, építőipari munkásokhoz, szerelőkhöz vagy éppen egy partner szervezet alkalmazottaihoz kell csatlakoznia. Abban az esetben, ha a csoport túl kicsi, és mindenki ismeri egymást, akkor a támadó úgy is tehet, mintha a társaság egy elkésett tagja lenne.[55]

2.1.4.6.2. Hamis belépőkártya használata

Ez a technika már sokkal komolyabb előkészületeket jelent, hiszen ha beléptetőrendszer van az adott szervezetben, akkor speciális technika segítségével lehet csak a kártyákat hamisítani. Azonban ha nincs beléptetőrendszer, csak a kártyát kell lemásolni, hiszen a biztonsági őr úgysem nézi meg a szervezet összes alkalmazottjának a belépőkártyáját közelről, minden részletét megvizsgálva.[56]

2.1.4.6.3. Piggybacking – Más jogosultságának a felhasználása

Ebben a módszerben a támadónak nincs belépési jogosultsága az adott helyre, ezért kiadja magát egy másik személynek, akinek van, és jogosultságát felhasználva jut be a szervezet épületébe.[57]

Például a támadó eljátssza, hogy otthon hagyta a kulcsát vagy a belépőkártyáját, és kéri, hogy engedjék be.

2.1.4.7. Dumpster diving – „Kukabúvárkodás"

A technika lényege a kuka átvizsgálásában rejlik. Az emberek bele se gondolnak, hogy milyen értékes információkat tudhat meg róluk a támadó az irodai vagy otthoni szemetesük átvizsgálásával.[58] Elég csak kidobni egy havi bankszámla részletezőt, a social engineer már tudja is a bankszámlaszámunkat. De elég, ha csak a jelszavas cetli belekerül a kukába, és máris tudják a belépésünk kódját. Ezeken kívül számtalan olyan egyéb információt kidobhatunk, amely segítséget nyújt a támadónak például a személyiségünk ellopásához vagy kényes információk esetében a zsaroláshoz is.

2.1.4.8. Shoulder surfing – „Váll szörfölés"

Ez a módszer a jelszó vagy PIN kód megszerzésére alkalmas. A támadónak nem kell az alkalmazott bizalmába férkőznie, még csak beszélgetniük sem kell, elég, ha észrevétlenül – a technika nevéből adódóan – átnéz a válla felett, miközben begépeli a jelszavát vagy PIN kódját. Egyetlen lényeges eleme van csak, hogy közel kerüljön az munkavállalóhoz. A támadó kiadhatja magát például rendszergazdának vagy az informatikai részleg munkatársának, és megkéri az alkalmazottat, hogy jelentkezzen be majd ki a rendszerből, és miközben a jelszavát gépeli a dolgozó, könnyen kifigyelheti azt.[59]

Összegezve: a támadók által alkalmazott lélektani módszerek, stratégiák és támadási módszerek megismerése elengedhetetlen a hatékony és eredményes védelem kialakításához. Hiszen ha megismerjük a támadók által tanúsított magatartásokat, a különféle támadási technikákat, akkor sokkal könnyebben fel tudjuk majd ismerni azokat a valós, éles helyzetekben.

---

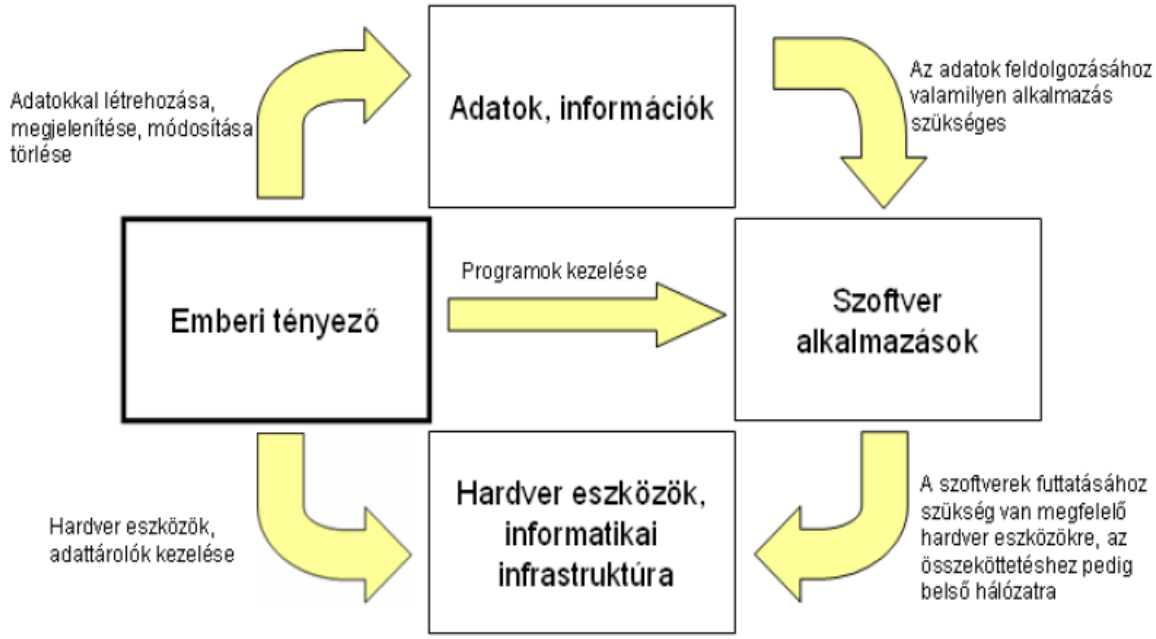
[55] Sörös et al. 2013, i. m. pp. 15.
[56] Sörös et al. 2013, i. m. pp. 15–16.
[57] Whitaker, Andrew – Evans, Keatron – Voth, Jack: *Chained exploits: Advanced Hacking Attacks from Start to Finish.* Pearson Education Inc., Boston, 2009.
[58] Oroszi 2008, i. m. pp. 37–38.
[59] Uo., p. 38.

2.2. A felhasználó lélektana

Napjaink egyik legnagyobb kihívását az információbiztonság megteremtése jelenti. Az infokommunikációs eszközök és rendszerek robbanásszerű fejlődésével a támadási technikák és módszerek is fejlődnek, éppen ezért szükségszerű, hogy az új támadási alternatívákkal szemben is felkészültek legyünk. Az információbiztonság megvalósítása érdekében a védendő értékeknek, mint például az információknak, a különféle alkalmazásoknak és informatikai rendszereknek, valamint az emberi erőforrás számára is megfelelő, hatékony és teljes körű védelmet kell biztosítanunk. A mai modern világunkban a különböző informatikai eszközök védelme már nagyon fejlett, így a támadó, ha például nem talál sebezhetőséget a felsőbb szinteken, mindig egy szinttel lejjebb fog menni, és addig csinálja ezt, amíg nem talál egy olyan pontot, amely sebezhető.

Sok esetben az informatikai rendszerek fejlett védelmének köszönhetően a bizalmas vagy érzékeny információk megszerzésére irányuló támadások a humán tényezőt célozzák. Éppen ezért felmerülhet a kérdés, hogy napjainkban, amikor a technológia már robbanásszerűen fejlődik, és naponta jelennek meg új és új fejlesztések, eszközök, mégis miért éppen egy állandóan változó, kiszámíthatatlan tényező áll a támadások középpontjában. A humán tényező fontossága abban rejlik, hogy ez a tényező van leginkább hatással a legtöbb védendő értékre,[60] amelyet az alábbi, 2. számú ábra tökéletesen szemléltet. Az emberi tényező kapcsolatban áll különféle belső és bizalmas információkkal, létrehozásuk, megjelenítésük, módosításuk vagy esetleges törlésük, megsemmisítésük érdekében számtalan művelet végrehajtására jogosultak. Ahhoz, hogy a felhasználó az adatokat fel tudja dolgozni, különböző alkalmazások, programok használatára jogosult, tehát a munkavállaló hozzáfér az alkalmazásokhoz mint védendő értékekhez. A szoftverek futtatásához szükség van megfelelő hardver eszközökre, az összeköttetéshez pedig a megfelelő belső hálózatra. A humán tényező a hardver eszközök és adattárolók kezelése érdekében hozzáfér egy másik védendő értékhez, az informatikai infrastruktúrához. Fontos megemlíteni, hogy a humán tényező hozzáférési jogosultsággal rendelkezik, számos adatbázis elérhető számára, számtalan belső és bizalmas információval rendelkezik, valamint az alkalmazottak kapcsolatban állnak egymással, ezáltal könnyedén oszthatnak meg információkat is egymással. Az alkalmazott ismeri az adott szervezet belső felépítését, amelyek hiába nem tekinthetők bizalmas információknak, ennek ellenére a támadónak kitűnő alapot nyújthatnak például a szervezet másik alkalmazottjának megszemélyesítésére.

[60] Flores, Waldo Rocha – Ekstedt, Mathias: *Shaping intention to resist social engineering through transformational leadership, information security culture and awareness.* Computers and Security, 2016, pp. 26–44.



2. ábra: Az emberi tényező hatása
Forrás: Leitold Ferenc: *Sebezhetőségvizsgálatok a gyakorlatban.* NKE Szolgáltató Kft., Budapest, 2014, p. 10.

2.2.1. A felhasználó kihasználható tulajdonságai

Az emberi tényező különféle kihasználható tulajdonságai miatt is kedvező célpontnak tekinthető. Ezek az alábbiak:

2.2.1.1. Segítőkészség

Számos, információk megszerzésére irányuló támadás épül az emberek segítőkészségére, hiszen ez a tulajdonság a legtöbb emberben benne van, ráadásul sokszor még olyankor is segítünk, ha előzőleg már valaki kihasználta ezt a tulajdonságunkat. E tulajdonság kihasználásával sokszor elég, ha a támadó egyszerűen csak megkérdezi a kívánt információt.

2.2.1.2. Reciprocitás, viszonzás

Sok esetben, ha valaki segítséget nyújt számunkra, akkor igyekszünk azt viszonozni, még akkor is, ha nem kértünk az adott személytől segítséget. Előfordulhat, hogy a támadó először valóban segít nekünk valamiben, és azután kér szívességet, például a támadó rendszergazdának vagy IT szakembernek adja ki magát, segít telepíteni vagy beállítani egy szoftvert, és csak ezután kéri el a jelszavunkat.[61]

2.2.1.3. Hiszékenység, naivság, kíváncsiság[62]

A hiszékenység is nagyon jellemző emberi tulajdonság, amely sokszor a segítőkészséghez is kapcsolódik. Megeshet, az alkalmazott elhiszi, hogy egy látszólag új munkatárs kér tőle segítséget, pedig közben lehet, hogy még csak nem is az adott szervezetnél dolgozik, szimplán csak jártas az adott területen. Másrészt sok esetben valójában nem hisszük el, hogy ez velünk is megtörténhet, illetve kíváncsiak vagyunk, ezért nem gondolunk bele az esetleges következményekbe vagy káros hatásokba.

[61] Németh L. Zoltán: *Pszichológiai manipuláció (Social engineering).* 2015. www.inf.u-szeged.hu/~zlnemeth/INFOSEC/AMKK_6_Pszichológiai_mainpuláció.pptx (2018. 10. 29.)
[62] Oroszi 2008, i. m. p. 20.

Továbbá az is jellemző, hogy ha kapunk egy érdekesnek, illetve fontosnak tűnő vagy netán ünnepi köszöntő tárgyú e-mailt, akkor az esetlegesen csatolt mellékleteket, valamint a különféle adathalász e-maileket, linkeket automatikusan megnyitjuk a naivitás és kíváncsiság jegyében, nem gondolva a veszélyekre. Számos esetben az alkalmazottak nem gondolnak arra, hogy a birtokukban lévő információ értékes lehet egy támadó számára, így nem is gondolják, hogy azt védeniük kellene.

2.2.1.4. Monotonitás, figyelmetlenség

Ha valaki például minden nap ugyanazt a rutin munkát végzi, minden nap ugyanolyan típusú feladatokat old meg, mivel nagyon sok hasonló kérés érkezik hozzá, nem biztos, hogy ki tudja szűrni a valótlan megkeresést, vagy esetleg figyelmetlenségből nem veszi észre a napi rutin feladatai és a támadó kérése között a különbséget.[63] A figyelmetlenség körébe lehet még sorolni a dolgozó íróasztalán felejtett különféle bizalmas információkat tartalmazó iratokat is, illetve azokat az eseteket, amikor az alkalmazott nem érzi magát jól a munkahelyén, ezért érdektelenségből nem foglalkozik azzal, hogy az adott megkeresés valós vagy sem.

2.2.1.5. Hanyagság

A hanyagság nagyon hasonlít az előbb említett figyelmetlenségre, azzal a különbséggel, hogy ebben az esetben a hanyag alkalmazottak tudatosan nem figyelnek oda feladataik szabályoknak megfelelő elvégzésére, a kapcsolódó információbiztonsági szabályok tartalmára, illetve betartására, éppen ezért kedvező célpontnak tekinthetők.[64]

2.2.1.6. Befolyásolhatóság[65]

A felhasználók befolyásolhatóságának kihasználása történhet meggyőzéssel, megfélemlítéssel vagy akár megvesztegetéssel. A befolyásolás sikerességéhez számos körülmény is hozzájárulhat. Ilyen például a munkahelyi környezet, amely esetében például sokkal könnyebb befolyásolni egy olyan alkalmazottat, aki nincs megelégedve a fizetésével, vagy éppen a munkahelyi környezet kellemetlen számára. A megfélemlítés esetében pedig, ha a támadó tudomására jut az alkalmazottról valamilyen kényes, érzékeny információ, akkor ezt kihasználva a bizalmas információ titokban tartásával veheti rá az együttműködésre a felhasználót.

2.2.1.7. A biztonságtudatosság hiánya

Abban az esetben, ha a felhasználók nem ismerik a különféle információk megszerzésére irányuló támadások technikáit, módszereit, felismerni sem fogják tudni azokat, valamint a védekezési alternatívákat sem tudják majd hatékonyan és eredményesen alkalmazni. Továbbá, ha a felhasználó nem ismeri a különféle információbiztonsági szabályokat, akkor az ezekből adódó mulasztásokat könnyedén kihasználhatja a támadó.[66]

2.2.1.8. A szakértelem hiánya

A szakértelem hiánya szintén hasonló problémákat eredményezhet, mint az előző tulajdonság. Fontos megemlíteni, hogy abban az esetben, ha az alkalmazott nem ért a munkájához, illetve csak felületes

[63] Oroszi 2008, i. m. p. 19.

[64] Deák Veronika: *A social engineering humán alapú támadási technikái.* 2017. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (2018. 10. 12.)

[65] Uo., p. 21.

[66] Deák Veronika: *A social engineering humán alapú támadási technikái.* 2017. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (2018. 10. 12.)

tudása van az elvégzendő feladataival kapcsolatban, akkor azt sem fogja tudni megállapítani, hogy mely adatokat és információkat kell bizalmasan kezelni, illetve mindezt hogyan lehet megvalósítani.

2.2.1.9. Elégedetlenség

Azokat a munkavállalókat, akik valamilyen okból kifolyólag elégedetlenek, például a feladataikkal, munkakörnyezetükkel, munkatársaikkal vagy akár a fizetésükkel, juttatásaikkal, sokkal könnyebb befolyásolni, valamint bizalmas információk kiadására buzdítani.

2.2.1.10. Fáradtság, túlterheltség

Azon alkalmazottak esetében, akik – munkahelyi vagy családi okból kifolyólag – fáradtak, illetve túlterheltek, sokkal könnyebb végrehajtani egy bizalmas információk megszerzését célzó támadást, hiszen nagy eséllyel nem veszik észre az átlagos, mindennapi feladatuk elvégzésére irányuló kérés, illetve az információ megszerzésére törekvő támadás közötti különbséget.[67]

2.2.1.11. Bosszúállás

Ha a dolgozó negatív érzéseket táplál a munkahelye iránt – például elbocsátják, vagy esetleg folyamatosan konfrontálódik egy felsőbb vezetővel vagy munkatárssal, aki ráadásul még a munkáját sem értékeli –, a bosszúállás számos módját alkalmazhatja. Ilyen például, hogy ezáltal könnyen megvesztegethető lesz, elad bizalmas információkat a konkurenciának, vagy esetleg a konkurens vállalatnál helyezkedik el, átadva az előző munkahelyen tapasztalt és megszerzett információkat, vagy akár nyilvánosságra hozza azokat. Sok esetben hiába vált munkahelyet a dolgozó, a rendszergazda vagy üzemeltető nem szünteti meg időben a korábbi hozzáférését, s hozzáférhet a régi információkhoz, mikor már az új munkahelyén dolgozik.[68]

Ezek mind olyan emberi tulajdonságok, amelyeket a támadó bizalmas információk megszerzése, módosítása, nyilvánosságra hozatala, illetve akár törlése vagy megsemmisítése céljából könnyen ki tud használni. Összességében elmondható, hogy hiába rendelkezik az ember számos kiszámítható tulajdonsággal, ha ismeri és betartja a biztonsági irányelveket és szabályokat, illetve megérti, hogy mások hogyan akarják befolyásolni bizalmas és belső információk megszerzése érdekében, akkor nagyobb eséllyel csökkenthető az információk biztonsági jellemzőinek megváltoztatására irányuló támadások. Az információbiztonsági szabályok betartása nagyban hozzájárul, hogy ne sérüljön az információk bizalmassága, sértetlensége és rendelkezésre állása, illetve a védendő értékek se sérülhessenek.

2.2.2. A generációk közötti különbségek[69]

Fontos kitérni a generációk közötti különbségekre, hiszen ezek jelentősen befolyásolják a felhasználók eszközhasználatát, biztonságtudatosságukat, illetve a védendő értékekhez való viszonyulásukat.

Az egyéneket az alábbi generációkba sorolhatjuk:

- „baby boom” korszak (1946 és 1965 között születettek)
- X generáció (1965–1980 között születettek)
- Y generáció (1980–2000 között születettek)
- a Z nemzedék pedig 2000-től napjainkig tart.

[67] Uo.
[68] Oroszi 2008, i. m. p. 22.
[69] Michelberger Pál – Lábodi Csaba: *Vállalati információbiztonság szervezése.* 2012, p. 281. http://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf (2018. 10. 29.)

Megállapítható, hogy a felhasználók korosztályonként eltérő információbiztonsági jellemzőkkel rendelkeznek. A „baby boom” korszakba tartozók kevésbé tudnak alkalmazkodni az információtechnológia fejlődéséhez, csak felnőttkorukban ismerkedhettek meg a különféle infokommunikációs eszközökkel, ezért jellemzően technikai és tudásbeli hiányosságaik is lehetnek. Az X generáció tagjai szintén csak életük során találkoztak ezzel a világgal, jobb esetben elfogadták és elkezdték használni a digitális világ új eszközeit; összességében elmondható, hogy sokkal nyitottabbak rá, mint a „baby boom”-osok. Az Y generációt jellemzi, hogy mivel a számítógépekkel együtt nőttek fel, életüket már el sem tudják képzelni a technológia nélkül, mindennapi életük nélkülözhetetlen részévé vált. A Z generáció tagjai pedig már beleszülettek a digitális technológiák világába, amelyben már elképzelhetetlen élni a különféle infokommunikációs eszközök nélkül. Számukra a közösségi média, az okostelefonok használata már egyfajta szükségletté vált. Jellemző rájuk továbbá, hogy napjaik nagy részét online töltik.[70]

A generációs különbségeknek kiemelt jelentőséget kell tulajdonítani az egyének információbiztonságban betöltött szerepe tekintetében, hiszen a korcsoportokhoz való tartozás jelentősen befolyásolja az infokommunikációs eszközök használatát, valamint a különféle információbiztonsági szabályok ismeretét, illetve az ezekhez való alkalmazkodási képességet. A probléma gyökerei a digitális bennszülöttek és a digitális bevándorlók fogalomköréhez vezethetők vissza. A digitális bennszülöttek azok a fiatalok, akik már beleszülettek abba a világba, amelyet egyre inkább meghatároznak a különböző digitális technológiák. Ezzel ellentétben a digitális bevándorlók azok a régebbi generációk, akik nem születtek bele abba a világba, amelyet egyre inkább meghatároznak a különböző digitális technológiák. Szinte alig töltenek időt az interneten, és nem igazán ismerik a legújabb technológiákat. Lényeges különbség a két fogalom és hordozói között, hogy míg az utóbbiak kevesebb időt töltenek az interneten, az előbbiek gyakorlatilag az IT világában „élik” életüket. Mobilon interneteznek, interneten barátkoznak, és órákat töltenek a számítógépek előtt, az egész életüket úgy élik le, hogy a digitális kor vívmányai (számítógép, okostelefon, tablet stb.) veszik körül őket. Mostanra világossá vált, hogy az őket körülvevő környezet és a környezettel való interakció gyakorisága miatt alapvetően másképp gondolkoznak, és másképp dolgozzák fel a környezetükből érkező információkat, mint elődeik. Addig, míg a digitális bennszülöttek ebben a digitális környezetben nőttek fel, a digitális bevándorlók tanulásuk során alkalmazkodnak ehhez a környezethez.[71] Éppen ezért elengedhetetlen az emberi tényező vizsgálata ebből a szempontból, hiszen a korábban említett korosztályok eltérő módon alkalmazkodnak az információs infrastruktúrához, a különféle hardverekhez és szoftverekhez, az alkalmazásokhoz, adatbázisokhoz, tehát az infokommunikációs világhoz. Éppen ezért fontos, hogy minden korosztály számára biztosítani kell – a hozzájuk illő módon – a szabályok ismertetését, alkalmazásának lehetőségeit, valamint a támadási és védekezési alternatívák bemutatását.

Összegezve, a generációs különbségek feltárása elengedhetetlen a megfelelő szintű információbiztonság kialakításához, hiszen a felhasználók korosztályonként eltérő képességekkel és készségekkel rendelkeznek az infokommunikációs eszközhasználatot, a biztonságtudatosságot, vagy akár az informatikai ismeretek megszerzését és a védendő értékekhez való viszonyulásukat illetően.

2.2.3. Az emberi mulasztás okai

Az információk bizalmasságának, sértetlenségének és rendelkezésre állásának sérülése az esetek jelentős részében valamilyen emberi mulasztás eredményeként következnek be. Az ember által

[70] Michelberger Pál – Lábodi Csaba: *Vállalati információbiztonság szervezése.* 2012, p. 281. http://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf (2018. 10. 29.)

[71] Marc Prensky: *Digitális bennszülöttek, digitális bevándorlók.* 2001, pp. 1–6. http://goliat.eik.bme.hu/~emese/gtk-mo/didaktika/digital_kids.pdf (2018. 10. 29.)

okozott károkat két csoportra lehet osztani, az egyik a tudatos, más néven szándékos károkozás, míg a másik a nem szándékos károkozás. Ezek okai igen különbözőek lehetnek.

Leggyakrabban a nem szándékos károkozás megvalósulhat gondatlanságból, személyes vagy munkahelyi problémák miatt kialakult figyelmetlenségből, a különféle szabványok, belső előírások, szabályok ismeretének hiánya miatt, valamint a képzetlenség, alkalmatlanság, hozzá nem értés és a szakértelem hiánya miatt. További okok közé sorolható a túl bonyolult munka vagy túl egyhangú munka miatti tévesztések, a különböző belső előírások, munkaköri leírások figyelmen kívül hagyása, a valós veszélyek fel nem ismerése, a felelőtlenség, a hibás munkavégzés, hanyagság, az előírások megszegése kényelmi okokból, a nem megfelelő előírások, szabályok alkalmazása vagy akár az ellenőrzések hiánya is.[72]

A tudatos károkozás az esetek döntő többségében akkor fordul elő, amikor például valakit megsértenek vagy esetleg elbocsátanak, ezért bosszúból rendszerismeretükkel vagy bizalmas információk kiadásával kárt okoznak. További okok közé sorolható a sértettség, rosszindulat, irigység, hirtelen felindulás, hírszerzés és ipari kémkedés támogatása vagy akár az információszerzés, anyagi vagy egyéb előnyökért.[73]

2.2.4. A biztonsági előírások szerepe

Napjainkban már minden szervezet rendelkezik valamilyen biztonsági szabályzattal, előírással. Ahány szervezet, annyi típusú szabályzattal találkozunk, de számos olyan előírás van, amelyeknek a szabályzatba való beépítésével és az alkalmazottakkal való ismertetésével a támadások bekövetkezésének valószínűsége csökkenthető. Az esetleges biztonsági előírások az alábbiak:

- fizikai biztonság/az épületbe való belépés ellenőrzése: a fizikai védelemre vonatkozó biztonságtechnikai szabályok megfelelő kialakítása (beléptetőrendszerek, biztonsági őrök);
- számítógépekre vonatkozó előírások: megfelelő jelszavak használata, a számítógép zárolására vonatkozó előírások, a különböző jogosultságok szintjének és az aszerinti hozzáférésnek a szabályozása, programok telepítésének korlátozása;
- hordozható eszközök kezelésére vonatkozó előírások: az adathordozók és hordozható számítógépekre vonatkozó megfelelő titkosítás alkalmazása, illetve az ezen eszközökön való adattárolás (pl. bizalmas adatok, személyes adatok) szabályainak meghatározása;
- leselejtezett eszközökre vonatkozó szabályok: ezek kezelésének, értékesítésének előírásai;
- hulladékkezelésre, iratmegsemmisítésre vonatkozó előírások: elektronikus és papír alapú hulladékok megfelelő kezelésének, megsemmisítésének szabályozása;
- felhasználók oktatásával kapcsolatos előírások: információbiztonsági oktatás;
- elektronikus levelezésre vonatkozó előírások: a levelezéssel kapcsolatos veszélyek ismertetése;
- telefonhívással kapcsolatos előírások: a különböző hívások-visszahívások szabályainak meghatározása (felettesektől érkező hívás, esetleges jelszavak a hívó fél azonosítására, értesítés gyanús telefonhívásokról).[74]

Fontos, hogy ezeket a szabályokat ne csak elkészítse az adott szervezet, hanem kiemelt figyelmet fordítson azok betartására is. A biztonsági szabályok elkészítését követően a legfontosabb a szabályok alkalmazottakkal történő megismertetése, melynek során tudatosítani kell a munkatársakban, hogy az ezen biztonsági előírások betartásával járó korlátozások az általuk végzett munka hatékonyságát és

[72] Schutzbach Mártonné: *Az informatikai biztonságot fenyegető tényezők.* 2003, p. 159. http://portal.zmne.hu/download/konyvtar/digitgy/nek/2003_2/12_schutzbach.pdf (2018. 11. 02.)
[73] Uo., p. 159.
[74] Oroszi 2008, i. m. pp. 65–69.

eredményességét is szolgálják. A szabályok bemutatása során ki kell térni az előírások okaira, mögöttes tartalmára is, hiszen ha az alkalmazottak megértik, hogy az adott szabály milyen célt szolgál, milyen fenyegetés, veszély elkerülése érdekében kell alkalmazni, akkor a betartásra vonatkozó hajlandóság is nagyobb lesz a körükben. Ezzel együtt a különféle veszélyekre történő felkészítés során konkrét, már korábban megtörtént esetekkel kell szemléltetni az adott szabály betartásának fontosságát. Rá kell mutatni arra, hogy az előírások miatti többletfeladat elvégzése, valamint az ezekre fordított idő is a biztonság kialakítását célozza.

Minden egyes szervezetnek az irányelvek írásbeli rögzítése mellett felelnie kell azért is, hogy a számítógépekkel dolgozó, illetve az anélkül dolgozó alkalmazottak is egyaránt tisztában legyenek az információk kezelésével kapcsolatos biztonsági szabályokkal. Az is lényeges, hogy az emberek a mögöttes tartalmat, az egyes szabályok alkalmazásának okát is megértsék, mert ha ezeket nem tudják, akkor az adott szabályt sem fogják érteni, így pedig nem alkalmazzák, s a támadó pont ez fogja kihasználni. Fontos, hogy az alkalmazottakat motiválni kell, hogy részt akarjanak venni a képzésen, illetve tudatosítani is kell bennük, hogy ez nemcsak a szervezet, hanem a saját érdeke is. A képzések kulcsfontosságú eleme, hogy minden olyan embert el kell érnie, akinek hozzáférése van a bizalmas információkhoz vagy a szervezet számítógépes rendszeréhez, illetve folyamatosnak kell lennie, és állandóan frissíteni kell, hogy az alkalmazottak naprakészek lehessenek a legújabb fenyegetések tekintetében is. A képzések fő célja, hogy minden alkalmazottban tudatosítsa, hogy a szervezetet bármikor támadás érheti, és hogy a bizalmas információk kiszivárgása elleni védelemben neki is részt kell vennie.

Ki kell térni a biztonsági szabályok szervezeten belüli ellenőrzésére és szankcióira is. Az előírások betartásában keletkezett hiányosságok és a kockázatok az információbiztonsági auditok segítségével tárhatók fel, mely során a szervezet informatikai rendszerének és más egyéb, kibertámadást érhető további területek felépítésének és működésének vizsgálata zajlik.[75] Ide tartozik a vállalat fizikai védelmének, a felhasználók képzésének, az informatikai eszközök és adathordozók kezelésének és a hozzáférés-védelemnek a vizsgálata is. Az audit során ellenőrzik, hogy a munkatársak hogyan alkalmazzák és tartják be a különféle biztonsági előírásokat és szabályokat. Ennek keretében a vizsgálat kiterjed:

- a vagyonvédelmi előírásokra (pl. infokommunikációs eszközök használatával kapcsolatos szabályok, beléptetés-csomagellenőrzés);
- az adathordozók és hordozható eszközök kezelésére vonatkozó szabályokra (pl. adathordozók kezelésére, eltávolítására, megsemmisítésére vonatkozó szabályok, USB portok letiltása, eszközök őrizetlenül hagyása);
- a hozzáférés-szabályozásra (pl. előre meghatározott jogosultságoknak megfelelő hozzáférés, jelszavak);
- a tiszta asztal és tiszta képernyő szabályra (pl. 5S módszer[76]);
- a fizikai biztonságra (pl. beléptetőrendszer – kártyamozgás);
- az adatvesztésre vonatkozó előírásokra (pl. biztonsági másolat készítése);
- a telefonhívással kapcsolatos előírásokra (pl. a hívó fél azonosítása);
- az elektronikus levelezéssel kapcsolatos szabályokra (pl. magáncélú levelezés tilalma).

[75] Shameli-Sendi, Alireza – Aghababaei-Barzegar, Rouzbeh – Cheriet, Mohamed: *Taxonomy of information security risk assessment (ISRA).* Computers & Security 57, 2016, 14–30. https://doi.org/10.1016/j.cose.2015.11.001 (2018. 11. 04.)

[76] Ez a módszer felelős a hatékony, biztonságos és minőségi munkavégzésre alkalmas, fenntartható munkakörnyezet kialakításáért és folyamatos fenntartásáért. Elemei: szükségtelen dolgok eltávolítása a munkaterületről, a szükséges dolgok logikus elhelyezése, a munkahely rendszeres takarítása, tisztán tartása, folyamatos felügyelés, ellenőrzés, a munkavállalók szemléletének kialakítása.

Az ellenőrzés során tapasztalt esetleges hiányosságokat, jó gyakorlatokat a vizsgálatot követően ismertetni kell az alkalmazottakkal. Ennek célja, hogy a feltárt gyenge pontok, biztonsági kockázatok és lehetséges következményeik bemutatásával a szabályok betartásának szükségessége tudatosuljon a felhasználókban.

Fontos, hogy a fentebb ismertetett biztonsági szabályokat nemcsak egy adott szervezetben dolgozóknak szükséges elsajátítani és betartani, hanem az átlagos felhasználók számára is hasznos iránymutatásként tekinthetők, ugyanis ezek betartásával jelentősen csökkenthető a kibertámadások bekövetkezésének valószínűsége.

2.2.5. Tudatosság

A tudatosság kialakításakor kiemelt figyelmet kell fordítani az alkalmazottak általi, az előbbiekben ismertetett biztonsági előírásokkal kapcsolatos előítéletek feltárására és azok kezelésére. Ennek érdekében a tudatossági képzések keretében külön ki kell térni a munkavállalók személyes véleményére, tapasztalataira és a szabályokhoz, valamint azok betartásához kapcsolódó hajlandóságukra. Ezek feltárását követően kerülhet sor ezen előítéletek, negatív meggyőződések feloldására. A feloldás szükségességét jelzi, hogy ennek hiányában az előítéleteknek köszönhetően az előírások betartása nem vagy csak részben valósul meg, a negatív meggyőződés kommunikációs nehézségeket és konfliktusokat generál. Az előítéletek csökkenthetők egy közös cél megfogalmazásával és a fontosságára történő rámutatással, amely jelen esetben az információbiztonság kialakítása és fenntartása. A feloldás részeként a munkatársakban tudatosítani kell a szabályok szükségességét és azt, hogy ezen előírások betartása az ő érdekükben is történik, illetve a hatékony és eredményes munkavégzés egyik alapfeltétele.

A tudatosság kialakítása során a döntési helyzetekkel kapcsolatos alapszabályok tisztázására is ki kell térni. Ennek keretében értelmezni kell a döntési helyzetek és folyamatok alapjait, amelyek a következők:[77]

- a döntési helyzetek felismerése,
- a döntéshez szükséges információk megszerzése, a bizonytalanságok csökkentése,
- alternatív cselekvési lehetőségek felvázolása,
- a cél megállapítása,
- a választási lehetőségek értékelése,
- a döntés lehetséges hatásainak felmérése,
- az esetleges kockázatok feltárása,
- a kockázatvállalás csökkentése,
- a vállalhatatlan kockázatok automatikus kizárása,
- a döntés meghozatala.

Összeségében elmondható, hogy elengedhetetlen az oktatási anyagok naprakészségének és minden felhasználó részére való hozzáférhetőségének biztosítása, valamint az oktatások megtartása, melyben:

- fel kell hívni a felhasználók figyelmét a szabályzat munkavégzésükre vonatkozó irányelveire és az ezzel kapcsolatos felelősségekre;
- ismertetni kell azokat a legfontosabb sebezhetőségeket, melyek a felhasználó adat- és rendszerbiztonságát veszélyeztető magatartását használják ki.

[77] Raffai Mária: *Döntéshozatal és döntéstámogatás – A döntési folyamat és a döntési folyamatot támogató rendszerek.* http://rs1.szif.hu/~raffai/org/dontesTamogat-2.pdf (2018. 11. 03.)

Minden új felhasználó számára a munkakezdést követően biztosítani kell az elektronikus oktatási anyag megismerését.

2.2.6. A biztonságra való törekvés mint együttműködés

Az alkalmazottakban erősíteni kell azt az érzést, hogy a biztonsági szabályok betartása és betartatása egyfajta együttműködés keretében valósul meg. Ennek célja, hogy a munkatársak az előírásokat ne csak azért kövessék és tartsák be, mert az kötelező, illetve az elhanyagolásuk súlyos szankciókkal sújtandó, hanem azért is, mert egy magasabb cél eléréséhez szükségesek. Fontos az alkalmazottak szabályok betartásával kapcsolatos belső motivációjának kialakítása, mely kiterjed arra is, hogy a munkatársak ne kényszerként, plusz teherként, hanem együttműködésként és közös célként éljék meg a szabályok követését. A betartás motivációi sokfélék lehetnek, az alkalmazottak egy része valamilyen jutalom reményében vagy szankciótól való félelem miatt tartja be a szabályokat. A cél az, hogy a munkatársak azonosuljanak a szabályokkal, az elsajátított szabályokat a sajátjukként éljék meg, és természetessé váljon azok mindennapos alkalmazása. Ennek megvalósulása elengedhetetlen, hisz így a munkavállaló szabálykövetése belső motivációjából fakad majd, beépül a személyiségébe, összefonódik már meglévő értékeivel, és természetessé válik ezen magatartás.

2.2.7. Az informatikai és IT biztonsági szakmai ismeretek szerepe

Az informatikai biztonság megteremtésének elengedhetetlen feltétele a felhasználók informatikai ismereteinek megléte. Abban az esetben, ha a felhasználók nem ismerik a különféle információk megszerzésére irányuló támadások technikáit, módszereit, felismerni sem fogják tudni azokat, valamint a védekezési alternatívákat sem tudják majd hatékonyan és eredményesen alkalmazni. Továbbá, ha a felhasználó nem ismeri a különféle információbiztonsági szabályokat, akkor a támadó könnyedén kihasználhatja az ezekből adódó mulasztásokat. Sok esetben előfordul, hogy az alkalmazott a szakmai ismeretek hiányára alapozva hárítja át a felelősséget valaki másra valamilyen információbiztonsági incidens bekövetkezése esetén, azonban fontos, hogy a szakmai tudás hiánya még nem jelent felmentést a szabályok betartása és az incidensek bekövetkezésének felelőssége alól.

Az alapvető szakmai ismeretek elsajátítása azért is nélkülözhetetlen, mert a mélyebb informatikai és IT biztonsági tudással rendelkező kollégákkal történő kapcsolat felvételének és az esetleges problémák elhárításának eredményességéhez nagyban hozzájárul a szakmabeliekkel való kapcsolatfelvételi képesség. A kapcsolatfelvételi hajlandóság pedig nagyban függ attól, hogy a munkatársak milyen alapismeretekkel rendelkeznek, ismerik-e a különféle szakkifejezéseket, ami nagyban hozzájárul a kapcsolattartás hatékonyságához.

Összességében megállapítható, hogy a felhasználók lélektanának mélyebb vizsgálata nélkülözhetetlen az információbiztonság kialakítása érdekében. Számtalan esetben az informatikai rendszerek fejlett védelmének köszönhetően a bizalmas vagy érzékeny információk megszerzésére irányuló támadások a humán tényezőt célozzák, éppen ezért a felhasználókkal kapcsolatos lélektani tényezők vizsgálata különösen indokolt. Ennek feltárása érdekében jelen fejezetben bemutattuk a felhasználók különféle kihasználható tulajdonságai, a generációs különbségek, az emberi mulasztás okai, a biztonsági előírások szerepe és lehetséges tartalma, a tudatosság, illetve a különböző szakmai és informatikai ismeretek elsajátításának fontosságát.

A következő fejezetben a szervezet vezetőinek információbiztonságban betöltött szerepét vizsgáljuk.

2.3. A vezető szerepe az információbiztonságban

2.3.1. A szervezet vezetőjére vonatkozó alapvető szabályok

A támadó és a felhasználó lélektanának és szerepének feltárást követően mindenképp ki kell térni a szervezetet vezető személyek funkciójának, felelősségének és az információbiztonságban betöltött szerepének vizsgálatára. A vezetők tanulmányozásának szükségességét igazolja, hogy a szervezetben döntéshozó pozíciókat töltenek be, ennek következtében nélkülözhetetlen szerepük van a különféle biztonsági szabályzatok elkészítésében, elfogadtatásában és mindennapos alkalmazásában. A vezetők alapvető feladatairól, felelősségeiről az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezik. A törvény 11. § 1. bekezdése alapján a szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről. A védelem biztosítása magában foglalja:

- a jogszabályban meghatározott követelmények teljesülésének biztosítását az elektronikus információs rendszerre irányadó biztonsági osztály és a szervezetre irányadó biztonsági szint tekintetében;
- az elektronikus információs rendszer biztonságáért felelős személy kinevezését vagy megbízását;
- annak meghatározását, hogy a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra milyen szabályok vonatkoznak;
- az informatikai biztonsági szabályzat kiadását;
- az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról való gondoskodást;
- a rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén annak biztosítását, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel a jogszabályoknak és a kockázatoknak;
- az elektronikus információs rendszer eseményeinek nyomon követhetőségéről való gondoskodást;
- biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával a biztonsági eseményre történő gyors és hatékony reagálást és ezt követően a biztonsági események hatékony és eredményes kezelését;
- az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködő igénybevétele esetén gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek;
- a szervezet az adatkezelési vagy adatfeldolgozási tevékenységhez közreműködő igénybevétele esetén gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek;
- az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatását;
- az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket megtételét.[78]

[78] 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról, 11. § (1)

Az Ibtv. által rendezett vezetői feladatok tisztázása után a következőkben olyan jelenségeket mutatunk be, amelyek a vezetők információbiztonsági feladatainak ellátása során jelentkeznek.

2.3.2. A tétlenség jelensége

A vezetők információbiztonságban betöltött szerepének vizsgálata során mindenképp ki kell térni a tétlenség jelenségére. Sok esetben előfordul, hogy vezetői döntés alapján a szervezet nem költ a megfelelő és hatékony biztonság kialakítására. A biztonság hiánya több problémát is felvethet. Vezethet egyrészt adatvesztéshez, a különféle belső vagy bizalmas információk nyilvánosságra kerüléséhez, illetve további adatokon végrehajtott művelet megvalósításához, mint például a szervezet kezelésében lévő információk módosításához, törléséhez, megsemmisítéséhez is. Másrészt hatékony védelem hiányában a szervezet által nyújtott szolgáltatások korlátozhatók, a szervezet által végzett munka hátráltatható, a különféle infokommunikációs eszközök használata – amelyeket az alkalmazottak a különböző feladataik elvégzéséhez használhatnak – akadályozható. Ez pedig komoly kiesést jelent a szervezet számára a költségvetés és a munkaerő szempontjából is, továbbá a szervezet szolgáltatásainak korlátozott elérhetősége, illetve elérhetetlensége miatt kialakult bizalomvesztés is jelentős hátrányt okozhat a szervezetnek. Abban az esetben, ha személyes adatok kerülnek jogosulatlan személyek kezébe, további bűncselekmények végrehajtására is szolgálhat, amely csak még tovább erősíti a bizalomvesztést és a szervezet iránti esetleges elköteleződés hátráltatását is. Sok esetben a vezetők úgy vélik, hogy addig nem költenek a biztonság kialakítására, míg nem történik komoly incidens, ám fontos kiemelni, hogy a biztonság egyfajta befektetésként és biztosításként is értelmezhető. Gondoljunk csak bele: lehet, hogy a megfelelő biztonság megteremtése komoly anyagi ráfordítást igényel, azt azonban nem szabad elfelejteni, hogy a hatékony védelem megvalósításával sokkal nagyobb összeg megspórolható, mint amit egy incidens bekövetkezése esetén a károk helyreállítása, az esetleges munkaerő és munka kiesése miatt, valamint az információk jogosulatlan felhasználása következtében ért káros hatások felemésztenek. Ezenkívül a különféle adatvédelmi és információbiztonság szabályok betartásának elmulasztása komoly szankciókat, bírságokat vonhat maga után. Éppen ezért elengedhetetlen a szervezet számára a hatékony és eredményes védelem kialakítása, amely többek között magában foglalja a különféle információbiztonsági és adatvédelmi szabályok, előírások, biztonsági intézkedések kidolgozását, betartását, az informatikai biztonság megteremtését, a sebezhetőségek, sérülékenységek folyamatos feltérképezését (például audit, behatolási teszt segítségével) és orvoslását, illetve az alkalmazottak biztonságtudatosságának kialakítását és fejlesztését.

2.3.3. Az információbiztonság kultúrája

Az információbiztonság szervezeten belüli kultúrájának kialakításában elsődleges szerepet játszik a szervezet vezetője. Ennek egyik oka, hogy a vezető felelős a különféle információbiztonsági értékek megfogalmazásáért, illetve az alkalmazottak irányába történő közvetítéséért, valamint ezek tudatosításáért.

Az ISO 27001 szabvány rendelkezik a szervezet felső vezetéséről is, mely szerint bizonyítania kell vezetői képességét és elkötelezettségét az információbiztonsági irányítási rendszer (továbbiakban: IBIR) irányába. A szervezet az információbiztonsági-irányítási rendszer keretében az információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzését végzi egy kockázatkezelési folyamat segítségével.[79]

[79] Magyar Szabványügyi Testület: Az információbiztonság irányítási rendszerének (ISMS) MSZ ISO/IEC 27001:2014 szerinti tanúsítása. http://www.mszt.hu/web/guest/msz-iso-iec-27001 (2018. 11. 03.)

A rendszer bevezetése csökkenti a visszaélések, valamint a szervezet kezelésében lévő belső és bizalmas adatok jogosulatlan kezelésének, felhasználásának kockázatait, biztonságosabbá teszi a szervezet külső kapcsolatait, megteremti a bizalmat az ügyfelek részéről, és az összehangolt adatvédelmi folyamatok révén biztosítja az ügymenet folytonosságát egy esetleges incidens bekövetkezése esetén is. A felső vezetés látja el az IBIR felső szintű irányítását, felel a működéséért és az eredményességért. Fontos, hogy a felsővezetés felelős az információbiztonsági politika megalkotásért, amelynek meg kell felelnie a szervezet céljainak. Az információbiztonsági politika tartalmaz információbiztonsági célokat, vagy kijelöli annak kereteit, magában foglalja az elkötelezettséget az információbiztonsággal kapcsolatos követelmények teljesítésére, illetve az IBIR folyamatos fejlesztésére vonatkozóan. Az információbiztonsági politikát dokumentált formában kell elkészíteni, valamint a szervezet és az érdekelt felek rendelkezésre kell bocsátani.[80] Ezen dokumentumok elkészítése a szervezet alkalmazottai és külső szereplők felé is sugallja a szervezet és a vezető információbiztonság iránti elköteleződését. Ezenkívül az ISO 27001 szabvány részletezi a vezetői képesség és elköteleződés alapvető szabályait.

Ezek alapján a felsővezetésnek bizonyítania kell vezetői képességét és elkötelezettségét az információbiztonsági irányítási rendszer vonatkozásában:

- annak biztosításával, hogy meg legyen adva az információbiztonsági politika és az információbiztonsági célok, valamint hogy ezek összhangban legyenek a szervezet stratégiai irányaival;
- annak biztosításával, hogy az IBIR követelményei beépüljenek a szervezet folyamataiba;
- annak biztosításával, hogy az IBIR-hez szükséges erőforrások rendelkezésre álljanak;
- azzal, hogy kommunikációt folytat az eredményes információbiztonság-irányítás és az információbiztonsági irányítási rendszer követelményeinek való megfelelés fontosságáról;
- annak biztosításával, hogy az információbiztonsági irányítási rendszer elérje várt eredményeit;
- azzal, hogy irányítja és támogatja a személyeket az információbiztonsági irányítási rendszer eredményességéhez;
- azzal, hogy előmozdítja folyamatos fejlesztését, és
- azzal, hogy támogat más fontos vezetői szerepet ellátókat abban, hogy bizonyíthassák vezetői képességüket saját felelősségi területükön.[81]

Összességében tehát elmondható, hogy a vezetőnek elkötelezettséget kell mutatnia az információbiztonság egészére vonatkozóan, valamint az ezzel kapcsolatos követelmények teljesítését és az információbiztonsági irányítási rendszer folyamatos fejlesztését illetően. A vezetői elköteleződés alkalmazottak irányába történő közvetítése elengedhetetlen ahhoz, hogy a munkatársakban is kialakuljon ez a fajta elkötelezettség, amely nagyban hozzájárul az alkalmazottak szabályok betartásával kapcsolatos belső motivációjának kialakításához. A belső motiváció szabálykövető magatartáshoz vezet, melynek során nem kényszerként és teherként élik meg az információbiztonságot, és melynek révén kialakítható egyfajta közösségi szellem is az információbiztonság folyamatos fenntartása és fejlesztése érdekében.

2.3.4. A biztonság szervezeti és szabályozási környezete

A felhasználók lélektanának vizsgálata során már említettük a különféle biztonsági szabályokat és előírásokat, illetve azt, hogy a megfelelő alkalmazás érdekében a szabályozási környezet kialakításakor

[80] Horváth Zsolt László: *Információbiztonsági belső auditor.* 2016, pp. 38–43. http://docplayer.hu/18071499-Informaciobiztonsagi-belso-auditor.html (2018. 11. 04.)
[81] Uo., pp. 38–43.

és fenntartásakor mire kell összpontosítani. Ezenkívül azonban érdemes kitérni arra is, hogy milyen további követelmények megvalósulására kell figyelni a tervezés során. A szabályozás azért rendkívül fontos, mert ezen keresztül testesül meg azon vezetői akarat és elkötelezettség, amely meghatározza az alkalmazottak viszonyát a szervezet kezelésében lévő adatok, információk bizalmasságának, hitelességének, sértetlenségének és rendelkezésre állásának megőrzéséhez.

A biztonsági szabályozás meghatározza az információbiztonság és az informatikai biztonság területein alkalmazandó védelmi alapelveket, amelyek hozzájárulnak a zárt, teljes körű, folytonos és kockázatokkal arányos védelem kialakításához és folyamatos biztosításához. A szabályozás hozzájárul a biztonsági előírások, intézkedések egységes értelmezéséhez.

A szabályozási környezet kialakításakor az első lépés azon kockázatok és lehetőségek meghatározása, amelyek hatással vannak a szervezet információbiztonságára, illetve amelyek segítségével megelőzhetők és csökkenthetők a nem kívánt káros hatások, illetve következmények. A kockázatok azonosítása során különös figyelmet kell fordítani az információk bizalmasságának, sértetlenségének és rendelkezésre állásának elvesztésével kapcsolatos kockázatokra a szervezet alkalmazási területén belül. A kockázatok meghatározásakor ki kell térni az esetleges következményekre, a bekövetkezés reális valószínűségére, valamint az információbiztonsági kockázatkezelési terv elkészítésére is. A szervezetnek meg kell terveznie az ezen kockázatokkal és lehetőségekkel kapcsolatos konkrét tevékenységeket, illetve azt, hogy ezek megvalósítása és a szervezet folyamataiba való beépítése hogyan, milyen formában valósul meg, továbbá hogyan történik ezen tevékenység eredményességének értékelése és ellenőrzése. A szabályozásnak egyértelműen tartalmaznia kell az információbiztonsági célokat, az elérésükhöz szükséges erőforrásokat, felelősségi köröket, határidőket, tevékenységeket és a célok megvalósulásának értékelését. Fontos, hogy a szabályozás elkészülését követően folyamatosan gondoskodni kell az alkalmazottakkal történő megismertetéséről és az esetleges frissítésekről, a naprakészen tartásáról. A vezető felelőssége, hogy az általa bevezetni kívánt szabályozást a munkavállalók elfogadják, egyfajta együttműködés keretében alkalmazzák, továbbá kialakítsa bennük a korábban említett szabályok betartásának belső motivációját, amelynek megvalósításához elengedhetetlen a megfelelő mennyiségű és minőségű kommunikáció.

A szabályozásnak tartalmaznia kell az információbiztonsági felelősségi körök kijelölését, konkrétan meghatározva a felelősöket és a hozzájuk tartozó tevékenységeket.

2.3.5. A biztonság mérése

2.3.5.1. A sebezhetőségek feltárása

Az első lépés a sebezhetőségek feltérképezése, hiszen csak ezek feltárását követően lehet a különböző irányelveket elkészíteni, módosítani, illetve a biztonsági intézkedéseket bevezetni. Fontos az alkalmazott eljárások folyamatos ellenőrzése és felülvizsgálata, illetve az emberek okozta sebezhetőségek feltérképezése egy általános információbiztonsági audit vagy akár egy betörésteszt segítségével.[82]

A sebezhetőség-vizsgálatoknak az alábbi területekre kell kiterjedniük:

- adminisztratív biztonság,
- személyi biztonság,
- fizikai és környezeti biztonság,
- hozzáférés-védelem,

[82] Oroszi 2008, i. m. p. 62.

- informatikai rendszer biztonság.

Külön figyelmet kell szentelni a korábbi felülvizsgálatok során vagy az adott időszakban észlelt hiányosságok vizsgálatára, a megvalósított védelmi intézkedések működőképességére.

2.3.5.2. Audit, felülvizsgálat

A védelem kialakításának fontos alkotóeleme, hogy felmérjük a jelenlegi helyzetet, feltérképezzük a sebezhetőségeket, hiszen a különböző óvintézkedések bevezetéséhez mindenképpen szükséges meghatározni azokat a területeket, amelyek különféle kockázatokat jelenthetnek. Ha feltártuk a hiányosságokat, a vizsgálatok eredményétől függően megkezdődhet a probléma orvoslása, ennek keretében további biztonsági előírások kidolgozása, a jelenleg alkalmazott szabályok esetleges módosítása, illetve az esetleges hiányosságok pótlása,[83] majd pedig a felhasználók biztonságtudatossági oktatása és az aktuális előírások ismertetése az audit során tapasztaltak függvényében. Összességében elmondható, hogy a hiányosságok és a kockázatok az információbiztonsági auditok segítségével tárhatók fel, csak akkor tudhatjuk meg, hogy egy konkrét támadás elleni védekezés hatékony és sikeres lesz-e a jövőben, ha ellenőrzéseket és vizsgálatokat végzünk. Tehát megállapítható, hogy az audit végrehajtása a védekezés szükségszerű elemét képezi.

Az audit fogalmának meghatározására számos definíció létezik.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerint az auditálás az előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés.[84]

Az auditokat kétféleképpen csoportosíthatjuk: egyrészt aszerint, hogy ki hajtja végre az adott auditot, másrészt pedig az audit tárgya szerint. Az audit tárgya szerint megkülönböztetünk rendszerauditokat, amikor az audit tárgya valamilyen irányítási rendszer (pl. információbiztonsági irányítási rendszer), ahol az audit azt vizsgálja, hogy ez az irányítási rendszer megfelel-e meghatározott követelményeknek (pl. az irányítási rendszer nemzetközi rendszerszabványának). Az audit tárgya szerinti csoportosítás második típusa a folyamatauditok, melyek esetében az audit tárgya az auditált szervezet egy kiválasztott folyamata vagy folyamatcsoportja, és az audit azt vizsgálja, hogy ezek megfelelnek-e az előre meghatározott elvárásoknak, illetve követelményeknek. A harmadik típust a termékauditok alkotják, melyek tárgya valamilyen kiválasztott termék vagy azok bizonyos jellemzői, és a követelményekhez viszonyított megfelelősségüket vizsgálják.[85]

Egy információbiztonsági audit keretében a szervezet informatikai rendszerének és más egyéb, kibertámadással fenyegetett területek felépítésének és működésének vizsgálata zajlik. Ide tartozik a vállalat fizikai védelmének, a felhasználók képzésének, az informatikai eszközök és adathordozók kezelésének és a hozzáférés-védelemnek a vizsgálata is.

A fizikai védelem vizsgálata alatt az általános biztonságtechnikai megoldásokat (pl. tűzvédelem), az alkalmazott beléptető és azonosítási eljárásokat, a külső alkalmazottak (pl. karbantartók) és látogatók (pl. ügyfelek, vendégek) kezelését értjük, és ezek alapos vizsgálata a cél. Az informatikai eszközök fizikai védelmén túl többek között felül kell vizsgálni a hozzáférés-védelmet, a megfelelő jelszavak használatát, a bizalmas adatok titkosított tárolását, illetve a kártékony programok elleni védekezés módszereit is.[86]

[83] Oroszi 2008, i. m. p. 62.
[84] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 1. § (1)
[85] Horváth 2016, i.m. pp. 17–18.
[86] Oroszi 2008, i. m. pp. 63–64.

2.3.5.3. Behatolási teszt

A szervezet alkalmazottai a behatolási vagy más néven betörési teszt végrehajtása során egy előre megszervezett támadás áldozataivá válnak.[87] Ez a teszt azért hatékony, mert ezáltal a munkatársak nemcsak elméletben tanulják meg, hogyan reagáljanak a különböző támadásokra, hanem a gyakorlatban, testközelből vizsgálják meg az adott támadást és az arra irányuló reakciókat is.

Az ezen munkavállalók biztonságtudatosságára alkalmas ellenőrzési módszerek során tapasztalt esetleges hiányosságok, gyenge pontok kiértékelését követően az eredmények ismertetése nélkülözhetetlen annak érdekében, hogy a jövőben ne fordulhassanak többet elő újra ezek a problémák. Ezenkívül azért is szükséges az értékelés, mivel ez egyfajta visszacsatolást is ad a szervezet vezetőjének és az alkalmazottaknak egyaránt arról, hogy a kialakított szabályozási és védelmi környezet mennyire működik hatékonyan és eredményesen.

Összegezve megállapítható, hogy a vezetők rendkívül fontos szerepet töltenek be a megfelelő szintű információbiztonság kialakításában, éppen ezért elengedhetetlen a vezetőkkel kapcsolatos feladatok és felelősségek mélyebb vizsgálata.

Az információbiztonság három fontos tényezőjének bemutatását követően a következő fejezetben a mindennapi feladatok ellátása során jelentkező problémákat, kihívásokat és veszélyeket szemléltetjük különféle esettanulmányok segítségével.

[87] Uo., pp. 64–65.

Esettanulmányok: az információbiztonsági tudatosság lélektani kihívásai a közigazgatásban

A következőkben az információbiztonsági tudatosság egyes lélektani kihívásait bemutató, megtörtént vagy lehetséges eseteket mutatjuk be konkrét problémákon keresztül.

3.1. A szervezeti szintű és az egyéni felelősség konfliktusa

A szervezeti szintű és az egyéni felelősség konfliktusának megjelenésére, valamint a felek által képviselt lélektani jellemzők bemutatására az alábbi két eset szolgál.

Az első esetben a konfliktus a szervezet tulajdonában lévő infokommunikációs eszközökre telepített operációs rendszerek központi frissítésén alapszik. A szervezetben alkalmazott infokommunikációs eszközök, számítógépek biztonsági, operációs rendszereinek frissítéseit csak központi úton lehet elrendelni, és ameddig ez nem történik meg, központilag nem engedélyezik a rendszerek frissítését, addig nem is kapják meg az esetleges biztonsági hibák kijavítását célzó javításokat az eszközök. Ezt a sérülékenységet használják ki többek között a spam-ek és a ransomware-ek.

A spammer programok elsődleges célja kéretlen e-mailek, illetve SMS üzenetek szétküldése a különféle hírlevéllisták és egyéb infokommunikációs eszközök felhasználóinak a fiókjaiba az azonnali üzenetküldő rendszerek levelezőlistái segítségével. A spam üzenetek jelentős részét arra használják a támadók, hogy adathalász támadást valósíthassanak meg az üzeneteken keresztül, és ezáltal jussanak bizalmas és személyes információkhoz.[88]

A zsaroló program, más néven ransomware célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsarolóprogramok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában. Ezt követően a támadó zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejében visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, a zsaroló kiterjeszti a fizetésre rendelkezésre álló időt, vagy törli az adatokat a felhasználó infokommunikációs eszközéről.[89]

Ezek a spamek és ransomware-ek sok esetben azt használják ki, hogy bár az adott operációs rendszerben felfedezett hibát már orvosolták, sok szervezetnél még nem futtatták le a patcheket, a frissítést, mert ennek engedélyezésének lefolytatása akár több napba is beletelhet. Ennek következtében az alkalmazottak olyan e-maileket is megnyithatnak, amelyek kártékony programot, például egy ransomware-t tartalmazhatnak. Jelen esetben a munkavállaló tudja, hogy a rendszert frissíteni szükséges, de a szervezeti szintű utasítás alapján a szervezet összes infokommunikációs eszközét csak és kizárólag egyszerre, vezetői döntés meghozatalát követően. Az alkalmazott tudja, hogy eszköze és a kezelésében lévő információk veszélynek vannak kitéve, hiszen a saját otthon számítógépén már lefuttatta az adott biztonsági hibát orvosló frissítést, azonban a munkahelyén ezt nem teheti meg. A konfliktus egyik oldala a szervezet vezetői szinten jelentkező érdeke, azon biztonsági szempontok érvényesítése, hogy a frissítés csak központilag valósulhat meg minden eszközön, miután megtörtént az adott frissítés jóváhagyása, biztonságának és megfelelőségének ellenőrzése. Ennek hiányában bárki bármit rátelepíthetne a szervezet infokommunikációs eszközeire, ami könnyedén vezethet kártékony programokkal történő megfertőzésükhöz. A konfliktus másik oldala a szervezet végrehajtói szintjén jelentkezik: az alkalmazott napi feladatainak elvégzése érdekében kénytelen

[88] Szőr Péter: A vírusvédelem művészete. SZAK Kiadó Kft., Bicske, 2010, p. 31.
[89] Yaqoob, Ibra – Ahmed, Ejaz – Imran, Muhammad: *The rise of ransomware and emerging security challenges in the Internet of Things.* Computer Networks, 6 September .2017. https://doi.org/10.1016/j.comnet.2017.09.003 (2018. 11. 12.)

megnyitni a beérkező leveleket, így előfordulhat, hogy olyan levelet is megnyit, és letölti tartalmát, amely akár kártékony programot, például egy ransomware-t is tartalmazhat.

A következő esetben tételezzük fel, hogy a munkavállaló az adóhatóság nyomozó osztályának munkatársa, s éppen egy összegző táblázatot készít az elkövetkezendő egy hónapban lefolytatandó ellenőrzésekről, felderítésekről. Mivel csúszásban volt a táblázat elkészítésével, ezért úgy dönt, elküldi az addig elkészült anyagot, valamint az ellenőrzésekről és felderítésekről rendelkezésre álló információkat tartalmazó dokumentumokat a saját magánhasználatú e-mail címére, hogy így ahhoz bármikor és bárhol hozzáférhessen, és amikor a szabadideje engedi – tömegközlekedési eszközön vagy akár otthon –, folytatni tudja az összegző táblázat szerkesztését, hogy időben elkészülhessen vele. Az alkalmazott azonban nemcsak a hatékony időgazdálkodás miatt küldte át a dokumentumokat a saját e-mail címére, hanem azért is, mert a szervezetüknél használt levelezőrendszerrel ellentétben a magán e-mail fiókja sokkal jobban optimalizált, több funkciót enged, kényelmesebb és könnyebb a kezelése, valamint egyéb hasznos kiegészítők is letölthetők hozzá, amelyek jelentősen megkönnyítik elvégzendő feladatait. Az adatok továbbításának köszönhetően az alkalmazottnak sikerült határidőre elkészíteni az összegző táblázatot, amelyet másnap továbbított is a felettesének. A munkatárs magáncélú e-mail fiókját feltörték, és hozzáfértek az oda továbbított, ellenőrzéseket tartalmazó listához. Később az adóhatóság nyomozói razziázni indultak egy olyan személyhez, aki valószínűsíthetően számos bűnszervezetben elkövetetett bűncselekményért felelős. Mikor a nyomozók megérkeztek a helyszínre, senkit nem találtak ott, valamint az épületet is teljesen kiürítették. Még azon a héten két próbavásárlás és egy hamis parfümöket áruló személy ellenőrzése során sem jártak sikerrel a nyomozók. Ezt követően a nyomozó osztály vezetői azon tanakodtak, vajon mi történhetett: a korábbi felderítő tevékenység során szerzett információk nem voltak eléggé megalapozottak, vagy esetleg információk szivároghattak ki a főosztályról. Megállapították, hogy az előzetes felderítések során szerzett információk hosszú hónapok munkájának eredményei, és az ennek során megszerzett bizonyítékok is azt mutatják, hogy a korábban megfigyelt egyének valóban bűncselekményt követtek el. A második variáció sem túl valószínű, hiszen a bizalmas adatok kezelésére nagyon szigorú szabályok vonatkoznak. Az osztály vezetője ezért megbeszélésre hívta munkatársait. A megbeszélésen feltárta a korábban történt problémákat, és elmondta a kollégáknak, arra keresi a választ, mi okozhatta az eredménytelen ellenőrzéseket. Elmondja, hogy a korábbi információszerzés a feltételezett gyanúsítottakról sikeres volt, így az ellenőrzés részleteire vonatkozó adatok nagy valószínűséggel valahogyan kiszivárogtak. Az alkalmazottak közül senki nem szolgált információval a vezetőnek az esetleges adatvesztést illetően. Pár nap múlva a korábban említett alkalmazott az e-mailjeit böngészte, amikor a spam mappában két olyan levelet is talált, amely arról szólt, hogy új bejelentkezés történt fiókjába egy számára ismeretlen eszközről. Az üzenetben szerepelt a bejelentkezés pontos időpontja is, s ekkor jött rá, hogy ő biztosan nem léphetett be hajnali 1 órakor a fiókjába. Másnap, mikor beért a munkahelyére, az irodában még mindig a sikertelen ellenőrzésekről beszélgettek a munkatársai, ekkor kapcsolta össze a hajnali belépést a fiókjába és a kiszivárgott adatokat. A munkatárs rögtön jelezte felettesének, hogy pár héttel ezelőtt továbbította a külső, magánhasználatú e-mail címére az ellenőrzéssel kapcsolatos információkat, illetve, hogy illetéktelen belépés történt a fiókjába. A szervezeti egység vezetője ezt követően közölte az ellenőrzést vezető nyomozóval, hogyan történhetett az adatok kiszivárgása, ami miatt a havi összegző táblázatban szereplő összes ellenőrzést fel kellett függeszteni. Ebben az esetben a konfliktus alapja, hogy a szervezeti szinten meghatározott a szervezet egészére vonatkozó biztonsági előírások és szabályok betartása nem valósult meg a végrehajtói szinten, tehát az alkalmazott szembement a kötelező szabályok egyikével, és ennek súlyos következményei lettek a szervezet alapvető feladatának ellátására nézve.

A fentebb felvázolt lehetséges esetek számos kérdést felvetnek:

- Ha az alkalmazott ismeri a szabályokat, és tisztában van azzal, hogy a szervezet kezelésében lévő információk továbbítása tilos, akkor miért vállalta a kockázatot?
- Hogyan kerülhető el a kártékony kódot tartalmazó e-mail-ek megnyitása?
- Hogyan kerülhető el a bizalmas információk alkalmazottak általi kiszivárogtatása?
- Milyen típusú információbiztonsági kihívásokat vetnek fel ezen problémák?
- Hogyan férhetnek hozzá az e-mail fiókokhoz, illetve ez hogyan akadályozható meg?

Következtetések

Napjainkra az e-mail az egyik legelterjedtebb kommunikációs formává vált, amit az üzleti életben és saját személyes ügyeink intézésére egyaránt használunk. Az e-mail használatával azonban előfordul, hogy mi válunk saját magunk legnagyobb ellenségévé, és a saját hibánk, hogy megszerzik a bizalmas információkat. Ezért szükséges rávilágítani azokra a hibákra, amelyeket a leggyakrabban elkövetünk, illetve arra, hogyan lehet ezeket elkerülni, hiszen ezek tudatában a felhasználók könnyebben megvédhetnék a különböző bizalmas információkat, jelentősen csökkentve a bizalmas adatok kiszivárgásának lehetőségeit.

Fontos: ha számunkra ismeretlen személytől érkezik valamilyen megkeresés, mindig bizonyosodjunk meg arról, hogy ki az a személy, rendelkezik-e az információ megszerzéséhez, illetve a feladat kiosztásához szükséges jogosultsággal, továbbá egy esetleges csatolmány esetén kérjünk a hitelességét igazoló szóbeli megerősítést vagy segítséget a szervezet informatikai szakemberétől.

Az esettanulmányban felvázolt lehetséges adatszivárgások megelőzésének kulcsfontosságú eleme a felhasználók biztonságtudatosságának kialakítása, melynek alapvető eleme a szervezet biztonsági szabályzatainak (informatikai, információbiztonsági, adatvédelmi) megismerése és gyakorlati alkalmazása. Elengedhetetlen annak tudatosítása, hogy ezen szabályok a szervezet kezelésében lévő adatok és információk biztonságát szolgálják, így betartásuk nélkülözhetetlen a megfelelő szintű információbiztonság kialakításának érdekében. Ezen előírások betartása elsőbbséget élvez az egyéni érdekekkel és meggyőződésekkel szemben.

3.2. Alacsony szabad beruházási és/vagy fenntartási forrás

Az eset alapjául szolgál, hogy a szervezetek gyakran nem akarnak sok pénzt költeni a megfelelő és hatékony védelem kialakítására. Ebben az esetben két dolgot kell mérlegelniük. Magas anyagi ráfordítással sokkal hatékonyabb és eredményesebb fizikai, logikai és adminisztratív biztonság alakítható ki, és a felhasználók oktatása is kevesebb forrást igényel, azonban, ha az informatikai biztonság alacsonyabb szintű, akkor sokkal magasabb szintű tudatosság szükséges a felhasználók részéről.

Az eset egy vidéki város önkormányzatában történik, ahol a szervezetnél nincs elegendő elkülönített forrás a magas szintű informatikai biztonság megvalósítására, ezért a szervezet vezetője úgy dönt, ahelyett, hogy egy külső céget bíznának meg a védelmi feladatok ellátásával és a védelem kialakításával kapcsolatos szolgáltatások nyújtásával, inkább csak vírusírtót telepítenek a számítógépekre az esetleges kártékony programokkal történő megfertőződés elkerülése érdekében. Egy délután az egyik alkalmazott egy „Fontos” címkével ellátott e-mailt kap, látszólag az egyik szomszédos település polgármesterétől. A munkatárs megnyitja és letölti az üzenet csatolmányát, aminek következtében zsarolóvírussal fertőződött meg az önkormányzat számítógépes rendszere. A támadó egy konkrétan meghatározott összeget követel a már megszerzett információk, valamint a számítógépes rendszer eredeti állapotának visszaállításáért cserébe. A szervezet vezetője, annak érdekében, hogy leállítsa a rendszereit túszul ejtő zsarolóprogram terjedését, több online szolgáltatást is felfüggesztett, valamint

arra utasította az alkalmazottakat, hogy kapcsolják ki és áramtalanítsák az infokommunikációs eszközöket az esetleges váltságdíj kifizetéséről szóló döntés meghozataláig vagy a vírussal való leszámolásig. A visszaállítás költségének kifizetését követően a szervezet vezetője biztonságtudatossági képzést írt elő minden alkalmazottnak.

Az eset által felvetődő kérdések:

- Kinek és mit kell csinálnia ahhoz, hogy ne történhessen meg ilyen eset?
- Milyen fenyegetések veszélyeztetik az alkalmazottak mindennapjait és a szervezet szolgáltatásainak rendeltetésszerű működését?
- Hogyan előzhetők meg ezek bekövetkezése?
- Szükséges-e az alkalmazottak információbiztonsági továbbképzése?
- A biztonságtudatossági oktatások, képzések segítségével javítható-e a szervezet biztonsága?
- Az alkalmazottak képesek lesznek-e felismerni a valós veszélyhelyzeteket?
- Az alkalmazottak képesek lesznek-e felismerni a szabályok betartásának fontosságát?

Következtetések

Egy szervezet életében kulcsfontosságú a kezelésében lévő információk védelme, ennek megvalósításához számos feltétel teljesítése szükséges.
A megelőzés lehetséges eszközei:

- fizikai, logikai és adminisztratív védelem kialakítása;
- információbiztonsági szabályzat;
- a biztonságtudatosság kialakítása, biztonságtudatossági képzés;
- sebezhetőségvizsgálatok, auditok végrehajtása.

Abban az esetben, ha a szervezet nem rendelkezik valamely feltétel teljesítéséhez szükséges forrásokkal, akkor valamely másik feltétel erősítése válik indokolttá. Így, ha a szervezet nem engedheti meg magának a magas szintű informatikai biztonság megvalósítását, akkor sokkal nagyobb hangsúlyt kell fektetni az alkalmazottak biztonságtudatosságának kialakítására és a felelősségek tisztázására. Hisz az alkalmazott felelőssége is az információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, s ennek megvalósításához elengedhetetlen a biztonsági előírások, szabályok betartása.

3.3. Nehezen elérhető szakmai konzultáció

Az eset főszereplője a szervezet adminisztratív munkatársa, aki egy „Sürgős” címkével ellátott e-mailt kap. Az üzenet érkezését követően úgy dönt, hogy mivel nem ismeri személyesen a feladót, és egy teljesen új típusú feladat elvégzése szerepel a levélben, ezért inkább megkérdezi a főnökét, vajon mi lehet ez. A főnökét nem találja bent, ezért megkeresi a szervezet informatikai munkatársát, hogy megnyithatja-e a csatolmányban található fájlt. A kora reggeli időpont miatt a rendszergazdát sem találja, így arra a döntésre jut, hogy letölti az üzenet mellékletét. A letöltés oka az alkalmazott belső motivációja: egy sürgős feladat ellátása érdekében kénytelen megnyitni az üzenet tartalmát, hiszen egyfajta belső kényszer azt sugallja számára, hogy sürgősen el kell végeznie a rá bízott feladatot. Ezt követően a titkárnő számítógépén keresztül a szervezet számos további eszköze megfertőződik, emiatt az adott szervezeti egység egészében leáll a munka, használhatatlanná válnak az eszközök. Ennek következtében a szervezet által nyújtott szolgáltatások akadoznak vagy teljesen elérhetetlenné válnak. A szervezet vezetője a gyors helyreállítás reményében külsős cég szolgáltatásait veszi igénybe. A

helyreállítást követően a vezető elindítja a szakmai konzultációt, melynek során felveszi a kapcsolatot több külsős tanácsadó céggel, és megindítja a közbeszerzési folyamatot.

Az eset kapcsán felmerülő kérdések:

- Kinek a feladata az alkalmazott tájékoztatása a különféle információbiztonsági kérdésekben?
- Milyen információbiztonsági kötelezettségei vannak az alkalmazottnak?
- Hogyan előzhető meg a hasonló esetek bekövetkezése?
- Milyen óvintézkedéseket kell megtennie az alkalmazottnak hasonló esetekben?
- Mi az előnye a külsős szakmai tanácsadásnak?
- Mi a hátránya a külsős szakmai tanácsadásnak?

Következtetések

A szervezetek mindennapi feladataik elvégzése során könnyedén szembe kerülhetnek azzal a problémával, hogy az alkalmazásukban lévő informatikai, információs rendszerek, valamint azok szoláltatásai, alkalmazásai nem támogatják megfelelően a folyamatokat, a feladatok végrehajtását és a megfelelő szintű információbiztonság megteremtését. Éppen ezért elengedhetetlen a különféle informatikai, információs rendszerek, folyamatok fenntartása és rendszeres fejlesztése. Ennek megvalósítása belső szaktudás vagy kapacitás hiányában szükséges külső, nagy tapasztalattal rendelkező szakértők bevonása a megfelelő szintű információbiztonság megteremtése érdekében. Ezen rendszerek, eszközök fejlesztésekor minden esetben figyelembe kell venni, hogy a magas szintű információbiztonság megvalósítása érdekében külsős szakértők segítségére lehet szükség. Fontos: ha a külső szakmai konzultáció, illetve a külső szakértők segítségével megvalósuló fejlesztések időigényesek, mindenképpen szükség van kiegészítő biztonsági intézkedésekre. Ilyen lehet például az alkalmazottak folyamatos biztonságtudatossági oktatása, melynek keretében ismertetik a különféle információbiztonsági kihívásokat, a megelőzésükre szolgáló eszközöket, módszereket, valamint az alkalmazottak konkrét tevékenységi és felelősségi körét az információbiztonság fenntartásával kapcsolatban.

3.4. Az elektronikus információs rendszer biztonságáért felelős személy

Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Feladatai:

- gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról;
- elvégzi vagy irányítja ezen tevékenységek tervezését, szervezését, koordinálását és ellenőrzését;
- előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot;
- előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását;
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit;
- kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.[90]

[90] 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról, 13. § (2)

Az eset egy önkormányzat szervezeti egységébe újonnan kinevezett elektronikus információs rendszer biztonságáért felelős személy tevékenysége köré épül. Az információbiztonsági felelős a fentebb említett feladatok ellátása és a szervezet elektronikus információs rendszereinek biztonsága érdekében újra és újra biztonságtudatossági oktatásokat tart a szervezeti egység dolgozói számára. A biztonságtudatossági képzések célja, hogy felhívják a munkatársak figyelmét az információbiztonság fontosságára, és bemutassák az alkalmazottakat fenyegető veszélyeket, illetve a támadás megelőzésének lehetséges módszereit. Ezen oktatások keretei közé tartozik például a vírusvédelem vagy a különféle támadási módszerek és védekezési lehetőségek ismertetése. A képzések során a felelős kitér a social engineering-re mint támadásformára is, hiszen ennek célpontja bármelyik alkalmazott lehet, függetlenül attól, hogy használ számítógépet vagy sem. A szervezet egyik dolgozója és a felelős között konfliktus alakul ki, mert az alkalmazott úgy érzi, hogy túl sok hasonló képzést meghallgatott már, ismeri az őt érintő veszélyeket, és feleslegesnek tartja ezen képzések ismétlését. Példaként azt említi, hogy nemrég felismert egy adathalász levelet, ami rossz magyarsággal íródott, és úgy érzi, nincs szükség a folyamatos információbiztonsági oktatásokra. A felelős felvázolja az alkalmazott számára, hogy manapság már egyre újabb, kifinomultabb és komplexebb támadási típusok jelennek meg. Tudatosítja, hogy a szervezetet bármikor támadás érheti, és neki is részt kell vennie a bizalmas információk kiszivárgása elleni védelemben. Sokan azt hiszik, hogy mivel az információbiztonság technológiai elemeket is tartalmaz, ezért a probléma gond nélkül megoldható különböző tűzfalakkal, vírusírtókkal vagy más egyéb biztonságtechnológiai eszközzel.[91] Ezzel szemben a felelős kiemelte, hogy a támadások célpontja számtalan esetben pontosan az ember, mivel megannyi kihasználható tulajdonsága van, ráadásul sokkal könnyebb és egyszerűbb az alkalmazott közelébe férkőzni, mint behatolni egy védett rendszerbe. Minden alkalmazottnak be kell látnia, hogy a kibertámadások valós dolgok, bármikor és bárkivel előfordulhatnak, és az információk elvesztése mind a szervezetre, mind pedig az alkalmazottra nézve jelentős hátrányt okozhatnak.

Az eset kapcsán felmerülő kérdések:

- Mi a céljuk a biztonságtudatossági képzéseknek?
- Hogyan növelhető ezen képzések népszerűsége?
- Milyen szerepet tölt be az információbiztonsági felelős a szervezet életében?

Következtetések

Az, hogy egy szervezet információbiztonság-politikai tájékoztatókat ad ki, és ismerteti dolgozóival, még önmagában nem csökkenti a támadások bekövetkezésének kockázatát. Minden egyes szervezetnek az irányelvek írásbeli rögzítése mellett felelnie kell azért is, hogy a számítógépekkel dolgozó, illetve az anélkül dolgozó alkalmazottak is egyaránt tisztában legyenek az információk kezelésével kapcsolatos biztonsági szabályokkal. Az is lényeges, hogy az emberek a mögöttes tartalmat, az egyes szabályok alkalmazásának okát is megértsék, mert ha ezeket nem tudják, akkor az adott szabályt sem fogják érteni, így pedig nem alkalmazzák, a támadó pedig pont ez fogja kihasználni. Fontos, hogy az alkalmazottakat motiválni kell, hogy részt akarjanak venni a képzésen, illetve tudatosítani is kell bennük, hogy ez nemcsak a szervezet, hanem a saját érdeke is. A képzések kulcsfontosságú eleme, hogy minden olyan embert el kell érnie, akinek hozzáférése van a bizalmas információkhoz vagy a szervezet számítógépes rendszeréhez, illetve folyamatosnak kell lennie, és állandóan frissíteni kell, hogy az alkalmazottak naprakészek lehessenek a legújabb fenyegetéseket illetően is.

[91] Mitnick 2003, i. m. pp. 253–262.

3.5. Az adatvédelmi kultúra változásai

Az eset az adatvédelmi kultúra folyamatos változásaira fókuszál, ezen belül pedig a magáncélra elterjedten használt megoldások hivatalokba történő beszivárgására. Az eset középpontjában a különféle webes alkalmazások állnak, amelyek jelentősen megkönnyíthetik az alkalmazottak munkáját. A szituáció főszereplője egy kormányhivatal alkalmazottja, aki gyakran használ webes pdf forgatót, Word-PDF online konvertálót, illetve pdf editáló alkalmazást. A PDF forgatót azért használja, mert segítségével új program telepítése nélkül, online tudja kedve szerint elforgatni a PDF oldalakat. Ezzel azonban az a probléma, hogy a feltöltött PDF oldalait a felhőben tárolják, és hiába ígéri az alkalmazás, hogy rövid időn belül törli a fájljaink, valójában ebben nem lehetünk száz százalékig biztosak, nem tudhatjuk, hogy hol tárolják még ezen fájlokat. A Word-PDF konvertálót is gyakran használja, hiszen ez egy ingyenes program, amely segítségével a Word dokumentumokat PDF fájlokká lehet alakítani, illetve fordítva is, PDF fájlokat Word dokumentummá, online, bármilyen más egyéb, akár fizetős program telepítése nélkül. Ezenkívül számos további hasznos lehetőséget nyújtanak ezek az alkalmazások: van, amelyikben PDF fájlokat lehet egyesíteni, összeállítani, tömöríteni, oldalakat törölni, képpé konvertálni, de számos további funkció is elérhető. A munkatárs leginkább a korábban említett forgatást, a konvertálást, valamint a digitális aláírást alkalmazza gyakran. Ez utóbbi lényege, hogy webes alkalmazás vagy weboldal segítségével megvalósítható az aláírás beépítése a PDF fájlba. Az aláírás beszúrható gépeléssel, rajzolással vagy egy aláírásfájl beillesztésével. Az aláírás beépítésének veszélye abban rejlik, hogy ilyen webes alkalmazás esetében, mivel az applikáció a felhőben fut, a saját aláírásunk is ott tárolódik, továbbá az aláírásunk bármilyen más egyéb dokumentumra is ráhelyezhető.

Az eset kapcsán felmerülő kérdések:

- Milyen veszélyei vannak az ingyenes webes alkalmazásoknak?
- Hogyan kerülhetők el ezen veszélyek?
- Hogyan előzhető meg a magáncélra használt alkalmazások beszivárgása a hivatalokba?

Következtetések

A nyilvánosan, ingyenesen elérhető webes alkalmazások használata, illetve letöltése előtt célszerű felmérni az applikáció használatával járó esetleges veszélyeket. A fentebb említett esettanulmány alapjául szolgáló pdf editáló alkalmazások számos veszélyt rejthetnek magukban. Tisztában kell lennünk azzal, hogy ha valamilyen szervezeti dokumentumot feltöltünk egy ilyen alkalmazásba az egyszerű és gyors szerkesztés reményében, akkor nem tudhatjuk biztosan, vajon eltárolják-e a dokumentumot, és ha igen, akkor hol és mennyi ideig történik ez. Így a hivatali dokumentumokhoz más is hozzáférhet, továbbá ha az aláírásunkat is feltöltjük, akkor annak birtokában számos további - akár illegális – cselekmény is megvalósítható.

Összességében elmondható, hogy ezek a webes alkalmazások számos előnyüknek köszönhetően népszerűnek tekinthetők, széles körben használatosak, azonban nem szabad elfelejteni, hogy ha valamilyen szolgáltatást ingyen kapunk, ez esetben mindig mi vagyunk a termék, jelen esetben az általunk feltöltött hivatali dokumentációk vagy akár a saját aláírásunk.

3.6. Incidensbejelentési hajlandóság

Az alábbi eset az incidensbejelentési hajlandóságot vizsgálja, ugyanis számos tényező hatással lehet az incidensek tényleges bejelentésére. Az incidensek következtében sérülhet az adatok sértetlensége és bizalmassága, ami komoly kockázatot jelenthet az érintett jogaira, szabadságaira, valamint a szervezet

rendeltetésének megfelelő feladatellátásra. A GDPR[92] hatálybalépésével az új szabályozás értelmében indokolatlan késedelem nélkül, ha lehetséges, a tudomásra jutástól számítva 72 óra alatt a szervezet köteles bejelenteni az incidenst a felügyeleti hatóságnál. Tehát törvényi kötelezettséggé válik az incidens bejelentése. A szituációban egy kormányhivatali dolgozó véletlenül nyilvánosságra hozott egy a szervezeti egység alkalmazottainak személyes adatait tartalmazó dokumentumot, melyben a munkatársak TAJ száma, adóazonosító jele és bankszámlaszáma is szerepelt. Ez azért nagyon veszélyes, mert ezen adatok számos visszaéléshez vagy akár bűncselekmény elkövetéséhez is felhasználhatók. Miután az alkalmazott rájött, hogy felkerült az internetre ez a dokumentum, nagy dilemmába esett, hogy közölje-e felettesével a nyilvánosságra hozatal tényét. Alaposan átgondolta a lehetséges következményeket, és arra jutott, hogy nem jelenti a vezetőnek ezt a problémát. Nem merte beismerni a felelősségét, túlságosan is félt attól, hogy emiatt hibáztatni fogják, el is bocsájthatják. Azt gondolta, nem derül majd ki, hogy miatta kerültek nyilvánosságra munkatársainak adatai.

Az eset kapcsán felmerülő kérdések:

- Melyek az incidensek bejelentésének előnyei?
- Hogyan ösztönözhetők a munkavállalók az incidens bejelentésre? Hogyan növelhető az incidensbejelentési hajlandóság?
- Milyen tényezők alapján döntenek az alkalmazottak az incidensek bejelentéséről?

Következtetések

Összességében tehát megállapítható, hogy az eleve adott törvényi kötelezettség ellenére nem minden esetben valósul meg az incidensek bejelentése. Ennek oka lehet, hogy nem derül ki az esetleges információvesztés vagy az információkon végrehajtott valamely művelet. Abban az esetben, ha tudomásra jut az incidens, a bejelentési hajlandóságot számos további tényező befolyásolhatja. Ilyen például az alkalmazott félelme beosztásának, pozíciójának elvesztésétől, a hibáztatás lélektani hatásai, valamint az ösztönzők hiánya. Ez azt jelenti, hogy a munkatárs nem érzi, hogy az incidens bejelentésének számára pozitív hatásai lennének, úgy gondolja, ha felhívja a figyelmet az általa elkövetett hibára, csak vesztesként jöhet ki a helyzetből, még akár a pozícióját, munkahelyét is elveszítheti ezáltal.

[92] GDPR – General Data Protection Regulation, (általános adatvédelmi rendelet), Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

Összegzés

Napjainkban a kezelt információk fajtáinak száma, mennyisége már sokszorosa a korábbiakénak, tárolásuk pedig igen nagy koncentrációban történik. Aki ezekhez hozzáfér, óriási erőforráshoz jut. A felhasználás céljai alapjaiban nem változtak, viszont tömegessé váltak a különféle információlopások és illegális felhasználás is. Aggasztó, hogy már szinte mindenkinek lehetősége van az internetről beszerezni a megfelelő információt, és a gazdasági szereplők, valamint a társadalom egyre nagyobb része használja fel a megszerzett adatokat. Így az információk kezelőinek óriásira nőtt a felelőssége, különösen az állami szerveknél, ahol mind a gazdaság résztvevőiről, mind az állampolgárokról, mind az állami szervekről óriási mennyiségű információ összpontosul.

Ez teszi kulcsfontosságúvá a biztonságtudatos viselkedés szabályrendszerének kialakítását, megtanítását és betartatását a legalsó pozíciótól a legfelső vezetői szintig. Az információbiztonsággal foglalkozó szakembereknek meg kell mutatniuk, hogy mekkora kárt tud okozni, illetve mekkora veszélyt jelent az adatok megfelelő védelmének hiánya, mekkora felelősség terheli az egyes résztvevőket, és hogyan tudnak megfelelni a biztonsági elvárásoknak.

Irodalomjegyzék

- 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról
- A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény
- Bérczes Attila – Pethő Attila: *Kriptográfia.* NKE Szolgáltató Kft., Budapest, 2014.
- Carabott, Emmanuel: *Hacking Motivations – Hactivism.* 2011. http://www.gfi.com/blog/hacking-motivations-hacktivism/ (2018. 10. 08.)
- Deák Veronika: *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során.* 2018. http://www.hadmernok.hu/183_29_deak.pdf (2018. 11. 03.)
- Deák Veronika: *A social engineering humán alapú támadási technikái.* 2017. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (2018. 10. 12.)
- Deák Veronika: *Biztonságtudatosság az információs környezetben.* 2017. http://www.knbsz.gov.hu/hu/letoltes/szsz/2017_3_szam.pdf (2018. 10. 21.)
- Dolánszky György: *Informatikai rendszerek sérülékenységvizsgálata.* 2013. http://users.nik.uni-obuda.hu/poserne/ibst/Frissitett_anyagok_2013/20130508_Serulekenysegvizsgalat_eSec_KURT_DGY.pdf (2018. 10. 12.)
- Flores, Waldo Rocha – Ekstedt, Mathias: *Shaping intention to resist social engineering through transformational leadership, information security culture and awareness.* Computers and Security, 2016.
- Fülöp Géza: *Az információ.* Erdélyi Múzeum-Egyesület, Kolozsvár, 2001.
- Gyebrovszki Tamás: *Stuxnet – mint az első alkalmazott kiberfegyver – A Tallini Kézikönyv szabályrendszere szempontjából.* 2014. http://hadmernok.hu/141_16_gyebrovszkyt.pdf (2018. 11. 04.)
- Haig Zsolt: *Információ – társadalom – biztonság.* NKE Szolgáltató Kft., Budapest, 2015.
- Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* 2012. https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf (2018. 10. 08.)
- Horváth Zsolt: *Az információbiztonság alapjai.* 2016. http://docplayer.hu/286483-Az-informaci-alapjai-bevezetes-az-informaciobiztonsag-es-informaciobiztonsagi-iranyitasi-rendszer-alapfogalmaiba-es-szuksegessegebe.html (2018. 11. 04.)
- Krasznay Csaba: *Az információbiztonság alapjai.* 2007. http://krasznay.hu/presentation/elte_01.ppt (2018. 10. 12.)
- Leitold Ferenc: *Sebezhetőségvizsgálatok a gyakorlatban.* NKE Szolgáltató Kft., Budapest, 2014.
- Magyar Szabványügyi Testület: Az információbiztonság irányítási rendszerének (ISMS) MSZ ISO/IEC 27001:2014 szerinti tanúsítása. http://www.mszt.hu/web/guest/msz-iso-iec-27001 (2017. 11. 03.)
- Michelberger Pál – Lábodi Csaba: *Vállalati információbiztonság szervezése.* 2012. http://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf (2018. 10. 29.)
- Mitnick, Kevin D.: *A legendás hacker – A megtévesztés művészete.* Perfact-Pro, Budapest, 2003.
- Mitnick, Kevin D.: *A legendás hacker – A behatolás művészete.* Perfact-Pro, Budapest, 2006.

- Németh L. Zoltán: *Pszichológiai manipuláció (Social engineering).* 2015. www.inf.u-szeged.hu/~zlnemeth/INFOSEC/AMKK_6_Pszichológiai_mainpuláció.pptx (2018. 10. 29.)
- Mouton, Francois et al.: *Socal engineering attack examples, templates and scenarios.* Computers and Security, 2016, pp. 186–209.
- Oroszi Eszter: *Social Engineering.* 2008. http://krasznay.hu/presentation/diploma_oroszi.pdf (2016. 10. 04.)
- Prensky, Marc: *Digitális bennszülöttek, digitális bevándorlók.* 2001. http://goliat.eik.bme.hu/~emese/gtk-mo/didaktika/digital_kids.pdf (2018. 10. 29.)
- Raffai Mária: *Döntéshozatal és döntéstámogatás – A döntési folyamat és a döntési folyamatot támogató* rendszerek*.* http://rs1.szif.hu/~raffai/org/dontesTamogat-2.pdf (2018. 11. 03.)
- Shameli-Sendi, Alireza – Aghababaei-Barzegar, Rouzbeh – Cheriet, Mohamed: *Taxonomy of information security risk assessment (ISRA).* Computers & Security 57, 2016, 14–30. https://doi.org/10.1016/j.cose.2015.11.001 (2018. 11. 04.)
- Schutzbach Mártonné: *Az informatikai biztonságot fenyegető tényezők.* 2003. http://portal.zmne.hu/download/konyvtar/digitgy/nek/2003_2/12_schutzbach.pdf (2018. 11. 02.)
- Sörös Tamás et al.: *Social engineering a biztonságtechnika tükrében.* 2013. http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/Inform%C3%A1ci%C3%B3biztons%C3%A1g/TDK-Social_Engineering-Soros-Vaci_orszagos.pdf (2018. 10. 21.)
- Twitchell, Douglas P.: *Social Engineering and Its Countermeasures. Handbook of Research on Social and Organizational Liabilities in Information Security,* Kennesaw, Georgia, USA, 2006.
- Whitaker, Andrew – Evans, Keatron – Voth, Jack: *Chained exploits: Advanced Hacking Attacks from Start to Finish.* Pearson Education Inc., Boston, 2009.

Ajánlott irodalom

- 187/2015. (VII. 13.) Kormányrendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól
- 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
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- Európai Tanács 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről
- Magyarország Nemzeti Kiberbiztonsági Stratégiája, 2013. Magyar Közlöny 2013/47, http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf
- Christián László: *Informatikai védelem. Információvédelem.* NKE Szolgáltató Kft., Budapest, 2015.

- Haraway, Donna: *Simians, Cyborgs and Women.* Free Association Press, London, 1991.
- Krasznay Csaba: *A polgárok védelme egy kiberkonfliktusban.* Hadmérnök 2012/4, 2012. http://hadmernok.hu/2012_4_krasznay.pdf
- László Gábor: *Kockázatértékelés, kockázatmenedzsment.* 2014. http://vtki.uni-nke.hu/uploads/media_items/kockazatertekeles_-kockazatmenedzsment.original.pdf
- Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* NKE Szolgáltató Kft., 2014.
- Munk Sándor: *Információbiztonság vs. informatikai biztonság.* Hadmérnök, 2007/különszám, http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html
- Resperger István: *Kockázatok, kihívások és fenyegetések a XXI. században.* ZMNE, Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest, 2002.
- Safa, Nader Sohrabi – Von Solms, Rossouw: *An information security knowledge sharing model in organizations.* Computers in Human Behaviour, 2016.
- Törley Gábor: *Adatbiztonság a közigazgatásban.* Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013.

Ábrajegyzék

Fogalomtár

- **Adat:** Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas, számos megjelenési formát vehet fel (pl. alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása. [1]
- **Adatbiztonság:** Az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni alatta. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében. [2]
- **Adathalászat:** Más néven phishing, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. [3]
- **Adatkezelés:** Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése. [2]

- **Adatkezelő:** Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja. [2]
- **Adatvédelem:** A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások. [4]
- **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot, nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens. [2]
- **Adminisztratív védelem:** A védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás. [4]
- **Backdoor („hátsóajtó") program:** A felhasználók számára általában nem látható elem, amely a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nemcsak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként. [5]
- **Bizalmasság elve:** Az elektronikus információs rendszer azon tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról, csak az arra jogosult és csak a jogosultság szintje szerint férhet az adathoz, és használhatja fel. [1]
- **Biztonság:** A biztonságot olyan állapotnak tekinthetjük, amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak a veszéllyel szembeni eredményes védekezés feltételei. [4]
- **Biztonsági esemény***:* Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. [4]
- **Biztonsági osztály***:* Az elektronikus információs rendszer védelmének elvárt erőssége. [4]
- **Biztonsági osztályba sorolás***:* A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása. [4]
- **Biztonsági szint:** A szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [4]
- **Biztonsági szintbe sorolás:** A szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [4]
- **Biztonságtudatosság:** A felhasználó azon magatartása, amikor betartja az információbiztonsági szabályokat, megérti az információbiztonságban betöltött szerepét, és figyel az őt esetlegesen érintő fenyegetésekre. [6]

- **CIA:** Az elektronikus információs rendszer védelme alapvető céljának: a bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) védelmi hármasának jelölése. [4]
- **Elektronikus információbiztonság:** Távközlési és informatikai, valamint egyéb elektronikus rendszerekben és a támogató infrastruktúrákban alkalmazott rendszabályok összessége, amelyek védelmet nyújtanak az elektronikusan előállított, feldolgozott, tárolt, továbbított és megjelenített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen. [3]
- **Elektronikus információs rendszer:** Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. [4]
- **Elektronikus információs rendszer biztonsága:** Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [4]
- **Fizikai védelem:** A fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptetőrendszer, a megfigyelőrendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, a klimatizálás és a tűzvédelem. [4]
- **Fizikai biztonság:** Fizikai biztonság körébe soroljuk az információrendszert működtető eszközrendszerek, például a számítógépek, tárolók, hálózati eszközök fizikai védelmét. A fizikai védelem eszközei többek között a beléptetőrendszerek, a lopásgátló eszközök, rácsok vagy biztonsági ajtók. [7]
- **GDPR:** A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, más néven általános adatvédelmi rendelet (General Data Protection Regulation). A GDPR közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó. Ennél fogva minden tagállamban ez a rendelet lesz a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekintetében, attól eltérni csak akkor lehet, ha azt maga a GDPR megengedi. A rendeletet 2018. május 25-től kell alkalmazni.
- **Hitelesség:** Az adat tulajdonsága, amely arra vonatkozik, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [4]
- **Információbiztonság:** Olyan tevékenység vagy állapot, amelynek középpontjában a bizalmasság, a sértetlenség és a rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (pl. alfabetikus, numerikus, grafikus, képi forma), és milyen adathordozón jelenik meg. [8]
- **Informatikai biztonság:** Egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ez azt jelenti, hogy egy az összes fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelmi rendszer. [4]
- **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 működtetéséhez. [1]
- **Kibervédelem:** A kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését. [1]

- **Kockázat:** A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye. Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek megvalósulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. [4]
- **Kockázatazonosítás:** Célja azon helyzetek, lehetőségek, események felismerése, melyek a kitűzött céloknak való megfelelést befolyásolhatják. Az azonosítás a lehetőségek felmérésén túl magában kell foglalja mindazokat a tényezőket, melyek a kockázat kialakulásának környezetét jelentik. Ebben ki kell térni azokra a folyamatokra, szabályozókra, technikai eszközökre, emberekre, rendszerekre, hardver és szoftver tényezőkre stb. melyek relevánsak a kockázat és környezet megértésének szempontjából.
- **Kockázatelemzés:** Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése. [4]
- **Logikai biztonság:** A logikai biztonság körébe tartoznak a vírusok, a rosszindulatú kódok, az adathalászattal kapcsolatos támadások, az ilyen típusú támadások elleni védekezés, a vírusok, a hackertámadások, az adatlopás, az illetéktelen hozzáférés és módosítás, illetve az illetéktelen közzététel. [7]
- **Logikai védelem:** Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem. [4]
- **Malware:** Az angol malicious software (kártékony szoftver, káros szoftver, rosszindulatú szoftver) összevonásából kialakított mozaikszó. Rosszindulatú szoftvernek tekinthetők azok a szoftverek, amelyek célja nem az információs rendszer működésének biztosítása és fenntartása, hanem bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek végzése. Ezen rosszindulatú szoftverek segítségével a támadó könnyedén zavart okozhat a célszemély számára, például túlterhelheti, működésében akadályozhatja, valamint akár működésképtelenné teheti a felhasználó bármely infokommunikációs eszközét. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program. [5]
- **Nulladik napi (0-day) sérülékenység:** Olyan számítógépes szoftveres biztonsági rés, amely ismeretlen azok számára, akik érdekeltek lennének a sebezhetőség enyhítésében, befoltozásában (beleértve a célszoftver gyártóját is). A biztonsági rést kihasználva a hackerek hozzáférhetnek a számítógépes programokhoz, adatokhoz, további számítógépekhez vagy hálózatokhoz. Egy nulladik napi sebezhetőségre irányuló támadást nulladik napi exploitnak (kihasználásnak) vagy nulladik napi támadásnak neveznek. [13]
- **Rendelkezésre állás elve:** Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak. [4]
- **Sértetlenség elve:** Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [4]
- **Sérülékenység:** Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [4]

- **Social engineering:** Az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését vagy éppen egy kártékony program terjedését és működését. [6]
- **SQL injection:** Más néven SQL befecskendezés. Ez olyan exploit, amely azokat az adatbázis-lekérdező programokat használja ki, ahol nem tesztelték le alaposan a lekérdezések metódusát. Az SQL injection parancsokat küld a web szerverhez kapcsolt SQL adatbázisnak. Ha a szerver nem megfelelően lett tervezve és erősítve, akkor az űrlap mezőkbe – mint például a felhasználónév – közvetlen parancs adható meg az SQL szervernek. Így például a támadó a megfelelő parancs megadásával kinyerheti az adott oldal összes felhasználójának nevét vagy egyéb kritikusabb táblák információit is. [9]
- **Személyes adat:** Az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosítójele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. [10]
- **„Tiszta asztal, tiszta képernyő" szabály:** E szabály alkalmazása elengedhetetlen, lényege, hogy az aktuális feladathoz csak a legszükségesebb anyagokat kell az asztalon hozzáférhetően, a képernyőn láthatóan tartani. Munkaidőn túl az iratokat az íróasztalokon nem lehet tárolni, el kell zárni azokat. [11]
- **Vishing:** Más néven telefonos adathalászat, amely hanghálózaton, elsősorban VoIP csatornán keresztül terjed. A technika lényege, hogy a támadó a tömeges tárcsázás módszerével végig telefonálja egy adott körzet összes hívószámát, és ahol felveszik a telefont, ott egy előre rögzített üzenetet játszanak le, amiben értesítik az áldozatot, hogy bizonyos problémák miatt zárolták vagy letiltották a bankkártyáját, ezért felajánlanak egy telefonszámot, hogy hívja fel a probléma megoldása érdekében. Amikor az ügyfél felhívja a telefonszámot, kérik, hogy adja meg bank- vagy hitelkártya információt, mint például a felhasználó nevét, kártyájának számát, banki azonosítóját, illetve a régi és új PIN kódját, hogy ezzel a kártyáját újra aktiválni tudják. [6]
- **Vírus:** A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve az által, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A vírusok a rendszerbe a felhasználó engedélye nélkül kerülnek be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD kártya, merevlemez, MP3 és videó lejátszó, mobiltelefon stb.) vagy akár hálózati kapcsolat (internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tartalmát is törölhetik vagy módosíthatják, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nemcsak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [5]

Irodalomjegyzék a fogalomtárhoz

[1] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[2] Nemzeti Adatvédelmi és Információszabadság Hatóság: Adatvédelmi Értelmező Szótár. Forrás: https://www.naih.hu/adatvedelmi-szotar.html (2018. 03. 22.)

[3] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[4] Muha Lajos: *Fogalmak és definíciók.* In: Az informatikai biztonság kézikönyve. 2004. http://lmuha.hu/defins.html (2018. 03. 22.)

[5] Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* 2012. http://hdl.handle.net/11410/285 (2018. 03. 24.)

[6] Oroszi Eszter: *Social Engineering.* Budapesti Corvinus Egyetem, Budapest, 2008.

[7] Gyurák Gábor: *Informatikabiztonság I.* Pécsi Tudományegyetem Műszaki és Informatikai Kar, Pécs, 2015.

[8] László Gábor: *Kockázatértékelés, kockázatmenedzsment.* 2014. http://vtki.uni-nke.hu/uploads/media_items/kockazatertekeles_-kockazatmenedzsment.original.pdf (2018. 03. 22.)

[9] Kaczur Gábor: *Spear phishing.* In: Célzott támadások. Dialóg Campus Kiadó, Budapest, 2018.

[10] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

[11] Gyaraki Réka Eszter: *Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban.* In: Célzott támadások. Dialóg Campus Kiadó, Budapest, 2018.