Visszaélések a kibertérben

(Online and Other Electronic Fraud)

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 jelen anyag átfogó, de felületes képet kíván adni a kibertérben történő visszaélésekről. Szemléletes, gyakorlati példákat hoz fel egy-egy kiberbiztonsági jelenség bemutatásához, miközben a téma elméletét, tudományos és gyakorlati leírását is bemutatja. A tananyag célja egyfajta szemléletformálás, annak bemutatása, milyen tényezőkből tevődik össze egy kibertérbeli visszaélés, milyen céljai vannak, és milyen aspektusai. Betekintést ad a malware-ek és a social engineering témakörébe, szervezeti és informatikai szabványokat, előírásokat mutat be. Megismertet a hatályos jogszabályok (Ibtv, GDPR stb.) néhány előírásával. Terjedelmi korlátainak keretein belül eszközöket nyújt az információs visszaélések megelőzésére, feltárására és elhárítására. Kiemelten foglalkozik a kiberbiztonság humán és szervezeti aspektusaival, illetve a korrupció és az információs rendszerekkel kapcsolatos összefüggések kérdéskörével.

Abstract

The present material intends to provide a comprehensive, but superficial picture of electronic frauds. It introduces remarkable and practical examples to present some notorious cyber-security breaches, meanwhile presenting the subjects' theoretical, scientific and practical. The purpose of the curriculum is to shape the attitude of the reader toward understanding the different aspects of cybercrime. The reader gains insights into topics like malware and social engineering. We present structural and IT standards and regulations. You will learn about some of the current laws (eg. GDPR etc.). Within our limits, we provide tools to prevent, detect and resolve information frauds. We focus on human and organizational aspects of cyber security, and the connections between corruption and information systems' frauds.

Kulcsszavak

kiberbiztonsági visszaélés, információs visszaélés, kiberbűnözés, social engineering, korrupció

1. Bevezetés

A XXI. század az emberiség történelmének máris sarokponti része. Optimista és pesszimista hangok, gondolatok és hírnökök, mint a történelem megannyi pillanatában, most is értékelik a jelent és a lehetséges jövőt. A jelen tanulmányban azonban nem a jövőkutatással mint izgalmas tudományos és irodalmi témával foglalkozunk, hanem a tényekkel. A tények, melyek azt mutatják, hogy az a realitás, amelyben az emberiség egész történelme során élt és alkotott, született és halálozott, megbomlott.

A XXI. században többé nem hihetünk annak, amit vaksi szemünkkel látunk, süket fülünkkel hallunk, vagy épp tompa agyunkkal gondolunk, hogy Bacsó Péter örökérvényű A tanú című filmjéből idézzek szabadon. Félreértés ne essék, a hiszékenység soha nem volt eredendő értéke és érdeke az embernek, nem véletlen alakult ki közmondásunk: „Messziről jött ember azt mond, amit akar.”, de érvényesnek tűnt a mondás – leszámítva az illuzionistákat –: „Hiszem, ha látom!” Századunkban azonban alaposabb körültekintésre van szükségünk a mindennapi életünkben, mint eddig valaha.

Ennek legfőbb oka, hogy bár az emberiség történelme során az egyének szubjektív valóságérzékelése mindig is teremtett alternatív értelmezéseket a tényeknek és összefüggéseknek, századunkra a technológiai fejlődés hatására nemcsak alternatív értelmezéseit találjuk meg a valóságnak, hanem maga a valóság alternatív síkokon játszódik. A valós tér, a kibertér, a kiterjesztett valóság tere és a virtuális valóság tere jelenünkben, de leginkább a közeljövőben úgy kuszálódik össze, olyan hatás-kölcsönhatás mechanizmusokkal működik, amelyet egy átlagos ember nem tud ésszel felfogni, és pláne nem képes teljes mértékben kiigazodni ebben a világban.

Tanulmányunk elkészítése során igyekeztünk csak nemzetközileg gyakran idézett forrásokat, illetve cikkek esetén elismert, komoly újságírói múlttal rendelkező oldalakat használni, a témában régóta jelenlévő szakértők (vagy cégek) állításaira hivatkozni. Mivel jelen tanulmánynak nem célja a különböző fogalmi definíciók tudományos ütköztetése és elemzése, így ettől eltekintünk, de ez nem jelenti azt, hogy fogalomhasználatunk ne lenne megalapozott.

Tanulmányunk címe: visszaélések a kibertérben, de ez a cím félrevezető, hiszen a kibertér visszaélései a valós, térbeli életünkre vannak a legnagyobb hatással, a valós, megfogható életünkben tett döntéseink pedig a kibertérbeli életünkre hatnak. Nem lehet már szétválasztani őket. A fejlődés kerekeit pedig nem vagyunk képesek visszafordítani, így meg kell találnunk azt az utat, amely ebben segítségünkre lehet. A jelen tanulmány pedig ebben kíván segíteni. A mű elkészítése során ismert híresebb és/vagy tanulságosabb gyakorlati példákat mutatunk be olyan visszaélésekre, amelyekből levonhatjuk a megfelelő tanulságokat, illetve megnézzük a tudomány és a kiberbiztonsági szakértők jelen tudásának egy csekély metszetét, hogy meg tudjuk előzni, fel tudjuk tárni vagy el tudjuk hárítani a fenyegetések nagy részét. Lebegjen előttünk azonban a közhely: „nincs tökéletes védelem”, de ettől még törekedni lehet rá.

2. Az információs visszaélések problémaköre, céljai és területei

2.1. A probléma megragadása fogalom-meghatározással

Ahhoz, hogy helyén tudjuk kezelni az elkövetkezendőkben leírtakat, meg kell ismerkednünk néhány fogalommal. Jelen esetben így két legyet ütünk egy csapással, mivel nem tudományos definíciókat ütköztetünk, hanem a fogalmak által előrevetítjük a kibervédelem csodálatos világának kihívásait is.

2.1.1. Kibertér

A témával kapcsolatban először is tisztáznunk kell a **kibertér** fogalmát, mert azt tudjuk, hogy ezt kívánjuk védeni, és ebből kifolyóan sejthetjük, hogy nyilván valakik támadják, vagy épp ebben támadnak, de mi ez? A kibertér meghatározásában és értelmezésében eltérő álláspontokat és nézeteket találunk, ahogy általában minden más tudományos definíció esetében is. Abban azonban a szakértők mindegyike megegyezik, hogy a kibertér a hálózatok és benne az internet, valamint a hálózathoz vezetéken vagy vezeték nélkül csatlakozó eszközök működési tartománya. Magát a kifejezést egyébként 1982-ben az amerikai, William Gibson sci-fi író használta először „Izzó króm" című novellájában, majd az 1984-es „Neurománc" című regényében, innen szivárgott át a köztudatba is. A kibertér kifejezés a görög kyber (hajózni) szóból származik, és hajózásra alkalmas teret jelent, ez azért is fontos, mert itt nem elsősorban egy technológia megnevezését értjük alatta, hanem egyfajta, négydimenziós világunkban nehezen értelmezhető térfogalmat.

A kibertérrel kapcsolatban az egyik legérdekesebb kérdés az, hogy mit értünk rajta pontosan, csak az internetet, vagy olyan, internettől elzárt, úgynevezett privát hálózatokat is, amelyek bár az internet címzési architektúrájában szerepelnek, tehát ugyanazt a technológiát használják, mégis ahhoz, hogy egy privát hálózatot az általunk ismert világhálóra rácsatlakoztassunk, külön hálózati címfordítóra (NAT) vagy proxyszerverre van szükség. Ezek a hálózatok is a kibertér részei? Ezek gyakran csak otthoni használatra készülnek, vagy épp egy-egy cég vagy kormány saját hálózatát alkotják. Természetesen tekinthetjük őket a kibertér részének, ahogyan egy magánlakás vagy egy cég jól őrzött létesítménye is a valós tér része. Kiberbiztonsági szempontból nüansznyi a különbség.

Tovább bonyolítja a helyzetünket, hogy ez a tér teljes egészében nem deríthető fel, kiterjedése, részeinek számossága folyamatosan változik. Egyfajta közhely, hogy „ami egyszer az internetre felkerül, az ott is marad", ennek az állításnak erős az igazságtartalma, köszönhetően az olyan szolgáltatásoknak (pl. archive.org), amelyek időről időre lementik az internet egyes részeinek, oldalainak az aktuális állapotát, és utána ezt egy idővonalon lekérhetjük, de az állítás igazságtartama nem abszolút, az internetről tűnnek el teljes website-ok, különféle tartalmak örökre is.

Amikor a kibertérről beszélünk, akkor soha ne csak az internetre, ne csak a számítógépünkre gondoljunk. Már egyre inkább megszokott, hogy a kibertér eszközein az okostelefonjainkat is értjük, de minden más okoseszközt is értsünk ide! Az okosórák, szenzorok, okostévék stb. egyaránt a kibertér részei, egyaránt adatokat tárolnak, közvetítenek, és egyaránt figyelnünk kell rájuk! Tegyük fel magunkban a kérdést, hány jelszót és fontos adatot tárolunk a telefonunkon. Védjük valamilyen tűzfallal, szoktunk malware (lásd később) ellenőrzést futtatni? Okosóránk, -televíziónk nem jelent-e szabad bejáratot az amúgy jól védett számítógépünkbe? De ne siessünk előre...

Több másik fogalom megértése is szükséges ahhoz, hogy a kibertérben történő visszaélésekről és felderítésükről alaposabb képet kapjunk. Ezek a következők: a mélyweb (deep web), a sötét web (dark web), a VPN és a proxy fogalmai. Nem kívánunk pontról pontra készült használati útmutatót adni ezekhez, és technológiai részletekkel sem foglalkozunk, az interneten minden könnyen elérhető,

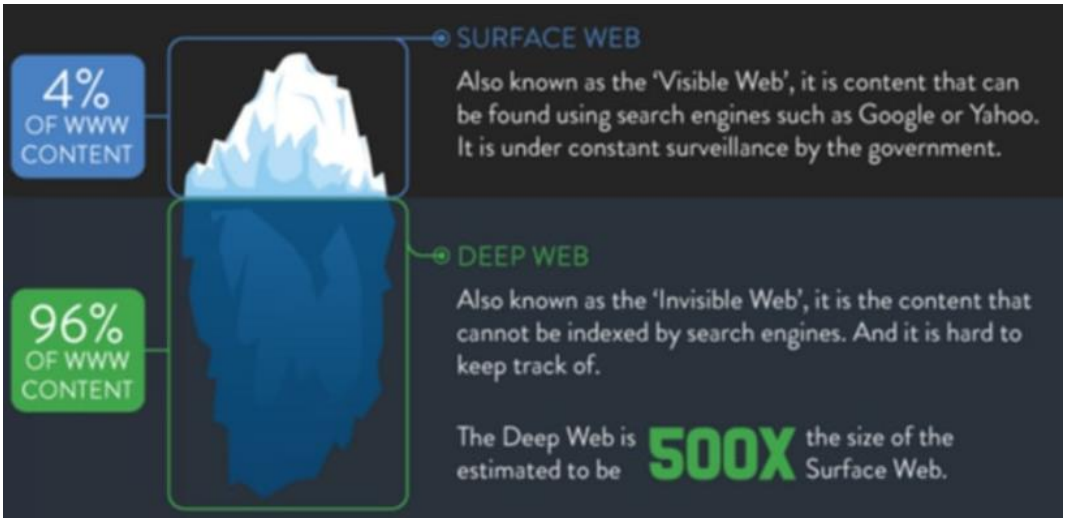
célunk, hogy átfogó képet adjunk, hogy a későbbiekben figyelembe vegyük e fogalmak gyakran ki nem mondott hatását, következményeit egy-egy visszaélés során.

2.1.2. Mély és sötét

Ahhoz, hogy teljes egészében megértsük a kibertér jelentette problémát, meg kell értenünk, hogy nem ismerjük az internetet. Ahogy Michael K. Bergman fogalmazott 2001-es munkájában: „Manapság az interneten keresni olyan, mint kifeszíteni egy hálót az óceán felszínén. Míg igen gazdag fogást találunk a hálóban, akad bőven információ a mélyben, amely kimarad a hálónkból. Az ok egyszerű: a Háló (hálózat) információi túl mélyen fekszenek, dinamikusan generált oldalakon, és a normál keresők soha nem találják meg." (Bergman 2001) Bergman a mély web-ről (elterjedt angol neve: deep web) ír.

A mély web olyan tartalmak gyűjtőneve, amelyeket a keresőmotorok (Google, Yahoo, Bing stb.) nem fednek le, tehát nem lehet őket úgy megtalálni, hogy beírjuk a keresőbe a nevüket vagy valamilyen tartalmat rajtuk. Ennek megértéséhez szükségünk van arra a tudásra, hogyan kerül be egy-egy weboldal a keresőmotorok látóterébe. Több módja is van: vagy adatbázisból szerzik az információikat, vagy keresőrobotok (úgynevezett crawlerek) gyűjtik be azokat. Az előbbiekhez önként is hozzáadhatjuk weboldalainkat, vagy bizonyos weblapkészítő programokkal automatikusan kerülnek be, az utóbbiak képesek az interneten fellelhető publikus, illetve a weboldal html kódjában tárolt robots.txt és robots metatag által engedélyezett tartalmak letöltésére, és valamilyen formában való elemzésére, az adatok eltárolására. A keresőrobotokat segítő weboldalak egyébként a keresőmotorok találatlistájában általában előrébb kerülnek, ezért a webszerkesztésben, webprogramozásban külön fogalom a keresésoptimalizálás (SEO – search engine optimization), ám ez jelen anyagunknak nem témája.

A keresőmotorok hálója által nem elkapott tartalmak kerülnek tehát a deep webbe. Ezen tartalmak egy része idővel feltérképezetté válik, egy része viszont a jelenlegi körülmények között soha nem kerül be a keresőmotorok látómezejébe, mivel direkt úgy készültek, hogy elkerüljék azokat. A deep web megmutatja, hogy egy látszólag egzakt, informatikai alapokon működő rendszer mennyire ismeretlen, olyannyira, hogy a méreteiről is csak becsléseink vannak, több tudós is foglalkozik azzal, hogyan lehetne erre a kérdésre megfogható választ adni. (Madhusudan–Poonam D. 2017)

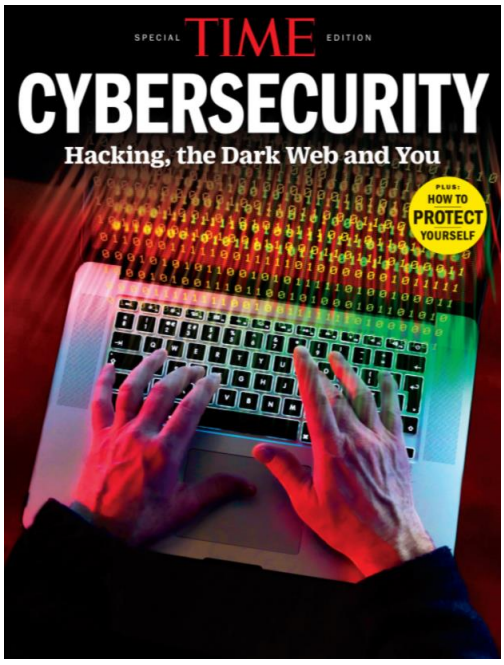


1. ábra: Egyes oldalak szerint a deep web 500-szor akkora, mint a rendes, kereshető web. Ez azonban erős túlzásnak, marketingfogásnak tűnik (a szerző).
Forrás: deepweb-sites.com 2016.

A következőkben bemutatjuk az úgynevezett sötét webet, amelyet gyakran – tévesen – a deep web szinonimájaként is használnak, holott érdemes elkülöníteni a két fogalmat. Különösen fontos az internetnek ez a része, amikor témánk a visszaélések a kibertérben, hiszen a dark web a visszaélések legnyíltabb tárháza.

Az úgynevezett dark web (sötét web) a leginkább ellenőrizhetetlen a hatóságok számára, illetve az internet publikus részét uraló magáncégek keresőbotjai, megosztási hálója sem ér el ide, emiatt mondhatjuk akár azt is, hogy ez az internet legszabadabb része, ahol az egyént semmilyen törvények és szabályok nem korlátozhatják. Legszabadabb, mert ez az internet az átlagfelhasználóktól elzárt vidéke, ahol nincs semmilyen cenzúra, nem szabályozzák a megjelenő tartalmat jogállamok és cégek, emiatt nem is alakul ki igazán semmilyen véleménybuborék, és felhasználói teljes anonimitás mögött lényegében bármit csinálhatnak, a törvény keze ritkán ér el ide. Pont emiatt azonban a modern szervezett bűnözés egyik bástyája is.

A dark webet átlagos böngészővel (pl. Chrome, Firefox vagy Microsoft Edge) nem lehet elérni, speciális böngészőre van hozzá szükség, az egyik legismertebb a Tor.[1] Maga a dark web kifejezés a Time magazin Cybersecurity (kiberbiztonság) különszámával került be a hétköznapi szóhasználatba 2018-ban, de legalább 2009 óta használjuk. A Tor böngésző, azon túl, hogy lehetőséget ad az internet sötét oldalán való szörfölésre, még anonimitást is garantál, emiatt nem feltétlenül kell rögtön gyanakodnunk, ha egy ismerősünknél megtaláljuk. A dark web ellenőrizhetetlensége nagyrészt nem bűnözőket takar, mégis a drog- és fegyverkereskedelem, az embercsempészet, a gyermek-pornográfia és más illegális szexuális aberrációk gyűjtőhelye. Az ilyen oldalakat üzemeltetni és egyes országokban látogatni is bűncselekmény. Éppen ezért vannak a dark weben a bűnözők is: itt nehéz felkutatni a készítőket, a felhasználókat beazonosítani meg még inkább problémás. Míg egy átlag felhasználó átlag gépe rengeteg nyomot hagy a neten való szörfözés során – emiatt a rendőrség gyorsan nyomára tud bukkanni egy átlag internetes zaklatónak –, a sötét web megvédi ezeket a felhasználókat saját nyomaiktól. (Sasvári et al. 2018)



2. ábra: A Time kiberbiztonsággal foglalkozó különszámának címlapja (2018. január 19-én jelent meg)

[1] Más hasonló eszközök: I2P, Freenet, Raffle. Ezek más-más technológiát, megoldást használnak a dark web böngészésére, a Tor jellegzetessége az onion service (lásd később).

Forrás: Time

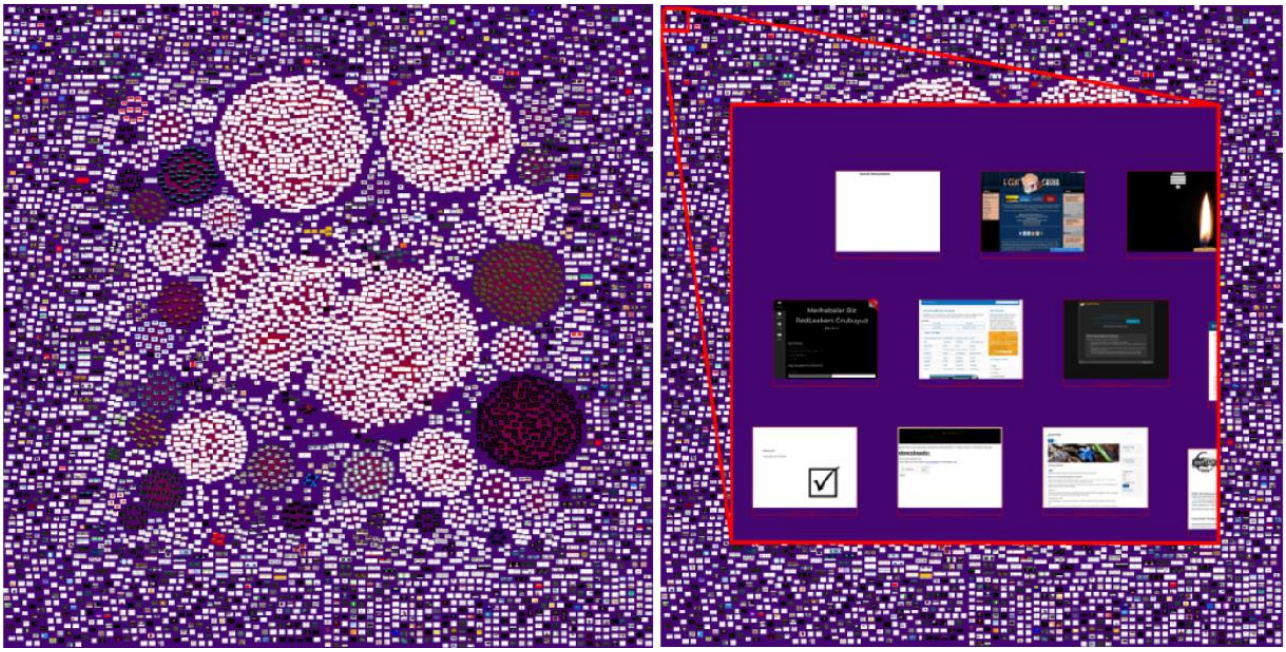
A Tor és más hasonló böngészők azon kívül, hogy elrejtik a felhasználója IP címét, így földrajzi tartózkodási helyét, elrejtik a weboldalak helyét is. Ezt a szolgáltatást hagyma-szolgáltatásnak nevezzük (onion service). Sok mindenre használják, ami nem mindig egyértelműen sorolható be a jó és a rossz kategóriájába, például egy elnyomó hatalmat kikerülni kívánó polgárok egymással szabadan beszélgethetnek rajta, újságírók így garantálják informátoraik anonimitásának megőrzését, illetve átlag állampolgároknak is jól jön, ha el akarják kerülni a real-marketing eszközeit, és azt, hogy mindenféle adatokat tároljanak róluk.

Felmerülhet a kérdés az Olvasóban: mit találunk a dark weben. Ehhez érdemes elolvasni az alábbi kutatást:

A Hyperion Gray kalandozása a dark weben

A bűnüldöző szerveknek és kutatóknak egyaránt izgalmas téma ugyanakkor valami módon a dark weben található oldalaknak a megismerése. A Hyperion Gray blog készítői erre vállalkoztak. A Tor böngésző adatai alapján 60 000 hagyma-szolgáltatást üzemeltetnek, a bloggereknek ebből 6608-at sikerült feltérképezni mesterséges intelligencia segítségével (a már korábban említett: crawler). (Hyperion Grey 2018)

Sok különféle oldalt találtak, például olyat, amely India postáit és irányítószámait tartalmazza, tehát teljesen ártatlan tartalom, akár a sötét weben kívül is működtethető oldal is lehetne.



3. ábra: A baloldali ábra a Hyperion Grey által készített dark web térkép, a jobb oldali a térkép egy részének nagyítása. Az elkészült térképen a háló pontjai weboldalak képei, míg a köztük húzott kapcsolat azt jeleníti meg, ha két oldalt „azonos”-nak tekintettek. Forrás: Hyperion Grey 2018.

Az elkészült térkép (lásd 1. ábra) a weboldalak nyitóképernyőiből áll, illetve a kapcsolatok (egy-egy beazonosítható alakzat, például ilyen kapcsolatok tömege) az „azonos” weboldalakat mutatják. Az azonosság a weboldalak kapcsán nem azt jelenti, hogy ugyanazok (lásd lentebbi ábra). Két oldal szerencsejátékokkal foglalkozik, és bár más a szín- és képi világa, feltételezhető, hogy ugyanaz a készítőjük.

4. ábra: Két azonos dark web oldal, mégis különbözőek. Számoljuk meg az azonos szerkezeti elemeket (pl. menüelrendezés, hírek menü a jobb oldalon stb.). A képek alján a dark weben elérhető nevük látható az utolsó négy karakter kitakarásával, mivel a Hyperion Grey csapatának nem az volt célja, hogy valamiféle brossúrát készítsen, hanem tudományos szempontból vizsgálták ezeket az oldalakat, így megőrizték anonimitásukat, nehogy a bűnözést támogassák vele. Forrás: Hyperion Grey 2018.

A dark weben a bloggerek találtak továbbá egy csomó olyan oldalt, amely Secure Drop-ot futtat, amely anonim szivárogtató rendszer, direkt azoknak kitalálva, akik cégükről, kormányukról vagy valami másról tudnak hiteles adatokat, valami sötét ügyletről, de nem akarják veszélyeztetni saját állásukat. Több nagy újság, pl. a The Guardian üzemeltet a dark weben oldalt kifejezetten az ilyen, szivárogtató emberek számára. Az ilyen oldalakat is egy nagyobb halmazba tömörítve látjuk a hálóban.

A Hyperion Grey oldalán, illetve külön az alábbi linken (https://www.hyperiongray.com/dark-web-map/) mi magunk is nézegethetjük a felderített weboldalak nyitóképeit, ugyanakkor mivel találhatunk köztük olyan tartalmakat, amelyek nem biztos, hogy jó hatással lennének közérzetünkre, mindenki csak saját felelősségére nézze meg ezeket.

A deep web és dark web fogalmak együtt jó képet adnak arról, hogy a kibertér visszaélései mennyire rejtve maradhatnak az átlagos felhasználók, de gyakran az államok és cégek szeme elől is. Még kevesebb tudásra van szükségünk azonban, ha magánemberként proxy-t vagy VPN-t kívánunk használni saját online lábnyomaink elfedésére.

2.1.3. VPN és proxy

A VPN (virtual private network – virtuális magánhálózat) olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva, így a nyilvános hálózaton (pl. internet) belül védett kommunikációt valósít meg. (Muha 2004) A biztonságosságot, tehát azt, hogy ez a kapcsolat valóban „magán” legyen, az biztosítja, hogy a VPN-re csatlakoztatott eszközök és köztük az információ titkosítva, kódolva (encrypted) történik. Gyakran használják magáncégek, közigazgatási szervezetek, de magánszemélyek is. A VPN lehetőséget ad arra, hogy egy saját hálózaton megosztott adatokhoz férjünk hozzá, de arra is, hogy a VPN-en keresztül csatlakozzunk a nyilvános hálózatra (internet).

Témánk szempontjából mindkettő fontos. Egy VPN hálózatra való jogtalan behatolás vagy tartalmának jogosulatlan kimásolása, megmásítása, törlése ugyanúgy visszaélés a kibertérben, mintha a publikus neten történne, sőt!

Itt azonban a VPN-nek másik aspektusa izgalmasabb számunkra, hogy gondolkodásunkat formáljuk: VPN-en keresztül is elérhetjük a nyilvános tartalmakat. Miért érdekes ez? Ekkor ugyanis az történik, hogy míg az internetet használó emberek a szörfözés során nyomokat hagynak, legtriviálisabban az IP-címük alapján (lásd későbbiekben a Domain azonosítása résznél!), a VPN-en történő csatlakozás egy hálózatra sok előnnyel jár: elrejthetjük a saját IP címünket, használhatunk más IP címet, helyadatainkat is megváltoztathatjuk (Például budapesti lakásomból VPN-ent használva kiadhatom magam úgy, hogy Oroszországban vagyok épp, ez hasznos lehet például videómegosztó oldalakon, ahol az adott országban valamiért el nem érhető tartalmat szeretnénk megnézni). (Cisco Systems 2005) Fontos továbbá megjegyezni, hogy a VPN szolgáltatás önmagában nem biztosít internetelérhetőséget, ettől virtuális a hálózat. Illetve, ha valami okból VPN-t szeretnénk használni, figyeljünk arra, hogy a kért szolgáltatás valóban VPN-e, ugyanis nem mindegyik VPN-t ígérő szolgáltató hálózata titkosított. (Gálffy 2017)

Nyilvánvaló előnyei vannak a VPN-nek. Például Kínában Facebookot használni csak VPN-en keresztül tudunk, vagyis fontos az úgynevezett **geo-blockolt** tartalmak elérésében, ezenkívül saját magunk követhetőségének nehezebbé tétele is elsődleges szempont lehet, gondoljunk csak bele, annak sem örülnénk feltétlenül, ha valaki folyamatosan feljegyezné, mikor mentünk boltba, mikor vagyunk munkában stb. Illetve legáltalánosabb felhasználását se feledjük: az alkalmazottak elérjék a céges, belsős hálózatot és erőforrásokat, amikor otthon vannak. (Például a munkahelyünk, iskolánk előfizet egy szoftver használatára, amit jó lenne otthonról is elérnünk, erre megoldás a VPN). (Ikram et al. 2016) Viszont a VPN, mint minden eszköz, egyformán lehet hasznos és ártalmas. A bűnfelderítésben, a céges vagy közigazgatási, netalán magánjellegű visszaélések esetén a visszaélő kezében hasznos eszköz. Mi a helyzet utolsó fogalmunkkal, a proxyval?

A proxy szerverek úgy írhatók le, mint egyszerű virtuális csatornák internetforgalmunk számára, miközben az úton van a célszerver felé. Az említett szerver (és az útközben lévő routerek) számára a forgalom úgy fog megjelenni, mintha a proxy szerver címéről jönne, miközben az IP címünk és aktivitásunk magán a proxy szerveren kerül naplózásra (vagy nem). Sokan használnak proxy szervereket VPN hálózatok helyett, melynek fő oka, hogy nagyon sok ingyenesen használható proxy szerver is létezik, ugyanakkor jóval kevesebb védelmet adnak a felhasználójuknak, mivel a rajtuk folyó tartalom ritkán kódolt. Két fő típusuk van: a HTTP és a SOCKS proxy szerverek; az előbbin csak a http és https oldalakat érjük el, az utóbbin történhet SMTP, FTP, Torrent (tehát non-HTTP) forgalom is, viszont lassabbak, mint a HTTP proxy szerverek. Proxy szerverekkel kikerülhető a geo-blocking, ugyanakkor sokkal kevésbé nehezítik meg a felhasználó beazonosítását, mint a VPN-ek. (vpnMentor 2016)

Érdekesség, amikor a filmekben azt látjuk, hogy a föld térképén ide-oda ugrálva próbálják lenyomozni, honnan érkezett egy informatikai támadás – a többszörös proxy szerverek mögé bújt hacker utáni kutatást igyekszik vizualizálni.

Egy mondatot megérdemel még ennél a témánál a már korábbi, keretezett részben említett Tor (The onion router, ugyanis használhatjuk a Tor protokollt, hogy titkosítsuk és anonimizáljuk az összes forgalmat azáltal, hogy installálunk egy helyi Tor klienst, vagy csupán egy Tor böngésző szoftver segítségével webböngészünk. A Tor hátrányai közé soroljuk, hogy a titkosítási procedúrák miatt a legnagyobb mértékben lassítja a böngészést.

Látnunk kell, hogy egy-egy informatikai visszaélés felderítését rendkívül bonyolulttá tesszük ezekkel az eszközökkel. És mi a helyzet az így elkövetett bűncselekményekkel, vagy még inkább: országok közötti támadásoknál? Vehetünk-e hadüzenetnek egy-egy nagyobb volumenű kibertámadást egy ország ellen?

A következőben arra a kérdésre keressük a választ, hogy amikor a hírekben arról olvasunk, hogy valamely ország, jellemzően egy nagyhatalom információs visszaélést követ el egy másik országgal szemben, akkor miért nem állnak hadban egymással. Szoros összefüggést láthatunk a proxy, vpn fogalmakkal.

Megtámadták az országom a neten, hadban állunk?

Az interneten különbözőképpen hadban állhatnak és állnak is az országok. Manipulálhatják a gazdaságot, titkos információkat szerezhetnek meg, és ami manapság sokat szerepel a hírekben, választásokba szólhatnak bele, különféle álhírekkel, propagandával zavarhatják össze a lakosságot stb. Ezen utólagos eszközöket hívjuk lélektani műveleteknek a katonai szakzsargon szerint. Adott a kérdés: ha ilyen külső ország elleni lélektani műveletek érik az országot, felmerül-e a Washingtoni (NATO) Szerződés 5. cikkelye szerinti kollektív védelmi műveletek kiváltása, tehát a NATO országok kollektív hadba lépése az egyik tagállamukat veszélyeztető ország ellen. (NATO 1949) A válasz bonyolult. A NATO elismeri a légi, a földi, a vízi és speciális egységek harcászati nemei mellett a kibert is, de ez önmagában nem jelentene hadicselekvés általi hadba lépést a tagállamok részéről. Sir Adrian Bradshaw NATO-parancsnok szerint az 5. cikkely akkor lép életbe, amikor politikai döntés születik arról, hogy életbe lép, s emiatt mondhatjuk, hogy igen, az ilyen akciók válhatnak casus bellivé. (Dearden 2017)

Jean-Claude Junckernek, az Európai Bizottság elnökének az Unió helyzetéről szóló 2017-es beszédében is külön fejezetet kapott a kiberbiztonság, és hangsúlyozta a tagállamok közös fellépésének szükségét. (Európai Bizottság 2017) A Bizottság a beszédet megelőző ülésén azonban felmerült az ilyen támadások indítója elleni közös fellépés egyik legnagyobb akadálya: a kibertámadások elkövetőjét nagyon nehéz beazonosítani, a technológiai sajátosságok miatt azt is nehéz megállapítani, hogy egyáltalán melyik ország területéről származik egy-egy kibertámadás (beleértve a dezinformációs tevékenységeket, az álhírterjesztést és a fizetett trollokat is), bizonyítékokat szerezni arra, hogy nem egy egyén vagy kisebb csoport önálló tevékenységéről van szó, hanem összekötni az esetet az adott ország kormányával kifejezetten nehéz, így emiatt esetleg hadba lépni egy másik országgal eléggé problematikus, sőt sokszor még azt is csak feltételezni lehet, hogy valóban az adott országból történtek-e ezek a támadások. (Muncaster 2017)

Tehát nehéz beazonosítani egy kormányt a támadás mögött, akkor is, ha erre rengeteg eszköz áll rendelkezésünkre. Egy kisebb cég vagy hivatal esetén ez szintén gondot okozhat: a probléma alapvetően az, hogy a támadónak sokkal olcsóbb és gyorsabb az álcázást végrehajtania, mint a megtámadott félnek a felderítés és beazonosítás folyamatának költségei, ráadásul sok esetben nem is sikerül.

Természetesen semmi sem zárja ki, hogy ezeket a megoldásokat valaki többszörösen alkalmazza és/vagy együttesen... Illetve érdemes megemlíteni azt is, hogy a legtöbb VPN szolgáltató szabályos, bejegyzett vállalat, akiket a hatóságok bizonyos feltételek mellett kötelezhetnek arra, hogy adatot szolgáltassanak egy-egy felhasználó tevékenységeiről.

2.2. Az információs visszaélések céljai és területei

A következő alfejezetben bemutatjuk, milyen céljai és módjai lehetnek a kibertéren történő visszaéléseknek. Alapvetően érdemes megkülönböztetnünk azt, hogy a visszaélés személy ellen történik, vagy valamilyen szervezet rendszere ellen.

A cégek, államok informatikai rendszerei ellen elkövetett visszaélések konkrét céljait alapvetően három csoportba oszthatjuk:

1. az információs rendszer működésének zavarása,
2. adat megszerzésére irányuló támadás,
3. adat módosítására irányuló támadás.

Ezek tehát az adat, információ úgynevezett rendelkezésére állását (1.), bizalmasságát (2.) és sértetlenségét (3.) fenyegetik. Ezek a fogalmak azért is fontosak, mert a hatályos magyar jogszabályozás is nevesíti őket, segíti a biztonsági esemény fogalmának értelmezését.

A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról hasznos olvasmány a téma iránt érdeklődőknek. Találkozni fogunk még vele a későbbiekben. A törvény 1. szakaszának 1. pontja a következőként definiálja a fogalmakat:

- „8. bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról";
- „38. rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek";
- „39. sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség), és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható."

Míg a biztonsági eseményt így:

„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."

Az információbiztonságban, a kibertér védelmében kiemelt helye van az információs rendszereknek, és főleg az adatnak mint az információ hordozójának. A támadások így ezeket célozzák. A belőlük remélt haszon pedig a következő lehet:

- Pénzügyi: Az elkövető közvetlen vagy közvetett módon pénzt tud szerezni támadásából. A közvetlen mód lehet bankkártyaadatok megszerzése, a közvetett pedig valamilyen üzleti titok megszerzése majd eladása, esetleg valamilyen káros szoftver értékesítése. Ide tartozik a részvények értékeinek manipulálása is vagy épp a zsarolás valamilyen bizalmas információ megszerzésével.
- Ideológiai: Az egyén, cég, állam, politikai párt stb. reputációját, hírnevét kívánja megsérteni. Ez sokféleképpen történhet: hamis hírlevéllel, szolgáltatás akadályozásával vagy helytelen működtetésével.
- Politikai: Cégpolitikai elsősorban, a cégek stratégiai döntéseinek, titkainak kikutatása.
- Presztízs vagy kíváncsiság: A támadás célja egyfajta játék, bizonyítási kényszer, kihívás elfogadása. (Például a Vatikán legendás tűzfalát, az arkangyalról elnevezett Michael-t feltöréséig feltörhetetlennek híresztelte a média, ami miatt számos cracker (hacker) célpontja lett [Tagliabue 1999])

Az adatokat, amelyek ellen a támadás történik, is kategorizálhatjuk mint az információs visszaélések területeit:

- pénzügyi adatok,
- személyes adatok,
- üzleti titok jellegű adatok,
- zárt állami nyilvántartások adatai.

Magánszemélyek (vagy kisebb méretű cégek ellen, akikkel az elkövetőnek valamilyen személyes kapcsolata van) ellen a támadások motivációi gyakran sokkal személyesebbek, de hasonlóképpen néznek ki. Adat megszerzésére irányulnak, a célpont hírnevének bemocskolását célozzák, az elkövető a saját hatalmát kívánja efféleképpen megélni a másik fölött. A jelen műben nem a magánszemélyek ellen elkövetett visszaélésekre koncentrálunk, ugyanakkor jegyezzük meg, hogy a legtöbb alább felsorolt módszer hatékony magánszemélyek ellen is, illetve gyakran a magánszemélyeket célzó visszaélések közvetett támadást jelentenek egy cég vagy hivatal ellen.

Érdemes még megemlíteni, hogy kik lehetnek az elkövetők:

- hackerek,
- ipari kémek,
- külföldi államok által megbízott hivatásos hírszerzők,
- személyes adatok ellopásával foglalkozó bűnözők,
- elégedetlen munkavállalók,
- konkurens vállalkozások megfigyelői,
- magánnyomozók,
- csalók,
- fejvadászok (akár bűnügyi, akár munkajogi értelemben),
- terroristák. (Muha–Krasznay 2014)

Az elkövetők motivációi széles skálán mozoghatnak. A következő esetben egy hackercsoport támadását mutatjuk be, ahol az egyik cél egy internetes portál által tárolt adatok biztonságának növelése volt (és egyfajta erkölcsi igazságtétel), persze az anyagi haszonszerzés mellett.

Ashley Madison breach

Az Ashley Madison társkereső oldal súlyos biztonsági sérülést szenvedett 2015-ben, amelynek következtében több mint 300 GB felhasználói adat került ki, beleértve a felhasználók valódi nevét, bankadatait, hitelkártyás tranzakcióit, titkos szexuális fantáziáit. Az Ashley Madison tökéletes példája lett a biztonsági menedzsment hibáinak.

A támadás után a The Impact Team hackercsoport fenyegető üzenetet küldött a site tulajdonosainak, akik azonban nem elégítették ki a hackerek igényeit, amire ők válaszként több ezer felhasználó személyes adatait hozták nyilvánosságra. Cselekedeteiket azzal indokolták, hogy az Ashley Madison hazudott a felhasználóiknak (diszkréciót ígért), holott nem védte megfelelően az adataikat. Az Ashley Madison többek között azt állította, hogy a felhasználók 19 dollár megfizetése után teljesen törölhetik személyes fiókjaikat. Azonban a The Impact Team szerint csak a fiókokat törölték, a hozzájuk tartozó adatok megmaradtak. Egy másik ígérete a cégnek az volt, hogy az érzékeny bank- és hitelkártya-információkat törlik a felhasználók kérésére. A vásárlási adatokat sem távolították el, a vásárlásokat tartalmazó adatbázisok a felhasználók valós nevét és címét tartalmazták.

Azóta a website tulajdonosai intézkedtek a helyes adatkezelésről, ugyanakkor még sokáig zsarolták őket a már kikerült adatokkal, arról nem is beszélve, hogy hatósági intézkedés is történt az oldal ellen helytelen adatkezelés miatt. A helytelen adatkezelésen túl további tapasztalatok is levonhatók az esetből. Az Ashley Madison felhasználói fiókjai, jelszavai nem voltak elég biztonságosak, illetve titkosításuk sem volt elég kifinomult, úgynevezett brute force módszerrel fel lehetett őket törni. További hiba volt, hogy a site korábbi fejlesztőinek a hibáit a későbbi fejlesztők nem javították ki, így biztonsági rések maradtak az oldalon. A kiberbiztonsági audit megállapította, hogy a belső, céges felhasználók is károkat okoztak a rendszerben, ezeket megfelelő, szigorú előírásokkal, naplózással, monitoringgal és auditálással ki lehetett volna szűrni. (Panda Security 2017)

Az esetből levonható tanulság, hogy lényegében bármi okozhat ellenünk támadást, bármiért lehetünk célpontok. Érdemes tehát a célponttá válás esélyének csökkentése mellett is figyelnünk az adatkezelésünk és rendszereink védelmére, akár magánszemélyként is.

3. Az információs visszaélések formái

Az információs visszaélések számos formáját ismerjük. Ezeket két csoportba tudjuk sorolni attól függően, hogy emberi tényezők által következnek be, vagy valamilyen informatikai rést használnak ki:

- valamilyen rosszindulatú szoftverrel (malware) előidézett információs visszaélés,
- social engineering módszerrel előidézett információs visszaélés (humán és nem humán eredetű visszaélések), korrupció.

A továbbiakban ezeket fejtjük ki.

3.1. Rosszindulatú szoftverrel (malware) vagy más informatikai megoldással előidézett információs visszaélés

A rosszindulatú számítógépes programokat a köznyelv vírusnak nevezi, egyfajta gyűjtőfogalomként, a szakértők inkább a malware[2] gyűjtőnéven foglalják össze őket. Ide soroljuk az alábbiakat elsősorban a Muha–Krasznay (2014, pp. 82–83.) szerzőpáros, illetve Adebayo és társai (2012) szerint.[3] Mindkét mű nemzetközileg is elismert szerzők tollából származik, akik átfogóan elemzik a kártevők témáját, ugyanakkor mindig akadnak újabb vagy kevésbé relevált malware-ek:

- **vírus (virus):** „Vírusnak egy olyan programot nevezünk, amely képes arra, hogy önmagát reprodukálja, azaz szaporodjon, figyelembe véve mindig változó környezetét. A vírusok számtalan fajtáját különböztethetjük meg. Egy részük a lemezek boot-területét fertőzi meg, ezek a bootvírusok. Mások a bináris programkódot tartalmazó programfájlokat támadják, és abban helyezik el a futtatandó víruskódot, ezek fájlvírusok. A harmadik nagy víruscsalád tagjai a fentiekkel ellentétben nem bináris kódú programokat fertőznek, hanem dokumentumfájlok belsejében helyezik el szerkeszthető szövegként vagy védetten, rejtetten programkódjukat, és célpontjaik, támadáspontjaik többsége is elsősorban, bár nem kizárólag, további dokumentumokra irányul. Ezt a víruscsaládot nevezzük makróvírusoknak. Mintegy mellékszolgáltatásként egyes makróvírusok képesek „hagyományos” bináris víruskód elszórására is (dropperek), valamint több tucatnyi makróvírusfejlesztő-készletet is ismerünk, amelyekkel bármiféle előképzettség nélkül is lehet újabb vírusváltozatokat is gyártani. A makróvírusok után egy újabb értelmezőt igénylő víruscsalád is megjelent, a scriptvírusok. Amíg a makróvírusok kódja bonyolult fájlszerkezetű dokumentumfájlokban rejtőzködik, addig a scriptvírusok többsége közönséges szövegfájlokban vagy áttekinthető és dokumentált struktúrát használó HTML-fájlokban található. Az utolsó típus voltaképpen nem a felépítés, hanem a preferált szaporodási mód miatt alkot egy egyre bővülő csoportot. Ez a levelezővírusok csoportja.”
- **féreg (worm):** „A rosszindulatú programok második típusa. A vírusoktól annyiban különböznek, hogy kódjukat nem a lemezek bootszektorába vagy más programok belsejébe építik, hanem azt egyszerűen önálló fájlban tartalmazzák, és ezt másolva sokszorozzák. A szaporodás során természetesen módosítják azokat a fájlokat is, ahonnan programindítás lehetséges. Az elektronikus levelezéssel és a hálózatos alkalmazások elterjedésével a programférgeknek számtalan típusa alakult ki.”
- **követő „sütik” (tracking cookies):** „Olyan kis adatok, amik a web böngészés során képesek egy adott weboldalon történő aktivitás követésére, ezáltal a weboldalról és felhasználóiról bizonyos adatok megszerzésére használhatók.”

[2] A malware az angol malicious software, azaz rosszindulatú program kifejezésből képzett mozaikszó.
[3] Ahol más forrást használtunk, külön feltüntettük.

- **logikai bomba (logic bomb):** „Olyan programkártevők, amelyek néha külön programként, de jóval gyakrabban nagyméretű és bonyolult szoftverek belső, rejtett rutinjaiként kerülnek be a számítógépes rendszerekbe. Ezek többségét olyan programozók követték el, akik bizonytalan vagy annak érzett pozíciójukat rejtett időzített bombák elhelyezésével igyekeztek megerősíteni. A rosszindulatú, a rendszer leállásával és sokszor teljes összeomlásával járó rutinok akkor aktivizálódtak, ha programozójuk például lekerült a fizetési listákról, vagy elmulasztotta átírni a késleltetési periódust megszabó programrészleteket. A levélbombák olyan kisméretű alkalmazások, amelyek egyetlen funkciója a pusztítás. Elnevezésük onnan ered, hogy gyakran érkeznek e-mailekhez csatolva."
- **trójai faló, trójai program (trojan horse):** „Közös jellemzője, hogy valamely más program programkódjába rejtve tartalmaznak oda nem illő, rendszerint kártékony hatású programrutinokat. A trójai program – amíg el nem indítják, és kártékony munkáját el nem végzi – hasznosnak látszik. Igen gyakran más hasznos, ismert program preparált változata. A trójai programok célpontjai azok a számítógép-felhasználók, akik ellenőrzés nélkül indítanak el az internetről letöltött, elektronikus levélben kapott vagy más, rendszerint ismeretlen és ellenőrizetlen (sokszor teljesen ellenőrizhetetlen) forrásból származó programokat. Vannak olyan trójai programok is, amelyek kémprogramokat, jelszó-tolvajokat, backdoor-programokat tartalmaznak, de ezeken kívül is sok más változatot különböztethetünk meg." Speciális változataik a dropperek: ezek az eszközre jutva legyártanak pár vírust vagy más malware-t valamilyen algoritmus alapján. Nem önmagát szaporítja, hanem új szoftvereket alkot. (Kovács 2018)
- **hátsó ajtó vagy csapóajtó (backdoor/trapdoor):** „A megtámadott gép felhasználójának tudomása és engedélye nélkül – a helyi hálózaton, soros vagy párhuzamos porton vagy modemen keresztül összeköttetést teremt és adatcserét biztosít a megtámadott gépre felkerült szerver-komponens és a támadónál üzemelő kliens-komponens között. Így a támadó adatokat tölthet le a megtámadott gépről, illetve azon keresztül a megtámadott hálózatról, vagy ez fordítva, azaz feltöltést (is) biztosít a backdoor. A megoldástól függően átveheti a vezérlést a rendszer felett."
- **Coin-mining:** Nem illegális eszközök, a kriptovaluták bányászását végző programok, amelyek számítási kapacitást használnak a bányászathoz, ami megjelenik a blockchain-ben (blokklánc – nem témája az anyagunknak). Egyes kriptovaluták (mint a legismertebb Bitcoin) nagyon magas számítási kapacitást igényelnek a bányászatuk során, míg mások (pl. Monero) egy otthoni személyi számítógéppel is könnyen bányászhatók. A fájl-központú bányászathoz programokat kell futtatni a gépen, a böngésző típusú bányászathoz pedig a webböngészőben script-eket futtatva „bányász". Ez utóbbi gyakran úgy történik, hogy amíg egy weboldalon tartózkodunk, a háttérben a gépünk számítási kapacitásának egy részét kriptovaluta bányászásra használja fel. A probléma az, hogy erről gyakran nem tud a felhasználó, vagy a kriptobányászok illegálisan bányászprogramokat telepítenek a felhasználó gépére. Mindkettő teljesítménycsökkenéssel, illetve magasabb elektromos áram fogyasztásával jár. A coin-mining is tehát egyfajta visszaélés a kibertérben. (Symantec, 2018)
- **mobil kód (mobile code):** Ezek olyan káros kódok, amelyek kifejezetten a mobileszközökön történő kommunikációt akadályozzák. A kódot egy távoli rendszerről továbbítják, és egy helyi rendszeren hajtatják végre. Vírusokat és férgeket is képesek továbbítani.
- **rootkit, a UNIX-os rendszergazda (root) és az installálócsomag (kit) összevonásából ered:** „A backdoor-programokhoz hasonlóak. Eredetileg Unix (Linux) platformra találták ki ezeket a kártevőket. A rootkitek igen kis méretűek, és valamilyen vírus vagy trójai program segítségével juttatják be a fertőzött számítógép operációs rendszerébe." Feladatuk például a számítógép

különböző erőforrásainak (pl. processzorkapacitás) elvonása. A számítógép létfontosságú erőforrásait (BIOS, Kernel, Boot betöltő stb.) támadják.

- **billentyűzetfigyelők (keylogger):** Egyszerűen telepíthető szoftverek, lényegében bárki használhatja őket, érdekességük, hogy visszaélések ellen is használják őket, illetve szülői felügyelet szempontjából is. Két fő típusuk van: az egyik csak a billentyűleütéseket naplózza, a másik a képernyőt is rögzíti folyamatosan vagy bizonyos időközönként. Ebből kifolyólag általuk ellenőrizhetők egy adott gépen végrehajtott műveletek, ami hasznos lehet valamilyen terminálról elkövetett visszaélés felderítésében, vagy szülőknek, ha gyermekeik internetezését akarják teljeskörűen ellenőrizni, de használják programozók is, például saját, munkafolyamataik közben elvétett hibáik felderítésében. A keyloggerek akkor válnak ártalmassá, ha tudtunkon kívül telepítik őket, és az adatokat megkapja valaki más, megszerezve így jelszavainkat, beszélgetéseinket. (Tuli–Sahu 2013)
- **kémprogram (spyware):** „A megfertőzött számítógép memóriájában vagy adattárolóin kutakszanak." Ezentúl, ahogy a nevéből adódik, lényegében képes egy kém munkáinak bizonyos szintű elvégzésére is: nemcsak információt tud szerezni, online vagy offline eszközökről, hanem módosításokat is elvégezhet, miközben titokban tevékenykedik, ezzel hamisítva adatokat, számítógépek beállításait, vagy mondjuk automatizált gyárak termelősorait.
- **bűnprogram (crimeware):** Speciálisan sokoldalú visszaélésre tervezett malware. Felhasználófiókokba való belépésre találták ki. Egy másik felhasználónak adja ki magát, és megszerzi a kívánt adatokat. Lényegében automatizálja a social engineering módszerekkel megszerezett adatokat, azok alapján a bejelentkezéseket és az adatlopásokat, mondhatni: három legyet egy csapásra!
- **agresszív reklámprogramok (adware):** Az olyan, interneten terjedő számítógépes programok összességét nevezzük így, amelyek célja, hogy egy terméket, számítógépes programot, annak készítőjét vagy egy céget reklámozzanak. Bár sok reklámprogram egyben kémprogram is (angolul: spyware), azonban mégis fontos a megkülönböztetés. A kémprogram minden esetben igyekszik elrejtőzni a felhasználó elől, működése során különféle károkat okoz, ezek miatt a legtöbb országban törvénytelen a használatuk, az adware-k viszont a felhasználó orra előtt működnek. Az általuk megszerzett információkat üzleti célokra (pl. célzott reklámok létrehozása, felhasználói statisztikák, profilok készítése stb.), vagy akár nem törvényes (kéretlen reklámlevelek, lásd spam) módon használják fel.
- **zsaroló programok (ransomware):** A megfertőzött eszközre jutva titkosítják a felhasználó fájljait. Az elkövető a titkosítás feloldását lehetővé tevő kódért váltságdíjat – pénzt vagy bitcoint – kér cserébe, természetesen saját adatait nem tárja fel.
- **ijesztgető programok, vagyis inkább báránybőrbe bújt farkasok (scareware):** Hamis vírusirtó szoftver, amely úgy tesz, mintha egy felhasználó eszközét ellenőrizné, és ott rosszindulatú programokat vagy biztonsági fenyegetéseket keresne. Ehelyett titkosítja a merevlemezt, így a felhasználónak fizetnie kell annak eltávolításáért. Egyfajta ransomware-ként működik. (Kovács 2018)
- **átverés, álhír, kacsa (magyarban is használatos: hoax):** Rémhírek vagy lánclevelek. E-mail, ami önmagában kárt nem okoz, magától nem terjed. A felhasználók azok, akik gondolkodás nélkül, lelkesen, akár több száz példányban is továbbküldik ezeket, és ezzel az esetleges rémhírterjesztésen kívül még hatalmas fölösleges forgalmat is generálnak a hálózaton. A „küldd el 20 ismerősödnek 5 napon belül, és akkor nagy szerencse ér" vagy a „szegény szerencsétlen rákos gyermekek, akik 1 dollárt kapnak minden elküldött levélért" szövegnél

csak „az első tíz beküldő egy notebookot kap” vagy „ha megnyitod a … fejlécű levelet, akkor a géped azonnal felrobban” szöveg a hatásosabb”.

- **levélszemét (spam):** A spam kéretlen, nagy példányszámban elküldött, azonos tartalmú elektronikus üzenet. Szó szerinti jelentése: löncshús konzerv, amely az elnevezés alapjául szolgáló Monthy Python burleszkben szerepelt. Kéretlen, mert a küldője nem kapta meg előzetesen a címzett hozzájárulását. Nagy példányszámú, ha lényegileg ugyanazt az üzenetet a feladó sok címre küldi el. Azonos tartalmúnak számítanak az üzenetek, ha csupán részletekben különböznek egymástól; azaz ha például különböző a címzett neve, ügyfélszáma, vagy véletlenszerűen elhelyezett szavak, karakterek, számok, képek szerepelnek a levélben; esetleg más szavakkal van megfogalmazva ugyanaz a téma. Fontos, hogy mindhárom feltételnek teljesülnie kell, ha spamről akarunk beszélni, a nagy példányszám és azonos tartalmúság például igaz a felhasználó által kért hírlevelekre is. A spamek önmagukban inkább csak idegesítőek, illetve a levelezőfiókban töltik ki a helyet, de velük gyakran érkezhetnek mellékletben, vagy hiperlink formájában más kártékony szoftverek is, ezért nem érdemes őket megnyitni, de a bennük található linkekre kifejezetten tilos kattintani. (virushirado.hu)
- **szolgáltatásmegtagadással járó támadások (közismertebben: DoS – Denial of Service):** A támadás alapvetése viszonylag egyszerű: olyan mennyiségű kérést (lekérdezést) kell intézni az adott célpont felé, amely azt kapacitás hiányában már nem tudja kiszolgálni. A nagy mennyiségű lekérdezés azonban egyrészt sok számítógépet, másrészt ezeknek a számítógépeknek az egyidejű és koordinált tevékenységét feltételezi. Három fajtája van: **hagyományos** (ekkor a támadó erőforrásai egyszerűen csak meghaladják a célpont erőforrásait, így kvázi az egyik gép legyűri a másikat); az **elosztott túlterheléses** (a hírekből is ismerhető DDos – Distributed Denial of Service; a támadó nemcsak egy, hanem sok olyan eszközt használ a megcélzott számítógép erőforrásainak túlterhelésére, amelyek nem egy végpontban, hanem a világon bárhol lehetnek. Az összehangolt támadók erőforrásai egy irányba hatnak, azaz összeadódnak, így haladva meg a megtámadott számítógép erőforrásait.); végül a **felerősített elosztott túlterheléses támadás** (ez abban különbözik a második kategóriától, hogy a támadónak nincs minden, az akcióban résztvevő gép felett ellenőrzése). A DoS támadások végrehajtásához gyakran használnak **botneteket:** ez olyan megfertőzött gépek hálózata, amelyek felett részben vagy egészben valaki más rendelkezik, úgynevezett zombigépeket hozott létre céljai elérése érdekében: bankot rabolni is jobb lopott kocsival, mint a sajátunkkal, nem igaz? (Kovács 2018)
- **tranzakció visszaélés (hamis tranzakciók – false transactions/tranzakció elfogás – intercept transactions):** Ezeknek a támadásoknak a közvetlen célja a pénzszerzés. Általában szükség van hozzájuk olyan emberre, aki ismeri egy adott bank vagy cég pénzügyi tranzakcióit. Vagy hamis tranzakciók indításával jut ingyen termékekhez, esetleg hátrál ki utána a vásárlásokból, hogy visszakapja a soha ki nem küldött pénzt, vagy a kimenő vagy bemenő tranzakciókat téríti el, hogy a pénz egy általa megjelölt számlán landoljon. A tranzakciók persze nemcsak pénzügyiek lehetnek, adatáramlásokról beszélünk általánosságban, ugyanígy meg lehet szerezni adatokat is, sőt ott leplezni lehet az egész műveletet úgy, hogy nem térül el az adatfolyam, hanem csak lemásolják. (Parker 2017)
- **APT (Advanced persistent threat):** Az APT magas szintű, tartós vagy más néven (és az anyagban is használt) célzott támadás, olyan titkos és folyamatos számítógépes hackerfolyamatok sorozatát jelenti, amelyeket gyakran meghatározott személy, személyek vagy szervezet ellen követnek el. Az APT általában magánszervezetek, államok vagy mindkettő ellen irányul, és üzleti vagy politikai motívumok vezérlik az elkövetőket. A cél általában

információszerzés, de előfordult már olyan támadás is, melynek célja a szabotázs volt. Tartós, megbúvó irányítása szerverek vagy más informatikai eszközök részét képezi.

Az egyik legösszetettebb támadási forma az APT malware-rel elkövetett támadás. A következőben nézzünk erre egy példát!

Carbanak támadássorozat

A Carbanak egy APT jellegű támadássorozat volt 2014-ben és 2015-ben.

A Carbanak hackerek a klasszikus, felhasználókat célzó támadások helyett a bankok belső rendszereit vették célba, és több mint 100 bank vált áldozatukká (átlagosan 8 millió dollárt szerezve tőlük). A csoport azt használta ki, hogy bár a bankok és más pénzügyi intézetek mindig kiemelten kezelték az ügyfeleikkel kapcsolatos adatbiztonsági előírásokat, de saját rendszereik kiberbiztonsági szempontból gyakran elavultak és elhanyagoltak voltak. Kezdetben phising e-mailekkel, megtévesztő mellékletekben tárolt malware-ekkel (trójai programokkal) jutottak be a gépekre, keyloggerekkel szerezték meg a hitelesítő adatokat. A banki rendszerek elavult irányítási és észlelési metodikái nem állították meg a hackereket. Végül a támadás napján elkezdődött a megszerzett gépek és adatok felhasználása, hamis számlákat hoztak létre, amelyekre utalgatták a pénzeket, majd azokról le, az ATM-ekhez csatolt gépekről (gyakran elavult, már nem támogatott operációs rendszer futott rajtuk, így lényegében semmi kihívást nem jelentettek a csapat számára) kiadatták az ATM-ekben lévő pénzeket, a csapat egy-egy megbízott embere pedig begyűjtötte. Felülírták a bankok saját és nemzetközi tranzakciós megkötéseit, hogy minél nagyobb tételeket tudjanak egyszerre elrabolni. Mindenféle e-pay vásárlást hajtottak végre. Azóta az ukrán hackercsapat tagjait letartóztatták. (Kessem 2015)

Az eset tanulsága: Ne könnyítsük meg a támadók dolgát, használjuk az anyagban is leírt szervezeti előírásokat, tartsuk frissen rendszereink védelmét. Használjunk megfelelő detektálási eszközöket, frissítsük rendszeresen szoftverállományunkat! A régi, elavult szoftverek könnyű célpontok, az elhanyagolt, de hálózatra csatlakoztatott hardvereink szintén szemet szúrhatnak a támadóknak; legyünk tisztában a teljes informatikai rendszerünkkel, és rendszeresen végezzünk ellenőrzéseket.

A kérdés már csak az, honnan szerezhetjük be ezeket a kártevőket. Hogy kerülhetnek magáneszközeinkre vagy hivatali, céges eszközeinkre ezek a programok? Nos, elég sokféleképpen, és általában emberi tényezők miatt jutnak be gépeinkre. Sokan mondják: nem kellene annyi pornót nézni! Köztudott ugyanis, hogy bizonyos emberi igényeket kielégítő weboldalakon hemzsegnek a malware lehetőségek. Azon se kell csodálkozni, ha ingyen akarunk megszerezni valamit (szoftvert, filmet), és kártevők jelennek meg gépeinken azokról az oldalakról, ahol végül megtaláljuk őket.

Személyes ismerős esete – hamis szoftverek

Személyes ismeretségemben (Molnár László a.k.a. szerző) is előfordult már, hogy valaki egy amúgy is ingyenesen letölthető webböngésző helyett éveken át egy megszólalásig hasonló szoftvert használt, név-felület egyaránt stimmelt; az buktatta le, hogy a felhasználói fiókomba nem tudtam bejelentkezni – természetesen az eset után a valós felhasználói fiókomnál jelszót változtattam. Nem emlékezett, honnan szerezte, valószínűleg megszokásból nem a cég oldaláról töltötte le, hanem valamilyen kétes szoftverbázisról. Szerencséjére nem használt webbankot.

Ami azonban még ijesztőbb, hogy sokszor ellenőrzöttnek hitt források is nyüzsögnek a malware-ektől. Nemzetközileg ismert informatikai cégek esetén gondol a legkevésbé az ember arra, hogy kártevővel szennyezett szoftverbázisokat tartanak fenn, a gyakorlatban azonban ez nem is olyan ritka eset.

Veszélyes mobilalkalmazások egyenesen a Google Play-ből és az AppStore-ból *(Horváth et al. 2016)*

A biztonsági cégek elemzői többször és alaposan átvizsgálták az Android és iOS (Apple) okoseszközökhöz tartozó alkalmazás-áruházakat: a Google Play-t és az Apple AppStore-t. Számos veszélyes applikációt találtak megbújva az elérhető alkalmazások között.

A Play áruházban scareware, phishing, ransomware és trójai programok is bőségesen akadtak. Ezek főként játékoknak, játék kiegészítőknek, közösségi alkalmazásoknak álcázták magukat. (Constantin 2015) Sok esetben ezek a kódok a telepítés után késleltetve, időzítetten változnak meg, és teljesítik ki kártékony, valódi tevékenységüket, így tudnak átcsúszni a Google szűrőin, amivel az áruház tartalmát hosszú távon is kompromittálhatják.

Az AppleAppStore-ba 300 fertőzött alkalmazás került fel, miután a támadók sikeresen elterjesztették az XCode (Ducklin 2015) fejlesztőeszköz fertőzött verzióit: az applikációk létrehozásához és a legális fejlesztői aláírás megszerzéséhez szükséges, ami nélkül nem engedélyeznek iOS alkalmazást. Az alkalmazás-fejlesztők így tudtukon kívül helyeztek el olyan, a programozás során automatikusan generált kódrészleteket applikációikban, amelyek a jövőben kártékonyak lehettek.

Emellett a szakértők még több mint 250 alkalmazást találtak az AppStore-ban (ESET 2015), amely valamilyen módon megsérti az Apple adatvédelmi rendelkezéseit, vagyis email címeket, bejelentkezési adatokat, kulcsokat, szériaszámokat gyűjtenek.

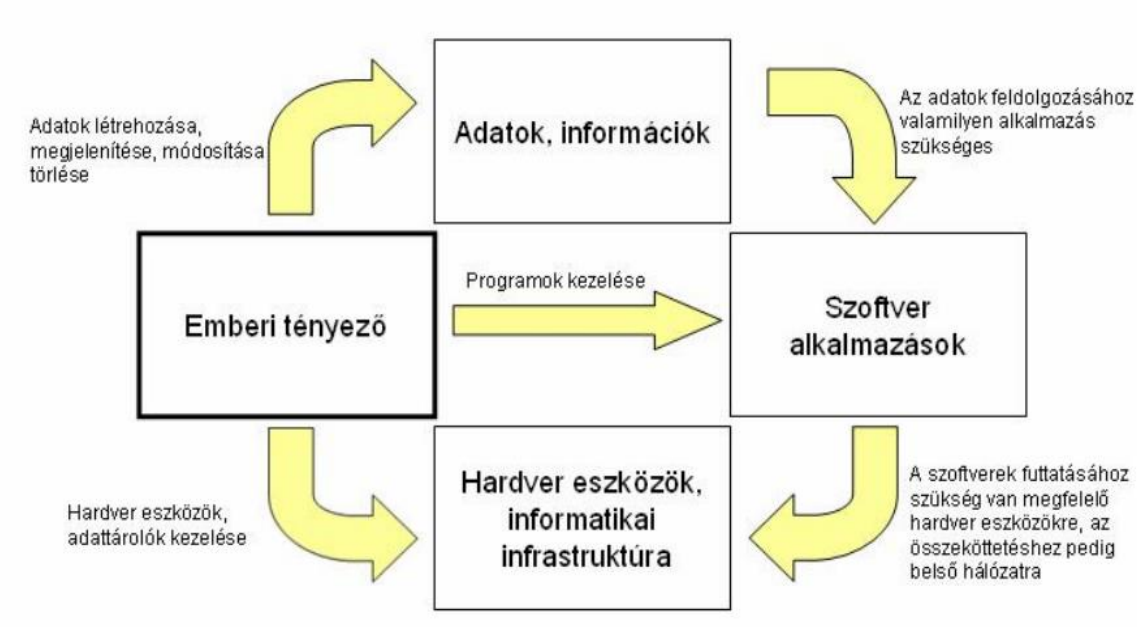
A tanulság, hogy nem bízhatunk meg senkiben és semmiben. A kiberbiztonsággal foglalkozó szakértők persze nem alaptalanul paranoiásak, mégsem kell teljesen csüggednünk. Több módja is van az ilyen veszélyek szűkítésének. Az egyik és legköltségesebb, ha saját magunk fejlesztünk mindent, ugyanakkor, mivel nehéz garantálni, hogy rendelkezünk az informatikailag 100%-os biztonságosság know-how-jával, illetve nincs korlátlanul rendelkezésre álló tőkénk sem szoftverfejlesztésekre, nézzük meg, milyen más eszközeink vannak.

Az egyik az, hogy nyílt forráskódú szoftvereket használok, amelyek esetében informatikusainknak lehetőségük van átnézni az esetleges problémákat, elemezhetik a szoftver működését. A telepítendő szoftver tesztelését elvégezhetjük zárt környezetben akkor is, ha szoftverbázisokról szereztük be. Érdemes figyelnünk a hálózati forgalmat is, a tűzfalbeállításainkat is. A rendellenes viselkedés eltűrése vagy a megalapozatlanul kiadott tűzfalengedélyek sok problémát okozhatnak. Letöltés és telepítés előtt pedig informálódjunk a szoftver készítőiről, a letöltést biztosító cégről, nézzünk felhasználói értékeléseket, esetleg fórumtémákat, amelyek érinthetik a szoftver kiberbiztonsági attribútumait.

3.2. Social engineering módszerrel előidézett információs visszaélés

A social engineering fogalomnak napjainkban nincs igazán jó magyar megfelelője, így viszonylag nehéz pontos definíciót alkalmazni rá. Kevin D. Mitnick, a „legendás hacker” az alábbiak szerint fogalmazott: „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.” (Bányász 2018 idézi Mitnick 2003-t.)

A fogalomdefinícióból láthatjuk, hogy érdemes elkülöníteni a számítógépes eszközzel és az anélkül lefolytattott social engineering módszereket. Ahhoz, hogy megértsük, miért is olyan lényeges terület az ember támadása a kibertérbeli visszaélések esetén, vizsgáljuk meg az alábbi ábrát:



5. ábra: Az emberi tényező kapcsolata a védendő értékekkel. Forrás: Bodó et al. 2018.

Az ábrán látható, hogy az emberi tényező hol játszik szerepet az információfeldolgozása során, a mindennapi hardveres és szoftveres eszközök használatában. „A felhasználók azok, akik dolgoznak a hardver eszközökkel, esetleg elvesztik, vagy felelőtlenségüknek köszönhetően könnyedén el lehet tulajdonítani tőlük azokat, de ugyanúgy ők dolgoznak a különféle szoftverekkel, alkalmazásokkal, melynek működését szívesen megmutatják egy esetleges támadónak, vagy épp nemtörődöm módon »leokézzák« az el sem olvasott üzeneteket a felugró ablakokban. Szintén az emberi tényező fér hozzá megfelelő jogosultságai révén szenzitív adatokhoz, egész adatbázisokhoz, melyekben véletlenül vagy akár befolyásolás hatására szándékosan is módosíthatnak rekordokat. Ezek mellett nem szabad elfelejteni azt sem, hogy a munkavállalók ismerik azokat a jelentéktelennek tűnő belső információkat (pl. szabadságolások, helyi szokások, helyettesítési rendek, folyamatok stb.), melyeket egy Social Engineeringgel kombinált visszaélés esetén remekül fel lehet használni egy támadás megtervezéséhez és kivitelezéséhez, hiszen helyismeretet szerezve mind az épületben, mind a virtuális térben könnyebben kiigazodunk potenciális támadóként. Nem szabad megfeledkezni arról sem, hogy a munkavállalók tartják a kapcsolatot mind egymással, mind külső felekkel (ügyfelek, partnerek, beszállítók stb.), mely akár telefonos, akár elektronikus kapcsolattartás esetén könnyedén kihasználható egy social engineer által. És talán a legfontosabb: az emberi tényező rendelkezik rengeteg kihasználható tulajdonsággal, melyet a social engineer beállítottságú támadók ismernek és előszeretettel ki is használnak.” (Bodó et al. 2018, p. 77.) Céljai ugyanazok, mint bármilyen más információs visszaélésnek, ám általában nemcsak adatokat, információkat és üzleti titkokat akar egyszeri alkalommal megszerezni a támadó, hanem hosszú távú, távoli elérhetőséget akar kiépíteni valamely védett szerverrel, géppel, hogy a zárt, belsős hálózatról vagy konkrétan egy-egy gépen tárolt offline adatokat bármikor el tudja érni, azok frissülésekor is.

A social engineering módszerek a kihasználható emberi tulajdonságokra épülnek. Ezeket a következőképpen tudjuk kategorizálni (Bodó et al. 2018):

- személyes tulajdonságok,
- munkahelyi tulajdonságok,
- pillanatnyi tulajdonságok,
- stresszhelyzet okozta tulajdonságok.

A humán alapú social engineering módszerek, amelyekhez közvetlen, személyes kontaktus szükséges a támadó és áldozata között, a következők (Muha–Krasznay 2014; (Leitold 2014):

- segítség kérése: a támadó segítséget kér, a célpont pedig szívesen segít;
- segítség nyújtása: általában a támadó teremt egy helyzetet, amikor felajánlhatja segítségét a célpontnak, így nyerve el bizalmát, és információkat szerez meg tőle;
- kölcsönösség kihasználása: a támadó korábban megtett valami az áldozatnak, most azt kéri vissza;
- megszemélyesítés: a támadás során a támadó egy hitelesített személynek (biztonsági cég alkalmazottja, vízszerelő) adja ki magát, így szerez meg bizalmas információkat;
- shoulder surfing – képernyő lelesése: a célpont válla fölött a támadó a mobilra, monitorra kukucskál;
- tailgating: bejutás a bejáraton más embert követve, annak tudtán kívül;
- piggybacking: bejutás a bejáraton más embert követve, annak tudtával;
- dumpster diving: információk felkutatása a hulladékban.

Klasszikusan nem szokás a social engineering módszerek közé sorolni (mivel a célpont ekkor nem marad ártatlan), de tényezőit vizsgálva mégis ideérthetjük a korrupciót, amiről még lesz szó a későbbiekben egy külön fejezetben.

A támadás felépítése a támadó részéről a következő négy lépcsőből áll (Leitold 2014):

1. Információszerzés: minőségi és mennyiségi információ szükséges ahhoz, hogy a támadó behatárolja a megfelelő embereket mint potenciális célpontokat. Általában a vállalati, szervezeti weboldalakról, közösségi portálokról, netes keresőkről könnyen meg lehet szerezni a szükséges információkat, ha mégsem, telefonon is érdeklődhet („XY vagyok a humánosztályról, szeretném kérni az informatikai vezetőt, mert főnököm ZX megkért...”), de történhet levélben, e-mailben, akár személyesen is vagy a szemetesből.
2. Kapcsolat kiépítése: ez lehet rövid távú, egyszeri segítségkérés például, de egy pszichopata elkövető akár arra is vetemedhet, hogy a célszeméllyel hónapokig tartó jó barátságot, vagy még többet alakít ki, hogy bizonyos adatokat meg tudjon szerezni, vagy be tudjon jutni valamilyen helyre.
3. Kapcsolat kihasználása: a kiépült kapcsolat révén alkalmat szerez, hogy a tervet végrehajtsa.
4. Támadás végrehajtása: a kapcsolat kihasználása révén például távoli hozzáférést szerez az elkövető bizonyos szerverekhez, számítógépekhez, eljött hát az aratás ideje.

A következőkben a számítógép-alapú Social Engineering módszereket mutatjuk be (ezek: adathalászat, hamis weboldalak használata és a baiting).

A következőkben egyfajta tömeges social engineering módszernek tekinthető megoldást mutatunk be. Célunk, hogy a manapság sokat citált és sajtókban is gyakran elhangzó álhírek (fake news) világába belelássunk, és lássuk, hogy nemzetállamok miként küszködnek ezzel az eszközzel.

Választási rendszerek és álhírek

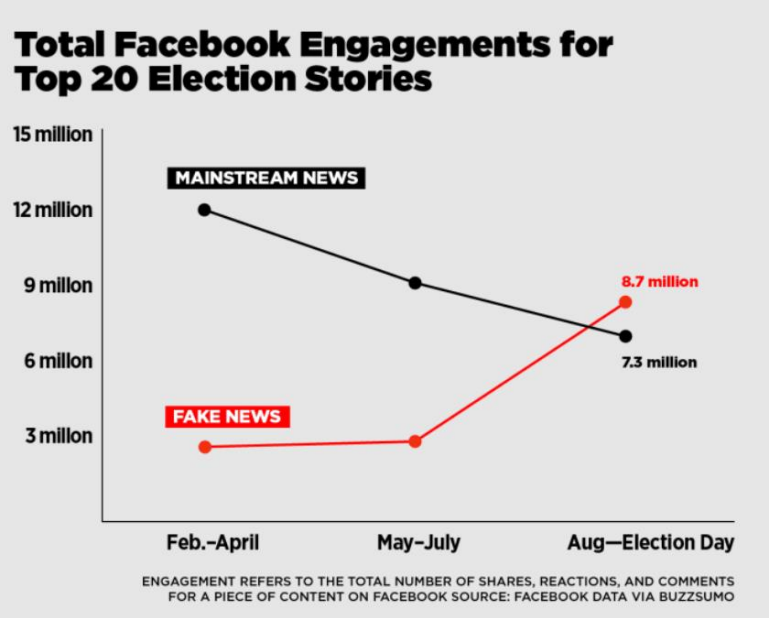
Manapság minden választás körül felsejlik a hír, hogy külső erők próbáltak beavatkozni. Emlékezzünk a bevezető részre: nem olyan egyszerű megállapítani, hogy valóban honnan érkeznek ezek a támadások, bár azt tudomásul vesszük, hogy általában Oroszország áll ezek mögött, hivatalosan gyakran nehéz bizonyítékokkal alátámasztani. Híres, kormányokat támadó hackercsoport az orosz hadsereghez kötött „Fancy Bear”, akik többek között 2014-ben más kelet-közép európai országokhoz

hasonlóan hazánkat is támadták, illetve 2015-ben a Bundestag-hack néven ismert német titkosított dokumentum szivárogtatás is hozzájuk köthető. (Beuth et al. 2017) Manapság minden jelentős hatalomnak megvan a maga titkos, féltitkos, nyilvános kiberhadviselő szerve, más kérdés, hogy mire és milyen hatékonysággal használják őket.

A 2016-os amerikai elnökválasztási kampány során történt kibertámadásokat, majd az azt követő érzékeny információk kiszivárogtatását az USA Belbiztonsági Minisztériuma, valamint az FBI közös elemzése egyértelműen Oroszországhoz kötötte. A későbbi elemzések és az ezek alapján készült jelentések azt mutatják, hogy a korábban feltételezettnél sokkal nagyobb a baj. A vizsgálatok megállapították, hogy az USA legalább 39 államában voltak kibertámadások a választási rendszerrel szemben. Illinois-ban pedig arra is találtak bizonyítékokat, hogy a támadók a választási névjegyzéket manipulálták, illetve azokban adatokat töröltek. (Kovács 2018)

2016-os hír, hogy az amerikai elnökválasztások kapcsán egy akkor 18 éves fiatal fiú, aki a makedóniai Veles-ből (ahonnan újságírók szerint több mint 150 álhírportált üzemeltetnek) származik, hat hónap alatt közel 18 millió forintnak megfelelő dollárt keresett álhírek írásával. Az üzleti modell semmiben sem különbözik a médiaoldalak modelljétől. Weboldalon cikkek jelennek meg és hirdetések, a cikkekre érkezett kattintások alapján számolható ki a reklámbevétel, a folyamatot a Google AdSense segítségével bárki megcsinálhatja otthon is. (Smith–Banic 2016)

Hogyan terjednek az álhírek? Rövid válasz: lényegében ugyanúgy, mint a hírek, de gyakran még jobban is. Erre világít rá a Buzzfeed News kutatása 2016-ból az amerikai elnökválasztások kapcsán, aminek az eredménye az alábbi ábrán jól látszik:



6. ábra: A Top 20 választási sztorira érkező összes Facebook kattintások. Jól látszik, hogyan győztek az álhírek a hírek ellen a választás közeledtével, a kampány intenzivitásával. Forrás: Silverman 2016.

Ássunk egy picit azért mélyebbre. Az online sajtóban ritkán van tényleges, hagyományos újságírói munka, amikor valaki napokig, hetekig, hónapokig vagy akár évekig dolgozhat egy nagyszabású ügyön, hogy legyen belőle egy óriási cikk. Egyszerűen a piaci alapokon működő hazai újságírás ezt nem teszi lehetővé. Nagyon fontos a napi cikkszám, azok generálják a kattintásokat. (Panyi 2017) Fehér Katalin és Király Olívia 2017-es „Álhíresülés – a hamis hírek dinamikája a médiában" című cikke a Századvég kiadványában körültekintően és részletesen bemutatja az álhírek médiában és közösségi médiában való terjedésének szabályszerűségeit és dinamikáit. A cikket szó szerint is érdemes lenne

idézni, de bizonyos terjedelmi korlátok közé kell magunkat szorítani. Pár nagyon fontos elemét ugyanakkor kiemelnénk:

- *Az álhírek eredeténél megfigyelhető a szándékos dezinformáció.*
- *A propagandacélú álhírek egyoldalú vagy egycsatornás kommunikációt követnek.*
- *Gyakori céljuk a pánikkeltés, amiből politikai vagy gazdasági haszon származhat valaki(k)nek.*
- *A jelen hírfogyasztása nagyon hasonló a gyorséttermek világában az ebédszünetek eltöltéséhez: random éttermek/hírforrások jönnek velünk szembe, és gyakran kiszámíthatatlan, hogy épp melyiket választjuk, és ott végül mit fogyasztunk el.*
- *Az álhíreket erősíti az adatrobbanás jelensége: ugyanis ha nagy tömegű adat gyűjthető a hírfogyasztókról, véleményük és viselkedésük közvetlenebb módon befolyásolható.*
- *Jellemző az úgynevezett churnalism (csurnalizmus): ellenőrizetlenül átvett források felhasználása az online médiában (pl. előre gyártott sajtóközlemények, különböző linkeket becsatoló és egyben ellenőrizetlen tartalmak, forrásmegjelölés nélküli vizualizációs tartalmak használata).*
- *Jellemző a prosumerism (producer+consumer; alkotó+fogyasztó): A médiafogyasztó a médiatartalom gyártója is egyben a közösségi média platformjain (gondoljunk cikkekre,[4] amelyek például egy Facebook-csoport[5] egy-egy megosztásából nőnek ki).*
- *Továbbá a szűrőbuborék-hatás, ami röviden úgy írható le, mint egy egyre szűkülő buborék, amely körülöttünk van, és a közösségi média a hírfogyasztási szokásainkból algoritmusok révén ajánl világnézetünkkel megegyező híreket. Ez azt eredményezi, hogy a valóságot nem látjuk teljes egészében, ha nem teszünk érte direkt, és a passzív hírfogyasztás egyoldalú hírfogyasztóvá tesz minket. (Fehér–Király 2017/2.)*

Ezek a tényezők közösen határozzák meg a mai modern, információs társadalom médiáját, és egyúttal közöttük is keresendők az álhírek és más dezinformációs jelenségek sikerességének a kulcsai. (Molnár 2017) Az álhírek nagyon speciális kibertér visszaélési eszközt jelentenek. Social Engineering eszközként azok közé tartozik, ahol a célpontok száma tömeges, ugyanakkor a támadó nem valamilyen adatot vagy információt akar megszerezni, áttételesen lehet célja a pénzszerzés, de nagyon gyakran a tananyag elején megnevezett harmadik célról van szó: adatot, információt kíván módosítani. Az álhírek kusza hálója azonban azért érdekes, mert ez az adatmódosítás sem célzott. Az álhíreket fogyasztók elméjét, gondolkodását kívánják manipulálni, sok esetben nem konkrét irányba. Az álhírek gyakran ellentmondanak egymásnak, részigazságokat tartalmaznak, a céljuk a bizonytalanság és bizalmatlanság szítása. Védekezni ellenük nagyon nehéz, a legtöbb kibertámadáshoz hasonlóan erre is igaz: a támadónak kevés idő és pénz kell a támadáshoz a védekező félhez képest. Léteznek olyan telefonos alkalmazások, amelyek jeleznek, ha bizonyos álhíroldalakra tévedtünk, ugyanakkor ezek rendszeres frissítés és ellenőrzés nélkül gyakran csak félmegoldások. Személy szerint a Marinov Iván álhírfelderítő oldalán magyar nyelven is elérhető ajánlásokat javaslom:

http://www.urbanlegends.hu/2017/03/mik-azok-a-kamuhirek-es-hogyan-vedekezzunk-ellenuk/

---

[4] Példa ilyen cikkre a hvg.hu-n: http://hvg.hu/itthon/20171026_Elontottek_a_zaklatastortenetek_az_egyik_legnepszerubb_magyar_Facebookcsoportot (2017. 11. 26.)

[5] https://www.facebook.com/Pesten-Hallottam-943046629083289/ a Pesten Hallottam csoport jelen esetben

3.2.1. Adathalászat

A phishing, vagyis az adathalászat (az angol fishing szóból ered) a számítógépalapú Social Engineering módszerek egyik válfaja. Két fő típusa van célpontok szerint: az általános és a célzott adathalászat. Az általános esetén az elkövető nem konkrét természetes és jogi személyeket céloz, hanem minél több célpontot próbál meg elérni, míg a célzott esetén célzottan egy intézmény, intézménycsoport vagy szektor ellen irányul. A támadó célja, hogy a felhasználót megtévesztve felhasználói vagy személyes adatot szerezzen, vagy bármilyen más nem nyilvános információt megismerjen. (Bodó et al. 2018)

Az adathalászat technikái közé soroljuk a következőket:

- **phising:** Ez az általános, klasszikus, a legrégebbi forma, lényegében a fentebb ismertetett információszerzési módszer, amely e-mailben történik. A támadás eredményességét növeli, hogy tömegesen küldik ezeket az üzeneteket, így bár százalékosan alacsony a sikerráta, darabszámra jól teljesít a módszer. A célzott phishing esetén magasabb a sikerszázalék, hiszen a fogalmazás sokkal pontosabb, hivatalosabb, gyakran az elkövető(k) belsős információkat is beleépítenek a levélbe, hogy hitelesebb legyen. Magyarországon egyébként viszonylag sikertelenek ezek a próbálkozások, mivel automata fordítással készül a legtöbb, ezért a rossz magyarság miatt gyanúsak. A whaling speciális formája a phising-nek. Az angol 'whale', bálna kifejezésből ered, és mint ez mutatja: nagy halakra történik a halászat. Rendszerint valamilyen szervezet felső vezetését célozzák, bank vagy állami szerv képébe bújva érkeznek a megkeresések.
- **vishing:** Azt használja ki, hogy az emberek a telefonos megkeresést hitelesebbnek érzik, mint az e-mailt. A vishing ugyanis hanghálózaton, elsősorban VoIP csatornán keresztül terjed, gyakran a phising üzenetben adják meg a telefonszámot, amit fel kell hívni, hogy meggyőződjenek hitelességéről, vagy tömeges tárcsázás (wardialing) módszerével hív fel egyszerre rengeteg embert, majd egy automata üzenetet játszik le nekik, melyben felhívják a figyelmüket valamilyen problémára, esetleg felhívatnak velük egy másik telefonszámot, vagy valami más módon, de igyekeznek rávenni az áldozatot, hogy adja meg bizonyos adatait.
- **smishing:** Hasonló, mint az előző kettő, csak épp SMS-ben történik. Szintén azt használja ki, hogy sokan pl. banktól érkező SMS-t automatikusan hitelesnek fogadnak el.
- **pharming** (magyarítva esetenként: farmolás) és **baiting:** lásd lentebb.

3.2.1.1. Hamis weboldalak használata, pharming

Részben informatikai, részben social engineering módszerrel történő fenyegetés. A hamis e-mailek és ál weboldalak készítése a legrégebbi adathalász támadási módszerek közé tartozik; az adathalászat egyik fajtája, bár kissé eltér tőle, mivel a pharming áldozatává válásban gyakran sokkal kevesebb szerep jut a szerencsétlen felhasználónak, mint a többi adathalász módszer esetén.

Ál weboldalakkal könnyen találkozhatunk: ha böngészőnkben elírunk egy betűt valamely általunk gyakran látogatott oldal url címében, lehetséges, hogy egy teljesen más weboldalra kerülünk (ezek rendszerint nem kínálnak valós szolgáltatásokat, sokszor reklámokkal vannak teletömve, hogy maximalizálják a hasznot a félregépelésekből származó látogatásokból). Előfordulhat az is, hogy látszólag ugyanarra az oldalra jutunk, amit eredetileg is szerettünk volna látogatni, csak annyi különbséggel, hogy például nem fogunk tudni bejelentkezni rá, helyette a bejelentkezési adatainkat, azok begépelése után, eltárolja valaki. Ezután rendszerint egy automatika meg is teszi a szükséges lépéseket, hogy az igazi oldalon átírja a jelszavunkat, e-mail címünket stb., hogy lehetőleg teljesen kizárjon minket, vagy, ha bankról van szó, megszerezzék pénzünket, mielőtt óvintézkedéseket tennénk.

A pharming kifinomultabb megoldás az adathalászatra. Ha a számítógépen található hosts-fájlba írja (vagy íratja egy malware segítségével) bele a meghamisított (pl. banki) oldalak címét, akkor DNS cache poisoning-ról beszélünk. Ennek megfelelően a megtámadott számítógépen a felhasználó hiába írja be a böngésző címsorába bankja URL-címét, a címfeloldás nem a megszokott DNS-szerveren történik, hanem helyben, az átírt hosts-fájl segítségével, és az ügyfél a hamis banki oldalon találja magát, ahol gyanútlanul megadja adatait.

A pharming történhet szerveralapú DNS cache poisoning módszerrel is: ekkor a szolgáltatónál található DNS-szervert támadják meg, bár mivel ezeket fokozottan védik, így ritkán esnek áldozatul. Ezzel szemben harmadik fajtája, a Cross-site Scripting (XSS) gyakrabban sikeres. Egy legitim weboldalba ágyazzák bele egy kívülről beírt kóddal a hamis weboldalra automatikusan átirányító scriptet (pl. az oldalon talál a támadó olyan űrlapot, amibe be tud írni olyan kódot, ami beágyazza magát a weboldal kódjába, és automatikusan átirányítja a felhasználókat egy másik, támadó által irányított tüköroldalra, ahova megpróbálnak majd bejelentkezni). (HUNCERT 2004)

3.2.1.2. Baiting

A baiting (magyarul: csalizás) szintén ötvözi a számítógépes és humán alapú technikákat. A támadó a célpontként funkcionáló szervezet telephelyén „véletlenül" elveszít néhány DVD-t vagy pendrive-ot. Az áldozatok ezeket megtalálják, és nagy valószínűséggel saját számítógépükön megnézik ezeket. Ekkor egy kártékony kód fut le a számítógépen, ami segít megszerezni a kívánt adatokat. A támadást elősegítheti az, ha a DVD-re valamilyen közérdeklődést kiváltó cím van felírva. (Muha–Krasznay 2014) Szintén kilóg a klasszikus adathalász megoldások közül, mert nem kell hozzá online kapcsolat.

A malware trendek figyelése magánemberként, munkavállalóként és vezetőként egyaránt segít a kiber visszaélésekre való felkészülésben. A legtöbb anti-malware cég, kiberbiztonsági intézet készít időnként jelentéseket a kibertérben történő visszaélésekről. A következőkben a tanulmány elkészültekor egyik legfrissebb adatokra támaszkodó jelentésből szemezgetünk, ez az amerikai Symantec 2018-as jelentése. A Symantec a világ egyik vezető információs adatvédelem és vírusirtó cége. Íme néhány állítás a malware-ek területéről: 2017-ben a „Coin Mining" jellegű támadások növekedtek a legjobban (**8500%-**kal nőtt meg az antivírusok általi detektálásuk 2006-hoz képest).

- A ransomware fertőzöttség 40%-kal emelkedett 2017-ben (főleg a **WannaCry-**nak köszönhetően) az előző évihez képest, 46%-kal nőtt továbbá a zsarolóprogramok variánsszáma,[6] bár az új víruscsaládok megjelenése csökkent. A ransomware támadások 59%-a (396 764) **cégek ellen** történt.
- A bankokat célzó egyik legnagyobb fenyegetést az Emotet trójai jelentette (2014-ben jelent meg), mely 2017 végére 2000 %-os növekedést mutatott.
- Míg 2016-ban összesen 357 019 453 különböző **malware variánst** detektáltak, 2017-ben ez a szám 669 947 865-re ugrott (igen magas %-ban a Kotver trójai variánsai teszik ki), tehát 87,65%-os növekedés figyelhető meg.
- Operációs rendszerek esetén a malware támadások száma így alakult:

  Mac 2015: 1 824 685 → 2016: 2 445 414 →2017: 4 011 252

  Windows 2015: 300 966 231 → 2016: 161 707 491 → 2017: 165 638 707

- Webes fenyegetések alakulása: **13-ból 1** URL fertőzött 2017-ben, 2016-ban 1:20-hoz volt az arány. A **phising** tevékenységet ellátó URL-ek aránya 2017-ben: **1:17** (2016-ban: 1:30).

[6] Egy-egy malware általában egy-egy malware-családhoz tartozik, illetve egy-egy malware-nek számtalan variációja létezhet, ezek a malware variánsai.

- 62%-kal növekedett a **botnet** aktivitás 2016-ról 2017-re (átlagosan napi 12 281 279 URL-cím nyitás, ami a napi URL webforgalom 1,1%-át tette ki).
- 2016-ról 2017-re csökkent a fertőzött e-mailek aránya. 2016-ban 1:131-hez volt az arány az összes e-mail forgalomhoz viszonyítva, 2017-ben: 1:412-höz, ugyanakkor az e-mail malware-eken belül nőtt a fertőzött URL-t tartalmazó mail-ek számaránya: 12,3%-ra (1,6%-ról) a fertőzött csatolmányt tartalmazó e-mailek kárára.

E-mail malware adatok 2017-ben		
Szektor	**E-mail malware ráta (fertőzött/összes)**	**E-mail malware felhasználónként egy évben**
Közigazgatás	***1:120***	***53,1***
Mezőgazdaság, erdészet, halászat	1:211	26,5
Bányászat	1:273	30,0
Nagykereskedelem	1:364	34,4
Gyártás, termelés	1:384	25,5
Szolgáltatások	1:400	12,1
Nem osztályozható létesítmények	1:437	21,8
Építőipar	1:472	18,1
Közlekedés és közműszolgáltatások	1:486	8,7
Kiskereskedelem	1:489	19,9
Pénzügyi, biztosítási és ingatlan szektor	1:612	9,1

1. táblázat: E-mail malware adatok 2017-ben gazdasági szektoronként. Forrás: készült Symantec, 2018 alapján.

- Ausztria a maga 1:102-es arányával a leginkább támadott ország e-mail malware alapján, hazánk a második 1:108-as arányával, míg a harmadik helyezett Indonéziának a fogadott e-mailjeiből csak 1:140 fertőzött. Hazánk a spamnek jelölt e-mailek számában is előkelő 5. helyezett, az e-mailjeink 60,4%-a spam.
- A fertőzött e-mailek leggyakoribb témái:
    - számlázás (15,9%)
    - e-mail kézbesítési hiba (15,3%)
    - jogi, törvényi végrehajtás (13,2%)
    - szkennelt dokumentum (11,5%)
    - csomagkiszállítás (3,9%)
- A célzott támadások 90%-a információszerzésre irányul. 71,4%-uk célzott (spear-) phising e-mail-el történik, 23,6 %-uk watering hole[7] támadás.
- A legveszélyeztetettebb böngésző a Microsoft Internet Explorer és Edge, majd a Google Chrome, aztán az Apple Safari, majd a Mozilla Firefox, végül az Opera, ugyanakkor évről évre egyre biztonságosabbak a böngészők.
- A mobil és IoT (Internet of Things) eszközökre évente nagy ütemben növekszik az azonosított fenyegetések száma: mobilok esetén 54%-os, míg IoT eszközök esetén 600%-os a támadások számának növekedése. Mobileszközök terén a támadások főleg az Egyesült Államokbeli

[7] A watering hole támadások esetén kifigyelik a célpont weboldal-látogatási szokásait, majd célzottan azt az oldalt fertőzik meg malware-ekkel.

eszközöket érik az azonosítások alapján (57%), míg IoT esetén Kína a leggyakoribb forrásország: az IoT támadások 21%-a származik Kínából IP-cím alapján. (Symantec 2018)

Az aktuális trendek alapján levonhatunk pár következtetést. Az egyik, hogy az új eszközök is egyre inkább a támadások célpontjaivá válnak, a másik, hogy az államigazgatás egésze kiemelt célpont. Egy harmadik tanulság lehet, hogy bár a nagyhatalmak harcának tűnhet elsősorban a malware-es kiberbűnözés, láthattuk, hogy hazánk is megjelenik néhány adatban mint kiemelt célpont. Szerzői megjegyzés: igaz az, hogy a spam és e-mail alapú támadások sikerességi rátája összefüggésben van a digitális készségekkel, az pedig a funkcionális analfabetizmussal mutat korrelációt, így hazánk, amelyik sajnos rosszul teljesít e kompetenciák terén, természetes célponttá válik e primitívebb támadások esetén, hiszen EU és NATO tagként van stratégiai jelentőségünk.

Negyedik következtetésünk lehet, hogy viszonylag nagy ingadozás figyelhető meg egyes támadások számossága terén egy-egy év alatt is, ez pedig azt mutatja, hogy a kiberbiztonsággal foglalkozó szakemberek nem tétlenkedhetnek, ahogyan egy-egy szervezetnek is folyamatos fejlődésre és belső tevékenységeinek meg-megújítására van szüksége hardveres és szoftveres eszközeinek folyamatos karbantartása mellett is.

A továbbiakban megnézzük, milyen lehetőségeink vannak az információs visszaélések megelőzése és feltérképezése terén.

4. Az információs visszaélések megelőzése, feltárása és elhárítása

Természetesen a pusztán informatikai támadások ellen elsősorban nem szervezeti és humán megoldásokra van szükség, hanem informatikai megoldásokra (pl. tűzfalak, anti-malware-ek stb.). A tananyag keretei szempontjából azonban most nem „hard” informatikai képzést tartunk, így ezek részletezésére nem térünk ki, helyette a mély IT tudást nem előfeltételező menedzsment, jogi és humán eszközök bemutatására teszünk kísérletet a teljesség igénye nélkül.

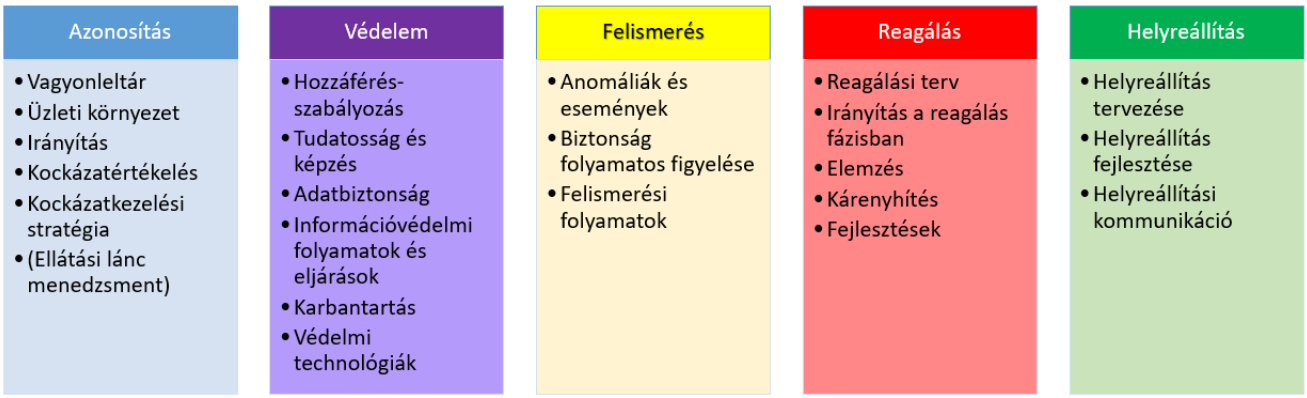
4.1. Szervezeti eszközök

4.1.1. A NIST és a 3 Vonalas Védelmi Modell

Az információs visszaélések megelőzése, feltárása és elhárítása összetett feladat egy szervezeten belül. Nagyban függ a szervezet méreteitől, ellátott feladatainak sokszínűségétől és az általuk használt informatikai eszközök (hardverek és szoftverek) mennyiségétől, bonyolultságától és sokszínűségétől. Az első fejezetben megnézünk pár ajánlást arra vonatkozóan, hogy milyen kategóriákra lehet bontani egyáltalán az információs visszaélésekkel kapcsolatos feladatokat, milyen ajánlások vannak arra vonatkozóan, hogy egy adott közigazgatási vagy üzleti szervezet az ezekkel járó feladatokat hogyan ossza ki.

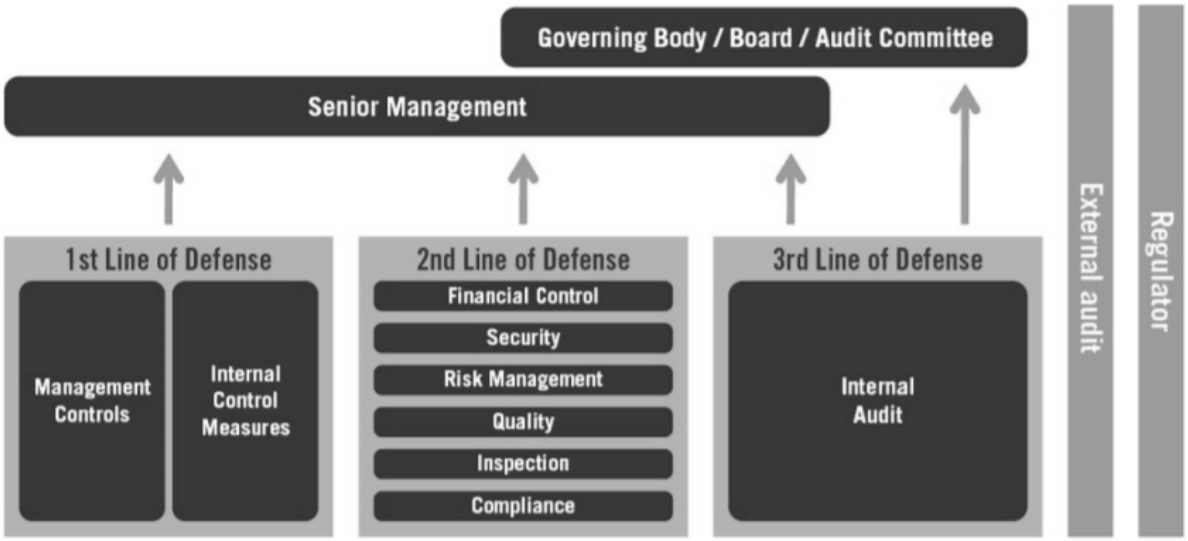
Az Amerikai Egyesült Államok Nemzeti Szabvány és Technológiai Intézete (NIST – National Institute of Standards and Technology) az egyik legismertebb szabványosítással foglalkozó szervezet a világon, amely több más terület között az információbiztonság területén is készít kiadványokat. 2013-ban kiadta a kiberbiztonsági keretirányelvet (1.0-ás verzió, 2018-ban megjelent az 1.1-es), amely többek között összefoglalja a figyelembe veendő szabványokat. A NIST keretirányelvei nevesítik az információs visszaélésekkel kapcsolatos teendőket, ezek a következők:

- Azonosítás: az a lépés, melyben kijelölik azokat az adatokat és infrastruktúraelemeket, amelyek védelme a működés szempontjából szükséges.
- Védelem: azon szabályok és tevékenységek összessége, amelyek segítségével az előző lépésben azonosított adatok védelme biztosítható.
- Felismerés: a rendszert ért támadás felismerésének folyamata. Ez nem kizárólag véletlenszerűen történik, előre definiált folyamatokkal és adminisztratív intézkedésekkel az esetlegesen még passzív támadások is felismerhetők.
- Reagálás: egy kiberbiztonsági eseményre megfelelő intézkedések és tevékenységek végrehajtása, válaszul az észlelt biztonsági incidensre. A folyamatban többnyire adminisztratív intézkedések végrehajtásáról beszélünk, de ez a szükséges műszaki eszközök és technológiák nélkül nem hatékony.
- Helyreállítás: az a tevékenység, melynek segítségével a szervezet információs rendszerének normál működése egy incidens után vagy alatt visszaállítható. A helyreállítás a vonatkozó terv alapján történik. (Berzsenyi et al. 2018)



7. ábra: A NIST keretrendszerben nevesített kategóriák és alkategóriák. Forrás: saját, NIST 2018 alapján.

A 6. ábra részletesebben bemutatja a NIST keretrendszer elemeit, legalábbis megnevezés szintjén, a jelen mű terjedelmi korlátai miatt ezeket nem részletezzük. Amit viszont érdemes még bemutatni: szervezeti szinten hogyan lehet ezeket implementálni, kinek milyen feladata lehet. Erre a kérdésre az egyik lehetséges választ az alábbi két modell adhatja meg:



8. ábra: A 3 Vonalas Védelmi Modell. (IIA 2013)

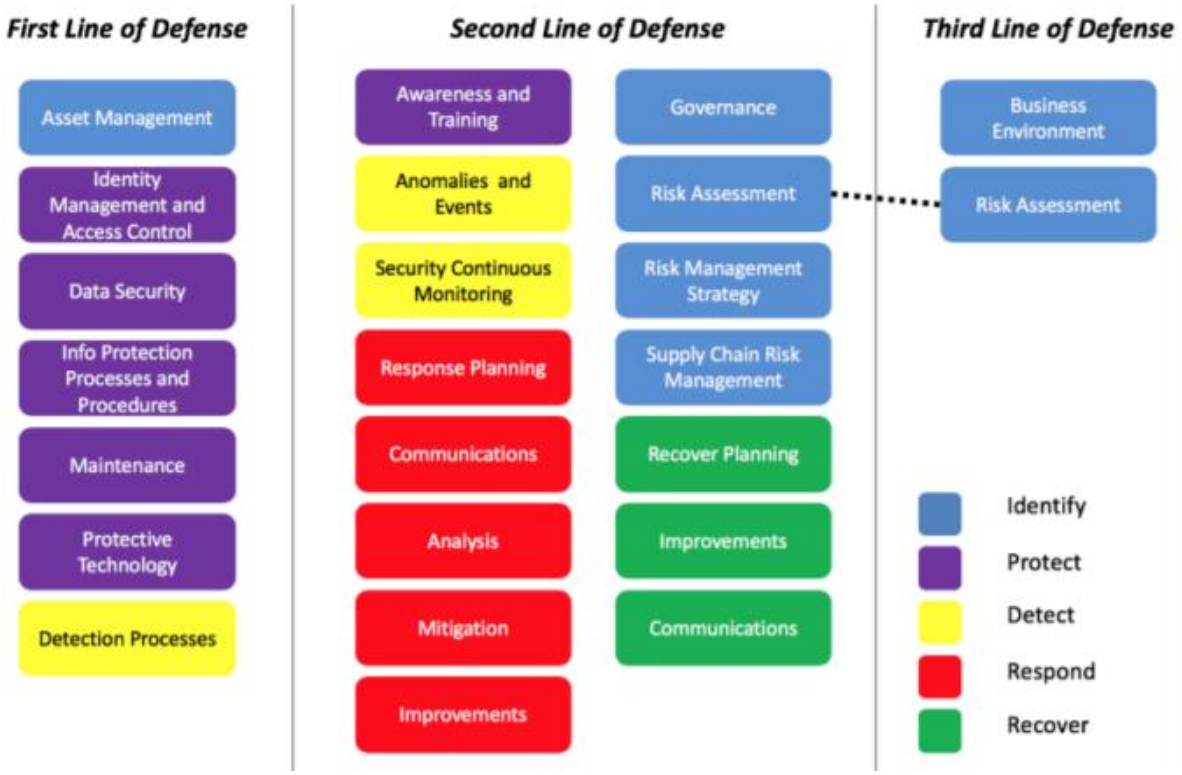
A 3 Vonalas Védelmi modell (Three Lines of Defense Model) az Belső Auditorok Intézete (IIA- Institute of Internal Auditors) által készített kiberbiztonsági ajánlás. Célja, hogy a biztonsági feladatokat, feladatköröket elhelyezze a menedzsment szintjein. Az általuk meghatározott 3 védelmi vonal a következő (IIA 2013):

1. Saját és irányítási kockázatok: Ezen a védelmi vonalon a napi IT biztonsági műveleteket végzik. A szervezet méreteitől függően ez egy elkülönült csapat vagy egyén feladata, de előfordulhat, hogy nincs külön dedikált csapat erre, hanem például a hálózati infrastruktúráért felelős csapat a hálózati infrastruktúrával kapcsolatos eseményekkel foglalkozik, a fejlesztési csapat a fejlesztéssel kapcsolatosokkal stb. A lényeg, hogy a saját és irányítási kockázatok szintjén operatív menedzsment feladatokat látnak el. Az ezen szint által ellátott feladatokért a 2. védelmi vonalat terheli a felelősség, az 1. vonalnak ehhez biztosítania kell számukra az ellenőrizhetőséget (pl. naplózással). Az 1. védelmi vonal felelős továbbá a magasabb vezetői szintekről érkező döntések

végrehajtásáért, a stratégiáknak és előírásoknak való megfelelésért, illetve ezen a szinten végzik a konkrét megelőzés, feltárás és elhárítás feladatát is.

2. Felügyelési kockázatok: Információbiztonsági team látja el. Feladatuk a menedzsment döntéseinek támogatása, feladatok kiszabása. Ők szolgáltatják a kockázatkezelési kereteket, képzéseket biztosítanak a kockázatmenedzsment eljárások kapcsán, részt vesznek az informatikai és információbiztonsági folyamatok kialakításában, figyelik a jogszabályi és más szabályozások, szabványok betartását, sőt pénzügyi és minőségbiztosítási kontrolt is ellátnak.
3. A függetlenség biztosítása: Az utolsó védelmi funkció az auditálás. Ellátói belső és külső auditorok. Különféle informatikai és humán teszteléseket végeznek, és figyelnek a harmadik, külső féltől érkező biztonsági kockázatokra is. (IIA 2013)

Mindhárom védelmi vonal különböző jelentéseket küld a saját munkájáról a felső, operatív vezetőségnek, a 3. vonal pedig az auditáló testületnek és/vagy az irányító testületnek is (pl. igazgatótanács vagy épp miniszter).



9. ábra: A NIST keretrendszer szabta feladatok helye a 3 Vonalas Védelmi Modellben. Forrás: Stone 2018.

David Stone kiberbiztonsági szakértő a NIST keretrendszer és az IAA által elkészített 3 Vonalas Védelmi Modelljét feleltette meg egymásnak, hogy megállapítható legyen: a NIST által nevesített feladatok az IAA védelmi vonalain hol jelennek meg. Látható, hogy egyes teamek, védelmi vonalak több különböző feladat elvégzésében is részt vesznek. Ezek segítenek a belső folyamatok megtervezésében, a különböző beépített kontrollok kialakításában a szervezeten belül.

4.1.2. Soc-team létrehozása

A fentebb ismertetett NIST keretrendszer és a 3 Vonalas Védelem Modell is átfogó eszközt kínál a különböző visszaélések megelőzése, felismerése és elhárítása területén. Ugyanakkor bizonyos esetben dönthetünk úgy, hogy az egész feladatot részben vagy egészben egy külön csoportra irányítjuk. Nagyobb szervezet esetén érdemes biztonsági műveleti központ vagy SOC (Security Operations

Center) létesítése: olyan csapatot jelent, amely éjjel-nappali műszakban működik, és amelynek egyaránt feladata a megelőzés, a felderítés és a kiberbiztonsági fenyegetésekre, eseményekre adható válaszok kidolgozása, valamint a szervezet vagy létesítmény biztonsági előírásainak vizsgálata és értékelése. (Berzsenyi et al. 2018) Ezt természetesen nem kell saját magunknak előállítani, általában olcsóbb és hatékonyabb is külső SOC-team igénybevétele.

Információs-rendszereink kialakításában is számos módszertan, ajánlásgyűjtemény lehet a segítségünkre, mi most az ITIL módszertant, illetve a COBIT-et mint az IT eszközök és folyamatok menedzselésére jó gyakorlatok felhasználásával kialakított keretrendszert nevesítettük. Ha nemzetközileg és szakmailag elismert módszertanok (esetleg szabványok) és jó gyakorlatok szerint tervezzük meg, fejlesztjük, működtetjük és figyeljük az egész szervezetünket behálózó informatikai rendszereinket, akkor már a visszaélések egy részét elkerülhetjük, de a detektálásban és elhárításban is hasznunkra lehetnek.

4.1.3. ITIL

Az ITIL (Information Technology Infrastructure Library – informatikai infrastruktúra könyvtár) átfogó módszertan és ajánlásgyűjtemény informatikai rendszerek üzemeltetésére és fejlesztésére. Ahhoz, hogy feladatát megfelelően lássa el, információbiztonsági előírásokat is tartalmaznia kell. Ugyanakkor nem elsősorban ezzel foglalkozik, az adat és információ védelmével kevésbé, inkább a szolgáltatás folytonosságának biztosításával foglalkozik. (Muha–Krasznay 2014)

Az ITIL csomagjából a tanulmány megírásának időpontjában a 3. verzió, az úgynevezett ITILv3 a legfrissebb. Ez az ajánláscsomag tulajdonképpen 5 fő kötetből, illetve a hozzájuk kapcsolódó kiegészítő anyagokból áll, melyek az incidenskezelés témakörére is kiterjednek. A szolgáltatásüzemeltetésről szóló kötet a szolgáltatás folytonosságához, az információbiztonság menedzsmentjéhez, hibamentes üzemeltetéséhez szükséges folyamatokat tartalmazza, amelynek egyik fontos eleme az incidenskezelés. (Berzsenyi et al. 2018)

4.1.4. COBIT

Az ISACA által készített COBIT (Control Objectives for Information and Related Technologies) az üzleti folyamatokra, valamint az ezeket támogató informatikai megoldások négy területére – tervezés és szervezés; beszerzés és üzembe állítás; informatikai szolgáltatás és támogatás; felügyelet – helyezi a fő hangsúlyt, és elsősorban nagyvállalatok informatikai megoldásainak támogatására készült.

A COBIT 5[8] folyamatai:

- Értékelés, irányítás és figyelemmel kísérés (Evaluate, Direct and Monitor, EDM)
- Összehangolás, tervezés és szervezés (Align, Plan and Organise, APO)
- Építés, beszerzés és megvalósítás (Build, Acquire and Implement, BAI)
- Szállítás, szolgáltatás és támogatás (Deliver, Service and Support, DSS)
- Figyelemmel kísérés, értékelés és felmérés (Monitor, Evaluate and Assess, MEA) (Muha–Krasznay 2014)

4.1.5. Információbiztonsági irányítási rendszer

A magasabb információbiztonsági érettség(re való igény), tudatosság szükségessé teszi információbiztonsági irányítási rendszer (IBIR) bevezetését. „AZ IBIR a vállalatirányítási rendszer azon

[8] 2018. 11. 12-vel megjelent a COBIT 2019 is, de ennek feldolgozása a mű elkészítésekor még nem történt meg.

része, amely átfogja és szabályozza a teljes informatikai tevékenységet, kiemelten kezelve az adatbiztonsági és adatvédelmi területeket. Segítségével a vállalat működésének kockázatelemzésén és kockázatkezelésén keresztül kialakítható a magas szintű információvédelem. A rendszer magában foglalja a szervezeti felépítést, a biztonságos működtetéshez szükséges szabályzatokat, a tervezési tevékenységeket, a felelősségi köröket, a gyakorlatot, az eljárásokat, a folyamatokat és az erőforrásokat." (Nador.hu 2016)

4.2. Jogszabályi megfelelés

4.2.1. Információbiztonsági törvény (Ibtv.)

Magyarországon a legrelevánsabb jogszabályi megfelelés az Ibtv. – Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény. Alapvetően a NIST által publikált kontrolljegyzék alapján dolgozták ki. A jogalkotó figyelembe vette a nemzetközi ajánlásokat, ennek megfelelően ezek figyelembevételével fogalmazta meg a vonatkozó szabályokat. A törvény bizonyos tevékenységeket határoz meg, amelyek az alábbiak:

- a szervezet aktuális biztonsági szintjének meghatározása – A biztonsági osztályba sorolás alapja a kockázatelemzés. A biztonság kialakítása nem általánosan, hanem a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából 5-5 biztonsági osztályban kell hogy megtörténjen, ez azért érdekes, mert a NIST által javasolt ajánlásban csak három szintű biztonsági besorolás van. A szervezetet a legmagasabb biztonsági osztályának megfelelő biztonsági szintbe kell sorolni, amely tulajdonképpen a szervezet biztonságkezeléssel kapcsolatos képességeit mutatja.
- a szervezet információbiztonsági céljának megfogalmazása, a szükséges elérendő biztonsági szint meghatározása;
- a biztonsági cél eléréséhez szükséges lépések meghatározása;
- megfelelő kommunikáció a külső és belső érdekeltek között.

A törvény egyik legfontosabb pontja a biztonsági szintek meghatározása, mivel a szintekhez köt konkrét előírásokat, szabályozásokat, amelyeket be kell tartani. A szintek hasznosak, a törvényből következő legfontosabb állítás betartását segítik elő: **a biztonságnak mindig kockázatarányosnak kell lennie.** A biztonsági szintek pontos definíciója megtalálható a végrehajtási rendeletben,[9] melyből az alábbi idézetek is származnak:

„Az érintett szervezet biztonsági szintje 1., ha a szervezet nem üzemeltet és nem fejleszt elektronikus információs rendszert, és saját hatáskörben erre más szervezetet vagy szolgáltatót sem vesz igénybe. Az adatfeldolgozás módját nem maga határozza meg, az adatkezelés tekintetében technikai vagy információtechnológiai döntést nem hoz, a használt elektronikus információs infrastruktúra kialakítása tekintetében döntési jogköre – ide nem értve a szervezet munkavégzését érintő informatikai rendszerelemek elhelyezését – nincs, egyedi adatokat és információkat kezel vagy dolgoz fel, és kritikus adatot nem kezel. A szervezet információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a mértékig, ameddig a szervezet vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni."

[9] 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

„Az érintett szervezet biztonsági szintje 2., ha a szervezet vagy szervezeti egység az 1. szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe."

„Az érintett szervezet biztonsági szintje 3., ha a szervezet vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe."

„Az érintett szervezet biztonsági szintje 4., ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt."

„Az érintett szervezet biztonsági szintje 5., ha a szervezet vagy szervezeti egység a 4. szinthez rendelt jellemzőkön túl európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység."

A törvény egyik kiemelkedő pozitívuma, hogy nagy hangsúlyt fektet a biztonságtudatosságra, az oktatás-képzés kialakítására.

4.2.2. Általános adatvédelmi rendelet (GDPR) és Hálózat- és információbiztonsági irányelv (NIS)

Az Európai Parlament és az Európai Tanács 2016 áprilisában elfogadta a GDPR-szabályozást (General Data Protection Regulation – Általános Adatvédelmi Rendelet). A rendeletet 2018. május 25-től kell alkalmazni, felváltotta a korábbi, idejét múlt 95/46/EK adatvédelmi irányelvet. Az EU kiberbiztonsági stratégiájának fontos része a hálózat- és információbiztonságra vonatkozó irányelv (NIS Directive – Network and Information Systems Directive – hálózati és információs rendszerek irányelv) is. Mivel többé-kevésbé azonos időben lépnek életbe, ezért gyakran összevonva kezelik rendelkezéseiket.

A GDPR olyan összehangolt adatvédelmi jogszabályt jelent az uniós tagországoknak, amelynek alapvető célja az uniós polgárok személyes és magán adatainak védelme. A GDPR vonatkozásában az egyik legtöbbet idézett szabályozás nem más, mint kiemelkedő büntetési tételei, illetve más szankcionálási tételek kilátásba helyezése. A büntetési tétel a szabályokat megsértő szervezet éves forgalmának 4%-áig terjedhet, vagy akár húsz millió euró is lehet (főszabály szerint amelyik az adott szervezet esetén a nagyobb összeg). Természetesen olyan legsúlyosabb jogsértések esetén szabják csak ki ezt az összeget, ahol például személyes adatok engedély nélküli feldolgozása és kezelése történt ipari méretekben. Ugyanakkor a direktíva az olyan szabályszegések esetén is, mint például a nem megfelelő adatnyilvántartás vagy jogsértés, a felügyeleti hatóság értesítésének elmulasztása 2%-os éves forgalommal egyenértékű büntetési tételt helyez kilátásba. Ezek a büntetési tételek vonatkoznak az adatkezelőkre és az adatfeldolgozókra is. (Kovács 2018)

***Adatkezelő**:*

„Az adatkezelő meghatározza a személyes adatkezelés céljait és módjait. Ha tehát vállalkozása/szervezete határozza meg, hogy miért és hogyan történik a személyes adatok kezelése, adatkezelőnek minősül. A szervezetében dolgozó, a személyes adatkezelést végző alkalmazottak ezt a munkát az ön adatkezelői feladatainak teljesítése érdekében végzik. Közös adatkezelőnek minősül, ha

egy vagy több szervezettel közösen határozzák meg, hogy miért és hogyan kell kezelni a személyes adatokat. Az általános adatvédelmi rendelet előírásainak való megfelelés érdekében a közös adatkezelőknek megállapodást kell kötniük a fennálló felelősségeik megoszlása tekintetében. A megállapodás főbb szempontjait közölni kell azon érintettekkel, akiknek személyes adatait kezelik." (Európai Bizottság 2018)

***Adatfeldolgozó**:*

„Az adatfeldolgozó kizárólag az adatkezelő megbízásából kezel személyes adatokat. Az adatfeldolgozó általában a vállalkozáson kívüli harmadik fél, azonban vállalkozáscsoportok esetében egyik vállalkozás működhet egy másik vállalkozás adatfeldolgozójaként.

Az adatfeldolgozónak az adatkezelővel szembeni kötelezettségeit szerződésben vagy más jogi aktusban kell meghatározni. Például a szerződésnek tartalmaznia kell, hogy mi történik a személyes adatokkal a szerződés megszűnte után. Az adatfeldolgozók egyik tipikus tevékenysége az IT-megoldások nyújtása, ideértve a felhőalapú tárolást. Az adatfeldolgozó csak akkor adhatja ki feladata egy részét alvállalkozásba egy másik adatfeldolgozónak és csak akkor jelölhet ki közös adatfeldolgozót, ha előzetes írásbeli engedélyt kapott az adatkezelőtől. Bizonyos helyzetekben egy szervezet lehet adatkezelő vagy adatfeldolgozó, vagy akár mindkettő." (Európai Bizottság 2018)

A GDPR számos új, nagyon szigorú rendelkezést tartalmaz az adatvédelem területén. Ilyen szabályozás például a szabálysértési értesítés. Ez arra vonatkozik, hogy ha az állampolgárok jogait és szabadságát veszélyeztető adatvédelmi szabályszegés következik be, a felügyelőhatóságot 72 órán belül értesíteni kell róla. Ugyanígy értesítési kötelezettsége van az adatfeldolgozónak is az ügyfelek felé, ha adatszegést észlel. (GDPR 2016)

A jogszerűség, tisztességes eljárás és átláthatóság szellemében adatkezelés szempontjából a direktíva előírja, hogy az adatalanyoknak (azaz kicsit leegyszerűsítve: az ügyfeleknek) joguk van az adatkezelőtől megerősítést kapni arról, hogy az őket érintő személyes adatokat mikor, hol és hogyan dolgozzák fel, azokat hol és hogyan tárolják, vagy esetleges kinek adták át őket. Ez növelheti az adatkezelés átláthatóságát. Mindezeken túl az adatkezelőnek elektronikus formában, ráadásul ingyenesen meg kell adnia az ügyfeleknek a róluk kezelt személyes adatok másolatát is. A GDPR meghatározza a törléshez való jog („az elfeledtetéshez való jog") fogalmát is. Ez azt jelenti, hogy az érintett jogosult arra, „hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje". (GDPR 2016, 17. cikk (1)) A tagállamok pedig gondoskodnak arról, hogy a hatóságok lépéseket tegyenek, ha valamely szolgáltató nem teljesíti az előírásokkal kapcsolatos feladatait (NIS Directive 2016, 17. cikk (1)), ha a meghatározott feltételek fennállnak. (Kovács 2018)

Ezek persze csak kiragadott szabályok a GDPR-ból, illetve a NIS-ből. Ilyen komplex joganyagokat jelenleg nem áll módunkban részletesen ismertetni, viszont a magyar jogalkalmazóknak, cégeknek egyaránt örömhír, hogy az Ibtv. előírásai többé-kevésbé korábban is lefedték az Uniós direktívák előírásait.

4.2.3. Büntető Törvénykönyv (Btk.)

Ha hazánkban a kibertérbeli visszaélésekről és konkrétabban a bűntényekről beszélünk, akkor elkerülhetetlen ki kell térni a Büntető Törvénykönyvről szóló 2012. évi C. törvényre, amelynek többek között az információs rendszer elleni bűncselekményekről szóló XLIII, TILTOTT ADATSZERZÉS ÉS AZ INFORMÁCIÓS RENDSZER ELLENI BŰNCSELEKMÉNYEK című fejezetében jelennek meg ilyen

bűncselekmények. A fejezet 423. szakasza ismerteti az „Információs rendszer vagy adat megsértése” tényállást:

„423. § (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz...”

Illetve 424. szakasza az „Információs rendszer védelmét biztosító technikai intézkedés kijátszása” című részben a törvény a következő vétséget nevesíti:

„424. § (1) Aki a 375. §-ban, a 422. § (1) bekezdés d) pontjában vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve
b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja...”

A Btk. további passzusai is fogalmaznak meg kiber-visszaéléssel kapcsolatos vétségeket:

Témánk szempontjából kiemelten fontos az „Információs rendszer felhasználásával elkövetett csalás” című szakasz, a 375. §:

„375. § (1) Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás jelentős kárt okoz, vagy
b) a nagyobb kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen nagy kárt okoz, vagy
b) a jelentős kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(4) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen jelentős kárt okoz, vagy
b) a különösen nagy kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(5) Az (1)-(4) bekezdés szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt.

(6) Az (5) bekezdés alkalmazásában a külföldön kibocsátott elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül."

A 287. § pedig a zártörések kapcsán említ kibertérbeli visszaélést:

„287. §

c) az elektronikus adat megőrzésére kötelezéssel érintett adatot jogosulatlan személy számára hozzáférhetővé teszi, illetve azt az eljárás alól elvonja vagy módosítja,
d) a büntetőeljárás során ideiglenesen hozzáférhetetlenné tett elektronikus adatot jogosulatlan személy számára hozzáférhetővé teszi, illetve azt az eljárás alól elvonja vagy módosítja..."

De a terrorcselekményeket felsoroló 314. szakaszt is említhetnénk, amely i. pontjában kitér az információs rendszer vagy adat megsértésére.

4.3. Humán (HR) eszközök

A szervezeti formákon, előírásokon, ajánlásokon túl hasznos megoldások lehetnek a humán tényező sérülékenységét csökkentő megoldások. A következőben ezeket mutatjuk be.

4.3.1. A feladatok szétválasztása (SoD – Separation of Duties)

A SoD (Separation of Duties – feladatok szétválasztása) kifejezést széles körben használják a pénzügyi elszámolási rendszerekben. A vállalatok (méretüktől függetlenül) megértik annak fontosságát, hogy ne egyetlen szerepkör (sok esetben egyetlen személy) feladatai legyenek az olyanok, mint a csekkek átvétele (fizetés a számlán), a leírások jóváhagyása, a készpénz letétbe helyezése, a bankszámlakivonatok összeegyeztetése és a fizetések átvétele, mert az a személy, aki az adott cég minden pénzügyi tranzakcióját végzi, lényegében teljhatalommal bír, és könnyen visszaélhet ezzel (egyéni vállalkozások esetén is lehet ezzel gond, amikor a vállalkozó nincs tisztában minden jogszabállyal, és például megörül, hogy mennyi bevétele van az ÁFA kifizetések előtt, és túlköltekezik).

A feladatok elkülönítése általános eljárás, amikor az emberek pénzt kezelnek, így a csalás, visszaélés két vagy több fél részvételét is igényli. Ez nagymértékben csökkenti a bűnözés valószínűségét. Az információkat ugyanígy kell kezelni, ezért elengedhetetlen, hogy egy szervezetet úgy alakítsunk ki, hogy senki ne legyen képes egymagában veszélyeztetni a biztonsági kritériumok teljesülését.

A SoD alkalmazásakor két elsődleges célt kell figyelembe vennünk:

- A különböző érdekütközések elkerülését, ugyanis ezek megjelenésekor megjelenhetnek a jogellenes cselekmények, a csalás, a visszaélések és a hibák a szervezet folyamataiban, s a munkavégzés nem tud gördülékenyen folyni.
- Szabályozási és irányítási hibák felderítése az alkalmazás során. Ezek magukban foglalják a biztonsági réseket, az információs lopást és a biztonsági ellenőrzések kijátszását. Tehát jogosulatlan hozzáféréseket ne adjunk a SoD alkalmazása során, ne forduljon elő, hogy valaki ellenőrizhetetlenné válik, vagy épp önmagát kell ellenőriznie.

A SoD korlátozza az egyén birtokában lévő hatalom vagy befolyás mértékét. A SoD helyes alkalmazásakor akkor járunk el helyesen, ha feltesszük magunknak a következő kérdéseket:

- Van egyetlen olyan személy, aki meg tudja változtatni vagy ki tudja törölni az adatokat anélkül, hogy az észrevehető, esetleg visszafordítható legyen?
- Van egyetlen olyan személy, aki ki tud szivárogtatni érzékeny információkat, el tud lopni adatokat a szervezet tárhelyeiről észrevétlenül?

- Van egyetlen olyan személy, aki teljesen felügyeli az ellenőrzéseket vagy az irányítást (részt vesz a folyamatok tervezésében, végrehajtásában és az ellenőrzésében is → magára szabhatja, alkalmazhatja a rendszert)?

A biztonság megtervezéséért és végrehajtásáért felelős személy nem lehet ugyanaz a személy, mint aki a biztonság teszteléséért , a biztonsági ellenőrzések lebonyolításáért vagy a biztonságot felügyelő személy. Ezért például az információbiztonságért felelős személy nem lehet beosztottja az informatikai vezető tisztviselőnek sem. Ne feledjük, hogy a feladatok szétválasztását szabályozó ellenőrzési technikákat külső ellenőröknek kell vizsgálniuk, ez szükséges az objektív és hatékony alkalmazásához. (Coleman, 2008.)

4.3.2. Munkakörrotáció (job rotation)

A szervezeten belüli munkavállalók rendszeres időközönként történő mozgatásának a gyakorlata a job rotation. Történhet például évente, kétévente egyszer a különböző munkaköri pozíciók vagy fizikai létesítmények között. A cél az, hogy a munkavállalók különböző időpontokban különböző munkákat végezzenek, és megakadályozzuk, hogy egy alkalmazott egyszerre ugyanazt a munkát végezhesse huzamosabb ideig. (Law Teacher 2013)

Biztonsági megoldásként a job rotation csökkentheti a visszaélések kockázatát egy vállalatnál. Általában összekapcsolódik a feladatok szétválasztásának (SoD) gyakorlatával, amit az előző pontban elmagyaráztunk.

Figyelnünk kell arra, hogy a munkatársak rendelkezzenek készségekkel és ismeretekkel ahhoz, hogy elvégezzék a többi feladatot is. Egyik előnye a módszernek, hogy abban az esetben, ha egy munkavállalónk valamilyen módon felfedezi a kiskaput, amelyet a szervezet adataival való visszaélésre használhat, a job rotation korlátozza, hogy tevékenységét mennyi ideig folytathatja. Egy másik kimutatott előnye pedig az, hogy a munkavállalók nem fásulnak bele a munkakörükbe, az újabb kihívások motiválóan hatnak rájuk, ez pedig növeli a szervezethez való elköteleződésüket, annál is inkább, hogy a munkakörváltást gyakran előléptetésnek élik meg (legalábbis az első pár alkalommal). Továbbá biztonsági szempontból nem elhanyagolható, hogy a módszer növeli a csalás felfedezésének esélyét is, hisz az utód látja, mit tett az elődje.

4.3.3. Azonosítás és hitelesítés – autentikáció és autorizáció

Egyszerű példa a két fogalom megértésére, ha én azt mondom: Bonaparte Napoleon vagyok, akkor én azonosítottam magam a francia császárként. Természetesen nehéz elhinni, hogy én vagyok az, de mi van, ha mégis? Hát akkor bizonyítsam be: hitelesítsem ezt az állítást!

A legtöbb kibertérbeli visszaélés kikerülhető megfelelő azonosítási és hitelesítési szabványok betartásával. Az azonosítási folyamat szervezeten belüli kialakításánál néhány alapvető követelményt figyelembe kell venni. Ezek a következők (Muha–Krasznay 2014):

- Az azonosítás biztonságos és dokumentált folyamat.
- Az azonosítók formátuma belső szabványban van leírva.
- Az azonosító nem utalhat az entitás funkciójára (pl. beosztás).
- Egy azonosító nem osztható meg több entitás között.
- Az azonosító ellenőrzése egyszerű folyamat kell hogy legyen.
- Az azonosító egyedi kell hogy legyen.

Az azonosítást minden esetben a hitelesítés követi, amelyet leginkább informatikai rendszerünk végez el. A hitelesítés típusai a 3 T (kivételesen nem a Kádár-rendszer Aczél-féle kultúrpolitikájára gondolunk):

- Tudás: amit az azonosított tudhat csak (pl. jelszó, bizonyos személyes információk – biztonsági kérdés?)
- Tulajdon: ami az azonosított tulajdonában van (pl. mobiltelefon – ezért kapunk egy kódot megerősítésre például online banki ügyintézés esetén, ha kérjük, ott nem az úgynevezett: O(ne)T(ime)P(assword)-jelszó megadása a lényeg, hanem a mobiltelefonunk!)
- Tulajdonság: ami az azonosított tulajdonsága (pl. ujjlenyomat, retina, hang, DNS stb.)

A kockázatokkal arányos, megbízható és erős hitelesítéshez a különböző típusú hitelesítési eljárásokat keverten, a háromból legalább kettőt együtt érdemes használni, ezt nevezzük két (vagy több) lépcsős hitelesítésnek (köznyelvben tévesen: azonosításnak). Fontos tehát, hogy két tudásalapú hitelesítés együttes használata nem tekinthető kétlépcsősnek!

Önmagában egyik sem nyújt kellő biztonságot, a mai technológiákkal a tulajdonság alapú azonosítás is könnyen lemásolható (gumiujj, felvett hangminta, pohárról szerzett DNS, nagyfelbontású 3d kép után készült műretina stb.).

A kémfilmekből néha túlzó, de manapság egyre inkább valóságos módszereket ismerhetünk meg a tulajdonság alapú azonosítás és hitelesítés kijátszására. A tulajdon önmagában talán a legkevésbé hatékony védelem, hisz ellopni, elhagyni valamit, ami hitelesíthet minket, nem a legnehezebb feladat. A tudás alapú védelem is erősnek tűnhet önmagában, hacsak nem kényszerítik ki belőlünk (kínzás, korrupció vagy zsarolás által) jelszavunk megadását. A helyzet az, hogy sokszor ehhez sem kell folyamodni...

LinkedIn hack

A LinkedIn karrier és üzleti közösségi média site-ot 2012-ben törték fel, ekkor 6,5 millió felhasználói fiók adatait szerezték meg. Ekkor az oldal értesítette felhasználóit, hogy változtassanak jelszót. Majd 2016-ban 117 millió felhasználói fiók feltörésével járó támadást hajtottak végre az oldal ellen. Történt ez úgy, hogy az oldal készítői nyilatkozták, hogy 2012 után új jelszó védelmi előírásként „sózták" a jelszavaikat.

A salt egy kriptográfiai kifejezés, lényegében véletlenszerűen generált adattal fűszereznek meg egy titkosítandó adatot (pl. jelszót), ezzel nehezítve a feltörését, a salt nélkül ugyanis minden jelszó – bár titkosítva tárolták, ugyanazzal a módszerrel lett titkosítva. (A LinkedIn esetében 2012-ben ez a Secure Hash Algorithm 1 (SHA1) volt), így, ha egyet feltörnek, feltörhető mind. A salting hatására minden egyes jelszó titkosításába kerülnek random elemek, emiatt egy jelszó feltörése által nem lesz még egy jelszó feltörhető. Ugyanakkor ez a „sózás" csak azoknál a jelszavaknál történt meg, amelyeket módosítottak 2012 után.

Az eset tanulságai:

- *Fontos a megfelelő jelszótárolás (matematikailag megfelelő erősségű titkosítással tároljuk a jelszavainkat, lehetőleg használjuk a salting-ot is).*
- *Írjunk elő megfelelően komplex jelszószabályokat a felhasználóknak (Windows ajánlás: legalább 8 tagú legyen, kis és nagybetűt, számot és speciális karaktert is tartalmazzon).*
- *Rendszereinket mindig feleltessük meg a hatályos kiberbiztonsági szabványoknak.*

- *A jelszavak tárolásának változásakor kötelező legyen minden felhasználónak új jelszót megadnia, illetve kötelezzük őket időnként jelszóváltoztatásra, ha érzékeny vagy személyes adataikat biztonságban szeretnék tudni.*
- *Felhasználóknak: Használjunk különböző jelszavakat különböző típusú oldalakon (pl. a közösségi média site-nak és e-mail fiókunknak ne legyen ugyanaz a bejelentkezési jelszava, mert, ha az egyiket feltörték, a másikkal megmenthetjük, ha össze vannak kapcsolva) (Wood 2016).*
- *Továbbá ne felejtsük el, se a tulajdonság, se a tulajdon, se a tudás önmagában nem elegendő. Saját adataink és szervezetünk adatai védelmére egyaránt érdemes többlépcsős azonosítást és hitelesítést használni!*

4.3.4. Kommunikációs/indoklási lánc

Szintén alkalmazottaink lojalitásának kiépítéséhez szükséges megteremtenünk a szervezeten belüli helyes, felülről lefelé és alulról felfelé áramló kommunikációs csatornákat, mert az egyes döntések indoklását, a szabályok megértését ezekkel tudjuk kommunikálni, illetve ellenőrizni, hogy megértették-e.

4.3.5. Integritás célú tudatosító képzések

A fentebbi eszközök és módszerek helyes működéséhez szükséges a szervezeti integritás megteremtése, hisz azon túl, hogy információbiztonsági tudatossági képzéseket tartunk, még fontos követelmény, hogy alkalmazottaink lojalitását is elérjük, hisz csak így érhetjük el, hogy minden esetben tartsák magukat a szervezet szabályaihoz. Ehhez az első lépés a szervezettel szembeni külső és belső elvárások (vezetői, de nem csak vezetői) tisztázása. Ez magában foglalja a szervezetre vonatkozó jogi és szakmai szabályok számbavételét, a szervezet (közcélú) rendeltetését, a fontosnak tartott értékek egyértelmű beazonosítását, rögzítését, szervezeten belüli deklarálását, illetve a külvilág számára történő kinyilvánítását, valamint az ezekkel való minél őszintébb és teljesebb azonosulást a vezetők és alkalmazottak egészére nézve; végül azoknak a viselkedés-, illetve magatartásformáknak az egyértelmű meghatározását, amelyet a szervezet vezetése fontosnak tart a szervezet társadalmi rendeltetésének betöltése érdekében. (Sántha–Klotz 2013)

Ehhez szükséges, hogy a szervezet belső működése a foglalkoztatottak számára átlátható és érthető legyen, a kommunikációs csatornák megfelelően működjenek. Fontos kiemelni a vezetők példamutatását: ha következetesek, és mindig a szervezet belső értékrendje szerint járnak el, akkor az alkalmazottak is hűségesebbek lesznek ezekhez az értékekhez. Illetve bizonyos ceremoniális alkalmak is hozzásegítik a szervezetet, hogy egységként működjön (évente pár alkalom, amikor minden alkalmazott, vezető találkozhat → kitüntetések, karácsony, dolgozói értekezletek). Fontos a szervezeten belüli előrelépések áttekinthetősége, esetleg feltételrendszerének megismerhetősége, tehát a korrekt személyzeti politika kialakítása. Érdemes lehet a közvetlen vezetők általi mentori feladatok ellátása is, illetve a felsőbb vezetőkkel való személyes találkozási lehetőségek kialakítása is.

A szervezeti integritást integritási képzésekkel is növelhetjük, melyeknek három fajtáját különböztetjük meg (Sántha–Klotz 2013):

- **Szabályközpontú képzési megközelítés:** a szervezet belső szabályzatait, stratégiáit stb. megismertető órák.

- **Értékalapú képzési megközelítés:** workshop jellegű képzések, ahol a foglalkozást vezető a szervezet értékeivel kapcsolatban vet fel témákat, a jelenlévők pedig ezekről beszélgetnek, ütköztetik érveiket stb.
- **Élethelyzetek feldolgozásán alapuló képzési megközelítés:** a szervezet életében már bekövetkezett vagy esetlegesen bekövetkező dilemmák eljátszása, megértése. Szintén kötetlenebb formában, a cél, hogy megismerjük a helytelen szituációkezeléseket és a szervezet értékítélete szerinti helyes viselkedést az egyes szituációkban.

Persze a szervezeti integritásmenedzsment kialakításánál legyünk figyelemmel az egyénekre, az egészséges szervezeti kultúra nem valamiféle fanatikus szektás rendszert jelent.

A szervezet értékeiben nem hívő alkalmazott kérdésköre bonyolult ügy. Szervezeti elköteleződés, integritás nélkül a legjobb emberünk is lehet áruló, ha nem tud azonosulni értékrendünkkel. Még a korrupcióra is nyitottabbá válik. A következőben egy olyan személy esetét mutatjuk be, akiről az Olvasó bizonyára már hallott korábban, megítélése rendkívül vegyes, hogy hős vagy hazaáruló, abban nem mi teszünk igazságot, de hasznos eset az integritás hiánya következményeinek felismerésében.

Snowden-ügy

Edward Snowden, az 1983-ban született informatikai szakértő dolgozott a CIA-nál és a Dellnél is, mégis az NSA-nél eltöltött néhány hónapos munkája – amelyet egyébként mint szerződéses munkatárs végzett – alapján híresült el. Snowden 2013-ban az NSA Hawaiin lévő állomásán több ezer titkos NSA- és CIA-dokumentum birtokába került, amelyeket újságíróknak átadva nyilvánosságra hozott.

A Snowden birtokába került titkos dokumentumok pontos száma azonban nem ismert. A dokumentumok az USA olyan globális elektronikus lehallgatási és kibermegfigyelési szervezeteiről, technológiájáról és akcióiról, valamint az ezek mögött lévő – nem mindig tisztázott eredetű – anyagi erőforrásokról rántják le a leplet, amelyeket a közvélemény korábban még sosem láthatott és hallhatott.

A világ ezekből a dokumentumokból ismerhette meg például azt a globális rendszert, amely a PRISM nevet viselte, és amelyet az NSA a legnagyobb internetes szolgáltatók bevonásával arra használt, hogy az interneten folyó teljes kommunikációt lehallgassa és elemezze. Edward Snowden jelenleg Moszkvában ismeretlen helyen él, miután az USA elfogatóparancsot adott ki ellene kémkedés vádjával, de Snowden Oroszországtól menedékjogot kapott. (Kovács 2018)

Tanulság:

Snowden megítélése sok tényezőtől függ, leginkább saját emberi preferenciánk határozza meg. Most ne ezt vizsgáljuk! Szeretnénk-e saját cégünkbe vagy hivatalunkban olyan embert, aki nem hisz a saját értékeinkben? A munkahely szabályainak, értékeinek megismerése, a szituációs oktatások azt a célt szolgálják, hogy lojálisabbá tegyük munkatársainkat. Persze érdemes feltennünk a kérdést, hogy a szervezet értékei valóban vállalható értékek. Mi magunk képesek vagyunk hinni bennük? Ha nem, és van lehetőségünk változtatni rajtuk, fontoljuk meg, hogy megtesszük. A hiteles menedzsment sokszor a legjobb eszköz az integráció javítására.

5. Az információs visszaélések feltárását segítő eszközök

Az előző fejezetben megnéztük, milyen eszközeink vannak, hogy helyes gyakorlatokat, motivációt, menedzsmentet építsünk ki, amivel megelőzhetjük, feltárhatjuk és akár el is háríthatjuk a visszaéléseket. A következőkben koncentráljunk csak a feltárásra. Vizsgáljuk meg sokkal konkrétabban, milyen eszközeink vannak arra vonatkozóan, hogy feltárjuk a kibertérben történő visszaéléseket.

Alapvetően három csoportba tudjuk sorolni feltárást segítő eszközeinket, amelyek így lehetnek:

- adminisztratívak,
- technikaiak, azon belül: passzív technikaiak és
- aktív technikaiak.

5.1. Adminisztratív eszközök

5.1.1. A „négy szem elv”

„**Négy szem elv**” – már a neve is beszédes. Nevezik még „két ember elvnek” is. Lényege, hogy egy-egy cselekvést, döntést, ellenőrzést legalább két embernek jóvá kell hagynia. Ez hatékonnyá teszi a különböző jelentésekben megbúvó inkonzisztencia, furcsa adatok észlelését, amelyek azért létezhetnek, mert valaki valamiféle visszaélést követett el, illetve ezen elv alkalmazásával lényegében a vezetők is ellenőrzik egymást. Hatékonysága az érintett személyek képességeire, integritására és gondosságára támaszkodik. Az alapelv finomítása során az engedélyezett személyek egyikének véletlen forgásával a második szempárt cseréljük, így a lehetséges elkövető egyáltalán nem lehet tisztában azzal, hogy melyik két személy fog foglalkozni egy adott döntéssel. A négy szem elv kiterjeszthető úgyis, hogy duplázzuk a szükséges jelszavakat valamilyen értékes adatbázisunkhoz, tehát legalább két ember kell, hogy módosításokat tudjunk bennük eszközölni. (Weatherhill 2017)

5.1.2. Audit

Az auditról lényegében már beszéltünk a Szervezeti eszközök című fejezetben. A különböző modellek, fejlesztési szabványok és jogszabályok egyaránt tartalmaznak az informatikai eszközeinket, adatbázisainkat és folyamatainkat ellenőrző eljárásokat, vagyis auditot. Az auditálás során figyelembe kell venni három kérdést:

- Ki támadhat?
- Mit kereshetnek, mit akarhatnak, és mi mit kockáztatunk?
- Vajon milyen taktikát alkalmazhatnak?

Az audit céljai a következők:

- az érzékeny adatok és szellemi tulajdon védelme,
- a hálózatok védelme,
- felelősségvállalás és felelősségre vonhatóság a szervezetért (illetve eszközért) és a tárolt/kezelt információkért. (NIST 2018)

Az auditot elvégző személyeknek:

- elegendő tapasztalattal és naprakész, mély tudással kell rendelkezniük az informatikai eszközök és biztonsági kihívások területén;

- munkájuk során a teljes rendszert, teljeskörűen auditálniuk kell, nem csak szúrópróbaszerűen ellenőrizni egyes elemeit;
- érdemes külső auditort is megbízni, a belsők személyét időnként cserélni, alkalmazni a négy szem elvet stb.

A kiberbiztonsági auditnak ki kell terjednie:

- a hálózathoz, adatbázishoz és alkalmazásokhoz kapcsolódó adatbiztonsági irányelvekre;
- az adatvesztés megelőzésére alkalmazott intézkedésekre;
- a hatékony hálózati hozzáférési ellenőrzések végrehajtására;
- a felderítő és megelőző rendszerek, szoftverek telepítésére és ellenőrzésére;
- a szervezet biztonsági módszereinek, eszközeinek ellenőrzésére (legyenek ezek fizikai, szervezeti vagy logikai eszközök);
- az incidenskezelési terv elkészítésére és implementálására. (NIST 2018)

Az auditálás külön szakma, amelynek megvannak a maga szépségei és részletei; ami fontos, hogy mindig tartsunk a szemünk előtt: rendszeres, átfogó ellenőrzések szükségesek ahhoz, hogy a különböző kibertérben történő visszaélésekre fény derülhessen.

5.2. Passzív technikai eszközök

5.2.1. DMZ

A demilitarizált zóna (a továbbiakban: DMZ) olyan hálózati szegmenst jelöl, ahol a nem-biztonságos felhasználóknak szolgáltatást nyújtó szerverek vannak. Ilyen szolgáltatás lehet az email, Web, proxy, fordított proxy szolgáltatás. Lényege, hogy a DMZ kompromittálódása esetén még nem férnek hozzá a belső hálózathoz közvetlenül, mivel azt aktív hálózati védelem választja el a DMZ-től. (Frész et al. 2014)

5.2.2. Naplózás

Gondoskodni kell az informatikai biztonsági rendszer önvédelméről, de úgy általában minden informatikai rendszerünk, adatbázisunk, kritikus elemeinek védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, valamint olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére.

A naplózás viszonylag egyszerű kérdésekre ad majd választ utólag, amikor valamilyen szoftverrel vagy manuálisan elemezzük azokat:

- Ki vagy mi,
- mikor
- és mit tett.

A naplófájljaink (log files) célszerűen automatikusan íródnak, folyamatosan nyomon követve az adott rendszerben az általunk kért eseményeket. Ez tényszerű események szövegkénti rögzítése. Míg korábban a naplózás volt az elsődleges eszköz az incidensek felismerésében, napjainkban inkább az incidensek feltárásában, az incidenshez kapcsolódó bizonyítékok megőrzésében van szerepe. A támadások fontos részei a nyomok eltüntetése, így a kifinomultabb támadáskor a naplókat törlik, vagy valami módon gátolják. (Bodó et al. 2018)

A naplózás történhet egy számítógépen végzett tevékenységekről, hálózati forgalomról, egy-egy szoftverben végrehajtott tevékenységekről, weboldalon történő böngészésről, de ide sorolhatjuk a szervezet épületébe történő beléptető rendszer log fájljait is.

A naplókat érdemes több példányban is tárolni, erre vonatkozóan az Ibtv. is tartalmaz előírást 5. biztonsági szint esetén.

Az incidensekről készült naplók elemzése már lényegében aktív eszköz, de nem feltétlenül technikai, ezt hívjuk logelemzésnek.

5.2.3. Konfigurációk és jogosultságok követése, felülvizsgálata

A szervezeti rendszerünkhöz szorosan kapcsolódik a jogosultságok követése és felülvizsgálata.

Figyeljünk a munkahelyi fluktuációra, a megváltozó feladatkörökre, az újonnan bevezetett adatbázisokra, alkalmazásokra. Ne hagyjunk meg jogosultságot megtekintésre vagy szerkesztésre arra már nem felhatalmazott személyeknek (esetleg szoftvereknek!), a meglévő jogosultságokat valahol tároljuk, tudjuk lekérni, legyen jogosultságkezelő rendszerünk, amelyen áttudjuk tekinteni, ki mihez és milyen mértékben fér hozzá, és tudjuk kezelni a különböző jogosultsági szinteket a szervezeten belül. Különösen fontos a naprakészség, ha munkakörrotációt és/vagy SoD-ot használunk.

A hardver konfigurációk és a szoftverek egymással való kölcsönhatásának informatikai vizsgálata is fontos tényező. Egy operációs rendszer vagy szerverfrissítés hatására lehet, hogy bizonyos informatikai védelmünk sérül. Ilyenkor fokozottan figyelnünk kell az esetleges behatolókra. Továbbá azért is érdemes a hardvereszközeinket figyelemmel kísérni, mert így észrevehetünk jogtalanul csatlakozó eszközöket.

5.3. Aktív technikai eszközök

5.3.1. Honeypot

A honeypot (mézesbödön) egy számítógép a monitorozott hálózati szegmensen vagy a DMZ-ben, célja a támadókat magához csalogatni, hogy ne a valódi, éles gépekkel foglalkozzanak. Az adminisztrátorok elérhetővé tehetnek néhány népszerű portot mint könnyű támadási célpont a honeypot rendszeren. Bizonyos honeypotok szolgáltatásokat emulálnak, valójában szolgáltatás nem fut. A honeypotok megtévesztésig hasonlóak az adott cég éles rendszereihez. Valójában a honeypot-ok a támadások korai felismerésének eszközei. Több honeypot egyidejű használata a honeynet. (Frész et al. 2014)

5.3.2. Honeytoken

A honeypot szerepet nem feltétlen kell egy hálózatra csatlakoztatott gépnek ellátnia, lehet csupán egy erőforrás (pl. hitelkártya-szám, Excel táblázatkezelő, PowerPoint prezentáció, adatbázis-bejegyzés vagy akár hamis bejelentkezés is), amellyel felkelti a támadó figyelmét. Ezt nevezzük honeytokennek: egy honeypot, amely nem számítógép, hanem valamiféle digitális entitás. A mézesmadzag számos formában vagy méretben létezhet, de mindegyikük ugyanazt a célt szolgálja: értékesnek látszani és lépre csalni. Előnye a honeypottal szemben, hogy a hálózaton a honeypotnak (ha egyáltalán volt) nem bedőlő külső támadót egy újabb csapdával lefülelhetjük, illetve a belső visszaélésekről is kaphatunk információt. A honeytokenre kattintva többféle dolog is történhet a támadóval, akár egy malware-t is elrejthetünk így, bár etikusabb az önbíráskodás helyett, ha a honeytoken megnyitása esetén csak egy jelzést kapunk, illetve a támadóról mindenféle adatot lementünk magunknak, ő meg megláthat egy igazából értéktelen táblázatot, vagy .ppt-t, ezután pedig megtehetjük a szükségesnek gondolt intézkedéseket. (Spitzner 2003)

A koncepció maga egyébként elég régi, már a régi térképkészítő mesterek is használtak ilyen csalikat, nem létező utcákat, városokat, utakat rajzoltak fel saját térképeikre azért, hogy lefüleljék azokat, akik róluk másolják a térképeiket. (Spitzner 2003)

5.3.3. Egyéb aktív, passzív vagy félaktív technikai eszközök

Érdemes még megemlíteni a tűzfalakat, amelyeknek különböző típusai vannak attól függően, hol helyezkednek el informatikai rendszereink, hálózatunk és az internet viszonylatában. Az IDS (Intrusion Detection System – behatolás-érzékelő rendszer) használata is segítségünkre lehet, ami nem feltétlenül informatikai, fizikai behatolás ellen például a biztonsági őrök is védenek, őket is az IDS részének tekintjük. Az IDS kiegészítéseként érdemes IPS-t (Intrusion Prevention Systems – behatolást megelőző rendszerek) alkalmazni, amely megszakítja az illetéktelen belépők tevékenységeit. (Frész et al. 2014)

6. Az információs visszaélések elhárítását segítő eszközök

6.1. Belső eszközök

A visszaélések elhárítását segítő eszközöket két csoportra bonthatjuk. Lehetnek belső és külső eszközeink. A belső eszközökbe azok a tevékenységek és módszerek tartoznak, amelyeket mi tehetünk meg egy-egy kibertérbeli visszaélés (incidens) elhárítására. Lényegében az eszközök jelentős részét a korábbiakban említettük (naplózás, honeypot, IDS stb.). Nézzük meg, hogy milyen céljai vannak az elhárítás eszközeinek:

- elszigetelés,
- visszamenőleges ellenőrzés,
- bizonyítékok rögzítése.

Eddigi eszközeink mellett a bekövetkező incidens kezelésére, elhárítására további eszközeink is vannak.

Szükségünk van az elhárításhoz **reagálási tervre,** amely elsősorban azt a célt szolgálja, hogy elkerüljük a visszaélések elhárítása során azt, hogy további bajt okozzunk. Reagálási tervet a kritikus adatok és rendszerek védelmére készítünk. A terv leírja a reagálási folyamatot, melyet megismertetünk az alkalmazottainkkal. (Berzsenyi et al. 2018)

Belső eszközeink közül a legfontosabb az elhárítás fázisában az **irányítás,** amely gyakran eltér a szervezet normál irányításától (pl. komolyabb visszaélés esetén ilyenkor megnő a kiberbiztonságért felelős vezető hatásköre). Az incidens során bejövő adatok alapján akár módosíthatja is az incidenstervet, hiszen az incidensek egyediségük és váratlanságuk miatt – keretek közé szorított – improvizációt igényelnek. A visszaélések széles skálája miatt mindig érdemes az érintett rendszert, rendszereket átfogóan megvizsgálni.

Miután lezajlott a visszaélés, meg kell kezdeni a **kárfelmérést**, és amennyire lehetséges, a **helyreállítást.** Adatvesztés, adatmódosítás esetén általában könnyű dolgunk van, a legtöbb rendszer, adatbázis redundánsan működik, így visszanyerhetők eredeti adataink. Érdemes biztonsági mentéseinket is külön tárolni a fő rendszerektől, hogy szükség esetén hozzájuk tudjunk nyúlni, ekkor azonban érdemes észben tartanunk, hogy lehet, már a biztonsági mentésünk idején a rendszerünkben volt a rés a pajzson. (Berzsenyi et al. 2018)

Minden visszaélés, akár sikeres, akár sikertelen (próbálkozás) volt, tanulság szervezetünknek. Belső folyamataink, incidenskezelésünk és általában: IT biztonságunk **fejlesztése** lehetséges a szerzett tapasztalatok alapján.

A továbbiakban nézzük meg a külső eszközöket.

6.2. Külső eszközök: szervezetek

Szerencsénkre az információbiztonság nem csak nekünk fontos. Világszerte számos különböző szervezet, intézmény jött létre, amelyek az információbiztonság elősegítéséért, biztosításáért, megteremtéséért, illetve fenntartásáért felelősek, és ezekhez is bátran fordulhatunk segítségért

Ilyen intézmények például a hálózat- és információbiztonsági hatóságok, az eseménykezelő csoportok, a nemzeti kiberbiztonsági központok (National Cyber Security Centers, NCSC), a kiberkiválósági központok, a biztonsági üzemeltetési központok (Security Operation Centers, SOC). A jelen anyagban – igaz, csak vázlatosan – az incidens kezelésért felelős, úgynevezett hálózatbiztonsági eseménykezelő

csoportokat mutatja be: ezek a CERT-ek és CSIRT-ek (lásd lentebb). A CERT és CSIRT egyaránt számítástechnikai vészhelyzetekre reagáló szervezet, mindkettő részt vesz a nemzetközi hálózatbiztonsági vagy kritikus információs infrastruktúrák védelmére szakosodott szervezetek munkájában. Mára már több száz különböző méretű, érettségi szintű CERT és CSIRT működik világszerte. (Berzsenyi et al. 2018)

6.2.1. CERT

A CERT a Computer Emergency Response Team (számítógépvészhelyzet-kezelő csoport) kifejezésből jött létre. Az Ibtv. előírja a Kormányzati Eseménykezelő Központ (GovCERT) működtetését, valamint lehetővé teszi ágazati eseménykezelő központok létrehozását is. A GovCERT feladatairól és hatásköreiről jelenleg a 185/2015. (VII. 13.) Korm. rendeletben olvashatunk bővebben.

A GovCERT alapvető rendeltetése az állami és önkormányzati szervek informatikai biztonsági támogatása, amely egyrészt megelőző jelleggel, sérülékenység menedzsment formájában a szoftver-sérülékenységek és információbiztonsági fenyegetések nyomon követésére, valamint a fenyegetés kiváltotta biztonsági esemény megelőzése érdekében az érintett IT rendszerek üzemeltetőinek tájékoztatására fókuszál. Ezen túlmenően pedig reaktív jelleggel ún. incidenskezelési tevékenységet lát el, amely a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és – több állami szervet érintően – a kezelésük koordinációjára irányul. (Cser et al. 2018)

A GovCERT feladatkörét bizonyos szempontból kiegészíti a NEIH (Nemzeti Elektronikus Információbiztonsági Hatóság), ahogy ez az alábbi ábrán látható.

	GovCERT	NEIH
Mit?	**technikai** támogatás és vizsgálat	**jogszabályi megfelelőség** támogatás és ellenőrzés
Mikor?	incidens esetén vagy **igény szerint**	a tervezőasztaltól **folyamatosan**
Hogyan?	incidenskoordináció, tájékoztatás, tudatosítás, oktatás, sérülékenységvizsgálat, gyakorlatok, …	megfelelőségvizsgálat, állásfoglalások, ajánlások, fejlesztések IT biztonsági kontrollja, …

10. ábra: A Nemzeti Kibervédelmi Intézet szakmai területei. Forrás: Cser et al. 2018, p. 160.

6.2.2. CSIRT

A CSIRT a Computer Security Incident Response Team (számítógép-biztonsági incidenskezelő csoport) kifejezésből jött létre. Többféle CSIRT-et különböztethetünk meg aszerint, hogy az adott szervezet milyen területen, szektorokban végzi tevékenységét, nyújtja a szolgáltatásait. Szinte minden országban működik nemzeti CSIRT, kormányzati CSIRT, kritikus infrastruktúra CSIRT, egyetemi CSIRT, katonai CSIRT, üzleti CSIRT, belső CSIRT (valamilyen szervezeten belül, általában valamilyen anyaszervezethez csatlakozik), szoftverkiadó CSIRT, egyetemi CSIRT stb., esetleg ezek tetszőleges kombinációja (bizonyos esetekben egy adott CSIRT több különböző típusú CSIRT funkcióját is ellátja). (Berzsenyi et al. 2018)

Megelőzést nyújtó szolgáltatások	Válaszintézkedést nyújtó szolgáltatások	Biztonsági minőségirányítás
Riasztások és figyelmeztetések **Incidenskezelés** Incidenselemzés Incidenssel kapcsolatos helyszíni válaszintézkedések Incidenssel kapcsolatos válaszintézkedések koordinálása **Sebezhetőség kezelése** Sebezhetőség elemzése Sebezhetőséggel kapcsolatos válaszintézkedések Sebezhetőséggel kapcsolatos válaszintézkedések koordinálása **Kártékony kódok kezelése** Kártékony kódok elemzése Kártékony kódokkal kapcsolatos intézkedések Kártékony kódokkal kapcsolatos intézkedések koordinálása	• Bejelentések • Technológiafigyelés • Biztonsági ellenőrzések és felmérések • Biztonsági konfiguráció beállítása és karbantartása • Biztonsági eszközök fejlesztése • Behatolásérzékelési szolgáltatások • Biztonsággal kapcsolatos információk terjesztése	• Kockázatelemzés • Üzletmenet-folytonosság és katasztrófa utáni visszaállítás • Biztonsági tanácsadás • Tudatosság növelése • Oktatás/képzés • Termék kiértékelése vagy tanúsítása

2. táblázat: A CSIRT-ek különböző szolgáltatásai. Forrás: Berzsenyi et al. 2018, p. 89.

A fenti táblázatban találhatjuk a CSIRT-ek különböző feladatait. Kiemelendők a válaszintézkedésre fókuszáló feladatok, melyek célja, hogy a CSIRT ügyfélköréhez tartozó szervezetektől, ügyfelektől érkező incidens bejelentésre, valamint a CSIRT rendszereit érintő fenyegetésre vagy támadásra vonatkozó válaszintézkedés, reagálás, valamint az általuk okozott kár enyhítése megtörténjen. (Berzsenyi et al. 2018)

Szerzői megjegyzés: a gyakorlatban igazából nincs különbség a CERT-ek és a CSIRT-ek között.

A GovCERT-en kívül Magyarországon a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja, a Katonai CERT, valamint a kormányzati szektoron kívül két, önkéntes alapon működő CSIRT: a Hun-CERT és a NIIFI-CSIRT is működik. (Berzsenyi et al. 2018)

6.2.3. Bűnüldözés

Természetesen a kiberbűncselekmények elkövetőinek üldözésére is alakulnak nemzeti és nemzetközi egységek, szervezetek, általában az állami vagy államközti szervek (EU, Interpol) rendőrségei, rendészeti, katonai rendészeti vagy más bűnüldözői, elhárítói szerveiken belül.

Az európai kiberbűnüldözési együttműködés tekintetében fontos előrelépés volt, amikor 2013-ban az Europol (amely szervezet a súlyos nemzetközi bűncselekmények és a terrorizmus elleni fellépésben nyújt segítséget a tagállamoknak) létrehozta az Európai Számítógépes Bűnüldözési Központot (EC3) annak érdekében, hogy megerősítse a kiberbűnözésre adott európai válaszokat. (Cser et al. 2018)

7. Korrupció

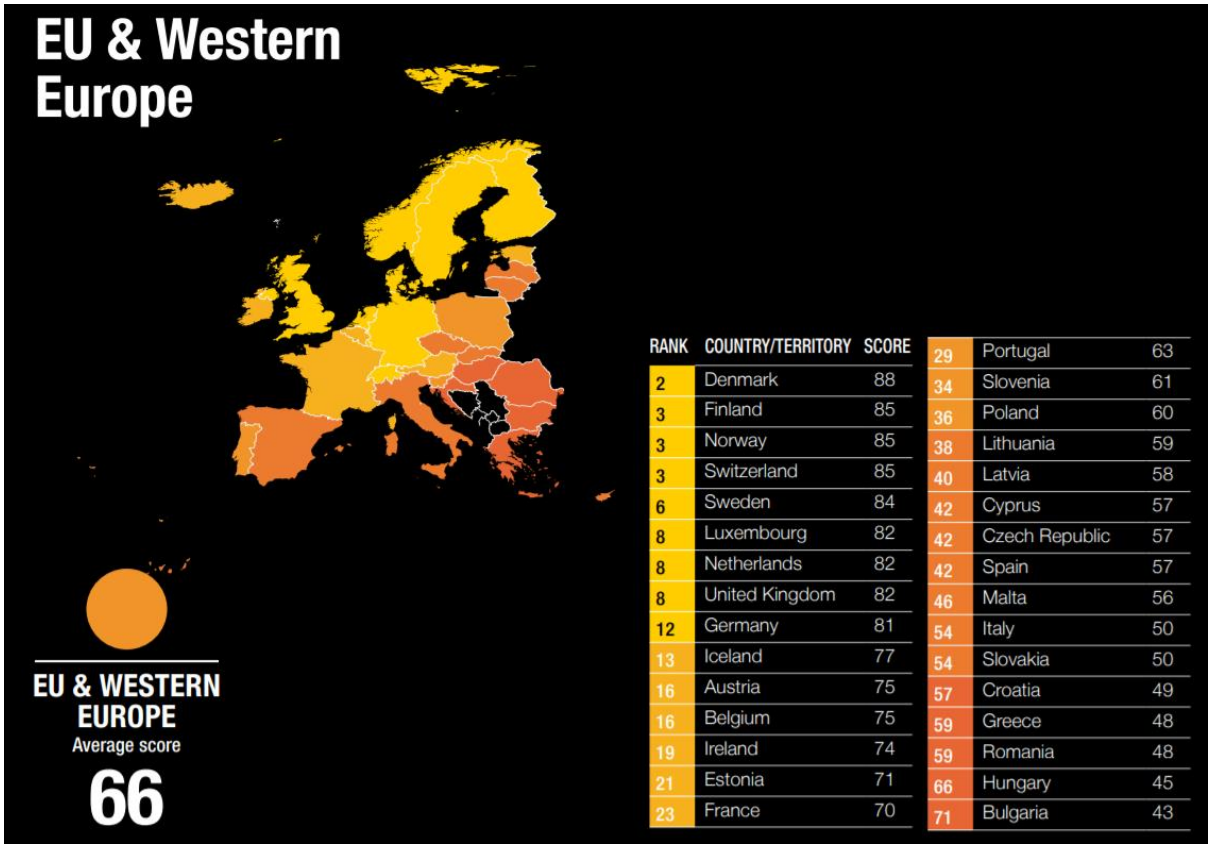
7.1. Fogalma és mérése

A tanulmány utolsó fejezetében témánk a korrupció lesz. A korrupció ritkán témája a kiberbiztonságról szóló szövegeknek, illetve ajánlásoknak, de ez nem jelenti azt, hogy nincs szoros összefüggés a két téma között. Gondoljunk csak bele: az információs rendszerek, amelyeket emberek használnak, és amelyekről tudjuk, hogy a social engineering eszközök által az emberek a gyenge pontjaik, nem hódolnak-e be a minden más rendszert is hatékonytalanná, költségessé és bűnössé tévő korrupció által. A különbség csupán annyi, hogy a social engineering eszközök használatakor beszélhetünk egy áldozatról, akit valakik átvertek, kihasználtak, a korrupció esetén inkább bűnrészes ez a fél.

A korrupció latinul („corruptio”) „leromlást”, morális romlottságot jelent; kifejező ez a szó. A korrupcióról köznapi gondolkodásunk során vegyes érzelmeink lehetnek, általános esetben ugye csak arról van szó, hogy XY ad egy 1000-est a hivatalnoknak, így hamarabb sorra kerül. A latin jelentésből azonban valami többlettartalmat is érzünk a kifejezés mögött. Bár maga a jelenség az emberiséggel vagy legalábbis a társadalmakkal egyidős lehet (erre utal, hogy már Hammurapi Kr. e. 1722-es híres törvényoszlopa is bünteti a megvesztegetést), mégsem találtuk meg igazán megszüntetésének eszközeit. Viszont törekednünk kell rá, hogy lehetőleg saját szervezetünket minél kevésbé sújtsa. Miért?

A korrupció egyik lehetséges definíciója: „az elfogadott szabályoktól való eltérő viselkedés egyéni haszon elérése érdekében”. (Takács et al. 2011) Ez a meghatározás kulcsfontosságú. Az alkalmazottunk, aki eltér a szervezet által elfogadott szabályoktól, fenyegetettséget jelenthet.

A korrupció hatásai társadalmi szinten: a politikai berendezkedésben, az állami szervekben, vezetőkben való bizalom hiánya; az adómorál és a gazdasági teljesítmény romlása, a szervezett bűnözés előretörése. (Interpol 2018) A szervezeti korrupció ezek leképződése, megfeleltetése: csökken a szervezeten belüli termelékenység, munkahatékonyság, növekszik a szabályszegések száma, csökken a menedzsment és a szervezet iránti bizalom, hűség.



RANK	COUNTRY/TERRITORY	SCORE
2	Denmark	88
3	Finland	85
3	Norway	85
3	Switzerland	85
6	Sweden	84
8	Luxembourg	82
8	Netherlands	82
8	United Kingdom	82
12	Germany	81
13	Iceland	77
16	Austria	75
16	Belgium	75
19	Ireland	74
21	Estonia	71
23	France	70
29	Portugal	63
34	Slovenia	61
36	Poland	60
38	Lithuania	59
40	Latvia	58
42	Cyprus	57
42	Czech Republic	57
42	Spain	57
46	Malta	56
54	Italy	50
54	Slovakia	50
57	Croatia	49
59	Greece	48
59	Romania	48
66	Hungary	45
71	Bulgaria	43

11. ábra: EU-tagállamok és nyugat-európai országok korrupciós érzékelési indexe 2017-ben. (Transparency International 2018

A Transparency International Korrupció Érzékelési Indexe (Corruption Perception Index) a korrupció közszférában érzékelt mértéke alapján rangsorolja az országokat az egész világon. A Korrupció Érzékelési Index összetett mutató, amely különböző független és elismert intézetek által készített szakértői felmérések korrupcióval kapcsolatos adataira épít. A CPI a világon a legszélesebb körben használt korrupciós mutató. A CPI áttekintést ad az adott pillanatban a korrupció érzékelésére a világon. Az index 0–100 között mutatja a korrupció érzékelését a közszférába, ahol a 0 azt jelenti, hogy az adott országban a korrupciót magas mértékben érzékelik. (Transparency International 2018) Hazánk az EU átlagtól lemarad, sőt a második legrosszabbul teljesített 2017-ben.

7.2. A korrupció megjelenése és jogi, szervezeti kezelése

A negatív társadalmi és gazdasági folyamatokon kívül a korrupció konkrét okai között a következőket említhetjük (Sántha–Klotz 2013):

- a folyamatok átláthatatlansága (felelősségi körök egybemosódása, visszaélések felderíthetetlensége);
- a szabályozó rendszerek tökéletlensége (szabályozás hiánya vagy épp túlszabályozás);
- nem jól működő ellenőrző és belső kontroll rendszerek (feladatmegosztás hiánya, rossz eredményesség);
- a külső kontroll rendszerek hiányosságai, a közvélemény és a médiaszereplők általános felkészületlensége, hiteltelensége;
- a korrupció kifizetődő volta (alacsony lebukási ráta, az egyén számára jó ár-érték arány);
- a (közszférában) foglalkoztatottak kellő anyagi megbecsültségének hiánya.

A korrupciós bűncselekmények fajtáit a 2012. évi C. törvény a Büntető Törvénykönyvről nevesíti, melyek a következők:

- vesztegetés,
- vesztegetés elfogadása,
- hivatali vesztegetés,
- hivatali vesztegetés elfogadása,
- vesztegetés bírósági vagy hatósági eljárásban,
- vesztegetés elfogadása bírósági vagy hatósági eljárásban,
- befolyás vásárlása,
- befolyással üzérkedés,
- korrupciós bűncselekmény feljelentésének elmulasztása.

A korrupció elleni harc minden jogállamnak kötelessége. Magyarországon a korrupcióellenes harc kormányzati elhatározását mutatja a Nemzeti Korrupcióellenes Program (2015–2018) meghirdetése. Ennek értelmében a belügyminiszter a korrupcióellenes tevékenységgel összefüggő kormányzati feladatokat a Nemzeti Védelmi Szolgálat (NVSZ) közreműködésével látja el.

Magyarországon az NVSZ kiemelt feladata a korrupció csökkentése, a szervezett bűnözői körök rendvédelmi és közigazgatási szerveken belüli térnyerésének megakadályozása, magas szintű felderítő munka folytatása, illetve a hivatásuk miatt veszélybe került munkatársak és családtagjaik számára a megfelelő védelem megszervezése. Az NVSZ feladata a szervezeti integráció növelésében való részvétel mint szakmai iránymutató, továbbá a korrupcióellenes feladatok koordinálását is e szerv látja el. Az NVSZ koordinációs feladatain túl komoly szerepet játszik a korrupciós cselekmények felderítésében is. A hatóságok visszaélés és részrehajlás nélküli, tisztességes ügyintéző tevékenysége megvalósításának egyik hatékony eszköze a megbízhatósági vizsgálat. A megbízhatósági vizsgálat a NVSZ által végzett eljárás. Célja annak megállapítása, hogy az érintettek eleget tesznek-e a jogszabályban előírt hivatali kötelezettségüknek. Ennek megállapítása érdekében a vizsgálatot lefolytató szerv a munkakör ellátása során a valóságban is előforduló vagy feltételezhető helyzeteket hoz létre mesterségesen.

A Nemzetbiztonsági Szakszolgálat (NBSZ) feladata Magyarország nemzetbiztonsági védelmének, a bűncselekmények megelőzésének és feltárásának, valamint az igazságszolgáltatás hatékonyságának elősegítése, így az NVSZ-t támogató szervként van jelen a korrupcióellenes harcban.

Az OLAF (Office Européen de Lutte Antifraude – Európai Csalás Elleni Hivatal) kivizsgálja az EU költségvetését károsító csalásokat, valamint az uniós intézményekben előforduló korrupciós cselekményeket és súlyos kötelezettségszegéseket, továbbá csalás elleni politikát dolgoz ki az Európai Bizottság számára. Az OLAF által felderített visszaélésekben a magyar hatóságok megkezdhetik azok kivizsgálását, egyébként az Európai Bizottság dönthet bírság kiszabásáról az adott ország irányába.

7.3. Korrupció és elektronizáció kölcsönhatásai

Bár sokszor és sok helyen találkozhatunk azzal a közhellyel, hogy az elektronikus közigazgatás visszaszorítja a közigazgatásban a korrupciót (Molnár et al. 2006), a kép kissé árnyaltabb. Kezdjük ott, hogy a korrupció egyik gerjesztő tényezője, ha az állam nagyon centralizált. Az elektronikus közigazgatás – bár a SZEÜSZ koncepciót decentralizált modellnek nevezzük – egyfajta centralizációs folyamat. A központi államigazgatás az elektronikus rendszereken keresztül magához veszi az ügyek széles körének intézését.

Miből fakad mégis ez a megállapítás? Nos, ez egyszerű: a korrupcióhoz emberek kellenek, akik döntéseket hozhatnak, az elektronikus közigazgatásnak hála, mivel egyes joghatásokat kiváltó ügyek az online térbe kerültek, így a korrupcióhoz szükséges személyes kontaktok száma csökken. Sőt, ha az állampolgárok korrupciót tapasztalnak a hivatalokban, lehetséges, hogy emiatt az elektronikus közigazgatás szolgáltatásai felé fordulnak.

Ugyanakkor a korábban felsorolt szervezeti és menedzsment eszközök nem megfelelő használata mellett egy-egy alkalmazottnak sokkal nagyobb hatalom lehet a kezében, mint korábban. Jó példa erre a Manning-ügy, ahol egy egyszerű közkatona államtitkokhoz fért hozzá. Ha egy ügynök ezért pénzt ad neki, korrupció történik, és bár számszerűleg lehet, hogy az elektronizáció és elektronikus közigazgatás miatt csökken a korrupcióval kapcsolatos bűncselekmények száma, az impakt-faktoruk sokkal-sokkal nagyobb lehet. Gondoljunk bele: korábban egy állami nyilvántartás papíralapú dokumentumait milyen időigényes és körülményes (így drága) lehetett korrupció útján megszerezni, ma meg egy rosszul kezelt rendszer, egy jogosulatlan hozzáférés az adatbázisokhoz, és máris egy pendrive-on vannak a bizalmas adatok.

A nem megfelelő jogosultságkezelés rés a pajzson, ha korrumpálható alkalmazottunk van, de nem csak a pénz vagy a hatalom miatt dönthet úgy valaki, hogy illetéktelen kezekbe juttat bizalmas adatokat. A Manning-ügy az USA hadseregének egyik legnagyobb botrányává nőtte ki magát, és iskolapéldája a jogosulatlan hozzáférésnek.

Manning-ügy

Századunk eddigi egyik legelismertebb visszaélése a Bradley Manning közlegény általi titkosított dokumentumok szivárogtatása a Wikileaks weboldalnak. Manning-nek feltételezhetően iraki szolgálata alatt hozzáférése volt olyan védett adatbázisokhoz a katonai kirendeltség védett hálózatán keresztül, amelyen titkosított adatokhoz fért hozzá. Manninget letartóztatták, miután egy társának (aki aztán az FBI-nak) bevallotta, hogy ő lopta el a szóban forgó adatokat.

Több hónap alatt Manning az ausztrál politikai aktivista, Julian Assange által alapított weboldalnak majdnem 100 000 titkosított katonai és diplomáciai dokumentumot juttatott el. Assange és csapata 2010 februárjában kezdte közzétenni a Wikileaks-en a dokumentumokat, amelyek közül több is az Egyesült Államok diplomáciai és katonai reputációját rontotta. (Lewis University 2014)

Az eset jól világít rá, hogy bármekkora energiát is fordítunk rendszereink informatikai védelmére, az emberi tényezőt nem zárhatjuk ki. Akár szándékosan vagy véletlenszerűen, olyan alkalmazottak, akik érzékeny információkhoz férhetnek hozzá, komoly problémát jelentenek a biztonság fenntartásában. Megfelelő jogosultságkezeléssel ez az eset elkerülhető lehetett volna. Persze felmerülhet a morális kérdés, hogy jobb-e a világnak, hogy ezek a dokumentumok kikerültek a nyilvánosságra, vagy fontosabb az államok hadititkokhoz való joga.

Ami még fontosabb kérdés, hogy Manning esetén hogyan történhetett ez meg. A hadseregekre jellemző katonás rend és fegyelem szigorú előírásokat írt elő Manning számára is, felettesei rendszeresen ellenőrizték munkáját. A gond ott volt, hogy a hosszabb közös munka mellett a szabályok betartása is lazult, bizalom alakult ki a közlegény és felettesei között. A bizalom persze erény, de a munka és a barátság nem mehet egymás rovására.

Az eset megmutatja továbbá, hogy az elektronizáció mennyire fel tudja nagyítani a korábbi, kisebb visszaéléseket. A nem megfelelő jogosultsággal kezelt adatbázisok és rendszerek pillanatok alatt komplett levéltárnyi anyagok megsemmisülését, módosítását vagy továbbküldését teszik lehetővé.

A korrupció a kibertérrel kapcsolatos döntésekben is megjelenhet. Döntéshozók, stratégiaalkotók, vezetők lefizetésével, befolyásuk megszerzésével kialakíthatók úgy egy szervezet belső folyamatai, hogy sérülékennyé váljanak. Ugyanez a helyzet akkor, ha egy informatikus hajlik meg a piszkos pénz vonzása előtt, és úgy ír meg egy kódot, hogy „véletlenül" kiskaput hagy benne. Külsős auditorok lefizetése is megtörténhet, hogy egy-egy alkalmazott saját hibáit leplezze, így a vizsgálati eredményeket meghamisítsa. Ezenkívül a közigazgatásban sem tűnhet el a személyes kontakton alapuló korrupció, hiszen a legtöbb közigazgatási ügy továbbra is intézhető személyesen.

A korrupció a legkülönbféle előnyökhöz juttathatja a felbujtót (ahol a hatalom, a pénz vagy a szex lehetősége megjelenik, ott a bűn is jelen lehet), emiatt önmagában az elektronizálás nem szünteti meg, talán, ha mesterséges intelligenciák vezérelnek majd mindent...

A korrupció elleni védekezés eszközeit az információs visszaélések megelőzését és feltárását segítő eszközök felsorolásánál érdemes újra átnéznünk. Ugyanis: a korrupció lényegében adatokkal, információval, döntési jogkörrel való visszaélés, tehát azon információbiztonsági megoldások, amelyek segítségével meg tudjuk védeni adatainkat és a döntéseinket, biztosítani tudjuk a megfelelő auditálást, segítségünkre lesznek a korrupcióellenes harcban is, a korrupció megelőzésében.

A korrupció megelőzésében az alkalmazott lojalitása és elköteleződése kulcsényező, képbe kerülnek tehát az integritáscélú tudatosító képzések, illetve általában az integritásmenedzsment eszközök. A korrupció ellen jó megoldás lehet a „négy szem elv", hiszen ha a döntésekbe több embert bevonok, akkor csökkentem a korrupció esélyét; a különböző tevékenységek naplózása, hiszen nyoma marad a jogosulatlan lekérdezéseknek, interakcióknak.

A következőben nézzünk meg egy konkrét büntetőügyet a közigazgatásban a korrupció és az elektronikus közigazgatás kapcsolódására Magyarországon.

Korrupciós bűncselekmények egy budapesti okmányirodában – vádat emelt a fővárosi főügyészség

2017. december 19-én vádat emelt a fővárosi ügyészség három személy ellen.

„A vád szerint a három ügyintéző korábban honosított személyek adataival állított ki más személyek részére jogosulatlanul magyar hatósági igazolványokat.

A vádirat szerint az I. rendű vádlott 2014. és 2015. évben anyagi ellenszolgáltatás fejében hivatali ügyintézésekben vállalt közreműködést.

Három vádlott társa a vádbeli időszakban a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEKKH) egyik budapesti kirendeltségén teljesített szolgálatot, egyikük kormánytisztviselőként, a másik két ügyintéző pedig főmunkatársi besorolásban. Mint okmányügyintézők, feladatuk közé tartozott egyebek mellett a személyi okmányok – személyazonosító igazolvány, lakcímet tartalmazó hatósági igazolvány, vezetői engedély, nemzetközi vezetői engedély – elkészítése, kiállítása.

A vád szerint az I. rendű vádlott hivatali ügyéntézései során ismerkedett meg a II. és III. rendű vádlottakkal, akikkel jó kapcsolatot alakított ki, majd később rávette őket arra, hogy az általa hozott ügyfelek részére más – korábban honosított – személyek adatainak felhasználásával hamis személyi okmányokat, így személyi igazolványt, vezetői engedélyt, útlevelet állítsanak ki. A vád szerint a IV. rendű vádlott, bár nem az I. rendű vádlott rábírására, de hasonló módon állított ki hamis okmányokat.

A hamis okiratok kiállításáért cserébe az I. rendű vádlott 2015 márciusában az egyik ügyintézőnek egy 120 ezer forint értékű, vidéki hotelbe szóló ajándékutalványt adott, amit az ügyintéző elfogadott.

A vád szerint továbbá a II. rendű és III. rendű vádlottak a fentiekhez hasonló, más bűncselekményt is elkövettek; eszerint 2015. első felében ismerősük, illetve hozzátartozójuk kérésére jogosulatlanul lekérdezték gépkocsik adatait a gépjármű nyilvántartásból.

A Fővárosi Főügyészség az ügyben hivatali vesztegetés, hivatali visszaélés, több rendbeli hivatalos személy által elkövetett közokirat-hamisítás bűntette és más bűncselekmények miatt nyújtott be vádiratot az illetékes bírósága." (Magyarország Ügyészsége 2017)

Az ügy tanulságai:

- *Viszonylag kis összegben is történhet a korrupció, emiatt bárhol és bármikor felbukkanhat, az emberi önzés határtalan tud lenni, gondoljunk a százmilliós autótulajdonosokra, akik a parkolást akarják megúszni...*
- *Bár az okmányügyintézéshez elengedhetetlenek az elektronikus nyilvántartások, azokba szabályozott az adatbevitel, és a hozzáférők köre is a megfelelő jogosultságkezelés mellett történik, mégis az esetből látszik, hogy támadható. Hasonlóan a gépjármű-lekérdezés esetén is, holott ott pár száz forint befizetése után, korrupció nélkül is hozzáfért volna a megrendelő az adatokhoz.*
- *Egy ügyintéző felügyeli az adatok bevitelét, igazából rajta áll, hogy valós adatokat visz be vagy sem. Tehát az elektronizált rendszer gyenge pontja itt is az ember.*
- *A nyilvántartásokban bekövetkező anomáliák lebuktathatják az ügyintézőt. Például egy-egy ember adataira hivatkozva látjuk, hogy más-más kép lett hozzárendelve, ezt személyes ellenőrzéssel vagy képfelismerő és szövegelemző szoftverekkel automatizálni is lehet, így az anomáliák által lebuktathatók a tettesek.*
- *Közokirat-hamisítás és jogosulatlan hozzáférés történt közadatokhoz, de ne legyenek kétségeink: a közigazgatásban a korrupció megannyi helyen felbukkanhat, ahol szintén elektronikus rendszer manipulálásával követik el a bűncselekményt, de látjuk, hogy ehhez emberi elkövetőre van szükség, ezért hangsúlyozzuk a humán eszközök fontosságát a kibertérben elkövetett visszaélések terén mint a megelőzés hatékony eszközeit.*

8. Összegzés

A jelen tanulmány célja átfogó kép kialakítása a kibertérben történő visszaélések területén. Ennek érdekében az Olvasó megismerkedhetett a téma néhány szemléletformáló fogalmával, úgymint a kibertér, a deep web és a dark web, illetve a VPN és a proxy. Ennek célja előrevetíteni a későbbi kibertérbeli visszaélések felderíthetőségének és beazonosíthatóságának nehézségét.

Megismerkedtünk az információs visszaélések lehetséges céljaival és területeivel, így a bizalmasság, sértetlenség és rendelkezésre állás fogalmaival is. Ezután részletesebben elmerültünk a malware és a social engineering támadási módszereiben. Ennek célja, hogy lássuk, milyen széles eszköztár van a támadók kezében, és ehhez mérten nekünk is a védekezés változatos palettáján kell tudnunk festeni, ha valaha kiberbiztonsági döntéseket kell hoznunk, vagy csak egy-egy kiberbiztonsági feladatot hajtunk végre, vagy valamilyen szabály betartására köteleznek vezetőink.

A következő fejezetben így azokat a szervezeti eszközöket és jogszabályokat néztük át, amelyek előírásokat és ajánlásokat kínálnak a szervezetek, azok jogi és szervezeti keretei számára. A NIST által azonosított 5 kategória és a 3 vonalas védelmi modell együttes használata hatékony lehet a szervezet kiberbiztonsági feladatainak szervezeti tervezése és napi működése során, de a későbbi ellenőrzés, az auditfolyamatok működésénél is. Majd megtanultuk, hogy a legjobb belső és külső szabályozás és menedzsment-rendszer sem működőképes, és funkcionalitását veszti, ha az alkalmazottainkra nem figyelünk kellőképpen. A kiber visszaélések humán megelőzése kiemelt jelentőségű, hiszen az ember az informatikai rendszereink leggyengébb pontja. Rendszereink egyik kulcsfunkciója az azonosítás és hitelesítés, hisz ehhez köthetjük a legtöbb nem kívánt eseményt, amikor valaki jogosulatlanul fér hozzá adatainkhoz, eszközeinkhez, így itt kiemeltük a több lépcsős hitelesítés gyakorlatát. Végül a visszaélések feltárását segítő adminisztratív és technikai eszközök világába kóstoltunk bele, hangsúlyozva, hogy a korábbi megelőzés módszertárára építünk. Jól megrajzolt belső folyamataink, a rendszeresen, szervezetileg biztosított audit, tehát a szervezetünk kiváló folyamatszervezése rengeteg visszaélést megelőzhet.

Végül lezárva a visszaélések történetét, bízva abban, hogy idáig nem jutunk el, bemutattuk az információs visszaélések elhárítását segítő eszközöket is. Röviden megnéztük, milyen belső eszközei vannak az incidens elhárításnak, majd részletesebben megvizsgáltuk, szervezetünk kikre támaszkodhat a bajban.

Utolsó fejezetünkben a már korábban is elő-előbukkanó korrupciót vizsgáljuk, és kérdéskörét hasonlítjuk össze a kiberbiztonság területével. Meglepődve vagy sem, de láthatjuk, hogy a két terület hasonló módon fejleszthető: humán és szervezeti eszközökkel ugyanúgy, mint informatikaiakkal. Végül néztünk egy átfogó példát arra, hogy milyen kapcsolat is lehet a közigazgatásban a korrupció és az elektronikus közigazgatás között.

Összességében láthatjuk, hogy a témakör nagyon szerteágazó, tanulmányunk nagyon sok konkrét terület bemutatására nem is tudott most keretet biztosítani. Az incidens-menedzsmentről, az anti-korrupciós eszközökről, a rendszerek informatikai védelméről több száz oldalas könyveket találunk, köztük jónéhányat az irodalomjegyzékünk is felsorol, így akit mélyebben érdekel a téma, a jogszabályok és szabványok száraz szövege mellett bőven talál izgalmas és érdekes olvasmányokat is benne.

Irodalomjegyzék

- Adebayo, O. S. – Mabayoje, M. – Mishra, A. – Oluwafemi, O.: *Malware Detection, Supportive Software Agents and Its Classification Schemes.* International Journal of Network Security & Its Applications (IJNSA), Issue Vol. 4, 2012, No.6., pp. 33-49.
- Bányász P.: *Az okos mobil eszközök jelentette kiberbiztonsági kihívások.* Budapest, 2018. Idézi: Mitnick, Kevin D.: *A legendás hacker – A megtévesztés művésze.* Perfact-Pro Kft., Budapest, 2003, p. 348.
- Bergman, M. K.: *White Paper: The Deep Web: Surfacing Hidden Value.* Journal of electronic publishing, Vol. 7, 2001, No.1.
- Berzsenyi D. és mtsai.: *Incidensmenedzsment.* Dialóg Campus Kiadó, Budapest, 2018.
- Beuth, P. – Biermann, K. – Klingst, M. – Stark, H.: *Merkel and the Fancy Bear (Cyberattack on the Bundestag).* 2017. https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia (2018. 11. 11.)
- Bodó A. P. és mtsai.: *Célzott Kibertámadások.* NKE, Budapest, 2018.
- *Cisco Secure Virtual Private Networks – Student Guide.* Cisco Systems, USA, 2005.
- Coleman, K.: *The key to data security: Separation of duties: This control works in finance, and it will work in information security.* 2008. https://www.computerworld.com/article/2532680/technology-law-regulation/the-key-to-data-security--separation-of-duties.html (2018. 11. 06.)
- Constantin, L.: *Scareware found hidden in Google Play apps downloaded by millions.* 2015. https://www.pcworld.com/article/2879952/scareware-found-hidden-in-google-play-apps-downloaded-by-millions.html (2018. 11. 03.)
- Cser O. A. és mtsai.: *Célzott kibertámadások.* Nemzeti Közszolgálati Egyetem, Budapest, 2018.
- Dearden, L.: *Russia's meddling in US election could be 'act of aggression', says Nato commander.* 2017. http://www.independent.co.uk/news/world/europe/russia-donald-trump-hacking-us-election-act-of-war-collective-defence-nato-commander-donald-trump-uk-a7609551.html (2017. 11. 18.)
- deepweb-sites.com: *How Big is the Deep Web? A Complete Guide about the Deep Web.* 2016. https://www.deepweb-sites.com/how-big-is-the-deep-web/ (2018. 11. 01.)
- Ducklin, P.: *Apple's App Store hit by the XCodeGhost of malware present.* 2015. https://nakedsecurity.sophos.com/2015/09/22/apples-app-store-hit-by-the-xcodeghost-of-malware-present/ (2018. 11. 03.)
- ESET: *Trends for 2015: Targeting the Corporate World.* 2015. https://www.welivesecurity.com/wp-content/uploads/2015/02/trends-2015-targeting-corporate-world.pdf (2018. 03. 11.)
- ESET: *Cybersecurity Trends 2018: The Cost of Our Connected World.* 2018. https://www.welivesecurity.com/wp-content/uploads/2017/12/ESET_Trends_Report_2018.pdf (2018. 11. 04.)
- Európai Bizottság: *Sajtóközlemény: Az Unió helyzetéről szóló 2017. évi beszéd – Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási képességet.* 2017. http://europa.eu/rapid/press-release_IP-17-3193_hu.htm (2017. 11. 20.)
- Európai Bizottság: *Ki az adatkezelő vagy adatfeldolgozó?* 2018.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_hu (2018. 11. 06.)

- Fehér K. – Király O.: *Álhíresülés – a hamis hírek dinamikája a médiában.* Századvég – Új folyam 84. 2017/2. Álhírek, pp. 39–50.
- Frész F. – Kálovics T. – Puha G.: *Hálózatok Biztonsága.* Nemzeti Közszolgálati Egyetem, Budapest. 2014.
- Gálffy C.: *VPN? Csak lassan a testtel!* 2017. https://www.hwsw.hu/hirek/56755/android-biztonsag-vpn-kapcsolat-titkositas.html (2018. 10. 27.)

  GDPR: *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 (általános adatvédelmi rendelet).* 2016. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN (2018. 11. 05.)
- Horváth A. és mtsai.: *A szoftver sérülékenységek kihasználási módozatai – Informatikai támadások, támadók és biztonság 2013–2016.* IT és hálózati sérülékenységek társadalmi-gazdasági hatásai (INFOTA), 2016, pp. *59*–108.
- HUNCERT: *Az adathalászatról (phishing, pharming).* 2004. https://www.cert.hu/az-adathalaszatrol-phishing-pharming (2018. 11. 04.)
- Hyperion Grey: *Dark Web Map.* 2018. https://www.hyperiongray.com/dark-web-map/ (2018. 03. 26.)
- IIA: *The Three Lines of Defense in Effective Risk Management and Control – IIA Position Paper — Strongly Recommended Guidance.* 2013. https://global.theiia.org/standards-guidance/recommended-guidance/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control.aspx (2018. 11. 05.)
- Ikram, M. et al.: *An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps.* IMC'16 *Proceedings* of the 2016 Internet Measurement Conference.
- Interpol: *Corruption.* 2018. https://www.interpol.int/Crime-areas/Corruption/Corruption (2018. 11. 13.)
- Kessem, L.: *Carbanak: How Would You Have Stopped a $1 Billion APT Attack?* 2015. https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/ (2018. 11. 11.)
- Kovács L.: *A kibertér védelme.* Dialóg Campus Kiadó, Budapest, 2018.
- Law Teacher: *The Meaning and benefits of Job Rotation.* 2013. https://www.lawteacher.net/free-law-essays/employment-law/the-meaning-and-benefits-of-job-rotation-employment-law-essay.php?vref=1 (2018. 11. 07.)
- Leitold, F.: *Sebezhetőségvizsgálatok a gyakorlatban.* Budapest: NKE, Budapest, 2014.
- Lewis University: *Top 3 High Profile Information Security Breaches of the 21st Century.* 2014. https://online.lewisu.edu/mscs/resources/top-3-high-profile-information-security-breaches (2018. 11. 11.)
- Madhusudan, P. A. – Poonam D., L.: *Deep Web Crawling Efficiently using Dynamic Focused Web Crawler. International* Research Journal of Engineering and Technology (IRJET) 2017, pp. 3303–3306.

- Molnár L.: *Megtévesztés az Információs Társadalom eszköztárában: Hírek és álhírek.* Budapesti Corvinus Egyetem, Budapest, 2017.
- Molnár S. és mtsai.: *Elektronikus közigazgatás – Éves Jelentés 2006.* http://mek.oszk.hu/05600/05683/05683.pdf (2018. 11. 13.)
- Muha L.: *Fogalmak és definíciók. Az informatikai biztonság kézikönyve.* Verlag Dashöfer Szakkiadó, Budapest, 2004.
- Muha L. – Krasznay Cs.: *Az elektronikus információs rendszerek biztonságának menedzselése.* Nemzeti Közszolgálati Egyetem, Budapest, 2014.
- Muncaster, P.: *EU to Declare Cyber-Attacks "Act of War".* 2017. https://www.infosecurity-magazine.com/news/eu-to-declare-cyber-attacks-act-of/ (2017. 11. 19.)
- NATO: *Az Észak-atlanti Szerződés.* 1949. https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=hu (2017. 11. 15.)
- Nador.hu: Szabályzatok és ITIR kialakítása. 2016. https://www.nador.hu/hu/szabalyzatok-es-ibir-kialakitasa (2018. 12. 20.)
- NIS Directive: *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.* 2016. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=EN (2018. 11. 05.)
- NIST: *Framework for Improving Critical Infrastructure Cybersecurity v.1.1.* 2018. https://www.nist.gov/sites/default/files/documents/2018/05/14/framework_v1.1_with_markup.pdf (2018. 11. 05.)
- Panda Security: *A dating site and corporate cyber-security lessons to be learned.* 2017. https://www.pandasecurity.com/mediacenter/security/lessons-ashley-madison-data-breach/ (2018. 11. 10.)
- Panyi S.: *Hírek, álhírek Magyarországon a média részéről.* 2017. [Interjú] (2017. 11. 18.)
- Parker, N.: *Cyber-attacks on business.* 2017. https://www.berrysmith.com/news/cyber-attacks-business (2018. 11. 03.)
- Sántha G. – Klotz P.: *Törzsanyag: az Integritásmenedzsment című tantárgyhoz.* Nemzeti Közszolgálati Egyetem (VTKI), Budapest, 2013.
- Sasvári P. és mtsai.: *Rendszerelmélet.* Kézirat. Ismeretlen szerző. Budapest, 2018.
- Silverman, C.: *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook.* 2016. https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.fg2VjMGMV#.nl2Gp3R3G (2017. 11. 23.)
- Smith, A. – Banic, V.: *Fake News: How a Partying Macedonian Teen Earns Thousands Publishing Lies.* 2016. https://www.nbcnews.com/news/world/fake-news-how-partying-macedonian-teen-earns-thousands-publishing-lies-n692451 (2017. 11. 23.)
- Spitzner, L.: *Honeytokens: The Other Honeypot.* 2003. https://www.symantec.com/connect/articles/honeytokens-other-honeypot (2018. 11. 11.)
- Symantec: *Internet Security Threat Riport 2018, Volume 23.* https://www.symantec.com/security-center/threat-report (2018. 11. 28.)
- Stone, D.: *Cybersecurity Organizational Structure & Governance.* 2018.

https://www.divurgent.com/wp-content/uploads/2018/08/Cybersecurity-Organizational-Structure-Governance.pdf (2018. 11. 05.)

- Tagliabue, J.: *Nun Opens Vatican Doors to the Net.* 1999. https://www.nytimes.com/1999/07/22/technology/nun-opens-vatican-doors-to-the-net.html (2018. 11. 03.)
- Takács I. – Csapodi P. – Takács-György K.: *A korrupció mint deviáns társadalmi attitűd.* Pénzügyi Szemle, 56. évf., 2011, 1. sz. kötet, pp. 26–42.
- Transparency International: *Korrupció Érzékelési Index.* 2018. https://transparency.hu/adatok-a-korrupciorol/korrupcio-erzekelesi-index/ (2018. 11. 13.)
- Tuli, P. – Sahu, P.: *System Monitoring and Security Using Keylogger – Research Article.* International Journal of Computer Science and Mobile Computing, Issue Vol. 2 2013, Issue. 3., pp. 106–111.
- vpnMentor: *Proxyk vs VPN-ek vs Tor – mi a különbség?* 2016. https://hu.vpnmentor.com/blog/vpn-ek-vs-proxyk-mi-kueloenbseg/ (2018. 10. 29.)
- Weatherhill, M.: *How Four Eyes Fits with Cyber Security.* 2017. https://www.alpha-gen.co.uk/how-four-eyes-fits-cyber-security/ (2018. 11. 13.)
- Wood, T. C.: *The LinkedIn Hack: Understanding Why It Was So Easy to Crack the Passwords.* 2016. https://www.linkedin.com/pulse/linkedin-hack-understanding-why-so-easy-crack-tyler-cohen-wood/ (2018. 11. 11.)

Ábrajegyzék

Táblázatjegyzék

Rövidítésjegyzék

APO (Align, Plan and Organise)	Összehangolás, tervezés és szervezés
APT (Advanced Persistent Threat)	Kifinomult, állandó fenyegetés
BAI (Build, Acquire and Implement)	Építés, beszerzés és megvalósítás
CERT (Computer Emergency Response Team)	Számítógép vészhelyzetkezelő csoport
CIA (Central Intelligence Agency)	Központi Hírszerző Ügynökség
COBIT (Control Objectives for Information and Related Technologies)	Irányítási célok információs és hasonló technológiák számára
CPI (Corruption Perception Index)	Korrupció érzékelési index
CSIRT (Computer Security Incident Response Team)	Számítógép-biztonsági incidenskezelő csoport
DDoS (Distributed Denial of Service)	Elosztott szolgáltatás-megtagadással járó támadás
DMZ (DeMilitarized Zone)	Demilitarizált zóna
DoS (Denial of Service)	Szolgáltatás-megtagadással járó támadás
DSS (Deliver, Service and Support)	Szállítás, szolgáltatás és támogatás
EDM (Evaluate, Direct and Monitor)	Értékelés, irányítás és figyelemmel kísérés
EU (European Union)	Európai Unió
FBI (Federal Bureau of Investigation)	Szövetségi Nyomozó Iroda
GDPR (General Data Protection Regulation)	Általános Adatvédelmi Rendelet
HTML (HyperText Markup Language)	Hiperszöveges jelölőnyelv
Ibtv.	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
IDS (Intrusion Detection System)	Behatolást érzékelő rendszer
IIA (Institute of Internal Auditors)	Belső Auditorok Intézete
IPS (Intrusion Prevention System)	Behatolást megelőző rendszer
ITIL (Information Technology Infrastructure Library)	Informatikai infrastruktúra könyvtár
MEA (Monitor, Evaluate and Assess)	Figyelemmel kísérés, értékelés és felmérés
NAT (Network Address Translation)	Hálózati címfordítás
NBSZ	Nemzetbiztonsági Szakszolgálat
NCSC (National Cyber Security Centers)	Nemzeti kiberbiztonsági központok
NIS/ NIS Directive (Network and Information Systems Directive)	Hálózati és információs rendszerek irányelv
NIST (National Institute of Standards and Technology)	Amerikai Egyesült Államok Nemzeti Szabvány és Technológiai Intézete
NSA (National Security Agency)	Nemzetbiztonsági Ügynökség
NVSZ	Nemzeti Védelmi Szolgálat
OLAF (Office européen de Lutte AntiFraude)	Európai Csalás Elleni Hivatal
OTP (One-Time-Password)	Egyszeri használatú jelszó
SEO (Search Engine Optimization)	Keresőmotor optimalizálás

SOC (Security Operations Center)	Biztonsági műveleti központ
SoD (Separation of Duties)	Feladatok szétválasztása
SZEÜSZ	Szabályozott elektronikus ügyintézési szolgáltatások
TOR (The Onion Router)	A Hagyma Elosztó
VPN (Virtual Private Network)	Virtuális magánhálózat