Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés

Szerkesztette
Bonnyai Tünde – Kiss Adrienn – Tóth András

LUDOVIKA
EGYETEMI KIADÓ

Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés

Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés

Kiber- és információbiztonsági tanulmányok

Szerkesztő
Bonnyai Tünde és Kiss Adrienn (I. rész)
Tóth András (II. rész)

LUDOVIKA
EGYETEMI KIADÓ
Budapest, 2023

Szerzők (I. rész):
Bányász Péter, Bottyán Sándor, Dobó Judit, Dub Máté, Gyaraki Réka, Hankó Viktória, Katona Gergő, Kiss Adrienn, Magas Bianka, Nimsz Vivien

Szerzők (II. rész):
Bányász Péter, Ináncsi Mátyás, Katona Gergő, Magas Bianka, Magyar Sándor, Mile Márió, Nimsz Vivien, Ruszkovics Patrik, Tóth András, Tóth Rebeka

Szerkesztők:
Bonnyai Tünde és Kiss Adrienn (I. rész)
Tóth András (II. rész)

Lektorok:
Krasznay Csaba
Szabó-Nyakas Zsolt Csaba

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Varga Zoltán
Olvasószerkesztő: Tomka Eszter
Korrektor: Bruckner Nóra
Tördelőszerkesztő: Stubnya Tibor

DOI: https://doi.org/10.36250/01170_00

ISBN 978-615-6598-68-4(elektronikusPDF)| ISBN 978-615-6598-69-1(ePub)

Tartalom

I. RÉSZ

Biztonságorientáció és -tudatosítás nagyvállalati környezetben

Vákát

Bevezetés

Az MVM Energetika Zártkörűen Működő Részvénytársaság (MVM Zrt.) és a Nemzeti Közszolgálati Egyetem stratégiai szintű együttműködésének égisze alatt született ez a tanulmány, amelyet azoknak a kiberbiztonsági és információbiztonsági kérdések iránt érdeklődőknek a figyelmébe ajánlunk, akik a tudatosságot – mint eszközt és képességet – kulcsfontosságúnak tartják egy szervezet biztonságorientált működése tekintetében. A 2020 őszén kötött megállapodás keretében indított kutatási projektünk egyik zászlóshajójának részeredményét mutatjuk be ebben az összefoglaló dokumentumban, azzal a céllal, hogy partnerszervezeteink jó gyakorlatain keresztül a biztonságtudatosság jelentőségét hangsúlyozzuk. Ennek részét képezi a tudatosítás során alkalmazható, bevált módszertanok – teljesség igénye nélküli – felsorolása, illetve egy vizsgálat alapján meghatározott alapvető tudásanyag, amelynek ismeretében általános értelemben véve végezhető tudatosítási tevékenység.

Kutatásunkban az MVM Zrt. delegált szakértői mellett a Vodafone Magyarország Zrt. és a Szerencsejáték Zrt. biztonsági területen dolgozó kollégái, valamint a vállalatok alkalmazottainak egy része is közreműködött, ezzel lehetővé téve, hogy a szakmában jól ismert NIS irányelv által érintett ágazatokban mérjük fel a munkavállalói tudatosság aktuális szintjét. Azt a célt tűztük ki magunk elé, hogy az energiaágazat, a digitális infrastruktúrák, valamint a digitális szolgáltatást nyújtó szereplők (DSP) halmazában jellemző, a jogszabályi követelményeknek eleget tevő szervezetek tudatossági szintjét vizsgálva úgynevezett *best practice-eket* mutassunk be, és egy univerzálisan használható, alapvető információbiztonsági tudásbázist építsünk fel.

A kutatási projekt fő pilléreit egy tudatossággal kapcsolatos kérdőív és a partnerszervezetek szakértőivel folytatott interjúk adták. Ezek eredményeinek bemutatásával és következtetések megállapításával arra törekszünk, hogy átfogó, közérthető formában ismertessük a tudatosítási tevékenység jelentőségét, szükségességét és lehetőségeit vállalati környezetben, illetve rendelkezésre bocsássunk egy olyan tudásbázist, amely általánosságban bármilyen szervezeti kultúrában alkalmas alapszintű ismeretek átadására.

Bár a kutatási projekt 2021-ben zajlott, és a tanulmány is ekkor készült, aktualitása mit sem csökkent, a mondanivaló továbbra is releváns. A biztonságtudatosság alapvető értékei ma is helytállóak, és a munkavállalók, illetve a szervezetek elvárásai annak oktatásával szemben továbbra is változatlanok.

Bonnyai Tünde

Vákát

1. Az aktuális helyzet bemutatása a partnerszervezeteknél végzett felmérés alapján

1.1. Kutatási célú kérdőív a biztonságtudatos attitűd feltérképezésére

A biztonságtudatosság felmérésére szolgáló kérdőív összeállítása során célul tűztük ki, hogy a vizsgált szervezetek munkavállalóinál feltérképezzük a tulajdonság szintjét a viselkedési, magatartási formák szempontjából. A kérdőív[1] ezen empirikus kutatás keretén belül a tudás–képesség–viselkedés modellen alapult, és a biztonságtudatosságon nyugvó tényleges magatartást vizsgálta. Ennek kimutatása érdekében az általános eszközhasználattól kezdve a képzéseken történő részvételen át a mások iránt tanúsított bizalomig igyekeztünk kitérni minden olyan kérdéskörre, amely által tisztább képet kaphatunk a tudatossághoz való hozzáállásról és aktuális mértékéről a projektben részt vevő szervezeteknél. Segítette a vizsgálatot, hogy 686 értékelhetően kitöltött kérdőív érkezett be, így az eredmény viszonylag reprezentatív a munkavállalók attitűdjére vonatkozóan.

Általánosságban elmondható, hogy a válaszadók biztonságtudatosnak tartják magukat, és a magatartásuk alapján a valóság is ezt tükrözi. Az ismeretlen személyek és infokommunikációs eszközök iránti bizalom alacsony, így a kitöltő dolgozókról összességében kijelenthető, hogy tudják, értik és átgondolják, mit, mikor és hogyan cselekszenek olyan helyzetekben, amikor a biztonság mint körülmény számottevő. Ebből arra lehet következtetni, hogy a vizsgált szervezeteknél fontosnak tartják a tudatosítást és az ehhez kapcsolódó képzéseket is.

A kérdőívben feltett kérdések és az azokra adott válaszok közötti összefüggéseket vizsgálva megállapítható, hogy azok a munkavállalók, akik biztonságtudatosító képzéseken vettek részt az elmúlt időszakban, tudatosabb magatartást tanúsítanak, mint azok, akik nem részesültek oktatásban. Ez csak egy kiragadott példa, viszont jól mutatja, hogy a biztonságtudatossághoz való hozzáállásra ténylegesen hatást gyakorol a felkészítés bármelyik formája.

A válaszok alapján tehát átfogó képet kaptunk arról, hogy a dolgozók előre megadott kérdéskörökhöz hogyan viszonyulnak elméletben és gyakorlatban is. A vizsgált szervezetekkel kapcsolatban megállapítottuk, hogy a kitöltők összességében hasonló, logikus és átgondolt válaszokat adtak a kérdésekre,

[1] Lásd a mellékletet.

ami a biztonságtudatosság feltételezhetően magas szintjéről tanúskodik. Végül pedig fontosnak tartjuk hangsúlyozni, hogy a nagyszámú kitöltés alátámasztja azt is, hogy a tudatosító képzések – vagyis a biztonságorientált gondolkodásmód és attitűd kialakítása és fenntartása – hosszú távon elengedhetetlen az erős védelem kialakításához.

1.2. A tudatosítás szintje a szakértői interjúk tapasztalatai alapján

Az interjúkon elhangzottakból és a kitöltött kérdőívekből megállapítható, hogy a tudatos felhasználót legtöbben úgy írták le, mint aki figyelmes, és ha valami kicsit is eltér a hétköznapokban megszokottól, észreveszi azt. A szakértőkkel folytatott beszélgetések során feltett kérdésekre adott számos válaszban megjelent az, hogy a tudatos felhasználónak kommunikálnia kell. Ez azt jelenti, hogy kérdezzen, ha valamiben nem biztos, illetve jelezze, ha valami nem hétköznapit tapasztal.

Ezenfelül – összességében – az látható, hogy a vizsgált szervezeteknél kivétel nélkül fontosnak tartják az információbiztonságot, amelynek egyik fő összetevője a tudatosság. Ezt a területet főleg tudatosító oktatásokkal, kampányokkal próbálják erősíteni és fejleszteni, amelyeknek szükséges mennyiségéről megoszlanak a vélemények. Némelyek úgy gondolják, hogy megfelelőek a megszokott számú és mélységű módszerek, ugyanakkor a másik oldalt – hogy sosem lehet elegendő tudatosító eszközt bevetni – is többen képviselik. Az ilyen eljárások javítását illetően a vizsgált vállalatoknál szinte egyhangúan az jelent meg, hogy színesebbé, érdekesebbé kell tenni az oktatást, amely így jobban felkelti a felhasználók figyelmét.

Ahogy azt már említettük, a tudatosító képzés fontosságát a kérdőíves felmérés is alátámasztotta azzal, hogy összefüggést mutatott ki aközött, hogy az illető milyen attitűddel rendelkezik egy adott kérdéskörben (jelszóhasználat, e-mailhasználat, közösségimédia-jelenlét, infokommunikációs eszközök alkalmazása, otthoni munkavégzéssel kapcsolatos szokások), és hogy részt vett-e tudatosító oktatáson. Főleg az figyelhető meg, hogy aki részesült ilyen oktatásban, vagy több ilyen kurzust hallgatott végig, az kisebb eséllyel tanúsít információbiztonsági szempontból jelentős kockázatot hordozó magatartást. Látható az is, hogy a kitöltők a biztonságnál kevésbé tartják fontosnak a kényelmet. Erre jó példa a jelszókezelés témaköre, amely kapcsán a válaszadóknak csak egy kis része – kevesebb mint 25%-a – gondolja úgy, hogy lehet ugyanazt a jelszót használni több profil

esetében is, és többségüknek eltérő belépőkódja van a különféle felületeken. Egy másik példa erre a képernyőzár: a kitöltők jellemzően – több mint 90% – inkább zárolják az eszközüket, mint felügyelet nélkül hagyják.

Mind az interjúkból, mind a kérdőívekből az jön le, hogy a tudatosításra a legjobb eszköz az oktatás. Az előbbiekből azonban ennek kapcsán az is leszűrhető, hogy számos tényező gátolhatja e tevékenységek sikeres kivitelezését. Ilyen például az erőforrás és az idő hiánya, a tananyagok interaktivitásának szűkössége és frissítésének elmaradása is. Emellett a válaszok között megjelent néhány esetben a felhasználók érdektelensége is, amelyre a szervezeteknél folytatott interjúk alanyai ugyan javasolhatnak megoldást, de annak megvalósítását illetően is korlátozó körülményként azonosítható az idő- és erőforráshiány.

1.3. A tudatosítás alkalmazott módszerei

Az emberi tényező okozta kockázatok és az azokból eredő incidensek csökkentésére az egyik leggazdaságosabb és leghatékonyabb módszer a felhasználók rendszeres, munkaköri és felelősségi szintjének megfelelő, célirányos továbbképzése és biztonságorientált felkészítése. A projektben részt vevő három vállalat által alkalmazott tudatosító módszertanok, jó gyakorlatok rövid összefoglalásával a biztonsági célú képzések, programok kialakítását megalapozó eljárásokat mutatjuk be. Az információbiztonsági tudatosítás eredményes megvalósítása egy komplex, szervezetre szabott, szervezetikultúra-fejlesztési program, amelynek egyaránt része az adott vállalatot érintő kockázatok felmérése, a kockázatkezelési stratégia meghatározása, az informatikai biztonsági szabályozás kiadása és a felhasználóktól elvárt viselkedési szabályok rögzítése. A felsorolt információk birtokában végezhető el a biztonságtudatosítási program személyre szabása, majd a dolgozók felelősségi és felkészültségi szintjének legmegfelelőbb képzési formák meghatározása, a tudás átadása, illetve ellenőrzése.[2]

A három vizsgált szervezet mindegyike alkalmaz ilyen programokat, kampányokat, egyéb módszereket azért, hogy a mindennapi munkavégzés – úgy az irodából, mint otthonról is – információbiztonsági szempontból a lehető legideálisabban történjen. A sokszor gyakorlati példákból összeállított biztonságtudatosító oktatások előírásként jelennek meg a nagyobb szervezetek életében, azonban a hatékonyság érdekében, hogy igazán lekössék a munkavállalók figyelmét, érdemes kreatívabb

[2] Horváth 2013.

megoldásokhoz, kampányokhoz nyúlni. Ami pedig a rendszeres képzéseknél talán még fontosabb, hogy különböző tesztekkel, szituációkkal mérjék is a kurzusok eredményességét.

Hétköznapi és elcsépelt módszernek tűnhet a szokásos e-mailek kiküldése, amelyek a már ismert közhelyekkel próbálják felhívni a dolgozók figyelmét a biztonságos munkavégzésre. Azonban a meghatározott időközönként kiküldött, az éppen aktuális, kiberbiztonsággal, kiberbűnözéssel kapcsolatos, tömör és közérthető hírekkel gazdagított hírlevelek rendszeres olvasmányként épülhetnek be a munkatársak életébe, így elősegíthetik információbiztonsági elővigyázatosságukat.

A céges csapatépítő programok egyfajta kiszakadást jelenthetnek a hétköznapi monotonitásból, azonban annak érdekében, hogy a kellemes össze legyen kötve a hasznossal, érdemes egy biztonságtudatosító szabadulószobával bővíteni ezeket az alkalmakat. Viszonylag könnyen lehet szimulálni egy „bakikkal" tarkított irodai közeget, ügyelve arra, hogy a környezet kizárólag szimuláció maradjon. A szabadulószobán túl akár egy vetélkedő is kellemesnek, ugyanakkor hasznosnak bizonyulhat, a megfelelő előkészítés után. A kreatív megoldások mellett célszerű egyszerű dolgokban is gondolkodni: egy laptopra ragasztható kameratakaró, egy-két jelmondattal ellátott poháralátét és egyéb, apró, irodai környezetben mindennapos használati eszközök is sikerrel tudják ráirányítani a figyelmet a megfelelő jelszóhasználat vagy akár a tiszta asztal, tiszta képernyő elv fontosságára.

A teljesség igénye nélküli felsorolásokból is láthatjuk, hogy számos módszer, eszköz áll rendelkezésre a munkavállalók tudatos moráljának szinten tartására, növelésére, azonban hangsúlyozni kell, hogy erre a tevékenységre nem tekinthetünk úgy, mint egy „extra szolgáltatásra". Elkötelezettség és tervezettség, illetve előrelátás és következetesség szükséges ahhoz, hogy az információbiztonság humán oldalról történő támogatása, az elvárt magatartásformák kialakítása és gyakorlása rutinszerűvé válhasson.

2. Biztonság és tudatosítás

A tanulmány elkészítésével elkötelezettségünket fejezzük ki a biztonságtudatosság mellett. Fontosnak tartjuk megjegyezni, hogy egy olyan összefoglaló dokumentumról van szó, amelynek szerzői bár partnerszervezetekkel együttműködve kutatták a tudatosságra vonatkozó legjobb eljárásokat, egyes fejezetei önállóan léteznek, és nem a vállalatok gyakorlatait mutatják be. Ebből adódóan különkülön is megállják a helyüket, elsősorban figyelemfelhívó szándékkal íródtak.

A kutatásban részt vevő partnerszervezetek az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) hatálya alá tartoznak, amely többek között a biztonsági események megelőzésével és kezelésével kapcsolatos kötelezettségeket állapítja meg. A törvényi kötelezés mellett egyéb jogi eszközök, mint például a 41/2015. BM rendelet[3] (a továbbiakban BM-rendelet), illetve egyedi belső szabályozók is meghatározzák a szervezetek információbiztonsági szempontú működését. Így hatással lehetnek a munkavállalók biztonságtudatossági szintjének javítására vagy fenntartására azáltal, hogy milyen megoldásokat alkalmaznak e célból.

A tudatosság és a tudatosítás természetesen egyéni és szervezeti szinten egyaránt fontos, hiszen a cég által biztosított képzések során elsajátított ismereteket a felhasználó a magánéletében is hasznosítani tudja. A biztonságtudatosságra koncentrálva a tanulmány e fejezetében szó lesz még a tudatosításról mint kockázatcsökkentő intézkedésről. A kockázatelemző-értékelő tevékenységek rendeltetésükből adódóan hivatottak szolgálni a vállalatok életében szükséges, megvalósítható védelmet. Ha feltárjuk a szervezetek esetében felmerülő veszélyeket, akkor reális képet kaphatunk a védelmi intézkedések lehetőségeiről, így képessé válhatunk az ismert rizikó lehető legminimálisabb mértékűre való csökkentésére. Tanulmányunk kockázatcsökkentő intézkedésekre vonatkozó alfejezetében rögzítjük a kockázat mint gyűjtőfogalom lényegét, majd ezzel összefüggésben kifejtjük a tudatosítás szükségességét és azt, hogy miből kell állnia az ezt célzó oktatásoknak. Az alfejezetből az is ki fog derülni, hogy hogyan járulnak hozzá az említett intézkedések a vállalati biztonság fenntartásához, és az is, hogy miért van szükség a biztonságtudatosságra mint szemléletre.

[3] Ez a 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 követelményeket taglalja.

Bár a tanulmánykötet megírása során a közreműködő partnerszervezetekkel kapcsolatos fókusz miatt merültek fel az említett és a továbbiakban kifejteni kívánt jogszabályok, módszerek és eszközök, tanulmányunk mégis általános jellegű. Célunk, hogy kötetünk bármely, az Ibtv. hatálya alá tartozó vállalatnak hasznos legyen, és a jövőben alkalmazhatóvá váljon a tudatosítást megcélzó szervezetek számára.

2.1. Jogi kötelezettség és vállalati érdek

A fejezet előszavában is szerepel, hogy a hazai jogszabályi környezet számos kötelezettséget ír elő a szervezetek számára, ilyen például a tudatosítási képzések szervezése, lebonyolítása, illetve a megszerzett ismeretek számonkérése. Rendkívül fontos azonban, hogy a vállalatok és vezetőik ne csak előírásként tekintsenek ezekre az elemekre, hanem lássák azt is, hogy milyen hatásai lehetnek a biztonságtudatos magatartás hiányára visszavezethető eseményeknek. A megelőzés, beleértve a felkészítés keretrendszerébe tartozó tudatosítást, az ő érdekük is, hisz a különböző incidensek, károk elkerülésével megóvhatják szervezetüket egy – a helyreállításra fordított – nagyobb anyagi kiadástól vagy akár presztízsveszteségtől. Ehhez kapcsolódóan bemutatjuk, hogy a kérdőívek és interjúk alapján a partnerszervezeteknek milyen, a témát illető tapasztalataik, jó gyakorlataik vannak.

A kapcsolódó jogi háttér

Ahogyan már említettük, az Ibtv. összetett kötelezettségeket állapít meg a vállalatok számára. Egyik eleme, hogy a hatálya alá tartozó szervezetek az elektronikus információs rendszer (EIR) biztonságáért felelős személyt (informatikai biztonsági felelős, IBF) kötelesek kinevezni vagy megbízni, valamint informatikai biztonsági szabályzatot (IBSZ) kötelesek alkotni. A törvény továbbá kimondja, hogy az IBF-nek és az EIR biztonságával összefüggő feladatok ellátásában részt vevő személyeknek – beleértve az EIR védelméért felelős vezetőt is – rendszeresen részt kell venniük különböző szakmai képzéseken,[4] illetve továbbképzéseken.[5]

[4] A szakmai követelmények és oktatási program kidolgozása a Nemzeti Közszolgálati Egyetem feladata.

[5] 2013. évi L. törvény (Ibtv.).

Azonban nemcsak a felelősök, hanem a vállalat összes dolgozójának oktatása ajánlott, hiszen a komplex biztonság kialakításának elengedhetetlen feltétele, hogy a szervezet minden tagja tisztában legyen saját, munkavállalói felelősségével, és ennek érdekében kellően biztonságtudatossá váljon. Ennek lehetséges eszköze a biztonságtudatossági tréning, amelyet évente érdemes (és célszerű) megtartani, ezáltal a munkatársak ismétlő jelleggel elsajátíthatják a biztonságos munkavégzéshez szükséges vállalati és jogszabályi követelményeket. Emellett például egy ilyen jellegű program, illetve kampány szervezése is jó megoldás lehet, amely szintén hozzájárulhat a dolgozók biztonságtudatossági szintjének fenntartásához és növeléséhez.[6]

A képzésen túl az IBSZ megalkotása szintén kiemelkedően fontos kötelezettség a szervezetek számára. A dokumentum – amely a vállalat belső szabályozóihoz illeszkedik – tartalmazza az információbiztonságra vonatkozó célkitűzéseket, a szabályzat (tárgyi, személyi és a szervezet jellegétől függően területi) hatályát, a kapcsolódó szerepköröket és a hozzájuk rendelt tevékenységet, illetve az ahhoz kötött felelősséget. Emellett ebben szükséges rögzíteni a cég jogszabály alapján meghatározott biztonsági szintjét és az EIR-ek biztonsági osztályait is. Mindezzel azonban még nem teljesül maradéktalanul a törvény által előírt kötelezettség, ugyanis a BM-rendelet 4. mellékletében szereplő védelmiintézkedéskatalógus szerint a szabályzat mellett eljárásrendek kialakítása is szükséges a teljes körű megfeleléshez.[7] Ezek működtetése és betartása minden érintett munkavállaló számára kötelező, így ismerniük is kell a tartalmukat, legalább a saját feladataik és tevékenységi körük relációjában.

Nemcsak kötelezettség, hanem szervezeti érdek

A biztonságtudatosságra mind külső (például jogszabályok, szabványok), mind belső tényezők (például belső szabályzatok, felső vezetői utasítások, ellenőrzés) hatással vannak. Fontos, hogy a biztonság a vállalati kultúra része legyen, hiszen az befolyásolja az egyének hovatartozási tudatát, helyzetét és szerepét a szervezeten belül. Ebből következik, hogy a biztonsági kultúra kialakítása, szintjének fenntartása/emelése önmagában is védelmi intézkedésnek számít. A biztonságtudatosság a különböző vállalati szokásokban, a belső kommunikációban

[6] Kárász 2019: 313–324.

[7] 41/2015. BM rendelet.

használt nyelvezetben vagy akár a szimbólumok alkalmazásában is megjelenhet. Ennek hiányában az egyén nem képes felismerni a fenyegető tényezőket, az őt körülvevő kockázatokat, sem pedig a rendkívüli biztonsági eseményeket, így azok következményeit sem, ami összességében akár oda is vezethet, hogy nem lesz képes ellátni a kötelező és a vállalt feladatait.[8] Ennek tervezett és tudatos megelőzése tulajdonképpen a biztonságba való beruházás. A felhasználók tudatos magatartásának kialakítása és fejlesztése által – többek között – a következő károk és szituációk védhetők ki:

- időszakos vagy tartós bevételkiesés az incidens következményeinek felszámolási időtartamától függően;
- időszakos vagy tartós működési zavarok az incidens jellegétől függően;
- ügyfelek vagy adataik elvesztése;
- ügyfelek vagy dolgozók által indított perek;
- személyazonosság lopása;
- vagyonlopás;
- a vállalat szempontjából bizalmas információk kiszivárgása.[9]

Hangsúlyozni szükséges továbbá, hogy minden esetben az embert kell meggyőzni arról, hogy tegyen magáért, a saját fejlődéséért, biztonságáért, aminek következtében aztán a munkahelyi magatartása is változik. Ahogy ez jellemző az élet minden területén – például az egészségünkért még a betegséget megelőzően kell tennünk –, úgy hasonló a helyzet a biztonságtudatossági szint fejlesztése tekintetében is, amely a biztonsági események megelőzéseként is értelmezhető. Ehhez megfelelő lehet egy követhető példakép, aki a megszokott tudásanyagon felüli ismereteket sajátít el, és motiválttá válhat arra, hogy a körülötte lévőket – munkahelyi közeg, magánéleti szereplők – biztonságtudatosságra ösztönözze.[10]

Összességében tehát az egyén képzése nemcsak rá lesz hatással, hanem a szűkebb és tágabb környezetére is, ami a többi alkalmazottat is ösztönözheti: ha látják, hogy egyes kollégák bizonyos módon cselekednek, ők is azt a példát fogják

[8] Horváth 2013.
[9] United Security Incorporated 2020.
[10] Nyikes 2017: 327–330.

követni. Általában minél többen viselkednek egyféleképpen, annál nagyobb az esélye annak, hogy mások is csatlakozzanak.[11]

A kérdőívek és interjúk eredménye

A tudatosítás fontosságát és a vállalati érdek gyakorlatiasságát – tehát azt, hogy a gyakorlatban is érződik, hogy a tudatosítás a szervezet érdeke – a kérdőív egyes kérdései igazolták. Ilyen például az IBSZ ismeretének mértéke, hogy szabad-e magáneszközt munkavégzésre használni, vagy az, hogy mennyire jártak tudatosító képzésekre a munkavállalók. A kérdőív kiértékelése során a kereszttáblaelemzés keretében az oktatáson való részvétel és az IBSZ ismerete közötti kapcsolat kimutatására irányuló vizsgálatot folytattunk, amely szignifikanciát mutat, továbbá jelen esetben egy gyenge kötelékről van szó.

Az interjúk tapasztalatai alapján elmondható, hogy általánosságban egy tudatos felhasználó az alapvető dolgok ismeretétől kezdve az óvatosságig különböző jellemzőkkel írható le. Az interjúalanyok véleménye szerint fontos továbbá, hogy merjen kérdezni, ha valamivel nincs tisztában, illetve ismerje a biztonsági kockázatokat, a kezelésükre irányuló szabályokat – azokat tartsa is be –, és a környezetétől is ezt a magatartást várja el. Hangsúlyos emellett az alapvető informatikai és jogszabályismeret, valamint a biztonságérzet. Kiemelendő, hogy utóbbi igen szubjektív, és mindig lehet tovább fejleszteni. Előfordul azonban olyan eset is, amikor az egyén úgy gondolja, hogy ő nem lehet célpont – ami nem feltétlen igaz, hiszen mindannyian azzá válhatunk –, így lazábban veszi a szabályozásokat, és ez kockázatot jelent. Ezzel kapcsolatban nem lehet figyelmen kívül hagyni azt sem, hogy naprakész legyen a felhasználó, valamint ismerje az aktuális trendeket és a lehetséges támadási formákat.

A munkavállalók tudatossági szintjének növelése érdekében a munkáltatók különböző eljárásokat alkalmaznak. Arra a kérdésre, hogy ezek elegendőek-e, különböző válaszokat kaptunk. Az egyik oldalról az a tapasztalat, hogy igen, a vállalat mindent megtesz a rendelkezésére álló jogi és technikai-szervezési intézkedések maximális kihasználásával. A másik oldalról viszont egyet kell értsünk azzal, hogy sosem lehet eléggé hangsúlyozni a tudatosságot, nagyon fontos az ismétlés, az alkalmazkodás a folyamatos kihívásokhoz, a változások

[11] *How IT Can Get Employees to Engage With Your Company's Security Awareness Program* 2020.

követése, illetve hogy különböző méréseket is végezzenek. Az interjúk alapján egyértelműen kijelenthető, hogy nem elegendő az oktatás, annak a hatékonyságát ellenőrizni szükséges. Nehézségként megjelent, hogy a költségkeret miatt nem lehetséges minden ötlet támogatása.

A szervezetek biztonságtudatossághoz való hozzáállásával kapcsolatosan elmondható, hogy mindhárom szervezetnél fontosnak tartják és kellő hangsúlyt kap ez a kérdés: megjelenik a szervezeti ábrában a dedikáltan ezzel foglalkozó egység, különböző módszereket és formát alkalmaznak a fejlesztésére, valamint egy biztonsági keretrendszer is ezt igazolja. A kérdőívek fényében kijelenthető, hogy a munkavállalók hasonlóan lényegesnek gondolják, sőt kiemelt jelentőséget tulajdonítanak neki – bizonyos esetben az utóbbi években a támadások növekvő száma nagy nyomást gyakorolt rájuk, ezáltal jobban odafigyelnek a tudatos viselkedésre. Azonban interjúalanyaink közül többen megemlítették azt is, hogy a benyomások alapján nem biztos, hogy tudatosak a munkavállalók, mert alkalmanként megfigyelhető az „ezt már tudom" hozzáállás is – amikor a kolléga felvértezettnek érzi magát, és hamis biztonságérzete keletkezik –, de szerencsére csak elenyésző mértékben.

Az interjúban részt vevő szakértőktől a biztonságtudatosság növelésével kapcsolatos tapasztalatok birtokában különböző ötleteket kaptunk, amelyek legfőbb célja, hogy felkeltsék a célcsoportok érdeklődését. A megvalósítási formát tekintve a fórumok, az ötletbörze, de akár egy könnyed hangvételű videó vagy rajzfilm is kitűnő, amelyet a munkaközi szünetben meg tud tekinteni a munkavállaló. Emellett kampányok, nyílt nap szervezése, továbbá különböző eszközök – VR,[12] AR[13] – használata is felmerül mint potenciális módszer. Végül, de nem utolsósorban – noha nem is kiemelt hangsúllyal – meg kell említeni a szankciók alkalmazását vagy előrevetítését, ami szintén eszköz lehet, amennyiben más módon nem sikerül célt érni. Nem feledkezhetünk meg ugyanakkor arról sem, hogy a biztonságtudatosság növelése kapcsán értelemszerűen ugyanúgy jelentkeznek akadályok, mind egyéni, mind pedig szervezeti szinten. Az egyéni szinten főként az érdektelenség, a negatív tapasztalat, valamint az idő hiánya jellemző, míg a szervezetnek a koordinációs nehézségekkel, a humán erőforrás

[12] VR: *virtual reality,* azaz virtuális valóság. Olyan, számítógéppel létrehozott környezet, amelyben a felhasználó is jelen van. Forgó–Komló 2015.

[13] AR: *augmented reality,* azaz kiterjesztett valóság. A virtuális valóság egy változata, ahol számítógépes grafikával egy átlátszó réteget hoznak létre, amely kiemeli a valóság bizonyos elemeit, illetve segíti a megértést. Forgó–Komló 2015.

hiányával, illetve az új fenyegetések nyomon követésével, oktatásba való beépítésével kell kihívásként szembenéznie.

A kiberbiztonsággal kapcsolatos jogszabályok számosságára tekintettel jelen tanulmányban csak a témához illő három legfontosabbat emeljük ki. Ezek az Ibtv., a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, azaz Infotv. és az ezzel összefüggésben emlegetett Az Európai Parlament és a Tanács 2016/679 rendelete, az Általános adatvédelmi rendelet (GDPR), amelyek mellett azonban megjelent az ISO 27001 szabványnak való megfelelőség szükségessége is a szervezetek életében. Felmerült továbbá az a kérdés, hogy a munkavállalók tisztában vannak-e azzal, hogy egy kiberbiztonsági incidens esetén kihez fordulhatnak. Ez szervezetenként nem mutat jelentős eltérést: egy incidens bekövetkezését a felhasználók különböző csatornákon – e-mailen, helpdeskvonalon, telefonon keresztül – jelezhetik, amiről mind a belső szabályozók, mind pedig a kötelező oktatásokon informálják őket.

Összegzés

Az eddigiekből egyértelműen láthatjuk, hogy a jogi szabályozás elrendeli az IBF kinevezését, valamint az IBSZ megalkotását, ami minden szervezeti forma számára alapot jelent a tudatosítási feladatok ellátásához. Mint azt bemutattuk, a jogszabály az IBF-nek és az EIR-ekért felelős személyeknek kötelezően előírja a részvételt az oktatásokon, azonban hangsúlyozni szükséges, hogy ez nem elegendő a vállalati biztonsági kultúra szempontjából. A biztonságtudatos munkahelyi környezet kialakítása érdekében a munkavállalók képzése is kiemelten fontos. Ennek az évenként szervezett biztonságtudatossági tréningtől – ahol a felhasználók átismételhetik a korábban tanultakat, és új ismeretekkel is gazdagodhatnak – egészen a játékos, szórakoztatva tanító programokig több lehetséges módja van. A szervezet IBSZ-e annak biztonsági szintje mellett tartalmazza az információbiztonsággal kapcsolatos célkitűzéseket, illetve a szabályozásban előírt eljárásrendeket egyaránt. Ezzel összefüggésben hangsúlyozandó, hogy a vállalatnak nemcsak kötelezettsége, hanem érdeke is, hogy betartsa és betartassa a belső és jogi szabályozásokat, ezzel tudatos környezetet teremtve dolgozóinak. A biztonság mint a vállalati kultúra része különböző anyagi és nem anyagi károkat előzhet meg, így oktatása és prioritásként való kezelése kiemelt fontosságú, hiszen az egyén képzése, tudatos viselkedése nemcsak önmagára

lesz hatással, hanem környezetére is, ezáltal hozzájárul egy biztonságtudatosabb közeg megteremtéséhez.

A kérdőív, illetve az interjúk tapasztalatai is a leírtakat támasztják alá. Jól látható, hogy milyen elvárásoknak kell megfelelnie egy tudatos felhasználónak, az óvatosságtól kezdve egészen a trendek követéséig. A megkérdezett vállalatok esetében kiemelt szerepet kap a biztonságtudatosság, amelyet az elmondottak alapján folyamatosan szinten tartanak, fejlesztenek. Ennek keretében különböző intézkedéseket tesznek, amelyek következtében fejlődés mutatható ki egyéni és szervezeti szinten is, de amelyekből sosem elég, így állandó napirendi pontnak kell lenniük a feladatlistában. Mindezek mellett a munkavállalók is egyre fontosabbnak tartják a tudatosság szintjének növelését, noha időnként nyűgnek érzik egy újabb ismétlő kurzus elvégzését.

2.2. A tudatosítás mint kockázatcsökkentő intézkedés

Amikor az elmúlt évtizedekre gondolunk, akkor megállapíthatjuk, hogy egyre inkább a mindennapi életünk részét képezik a különböző informatikai rendszerek. Akár a magán-, akár az állami szektorban helyezkedik el egy munkavállaló, elkerülhetetlen, hogy elektronikus eszközökkel találja szembe magát. Mivel ezek a rendszerek manapság már nélkülözhetetlenek a munkavégzéshez, a sérülékenységük[14] vagy kiesésük is bizonyos rizikóval jár, így hatást gyakorolhat a szervezetek működésére is.[15]

Általános igazság, hogy egy vállalat szempontjából elengedhetetlen mindennemű kockázat legkisebb mértékűre csökkentése, lehetőség szerinti elkerülése. De pontosan mit is definiálhatunk kockázatként? Intenzitását egy adott fenyegetés[16] bekövetkezésének valószínűsége és az általa okozott kár nagyságának szorzata adja. Ebből kiindulva annak az esélyét, hogy egy fenyegetés mint esemény megvalósuljon, redukálni kell. A cél az, hogy a szervezet esetében a döntéshozó által meghatározott – az esetek jelentős többségében jogszabályok által előírt – szintű biztonságot elérjük és fenntartsuk.[17]

[14] Sérülékenység: az elektronikus információs rendszer egy része, amelyen keresztül megvalósulhat valamely fenyegetés.

[15] Pósernné 2007: 206–207.

[16] Fenyegetés: lehetséges esemény, amely biztonságot sérthet.

[17] László 2014: 1–5.

Egy vállalat életében például kockázat lehet dokumentumok, fontos iratok sérülése, azok bizalmasságának vagy sértetlenségének veszélybe kerülése vagy akár egy eszköz, berendezés rendelkezésre állásának ellehetetlenülése, tehát a szervezet érdeke, hogy ezeket megelőzze. Az egyéni (munkavállalóhoz fűződő) érdek és az ehhez tartozó kockázatok felmerülése ezzel szemben elsősorban a magáneszközök, személyes adatok biztonságára vonatkozik, bár ugyanúgy érinthet dokumentumokat, iratokat, eszközöket és berendezéseket is. A vállalat és az egyén szintjén is fontos tisztában lenni azzal, hogy milyen következményekkel járhat a kockázatok biztonsági eseményként történő bekövetkezése. Ez például, ahogy arról már volt szó korábban, anyagi kárral járhat, a vállalat szempontjából kiemelten fontos bizalomvesztést okozhat, vagy nagymértékben akadályozhatja a szervezeti célok megvalósulását.[18]

Kockázatcsökkentés általánosságban

A fentiek alapján egyértelmű, hogy a felmerülő kockázatokat csökkenteni kell a biztonság fenntartása és fejlesztése érdekében. Milyen intézkedésekkel célszerű mindezt megvalósítani? A biztonság ilyen szempontból történő megteremtése – így a veszélyeztetettsége is – több összetevőből áll: emberi, adminisztratív, fizikai, logikai és egyéb tényezőkből, amelyek hatással lehetnek a védelem ténylegesen megvalósított szintjére. Példaként hozhatjuk az embert mint a „leggyengébb láncszemet", az intézmény szabályzatait, személyes adatokat tartalmazó és belső dokumentumait, tanúsításait, az épületet, a berendezéseket, az eszközöket és a szervezet vezetőjének döntéseit is. Ezek a tényezők mind befolyásolhatják a vállalat életében felmerülő veszélyek mértékét, nem idesorolva természetesen azokat a komponenseket, amelyekre nincs ráhatása az embereknek (például természeti katasztrófák).

Összességében megállapítható, hogy a kockázatcsökkentő intézkedések alapvetően járulnak hozzá a szervezet biztonságának szavatolásához. Palettájuk rendkívül széles: megemlíthetjük az infokommunikációs eszközök (IKT vagy IKT-eszközök) védelmére szánt programok használatát,[19] a dolgozókra nézve

[18] Pósernė 2007: 208–210.

[19] Például vírusirtók, weboldalt blokkoló szoftverek.

kötelező jelszószabályok alkalmazását,[20] a belépések relációjában az azonosítás[21] kérdéskörét, a különböző szabályzatok[22] készítését, a beépített biztonsági rendszereket[23] és végül, de egyáltalán nem utolsósorban a munkavállalók biztonságtudatossági oktatását is.

Az utóbbival kapcsolatban mindenképpen fel kell tenni a kérdést, hogy a vállalatnak (akármelyik ágazathoz tartozzon is) miért fontos a munkavállalók biztonságtudatossága. Meg kell állapítanunk, hogy akár a jelszóhasználatot, a tiszta asztal elvét, az otthoni munkavégzést, akár az adathalászatot, a trükkös csaláson *(social engineering)* alapuló támadásokat, esetleg az infokommunikációs eszközöket vagy a közösségi média használatát nézzük, egy tényező mindig jelen van, ez pedig az ember, maga a felhasználó. Ő az, akinek – ha nem elég óvatos – könnyen feltörhetik a fiókjait vagy megszerezhetik a belépési adatait, és aki akár áldozatul eshet célzott támadásoknak is. Továbbá a megfelelő felkészültség hiányából fakadóan – szándékosság nélkül is – használhatatlanná tehet IKT-eszközöket, illetve veszélybe sodorhatja azok tartalmának biztonságát. Mindezek fényében kijelenthetjük, hogy a humán alapú kockázat gyakorlatilag minden szervezetnél jelentős, de a biztonságtudatosság növelésével[24] markánsan csökkenthető a munkaerővel kapcsolatos legtöbb fenyegetés bekövetkezésének valószínűsége.

Humán kockázatok csökkentése tudatosítás útján

Ahogy azt már korábban hangsúlyoztuk, a biztonsági kultúra kialakítása kiemelt szerepet kell kapjon egy vállalat életében. Előfordul, hogy a szervezet saját alkalmazottai sincsenek tisztában az információbiztonsági tudatosság hiányából fakadó tettek következményeivel. Hiába alkalmaz ugyanis a vállalat különböző technológiai, védelmi megoldásokat, ha a felhasználók nincsenek tudatában annak, hogy a magatartásuk által az ő felelősségük és feladatuk is a biztonság szavatolása. Enélkül a legjobb védelmi mechanizmusok sem lesznek képesek

[20] A kapcsolódó témakört a *Jelszó* című alfejezet tartalmazza.
[21] Szakmai terminológia szerint autentikáció (bővebben lásd a *Jelszó* című alfejezetben).
[22] Például vírusvédelmi, adatvédelmi szabályzatok.
[23] Például tűzjelző berendezés, riasztó, élőképrögzítés.
[24] Biztonságtudatosság: egyének veszélyérzete (személyes és szervezeti szintű).

a megfelelő szintű, tőlük elvárt biztonságot nyújtani.[25] Megállapítható tehát, hogy a biztonságtudatosságra mint szemléletre szükség van.

Egyfajta kihívást jelent a biztonságtudatosság mint célkitűzés esetében az, hogy költséges, de nem produkál számottevő kézzelfogható eredményt. Energiát, időt és anyagi forrásokat kell belefektetni, de a kapcsolódó intézkedések következménye nem olyan egzakt, mint például egy konkrét tárgyi beszerzésé. Ettől függetlenül azonban kétségtelenül szükség van rá, hiszen – ahogy korábban már utaltunk rá – egy incidens valószínűleg sokkal nagyobb anyagi kárt okoz, mint amennyit egy biztonságtudatossági képzésre kell fordítani a megelőzés keretében.

Egy másik fontos kérdés, hogy mikor tekinthetjük a biztonságtudatosságot megvalósult célnak vagy elsajátított képességnek. Erre nehéz egzakt választ adni, de általánosságban talán akkor, amikor elmondhatjuk, hogy az emberek tudják és értik is, mit, hogyan és milyen következményekkel cselekszenek a kibertérben. Mindehhez a kulcs a digitális kompetencia célirányos fejlesztése, a képzés. A megfelelő szabályozók mellett, amelyeket a munkavállalóknak kötelességük betartani, fontos, hogy tudják, mit kell és mit nem kell tenni a gyakorlatban egy incidens előtt (a megelőzés érdekében), alatt (a kezelés idején) és az utókezelés során (helyreállítás közben). Azt is meg kell jegyezni, hogy a tudatosság oktatása önmagában nem elég, és szóba jön ilyenkor a biztonsági éberség is mint eszköz. Nemcsak az egyénnek fontos, hogy biztonságban érezze magát és tudatosan járjon el minden helyzetben, de ez a vállalat számára is elengedhetetlen tényező ahhoz, hogy a profit egy részét megelőzésre lehessen fordítani, és ne a helyreállításra kelljen rendszeresen áldozni.[26]

Ugyanezt a kérdést támadói oldalról vizsgálva megállapíthatjuk, hogy jellemzően jóval alacsonyabbak a költségek egy támadás előkészítése és lebonyolítása, mint a védelem (és a helyreállítás) finanszírozása esetén. Ez is megerősíti, hogy a tudatosítás, a képzés egyrészt pénzügyileg sokkal kifizetődőbb, másrészt az egyik legolcsóbb – és legáltalánosabb – módja is a védekezésnek.

Ahogy említettük, a tudatosság oktatása önmagában még nem lehet tartósan célravezető. A szervezeti biztonsági kultúra kialakításához elengedhetetlen a szándék megteremtése a dolgozókban, mert az adja meg az intézmény biztonságos működéséért történő felelősségvállalást és az erkölcsös döntések meghozatalának tudatosságát. Miért jó, ha jelen van az így kialakuló tudatos

[25] *Biztonságtudatos szemlélet kialakítása* 2018.
[26] Nyikes 2017: 327–330.

szándékosság? Azért, mert egy nem egyértelmű szituációban ez fogja szolgálni a szervezeti biztonságot. A munkahelyi erkölcsi környezet követése és az ehhez tartozó helyes magatartás hozzájárul a biztonság megőrzéséhez, a legtöbb esetben még incidensek bekövetkezésekor is. Tehát összességében vezetői beavatkozásra sincs feltétlenül szükség, mert a szervezet tagjai saját magukat motiválják és irányítják abban, hogy a helyes viselkedést fenntartsák.[27]

Egyértelműen látható, hogy mennyire fontos a biztonsági kultúra kialakítása és ezáltal a tudatosítás ahhoz, hogy a vállalat megőrizzen egy adott biztonsági szintet, illetve továbbfejlődhessen. Természetesen intézményenként eltérő lehet a választott technikák fajtája és használatának miként je, ehhez kapcsolódóan következzen néhány lehetséges módszertan. Az információ áramlását szervezettől függetlenül olyan módszerekkel célszerű biztosítani, mint a hírlevelek, tudatosító, tájékoztató honlapok vagy – a megfelelő tartalomszűrést követően – közösségi médián keresztül elérhető információs csatornák. Ezek mindegyikénél lehet alkalmazni az olyan segédeszközöket, mint a rendszeres hírlevelek, brosúrák (tájékoztató célú) kibocsátása, különféle kérdőívek kitöltése, akár nyereményjátékkal összekötve, vagy esetleg rövid, közérthető videók közzététele. Időközönként ajánlatos szervezni közösségi programokat, akár az Európai Kiberbiztonsági Hónap[28] keretén belül, akár belső, szervezeti indíttatásból, amelyeken már megjelenhetnek az egyszerűbb játékok, szabadulószobák vagy csapatversenyek is, kifejezetten az információbiztonságra összpontosítva. Amikor a képzésekre gondolunk, akkor rögtön a hagyományos (frontális) oktatás jut eszünkbe, továbbá az egyre nagyobb népszerűségnek örvendő e-learning-tanfolyamok, gyakorlati képzések, amelyeket mind összeköthetünk a játékosítás módszereivel (gamifikáció),[29] hogy a résztvevők élvezzék is a tanulást.

Külön műfajnak tekinthető a szakmai konferenciák szervezése vagy azok látogatásának ösztönzése, amely téren egyszerre több módszerrel is találkozhatunk. Az ilyen események nemcsak a szakmai kapcsolatok gyarapítását és az oktatást,

[27] Lazányi 2016: 143–150.

[28] Kiberhónap: az Európai Kiberbiztonsági Hónap (ECSM) elnevezésű kampányt az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) koordinálásával 2012 óta minden év októberében megszervezik Európa-szerte. A kampány célja a kiberbiztonság köznyelvbe emelése, hogy a szakértőkön túl az állampolgárok szélesebb köréhez eljussanak annak aktuális kihívásai és trendjei. Egyéb értelemben a kampány hasonlít a jól ismert „Movember"-hez, ugyanis ezen akciók célja a veszélyekre történő figyelemfelhívás és a megelőzés.

[29] Gamifikáció: olyan eszköz, amellyel játékos formában tudunk információkat közölni és átadni, ezáltal segítve azok befogadását.

tudatosítást illetően lehetnek hasznosak, de a brosúráktól kezdve a szabadulószobáig szinte mindent be lehet vonni ezekbe. Egy többnapos konferencia így nemcsak kimozdítja a munkavállalót a szürke hétköznapokból és a komfortzónájából, de tanul is belőle, kapcsolatokat alakíthat ki, és mindeközben jól érzi magát a környezetében. A jó komfortérzet pedig hozzásegíti ahhoz, hogy jobban tudjon koncentrálni, és fokozatosan egyre inkább érdeklődjön a tudatosításhoz köthető (alapvetően szárazabb) tananyagok, ismerethalmazok iránt is. Végezetül pedig a kötelező és szúrópróbaszerű vizsgák vagy tapasztalatszerzésre irányuló incidenskezelési gyakorlatok szervezése említhető, amelyek visszakövethetővé teszik a megszerzett tudást, és ébren tarthatják a munkavállaló védelmi képességeit.

Látható tehát, hogy a biztonsági kultúra kialakítása alapvetően teljesen szervezetfüggő, ugyanakkor napjainkban széles spektrumon mozognak azok a lehetőségek (módszerek és segédeszközök), amelyek között egy vállalat válogathat.

A kérdőívek és interjúk eredménye

Az eddig megállapított szükségletek (kockázatcsökkentés, tudatosítás) és lehetőségek (intézkedések, módszertanok) vonatkozásában van két nagyon fontos kérdés, amelyet minden szervezetnek fel kell tennie, ahol biztonsági kérdésekkel kapcsolatos döntéseket hoznak. A kitöltött kérdőívek, valamint a szakértőkkel folytatott interjúk alapján ezeket az alábbiak szerint válaszolták meg a kutatásban részt vevők.

Biztonságtudatosság – ki a felelős?

Általánosságban azt mondhatjuk, hogy nem lehet konkrét személyt kiemelni, ha a felelősség kérdését vitatjuk. Az interjúk tapasztalatai azt mutatják, hogy az illetékesség kettébontható, ugyanis nagyrészt konszenzusként kaptuk a választ, hogy a biztonságtudatosság mindenki felelőssége, de a vezetés feladata, hogy összefogja azt. Tehát egy szervezetnél a vezetőség felelős a biztonságtudatosság kialakításáért és fenntartásáért.

A vizsgált intézmények esetében megállapítható, hogy a biztonságtudatossággal kapcsolatos oktatások és kampányok ma már szerves részei a mindennapoknak.

Tehát a képzések (e-learning, jelenléti) ezek számonkérései, illetve a különböző konferenciák, fórumok tartása, infografikák, hírlevelek küldése és egyéb, interaktív tudatosító módszerek (például szabadulószoba) mind-mind jelen vannak, csak változó gyakorisággal. Maga a klasszikus formájú oktatótevékenység negyedévente, félévente vagy évente jellemző, a kampányok, infografikák, hírlevelek küldése pedig rendszeresen, struktúrától és témakörtől függően havonta vagy hetente. Az interjúk során volt olyan kolléga, aki úgy vélte, ezeknél többet már nem lehet tenni, de olyan szakértő is, aki szerint az új ötletekből sosem elég. Ezzel együtt senki sem tartotta kevésnek a szervezete által végzett, biztonságtudatosságot célzó tevékenységet. A tudás elsajátítását mind elméleti, mind gyakorlati szinten fontosnak tartják a megkérdezettek, akik összességében úgy gondolják, hogy a gyakorlatnak a megszerzett elméleti alapokon kell nyugodnia.

Mi az, ami nehézséget jelent a tudatosítás szempontjából?

Megállapítható, hogy az érem másik oldala természetesen a feladat anyagi hátteréhez kötődik, hiszen köztudott, hogy a biztonság szavatolása költséges, ami nehezítheti a tudatosítási tevékenységek hatékonnyá tételét. A „láthatatlan dolgok" anyagi fedezetének biztosítása, szükségességének alátámasztása rendszeres kihívás a biztonsági területek szakértői számára.

Tovább csökkenti a hatékonyságot, ha olyan személy(ek) végzi(k) a tudatosítást, aki(k)nek nincs meg a megfelelő biztonságtudatossági szakértelmük. Mindemellett a szervezet nagysága, kiterjedése is nehezítő tényező lehet, főleg ha a vezető sem kellően elkötelezett. Ugyanakkor az sem kizárt, hogy egyes munkavállalók érdektelenek a tudatossággal kapcsolatban (főleg addig, amíg egy tényleges incidens meg nem történik velük), ami másokat is azzá tehet, sőt akár gátolhatja is a kollégák tudatos magatartási formákra való nyitottságát.

Mindezek alapján elmondható, hogy számos nehézséggel kell szembenéznie egy vállalatnak, ha azt szeretné, hogy a dolgozói tudatosak legyenek, azonban kijelenthető, hogy az előbb felsorolt elemeken következetes célokkal és intézkedésekkel lehet változtatni.

Összegzés

Napjainkban körbevesz minket a technológia, így a dolgozók napi szinten találkoznak vele, tehát kiemelten fontos, hogy bárminemű eszközt a megfelelő tudatossággal tudjunk használni. A biztonságtudatosság azonban nem velünk született dolog, oktatni és tanulni, fejleszteni kell. Egy szervezetnél, ahol rengeteg értékes adat, információ található, célirányosan kell védeni ezeket. Ehhez viszont ki kell alakítani a megfelelő biztonsági kultúrát, amelynek keretén belül egy munkavállaló képes és hajlandó felelősségteljesen cselekedni és tevékenykedni.

Az, hogy egy vállalat biztonságtudatosságra törekszik, önmagában megteremti a lehetőséget, hogy a felmerülő kockázatokat humán oldalról a lehető legkisebb mértékűre csökkentse. A biztonság (amelynek egyik letéteményese a humán erőforrás) az ahhoz való hozzáállástól és az oktatástól is függ. Tegyük fel, hogy ha megfelelő módszerekkel kommunikáljuk szervezetünkben a tudatosság jelentőségét, és hatékony eszközökkel biztosítjuk annak elsajátítását, lehetővé téve a folyamatos fejlődést, akkor idővel a munkavállaló magától is igényelni fogja a tudást. Ezek viszont ugyanúgy függnek az emberi hozzáállástól, így ha a dolgozók nem tanúsítják a megfelelő és elvárt magatartást a biztonságtudatosság területén, akkor a szervezetnek számolnia kell azzal, hogy a fenyegetések bekövetkezésének valószínűsége a lehető legkisebbnél mindenképpen nagyobb lesz.

A vizsgált szervezeteknél a már említett biztonsági kultúra optimálisan kialakult, amihez elengedhetetlen volt a vezetői elkötelezettség és a munkavállalói hajlandóság. Kockázatcsökkentő intézkedések által pedig megerősítették a gyakorlatban azt, amit eddig elméletben fejtettünk ki, vagyis hogy jóval kisebb az egyes incidensek bekövetkezésének valószínűsége akkor, ha a munkavállalói biztonságtudatosság mint készség jelen van.

Összességében tehát a gyakorlatban is nagyon jól látható, hogy a megfelelő mértékű, fajtájú és minőségű tudatosító módszerek kockázatcsökkentő hatást fejtenek ki. Ez a fajta preventív megoldás sokkal hatékonyabbnak nevezhető, mint ha utólag kellene megfizetni a tudatosság hiányából fakadó károk árát.

Vákát

3. Jó gyakorlatok és minimumismeretek

3.1. Az interjúk általános tapasztalatai

A már említett interjúkat a partnerszervezetek által delegált szakértőkkel folytattuk le. Maga az interjúztatás kiemelten hasznos módszer egy adott kérdéskör feltérképezésére, különösen akkor, ha az előzetesen megküldött kérdésekre adott írásbeli, aránylag visszafogott, már-már túlzottan megfontolt és a vártnál kicsit kevesebb információt tartalmazó válaszok megindítják a beszélgetések szakmai párbeszédeit. A kérdéseket a már szintén említett kérdőívvel összhangban állítottuk össze, hogy a szakértők által adott szóbeli interjúk tartalma a munkavállalókra irányuló felméréssel párhuzamban legyen. Ez meg is valósult: a kitöltött kérdőívek és a szóban elhangzottak határozott összhangban állnak egymással. Ami esetleg az interjúnál hatékonyabb lett volna, az a szervezeten belüli csoportos beszélgetés, amelynek résztvevői az ismerős környezetben magabiztosabbak lehettek volna.

Mindezek alapján egyértelműen következtethettünk arra, hogy a szervezetek nagy gondot fordítanak a munkavállalók képzésére és rendszeres tudatosítására. A vállalatoknak fontos a biztonság, így a dolgozók sem állhatnak hozzá másképp. Példaként említendő az, hogy amikor a talált pendrive tipikus esetét hoztuk fel, a „mit fog tenni vele?" kérdésre kihegyezve, akkor kaptunk olyan választ is, hogy ez már nagyon régi történet, és az adott cégnél ez már unalmasnak számít, ugyanis a munkavállalók napjainkban már nem sétálnak bele efféle csapdákba. Koherencia mutatkozik a partnerszervezeteknél tapasztalható szemléletmódok között azt illetően, hogy mi jellemez egy tudatos felhasználót (például óvatos, tudja és érti, hogy mit csinál, követi a trendeket, önszántából készíti fel magát egy esetleges támadásra, incidensre).

De nem ez az egyetlen kérdés, amelyre mind a három cég képviselőitől hasonló választ kaptunk. Az, ahogyan az interjúalanyok látják a tudatosítás módszereit, nagyban egyezik az adott szervezeti kultúrával is. Elmondásuk alapján ők szinte teljesen elégedettek a vállalat által nyújtott tudatosítással, épp csak egy-két dolgon változtatnának. Véleményük szerint a munkavállalók rendelkeznek a tudatos felhasználó ismérveivel, így a cégek vélhetően nem csak az információbiztonsági képzések meglétét tartják fontosnak. Az incidensek mennyiségéről és kezeléséről szóló kérdésre azt a választ kaptuk, hogy nem gyakoriak a támadások, és ha elő is fordulnak, a dolgozók többsége rögtön tudja, kihez forduljon, és hogyan kezelje őket. Ez arra enged következtetni, hogy a munkavállalók igyekeznek mindig pontosan tudni a feladataikat és az eseti teendőiket. Egy biztonságtudatos személy

nemcsak azzal van tisztában, hogy adott tennivalókat milyen módon végezzen el, hanem azzal is, hogy azok során milyen potenciális kockázatok merülhetnek fel (például adathalász-e-mail a munkaköréhez tartozó tárgyban), és hogy ezeket a fenyegetettségeket hogyan kell kezelni.

Összefoglalásképpen tehát az interjúk által kívántuk feltérképezni a vizsgált szervezetek biztonságtudatossághoz való hozzáállását, ami a delegált szakértők közreműködésével meg is valósult. Átfogó képet kaphattunk a tudatosságról magáról, a tudatosítás alkalmazott módszereiről és azok hasznosságáról, betekintést nyerhettünk abba, hogy a válaszadók hogyan ítélik meg a munkavállalók biztonságtudatosságát, és abba is, hogy a vállalatok milyen fenyegetésekkel néznek szembe, illetve hogyan biztosítják a szervezeti biztonsági kultúra kialakulását, fenntartását és szükséges fejlesztését.

3.2. Átfogó tudásbázis

A kutatás keretében végzett interjúkból, valamint a kitöltött kérdőívekből megállapítható, hogy a vizsgált cégek számos jó gyakorlatot alkalmaznak, és munkavállalóik felkészültsége megfelelő. A biztonságtudatos szemlélet a mindennapjaik részét képezi, és törekszenek annak megújítására, amennyire az lehetséges. A megszerzett tudás tekintetében ugyanakkor nem jelenthetjük ki, hogy alapvető szintű ismerethalmazt birtokolnak, jellemzően eltér a szervezetek fókuszba helyezett információinak típusa.

Ez motiválta szerzőink körét arra, hogy egy hét témakörből álló, alapvető és átfogó tudásbázist állítson össze annak érdekében, hogy bármely intézmény bármely munkatársa, előképzettségtől és munkakörtől függetlenül, elsajátíthassa a legszükségesebb ismereteket az információbiztonsági tudatosságról. Ebben a tudásbázisban a hatékony jelszókezeléssel, az elmúlt hónapokban elterjedt otthoni munkavégzés biztonsági szempontrendszerével, a tiszta asztal elv jelentésével, a rendelkezésre bocsátott (és magán-)IKT-eszközök használatának kihívásaival foglalkozunk, általános értelemben a közösségimédia-jelenléttel, valamint az olyan gyakori támadási formákkal, mint az adathalászat és a trükkös csaláson alapuló megtévesztések.

3.2.1. Jelszó

A „szezám, tárulj!” mondatot mindannyian ismerjük, hála a középkori arab irodalom egyik népszerű meséjének. A jelszó szimbolikája már ebben a formájában is a védendő értékekhez vezető kulcs volt.[30] Bár ott még varázsigeként jelent meg, a történelmünkben évszázadokon át a jelszavakat hívták segítségül ahhoz, hogy bizonyosságot nyerjenek arról, ki barát és ki ellenség.[31] Ezek mindvégig a saját biztonságunkat szolgálták, és ez napjainkban sincs másként, csak a fogalmi meghatározást övező tényezők alakultak át 21. századivá. Ma már a jelszó elnevezés alatt egy rövid karakterláncot értünk, amelyet a felhasználók hitelesítésére használnak informatikai rendszerek azonosítási folyamataiban. Sajnos az idők során egy tényező nem változott a jelszóval kapcsolatban, mégpedig az, hogy ha már nem titok, akkor jelentős veszélyt hordoz magában az alkalmazása. Ez a tanulmányrész rövid útmutatást kíván nyújtani ahhoz, hogy ezt a kockázatot minimalizáljuk, vagyis hogy elősegítsük a jelszótitok megőrzését, amivel képesek vagyunk megvédeni magunkat a kibertér egyik legsúlyosabb következménnyel járó fenyegetésétől, a jogosulatlan hozzáféréstől.

Mindennapjaink jelszavai

Manapság a jelszavainkat felhasználónévhez társítva alkalmazzuk olyan digitális eszközökön, amelyeken a futtatott szoftverek ezzel a hitelesítési protokollal szabályozzák magát a hozzáférési jogosultságot, vagyis gondoskodnak arról, hogy az adott felhasználó csak a számára biztosított hatáskörben használja az adott rendszert. Lehetnek jelszavaink a számítógépünkön vagy a mobiltelefonunkon futó operációs rendszerhez, és bizonyosan van online bankoláshoz, e-mailezéshez, közösségi oldalakhoz vagy bármely más szolgáltatáshoz is. Valószínűleg megtörtént már velünk, hogy bosszankodtunk, mert jelszavunk megadása közben félreütöttünk pár karaktert, és ezzel meghiúsult a belépésünk valamely platformra, vagy mert ritkán használtuk, így esetleg elfelejtettük a kódot, és hirtelen nem tudtunk hova fordulni megoldásért. Talán azt gondoljuk, hogy a rutinosabb felhasználók ebben a helyzetben feltalálják magukat, hisz van egy kis könyvük a munkaasztalon, amelybe beírták jelszavaikat, vagy van

[30] Waksman 2013.

[31] A magyar nyelv értelmező szótárának *Jelszó* szócikke.

egy munkatársuk, aki tudja az adatokat, és segíthet egy ilyen szorult helyzetben, de az is lehet, hogy olyan egyszerű és könnyen megjegyezhető jelszavakat használnak, amelyek kizárják az említett esetek bármelyikének bekövetkezését. Valójában azonban ők vannak kitéve a legnagyobb veszélynek, hisz bármennyire bosszantó, ha nem érjük el védett értékeinket a kibertérben, a legrosszabb mégis az, ha egy illetéktelen személy átveszi az uralmat e rendszerek és információk felett azért, mert rosszul választottuk meg vagy helytelenül kezeltük jelszavainkat.

A jelszavak fenyegetettsége

Fontos kérdés, hogy kivel állunk szemben, ha a jelszavaink védelméről van szó. Kitől kell megóvnunk saját – akár vállalati, akár magánéleti – digitális birodalmunkat, és milyen fenyegetésekkel kell számolnunk? A virtuális térben a legnagyobb veszélyt a kiberbűnözők[32] és tevékenységeik jelentik: napjainkban az elkövetett bűncselekmények számának felét már a kiberbűncselekmények teszik ki Európában. Az általuk okozott kár eléri a több százmillió eurós nagyságrendet, és ezek a számok növekvő tendenciát mutatnak.[33] Sok esetben magánszemélyektől megszerzett hozzáférési jogosultságok jelenthetik a kulcsot ahhoz, hogy illetéktelenek bejussanak nagyobb vállalatok rendszereibe, és így képesek legyenek akár egy egész országot megzavaró csapást mérni a víz- vagy áramellátásra, illetve más létfontosságú erőforrásra. Emellett természetesen az egyszerű felhasználók eszközei feletti uralom átvétele is potenciális és jól jövedelmező cél, például a kriptobányászat, azaz a *cryptojacking*[34] esetében.

A kiberbűnözők módszerei a jelszavak feltörésére, kinyerésére, avagy megszerzésére irányulnak. Ilyen lehet a jelszó kitalálása, ha az például kedvenc autómárkánkhoz vagy háziállatunk nevéhez köthető. Hasonló eljárás az, amikor a leggyakrabban használt jelszavak listáját futtatják le a belépéshez. Létezik egy, a nyers erőt kihasználó, *brute force* elnevezésű, eredményes támadás, amely viszont időigényes, mivel az összes lehetséges kombinációt kipróbálva határozza

[32] Számítógépek vagy számítógépes rendszerek segítségével bűncselekményeket elkövető személy.

[33] *Internet Organised Crime Threat Assessment (IOCTA) 2020* 2021.

[34] A *cryptojacking* a számítógépes bűnözés egyik új formája, amely úgy valósul meg, hogy az elkövető jogosulatlanul felhasználja a magánszemélyek eszközeinek erőforrásait kriptopénz bányászására.

meg a helyes kulcsot. Nehezen kivitelezhető, mert nagy számítási kapacitást igényel, ha azonban a jelszó gyenge, akkor másodpercek alatt, különösebb erőfeszítés nélkül sikeres a támadás.[35] Megemlíthető még a *keylogger*[36] program, amely az eszközre telepítve könnyedén naplózza a billentyűleütéseinket, ha nem védekezünk ellene. Egyre népszerűbb és célravezetőbb fenyegetés a trükkös csaláson alapuló, ún. *social engineering*[37] támadás, amely az emberi tényező gyengeségére épít,[38] és annak kihasználásával éri el a céljait. Természetesen ezen incidensek sikeres elhárításához számos védekezési stratégiával tudunk hozzájárulni, de a legfőbb védvonalunk csakis a biztonságos jelszó lehet.

A biztonságos jelszó ismérvei

Hogyan lehet egy jelszó biztonságos? Ehhez két feltétel együttes fennállása szükséges. Nem elég egy erős jelszó, hanem ugyanilyen fontos a jó jelszópolitika, más néven az ezzel kapcsolatos biztonságtudatosság. Azt, hogy milyennek kell lennie egy erős kódnak, már azóta tudjuk, amióta léteznek a mai értelemben vett jelszavak. Feltétel például, hogy ne tartalmazzon születési dátumot, nevet vagy annak egy részletét, betű- vagy számsorokat, helység- vagy országnevet, és ne legyen megtalálható a szótárban. Törekednünk kell egy legalább 8 karakter hosszúságú, nagy- és kisbetűk, számok, valamint speciális karakterek (például: !@?Ł#) keverékéből álló jelszó megalkotására.[39] Kiemelkedően hasznos és kreatív technika is egyben, ha jelszavainkban olyan különleges elemet is elhelyezünk, mint például az ismert *smiley,* mivel ezek jó eséllyel kívül esnek a feltörési programok karaktertartományán.[40] Ezzel biztosíthatjuk, hogy a már említett *brute force* módszer se járjon sikerrel pillanatok alatt, és így a kódjaink megszerzésére irányuló eredményes támadások számát minimálisra csökkenthetjük. Ha már van egy erős jelszavunk, és azt szeretnénk, hogy éles kardként védelmezzen bennünket, fel kell vérteznünk magunkat egy értékes tulajdonsággal, a jelszavak használatával kapcsolatos tudatossággal.

[35] Burnett 2005.

[36] A program a felhasználó tudta nélkül rögzíti annak billentyűleütéseit, majd e naplózás révén az elkövetők előtt megnyílik az út jelszavainkhoz.

[37] *Internet Organised Crime Threat Assessment (IOCTA) 2020* 2021.

[38] Részletesebben kifejtve az *Adathalászat* című alfejezetben.

[39] *10 Rules for Creating a Hacker-Resistant Password* 2009.

[40] *Strong Password.*

A tudatosság szabályai nem bonyolultak, mind egyszerű racionalitáson alapul. Ha böngészőnkben tároljuk jelszavainkat, az különösen kényelmes megoldás, de nem a legmegbízhatóbb, hiszen léteznek speciális programok, amelyekkel ezek a kódok könnyedén „előhúzhatóak" a böngészőalkalmazásból. A jelszókezelők[41] többsége megfelelően ötvözi a megbízhatóságot és a kényelmet. Az ilyen applikációk könnyedén generálnak nekünk professzionálisan hosszú és erős jelszavakat, de nem mindenki képes e programok konfigurálására és mindennapi alkalmazására.[42] Számos jelszókezelő segítségével saját eszközeinken (okostelefon, tablet) tárolhatjuk kódjainkat, és csak biometrikus azonosítással férhetünk hozzá azokhoz, így ezek felhőhasználat nélkül is igénybe vehetők. Értelemszerűen ez sem jelent teljes körű védelmet, hiszen a biometrikus adatokat tartalmazó adatbázisok is feltörhetőek, de az ilyen típusú alkalmazások használatával jelentősen csökkenthetjük a kockázatokat. A felhőalapú applikációkkal kapcsolatban azonban fel kell ismernünk azt a kényes bizalmi helyzetet, hogy jelszavainkat kiadjuk egy harmadik félnek, aki természetesen törekszik arra, hogy titkosítva és helyesen kezelje adatainkat, de a biztonsági kockázat folyamatosan jelen van itt is, sőt, ezek a „jelszószéfek" sokkal potenciálisabb célpontok az elkövetők számára, mint a csak általunk felügyelt kódok.[43]

Rendkívül fontos, hogy ne írjuk ki jelszavainkat memóriacetlikre, és ne ragasszuk ki ezeket a monitorra vagy a munkakörnyezetünk egyéb pontjaira, ahol illetéktelenek könnyen hozzáférhetnek, és visszaélhetnek velük. Rendszeresen változtassuk meg a kódjainkat, és haladéktalanul tegyük ezt meg akkor, ha úgy érezzük, azok valaki birtokába kerülhettek. Ha most ráébredtünk, hogy eddig gyenge jelszónk volt, cseréljük le azt. Ne osszuk meg és ne használjuk belépőkódjainkat másokkal közösen, továbbá ne írjuk be őket olyan eszközökön, amelyeket nem ismerünk. Az erős jelszó sajnos nem ér sokat tudatosság nélkül, így az csak a megfelelő jelszókezeléssel együtt járul hozzá a sikerhez, a biztonsághoz. Ezt még tovább tudjuk fokozni, ha alkalmazzuk a kétfaktoros vagy kétlépcsős azonosítást, amely már a legtöbb jelentős szolgáltatónál (Facebook, Instagram, Google, Twitter stb.) elérhető. Ez tulajdonképpen egy biztonsági mechanizmus arra az esetre, ha egy új eszközzel kívánunk belépni fiókunkba. Ekkor a rendszer kérni fog egy második hitelesítési forrást, amely például vagy

[41] A jelszókezelők olyan alkalmazások, amelyek segítségével egy helyen és biztonságosan tárolhatjuk a többféle online fiókunkhoz tartozó jelszavainkat.

[42] *A weboldal jelszavainak tárolásának 4 módja – előnyök és hátrányok.*

[43] *Felhőtárolás jelszó kezelőkhöz – ellene vagy mellette?* 2017.

egy kódot tartalmazó, a már megadott telefonszámunkra érkező SMS, vagy pedig egy mobilalkalmazás által generált kód.[44] Ezzel a módszerrel már kellőképpen védekezhetünk az illetéktelen hozzáférés ellen.

A kérdőív eredményei a jelszóhasználat relációjában

A kérdőív jelszóhasználatra vonatkozó kérdéseire adott válaszokból összességében pozitív eredmény olvasható ki. A kitöltőknek csak egy kis része tartja úgy, hogy lehet ugyanazt a jelszót alkalmazni különféle felületeken, ugyanis a többségük más-más kódot használ az egyes applikációk esetében, és nem is osztja meg ezeket másokkal, ami biztatónak mondható. A kiértékelés során nem volt felfedezhető eltérés vagy összefüggés abban a tekintetben, hogy a munkavállalók mely szegmensben dolgoznak, így elmondhatjuk, hogy a jelszóhasználatra vonatkozó válaszok minden munkaterületre jellemzőek. A biztonságtudatosítási képzés kérdésköréhez kapcsolódó eredmény releváns, egyértelműen meghatározható volt a szignifikancia abban a tekintetben, hogy aki részt vett ilyen képzésen az elmúlt két évben, az kevésbé osztja meg jelszavait másokkal. A vizsgált vállalatok az elmúlt években hangsúlyt fektettek a felhasználók oktatására, ami tükröződött a válaszokban is. Ezzel a biztonságtudatossági képzés egyértelműen bizonyította hasznosságát, és biztosította létjogosultságát a jövőre nézve is. Emellett érdekes eredménynek mondható, hogy a megkérdezett dolgozók több profilon való azonos jelszó használatával kapcsolatos szokásai attól függően mutatnak eltérést, hogy melyik vizsgált vállalathoz tartoznak a munkavállalók. Ez alátámasztja azt, hogy a tudatosság szintjét nagymértékben befolyásolja, milyen típusú, tartalmú, mélységű és mennyiségű felkészítésben részesülnek az egyes szervezetek alkalmazottai.

[44] Itt az idő, hogy mindenki, mindenhol bekapcsolja a kétlépcsős azonosítást! Mutatjuk, hogyan 2017.

Összegzés

Összegzésképpen elmondhatjuk, hogy amennyiben egyfaktoros autentikációs[45] folyamatokat veszünk igénybe, akkor a legfőbb feladatunk – a védekezés jegyében – az erős jelszavak biztonságtudatos használata. Használjunk erős jelszavakat, és lehetőleg minden felületen másikat, ha nehezen tudjuk megjegyezni, használjunk jelszókezelőt. Találjunk ki egy könnyen megjegyezhető mondatot, majd alakítsuk erős jelszóvá úgy, hogy használjuk a fantáziánkat és a speciális karaktereket. Például a „115 darab alma van a fán" mondatból előállíthatjuk a „115DB@lm@FäN" jelszót, amely már kimondottan erős, és körülbelül négyezer év szükséges a visszafejtésére.[46] Ellenőrizzük az általunk használt szolgáltatásokat, és ha még nem aktiváltuk a kétlépcsős azonosítást, bátran alkalmazzuk azt. Lehetőleg vegyünk részt minél több biztonságtudatosságot fejlesztő képzésen, így megismerhetjük a legújabb fenyegetéseket és legjobb védekező módszereket. Ezen ajánlások együttes megvalósításával jó eséllyel képesek leszünk sikeresen titokban tartani saját jelszavainkat, ők pedig viszonzásképpen szüntelenül őrködnek a kibertérben elhelyezett védendő értékeink fölött.

3.2.2. Tiszta asztal

Mindannyiunknak megvan az a fajta ideális munkakörnyezete, ahol a leghatékonyabban tudjuk a ránk eső munkát elvégezni, azonban a kényelem mellett szükséges ügyelni az információbiztonsági szempontokra is. Sok esetben nem is gondolnánk, hogy az íróasztalunkon hagyott akár egyetlen, kósza jegyzetekkel teli emlékeztető milyen mértékű biztonsági kockázatot jelenthet a szervezetünk számára azzal, hogy idegen kezekbe kerülve számottevő hátrány idézhető elő vagy súlyos károk okozhatók.

Tanulmányunk következő alfejezete a tiszta asztal, tiszta képernyő elv bemutatásával a biztonságtudatos irodai atmoszféra kialakításának szükségszerűségét hangsúlyozza, amelynek lényege, hogy a belső céges adatok ne kerüljenek a kezelésükre nem jogosult, ismeretlen vagy akár ártó szándékú felek kezébe. A tiszta

[45] Olyan informatikai eljárás, amely során meggyőződünk arról, hogy valamely információ (legtöbbször egy felhasználó azonosságára vonatkozó állítás) megfelel a valóságnak. Az Egészségtudományi fogalomtár *Authentikáció* szócikke.

[46] A jelszó erősségének mérésére lásd: www.passwordmonster.com/.

asztal többek közt azokra a fontos iratokra utal, amelyek az asztalon heverve hozzáférhetővé válnak, a tiszta képernyő pedig azokra az elektronikus vállalati adatokra vonatkozik, amelyekhez mások is könnyen hozzájutnak, abban az esetben például, ha a számítógépet nem zároltuk a távozásunkat megelőzően.[47] Fontos azonban megemlíteni, hogy az elv nem kizárólag a fizikai és a digitális asztalra vonatkozik. Alkalmazási területe kiterjed a munkavállalót körülvevő egész irodai környezetre, így szignifikáns szerepet játszanak a fizikai biztonságot szolgáló, a dokumentumok elzárására alkalmas, kulccsal zárható fiókok, illetve páncélszekrények, továbbá konkrétan az iroda mint helyiség zárására vonatkozó szabályok is.

A tiszta asztal, tiszta képernyő elv azokra a gyakorlatokra vonatkozik, amelyek biztosítják, hogy a belső céges fizikai és digitális formátumú adatok, valamint az eszközök (például notebookok, mobiltelefonok, táblagépek stb.) ne maradjanak védtelenek a munkaterületeken (akár irodai környezetre, akár távmunkára gondolunk), amikor nincsenek használatban. Az elv célja, hogy elősegítse a vállalati információbiztonság garantálását, valamint csökkentse az információk kikerülésének kockázatát. De milyen gyakorlatok járulhatnak hozzá a biztonságtudatosabb irodai légkör és környezet megteremtéséhez?

Ha a fizikai irodai munkakörnyezetünkre gondolunk, munkavégzés során érdemes az iratokat rendszerezetten, mindig célhoz kötötten kezelni, a nap végét pedig a dokumentumok, emlékeztetők biztonságos helyre pakolásával (például páncélszekrény), esetleg megsemmisítésével zárni. A tiszta asztal elv elsősorban a digitális dokumentumok használatára ösztönöz a papíralapú példányokkal szemben, ráadásul ez környezetkímélő is. Abban az esetben, amikor a nyomtatás elkerülhetetlen, törekedjünk arra, hogy belső céges adatokat tartalmazó iratokat véletlenül se felejtsünk a nyomtatóban.[48] A munkavégzés megszakításakor minden vállalati adatot tartalmazó dokumentumot, információhordozót el kell tenni az asztalokról, és elzárt helyen szükséges biztonságba helyezni. A tiszta képernyő érdekében a számítógépes asztalon minél kevesebb alkalmazás, dokumentum legyen egyidejűleg megnyitva, lehetőleg csak azok, amelyek az adott munka végzéséhez szükségesek. A számítógép rövid idejű elhagyása esetén megfelelő eljárással (zárolás, jelszavas képernyővédelem alkalmazása) gondoskodni kell arról, hogy kívülállók ne tekinthessenek be a rendszerbe. Hosszabb idejű – kb. egy órán túli – távollét esetén pedig érdemes kijelentkezni az alkalmazásokból

[47] *Adatvédelmi kihívások az otthoni munkavégzés során* 2020.
[48] *Policy tiszta asztal, tiszta képernyő.*

és kikapcsolni a számítógépet. A tiszta asztal, tiszta képernyő elv implementálása során lényeges, hogy ne kizárólag az egyedi íróasztalokra koncentráljunk, hanem azokra a szélesebb munkaterületekre, amelyeket az alkalmazottak használatba vehetnek. Ahhoz, hogy az erre vonatkozó ajánlások áttekinthetővé és elérhetővé váljanak a munkavállalók számára, érdemes belső szabályzatba foglalni a helyes eljárások menetét.

A 2020-ban a koronavírus-járvány kapcsán nagymértékben elterjedő otthoni munkavégzés új fejezetet nyitott sok vállalat információbiztonsággal kapcsolatos hozzáállásában, ezért az új körülményekből adódóan ma már a „tiszta környezet" koncepciójáról is érdemes beszélni. Az otthonok jó része nincs (vagy nem volt) felkészítve arra, hogy több munkaállomásnak biztosítson helyet, vagy garantálja a szükséges információbiztonsági szabványok teljesítését. Noha a papírfelhasználás visszaszorulóban van, gondolni kell arra, hogy a háztartások többségében nem adott a biztonságos dokumentumtárolás és az iratmegsemmisítés lehetősége sem. Előfordulhat továbbá, hogy egy háztartáson belül egy időben ketten is videókonferencia-hívást bonyolítanak le, és tisztán hallják a másik beszélgetésben elhangzó információkat. Ilyenkor számolni kell azzal, hogy a másik hívásban részt vevő összes személy hall minket, sőt véletlenül akár rögzítheti is az adatokat a webkonferencia során.[49] Ennek következményeként akaratlanul kerülhetnek – akár szenzitív – információk illetéktelen kezekbe. Ez a későbbiekben az adott vállalat, illetve munkavállaló számára kedvezőtlen következményekkel járhat.

Az ún. *open-office* típusú (nagy légtérben sok munkaállomásnak teret adó) irodák és a megosztott számítógépes munkaállomások népszerűségével nagyobb szükség van a szervezet információinak védelmére, így a hatékony tiszta asztal, tiszta képernyő elv kulcsfontosságú eleme lehet a szervezeten belül jó működő információbiztonsági irányítási rendszernek. A már említett elv jelentőségére mutat rá az a tény is, hogy számos szabványban megjelenik, mint például a közismert információbiztonsági keretrendszer, az ISO/IEC 27001 A.11.2.9 pontjában, valamint az ISO/IEC 27002 szabvány A.11.2.9 pontjában.

A tiszta asztal, tiszta képernyő elv viszonylag könnyen implementálható a szervezetek mindennapi életébe, ezáltal jelentős kockázatcsökkentő intézkedést jelenthet abban az esetben, ha a munkavállalók valóban körültekintően viszonyulnak a mindennapi munkavégzéshez az irodai munkakörnyezetben.

[49] *Adatvédelmi kihívások az otthoni munkavégzés során* 2020.

A kérdőív és az interjúk eredménye a tiszta asztal elv relációjában

A kérdőív tekintetében a kitöltők válaszai alapján a tiszta asztal, tiszta képernyő irányelvvel kapcsolatban megállapíthatjuk, hogy a munkavállalókra összességében az jellemző, hogy nem hagyják őrizetlenül a dokumentumokat, mert azt kockázatosnak tartják, továbbá tisztában vannak azzal, hogy nem is nagyon hagyhatják őrizetlenül azokat.

Az IKT-eszközök képernyőjét összességében főként akkor zárolják a kitöltők, ha elhagyják a munkaállomást vagy az irodát, hiába zár le a képernyő egy idő után önmagától is. Szignifikancia figyelhető meg aközött, hogy az illető melyik szervezethez tartozik, és mennyire jellemző rá, hogy őrizetlenül hagyja a dokumentumokat, továbbá aközött is, hogy valaki melyik szervezet tagja, és hogyan áll a képernyő zárolásának kérdésköréhez.

Ezek alapján elmondható, hogy a munkavállalók az általuk használt eszközöket – mind a dokumentumokat, mind pedig az IKT-eszközöket – kellő körültekintéssel kezelik, így a munka befejeztével elzárják azokat. Ez pedig a biztonságtudatos viselkedés egyik alappillére, amelyet nemcsak egyéni, hanem vállalati szinten is alkalmazni szükséges.

Összegzés

Az egyre inkább tudásalapúvá váló társadalomban és gazdaságban az információ a gazdálkodó szervezet számára olyan érték, amely a vezetői döntések, illetve az üzleti sikeresség alapja, ezáltal a működés hatékonyságának meghatározó eleme, tehát védeni kell, technológiai és humán alapon egyaránt. A szervezeti információbiztonságot fenyegető kockázatok jelentős része emberi tényezőből ered. Ezeket teljes mértékben kiküszöbölni nem lehet, azonban megfelelő képzésekkel, körültekintő magatartással és a megfelelő alapelvek alkalmazásával jelentősen csökkenthetők.[50] Ilyen alapelv a fentiekben röviden bemutatott tiszta asztal, tiszta képernyő is, amelynek kapcsán „csupán" olyan apró cselekedetekről van szó, mint például a képernyő zárolása vagy éppen a cetlikre írt jegyzetek eltávolítása, elmulasztásuk mégis akár beláthatatlan következményekkel is járhat a szervezetek működését érintően. A hatékony és biztonságtudatos vállalati atmoszféra kialakításának érdekében napjainkban már nem csak a szó szoros értelmében vett

[50] Michelberger–Lábodi 2012: 241–302.

asztalra, illetve képernyőre szükséges koncentrálni. Nélkülözhetetlen, hogy az irodai környezet egészét vegyük górcső alá, annak „tisztaságára", vagyis biztonságosságára törekedve.

3.2.3. Otthoni/távoli munkavégzés

Az infokommunikációs technológiák folyamatos fejlődésével lehetővé vált az, hogy egyes munkakörök esetében a munkavállaló képes elvégezni feladatait a munkahelyén kívül is. Ezt az atipikus munkavégzési formát nevezzük távoli munkavégzésnek. A távmunka jelentősége felértékelődött a Covid–19-járvány megjelenésével, ugyanis ez tűnt a legbiztonságosabbnak az emberek számára egy olyan pandémiás helyzetben, amelyet az elmúlt időszakban megéltünk.

A munkáltatók által beszerzett és működtetett irodai rendszerek révén biztosított védelmek (például tűzfalak és feketelistára tett IP-címek) nélkül sokkal kiszolgáltatottabbak a dolgozók a számítógépes támadásoknak. Ebből adódóan a legalapvetőbb kockázat a távmunka során, hogy a munkavállalók feladataik nagy részét online végzik, távol a munkáltató által egységesen kiépített és üzemeltetett megoldásoktól. Természetesen a vírus megjelenése előtt is létezett a távmunka, viszont aránya magyarországi viszonylatban nem volt magas, a Covid–19 megjelenésével azonban ez jelentős mértékben megváltozott. A következőkben azokat a kockázatokat ismertetjük, amelyek releváns fenyegetést jelentenek az olyan szervezetekre és munkavállalóikra nézve, amelyek engedélyezik a távoli munkavégzést.

Személyes eszközök és személyes vagy nyílt hálózatok kockázata

A saját eszközök munkahelyi használata – más néven *bring your own device* (BYOD) – ma már egyre jellemzőbb a távoli munkahelyi környezetekben, függetlenül attól, hogy mi a munkavégzés irodai környezeten kívüli, pontos helyszíne. Ez esetben a munkáltató nem biztosít vállalati eszközöket (azaz a vállalat tulajdonában lévő hordozható eszközt, amely közvetlen hozzáférést biztosít a belső rendszerekhez, és amelynek védelmi szintje hasonló a munkahelyen használt, szintén vállalati számítógépekéhez) a távoli munkavégzéshez. Az alkalmazottak tehát saját eszközeiket használják a kiszolgálók távoli eléréséhez, és mindezt legtöbbször egy privát wifihálózaton hajtják végre. Ezek a személyes végpontok

(laptopok, táblagépek, számítógépek) és az otthoni vezeték nélküli kapcsolatok potenciális támadási célpontok a kiberbűnözők számára, amennyiben nem alakították ki a megfelelő biztonságot.[51] További kockázattal jár az olyan távoli munkavégzés, amikor a munkavállaló valamilyen publikus helyen, például kávézóban vagy vonaton dolgozik. Ekkor olyan hálózatok szolgáltatását veheti igénybe, amelyek nem megfelelően védettek, és fennáll annak a lehetősége, hogy a kommunikáció során továbbított adatokat illetéktelen személyek megismerhetik és módosíthatják.

Az otthoni munkavégzés lélektani hatásai

Az otthoni munkavégzés során a munkavállalók nehezen tudják elkülöníteni a munkát a magánélettől, hiszen az életterük egyben az irodájuk is. Így gyakran elfelejtenek szünetet tartani, vagy munkájukat nem a megszokott napszakokban végzik, sokszor túlórával. Ezáltal fáradtabbak és dekoncentráltabbak lesznek, aminek egyik feltételezhető következménye, hogy kevésbé figyelnek arra, mikor mire kattintanak. Ez a tényező nagyban elősegíti a trükköscsalás-alapú, ún. *social engineering* támadások sikerességét. Ezek során az elkövetők nem a technológiai sebezhetőséget használják ki, hanem az emberi befolyásolhatóság a fő fegyverük, erről a *Trükkös csalás* című alfejezetben lehet bővebben olvasni. Hasonló ehhez az adathalászat, amely szintén az emberi tulajdonságokra – például a kíváncsiságra – alapoz, és amelyről az *Adathalászat* című alfejezetben részletesebben lesz szó.

Egy másik kedvelt támadási forma a zsarolóvírus, vagyis olyan rosszindulatú programok használata, amelyekkel a támadók a megfertőzött eszközt lezárják, ezzel elérhetetlenné téve az áldozat adatait. Az egyik legnagyobb kockázat a zsarolóvírus-támadások elmúlt években tapasztalható növekedése, ami jelenleg komoly problémát jelent a vállalkozások számára.[52] Ha a távmunkában dolgozó alkalmazottak nem szabványos e-mail-, üzenetkezelő vagy fájlmegosztó rendszereket használnak (például az adatokat elküldhetik privát levelezési fiókjukról vagy a Microsoft Teams helyett a Viberen), amelyek nem tudják megfelelően

[51] Seymour 2020.

[52] A legutóbbi ilyen, nagy kiterjedésű támadást az Európában piacvezető elektronikai kiskereskedelmi áruházlánc, a Media Markt szenvedte el, ami Magyarország mellett Németországban és Hollandiában is súlyos zavarokat okozott a szolgáltatások nyújtásában.

kiszűrni a fenyegetést hordozó e-maileket és állományokat, akkor teret engednek olyan veszélyeknek, amelyek az egész vállalatot akár meg is béníthatják, vagy hatalmas anyagi károkat okozhatnak.[53] Az Interpol felmérésére válaszoló tagországok körülbelül kétharmada számolt be arról, hogy a járvány kitörése óta a Covid–19-cel kapcsolatos témákat jelentős mértékben használják adathalászatra és más online csalásra.[54] Ilyen például a kétes linkekre való kattintás és a rosszindulatú programokkal fertőzött mellékletek vagy alkalmazások letöltése.[55]

Meg kell említeni a fizikai értelemben vett kockázatokat is, például a lopást vagy a rongálást. Mivel a távmunka során az eszközeinket magunkkal hordjuk olyan publikus helyeken, mint tömegközlekedés vagy közterületek, fennáll annak a veszélye, hogy elveszítjük vagy eltulajdonítják azokat, így a rajtuk lévő adatokat is. Ha nem áll megfelelő védelem alatt az eszközön tárolt adat, akkor ennek ellopása hatalmas kárt tud okozni a szervezetnek. Fennáll annak a veszélye is, hogy a munkavállaló fizikai beavatkozást hajt végre az eszközén, amivel egy hibát, sérülést akar kijavítani, ám ezzel ismeretlen forrásból származó komponenseket épít be a vállalati eszközbe, amelyek befolyásolhatják annak működését. A szaktudás hiányában elkezdett javítások miatt az eszközön tárolt adatok meghibásodhatnak vagy elérhetetlenné válnak. Mindezek érinthetik az üzletmenetet támogató állományokat is, amelyek kiesése zavart okozhat a vállalat működésében.

Lehetséges kockázatcsökkentő intézkedések

Ahhoz, hogy egy szervezet a távoli munkavégzés során felmerülő összes kockázatot meghatározza, értékelje, majd, ha szükséges, kezelje, egy olyan keretrendszert kell használni, amely nemzetközi szabványokon és jó gyakorlatokon alapul. Ennek kialakításához nyújt segítséget az NIST Special Publication 800-46 szabvány, amely útmutató a vállalati távmunkához, a távoli hozzáféréshez és a BYOD biztonságos alkalmazásához. Érdemes kiemelni emellett a Magyar Nemzeti Bank 12/2020. (XI. 6.) számú ajánlását is a témával kapcsolatosan, amely a távmunka és távoli hozzáférés informatikai biztonsági követelményeit ismerteti. Fontos hangsúlyozni, hogy kellően részletes, mindent lefedő szabályozás kialakítására

[53] Curran 2020: 11–12.
[54] *Interpol Report Shows Alarming Rate of Cyberattacks During COVID-19* 2020.
[55] Adelmann–Gaidosch [é. n.].

kell törekedni a szervezeteknél, akármelyik iránymutatást veszik is alapul. Meg kell határozni például azt, hogy a távmunkát hol engedélyezett és hol tiltott végezni. A következőkben olyan alapvető kockázatcsökkentő lépéseket mutatunk be, amelyek a fent említett dokumentumon alapulnak, és fő céljuk, hogy az előző pontokban ismertetett fenyegetések valószínűségét csökkentsék.

Online értekezletek

Az ún. telekonferenciákat az ideálisan szabályozott információbiztonsági irányítási rendszerrel rendelkező vállalatoknál – a kizárólagosság elvét szigorúan betartva – csak az általuk támogatott felületen lehet lebonyolítani, és óvni kell az illetéktelen hozzáféréstől. Törekedni kell arra, hogy minden szervezetnél legyen legalább egy, a célnak megfelelően kiválasztott, biztonsági és funkcionális értelemben tesztelt és karbantartott alkalmazás, amelyet ebből a célból priorálnak. Tekintettel arra, hogy a munkavállalók nagy mennyiségű érzékeny információt továbbítanak és osztanak meg a telekonferencia alkalmával, a megfelelő szintű információbiztonság garantálása szempontjából elengedhetetlen a sebezhetőség felmérése és a használat körülményeinek eljárásrendszerű meghatározása az ilyen alkalmazások tömeges használata előtt. Ennek megfelelően a telekonferencia résztvevőinek mind technikai, mind eljárási eszközökkel hitelesíteniük kell magukat, hogy ténylegesen jogosultak részt venni az adott megbeszélésen. Fontos továbbá szabályozni azon eseteket is, amikor az adott felület rendelkezésre állása akadályokba ütközik (például akadozik, megszűnik). A szabályozásnak biztosítania kell annak megakadályozását, hogy a munkavállaló önhatalmúlag egy nem biztonságos platformot használjon.

A kritikus folyamatok biztosítása

A távoli munkavégzés biztonságának szavatolása érdekében a vállalatoknak további biztonsági ellenőrzéseket kell bevezetniük azokhoz a kritikus funkciókhoz, amelyek általában nem működnek távolról. Például az ilyen tevékenységeket végző felhasználók csak olyan, a cég tulajdonában lévő és általa ellenőrzött eszközökkel csatlakozhatnak, amelyeket állandóan frissítettek, és magas szintű biztonsági konfigurációval láttak el. Ezenfelül az ilyen folyamatok esetében érzékeny adatokat nem szabad lokálisan tárolni, hanem olyan, a vállalat által

üzemeltetett és biztosított környezetben kell elhelyezni őket, amelyben az adott munkavállalónak igen korlátozott jogosultsága van, és ahonnan bármikor kitiltható (ilyen megoldás például a fájlszerver vagy felhőszolgáltatás használata).[56]

A kérdőív és az interjúk eredménye az otthoni munkavégzés relációjában

A kitöltött kérdőívek és az interjúk kielemzéséből megállapítható, hogy a munkavégzés céljából kapott eszközöket a megkérdezettek – szervezeti hovatartozástól függetlenül – kevésbé használják hasonló vagy ugyanolyan módon, mint a sajátjukat. Azzal viszont majdnem mindannyian tisztában vannak, hogy a munkára kapott eszköz saját célú használata kockázatot jelent a szervezetre nézve. Összességében kijelenthető a válaszok alapján, hogy a kitöltők támogatják az olyan korlátozások bevezetését, amelyek megszabják, a munkavégzésre kapott eszközöket magáncélra meddig/milyen módon szabad használni.

Összegzés

Összegezve elmondható, hogy számos kiberbiztonsági kihívás jelenik meg a távoli munkavégzés témakörében, és e fenyegetések a pandémia alatt még nagyobb kockázati értéket hordoznak a szervezetekre nézve. Azonban már megjelent számos ajánlás, jó gyakorlat, amellyel biztonságossá tehető a távmunka. Az empirikus felmérésből leszűrhető, hogy a munkavállalók el tudják különíteni a vállalati és magáncélú eszközfelhasználást, továbbá támogatják azt, hogy csak korlátozásokkal tudják a céges erőforrásokat felhasználni. Ebből látható, hogy tisztában vannak a magáncélú felhasználás számos kockázatával.

3.2.4. Infokommunikációs eszközök használata

Arról már volt szó a korábbi fejezetekben, hogy mennyire általánossá vált az infokommunikációs technológiák vagy eszközök[57] (IKT vagy IKT-eszközök) használata a mindennapok során. Az emberek elektronikus eszközök segítségével

[56] Souppaya–Scarfone 2016; A Magyar Nemzeti Bank 12/2020. (XI. 6.) számú ajánlása.
[57] Másképpen: információs és kommunikációs technológiák.

végzik a munkájukat, kommunikálnak egymással, és már a kikapcsolódáshoz is aktívan igénybe veszik azokat. Fontos azonban tudnunk, hogy pontosan mit értünk infokommunikációs eszközök alatt, és milyen kihívásokkal nézünk szembe a használatuk során. Ezzel kapcsolatos a következő tanulmányrész.

Az IKT-eszközök halmazába sorolunk minden olyan technológiát és alkalmazást, amellyel bármilyen szinten (egyéni, állami, vállalati) minőség- és hatékonyságjavulás (és/vagy eredményességjavulás) érhető el.[58] Az emberek életében betöltött szerepükre példaként (erről még lesz szó a későbbiekben) többek között a számítógépeket, telefonokat, számviteli/ügyviteli rendszereket vagy bármely egyéb információs rendszert lehetne említeni. Az IKT-t különböző megközelítés szerint lehet hívni eszköznek, automata vagy szervezési technikának, esetleg fejlesztési és társadalomalakító folyamatnak is, tehát értelmezése sokrétű.

Napjaink gyakorlatában ez úgy néz ki, hogy videót vagy fotót készítünk az okostelefonunkkal, interaktív táblán békát boncolunk az iskolában, Facebookon megosztjuk egy bevált csokis süti receptjének linkjét, vagy a Microsoft Wordben megírjuk a tanulmányunk egy részét, és kinyomtatjuk, hogy lefekvés előtt átolvashassuk. Küldünk egy e-mailt az irodába, este pedig otthon a családdal megnézünk egy filmet, amelyet projektorral kivetítünk a falra a jobb moziélmény kedvéért. Milyen tevékenység hangzott el az összes példával kapcsolatban? Az IKT-eszköz-használat, amely a mindennapjainkban körülvesz bennünket.

Nem elegendő azonban ismerni az infokommunikációs eszközök jelentését és használatuk természetességét, célszerű átlátni, hogy milyen csoportokba sorolhatjuk őket, kiemelten egy vállalat szempontjából. Ennek alapján megkülönböztetünk:

- mobilkommunikációs eszközöket;
- webkamerát;
- tableteszközöket;
- interaktív táblákat;
- számítógépeket.[59]

[58] Lengyelné molnár – Kis-Tóth 2015.

[59] Nádasi–Racskó 2013: 182.

A személyi számítógép történetét 1981-től számítjuk, ekkor minden megváltozott az emberek életében. A 90-es évek elejére már elterjedt a használata, majd a hálózatra történő csatlakozás is, és aztán nem volt megállás.[60] Napjainkban a vállalaton belüli IKT-eszközök alkalmazása nemcsak általánossá vált, de magukból az eszközökből is széles választék áll rendelkezésre a munkavállaló számára. A szervezeten belüli infokommunikációs eszközök használati szabályozásának kiemelkedően fontos szerepe van a biztonság megőrzésében. A biztonsági, jogi és technikai keretrendszer az alapja annak, hogy jogosulatlan személyek ne férjenek hozzá bizalmas adatokhoz, a különféle házirendek (például Felhasználói informatikai biztonsági házirend) pedig segítik a munkavállalót, hogy az információvédelem és az informatikai infrastruktúra biztonságos működésének fenntartása a közvetlen közreműködésével megvalósulhasson.[61] Mindehhez a vonatkozó szabályozókban meg kell határozni az eszközök biztonságos használatának módját, az incidensek bekövetkezésekor végrehajtandó cselekvéseket, illetve a szankciókat a szabályok megszegése esetére.

A veszélyekre kitérve az IKT-eszközök kapcsán beszélhetünk a már említett, különféle adathalászmódszerekről[62], de akár a trükkös csalásokról[63] vagy a 2020 óta tartó járványhelyzet miatt elterjedt otthoni munkavégzés következtében megnövekedett számú, különböző zsarolóvírus (ransomware)-,[64] rosszindulatúszoftver (malware)-[65] és spamtámadásokról, illetve a szolgáltatásokat célzó hackertevékenységekről is.[66] A távoli munkavégzés[67] kapcsán pedig meg kell említenünk az IKT-eszköz-használat szabályaiban gyakran tapasztalható bizonytalanságot, hiányosságokat. Utaltunk már arra, hogy egy szervezet életében nem mindegy, hogy a munkavállaló a távoli munkavégzés során a saját, a vállalati vagy mindkét eszközét használja

[60] Adelmann–Gaidosch [é. n.].
[61] Nádasi–Racskó 2013: 182.
[62] Lásd az *Adathalászat* című alfejezetet.
[63] Lásd a *Trükkös csalás* című alfejezetet.
[64] Ransomware: kártékony szoftver, amely tömören fenyegetéssel csal ki valamilyen értéket (legtöbbször pénzt) a felhasználóktól.
[65] Malware: kártevő szoftver, a rosszindulatú számítógépes programok összefoglaló neve.
[66] *Remote Work Monitoring.*
[67] Lásd *A közösségi média használata* című alfejezet.

feladatainak ellátásához. Tehát a már sokszor említett biztonsági kultúra kialakítása során gondolni kell a hatékony autentikációra, az internetcsatlakozás körülményeire (például nem ajánlott a nyílt wifihálózatra kapcsolódni), a felhőalapú szolgáltatásokra, a belső hálózatra való csatlakozásra, illetve az eszközökön megtalálható biztonsági szoftverekre egyaránt. Ha az alkalmazott mind a saját, mind a vállalati eszközét használja a munkavégzés során, ez a megosztottság sok kockázatot rejt magában. A fenyegetettségek ismeretében célszerű megfogadni bizonyos védelmi ajánlásokat. Többek között ilyen az, hogy valósuljon meg:

- a szoftverek és a rendszer naprakészen tartása;
- a jelszavak folyamatos frissítése;
- a csak jogtiszta tartalmú, megbízható fájlok letöltésének engedélyezése;
- a kétfaktoros autentikáció;[68]
- a dedikált felhasználói fiók léte (amennyiben többen használják a gépet).

A fent említett veszélyek legtöbbje megfelelő tudatossággal kezelhető. Aki tudatos, az a jogtiszta, folyamatosan naprakészen tartott szoftvereket alkalmazza, felelősségteljesen használja az eszközeit, és – hacsak nem feltétlenül szükséges – nem adja át azokat másnak. Továbbá nem kattint gyanús linkekre és nem csatlakozik ismeretlen hálózatokra, összességében tehát az infokommunikációs eszközök használatára vonatkozó szabályokat munkavállalóhoz méltón betartja. Mindezek mellett természetesen bekövetkezhetnek incidensek, hiszen a 100%-os védelem nem garantálható, de ezek könnyebben kezelhetők az előbb ismertetett szabályokat betartó környezetben, mint akkor, ha valaki felelőtlen az IKT-használat és a munkavégzés egyéb területén.

Hasznos gyakorlati megvalósítási lehetőségek

A korábbiakban már említettük, hogy kockázatokat rejt magában az, ha a munkavállaló a saját és vállalati eszközét egyszerre használja munkavégzésre. Fenyegetettséget jelent például az, hogy a saját eszköz alkalmazása közben csökken a figyelem és a védelmi felkészültség (például a nyitva hagyott, bekapcsolt laptop), ugyanis a felhasználó alapvetően biztonságban érzi magát, ha a saját eszközén dolgozik.

[68] *Remote Work Monitoring.*

Fontos, hogy el tudjuk választani az IKT-eszközök használatának módját és célját, illetve hogy mindig körültekintően járjunk el alkalmazásuk során. Ehhez kapcsolódóan egy általános példának tekinthető, hogy ne a vállalati telefonon intézzük ételrendeléseinket, webes felületen pedig ne a céghez köthető e-mail-címünket adjuk meg ilyen célból, akkor se, ha a munkahelyünkre rendelünk. Az sem mindegy, hogy magánügyeinket hogyan, illetve hol intézzük, ugyanis nem célszerű a szervezettől munkavégzés céljából kapott laptopon bonyolítani ezeket. Egyrészt azért, mert biztonsági kockázattal jár, másrészről eredményeképpen bizalomvesztést is tapasztalhatunk a munkatársak, a felettesünk részéről. Ezek elkerülése érdekében ajánlatos a munkahelyi eszközt csak különösen indokolt esetben saját célokra használni. Az sem újdonság manapság, hogy a munkavállalók tömegközlekedési eszközökön (például többórás vonatúton) is végzik a munkájukat. Attól eltekintve, hogy saját vagy vállalati eszközről van-e szó, semmiképpen nem célszerű úgy dolgozni, hogy arra nem jogosult személyek is lássák az eszközön történő tevékenységeket és folyamatokat. Tehát vagy válasszunk védettebb helyet, ha erre van lehetőség, vagy halasszuk el a munkát, hiszen fontosabb a biztonság, mint egy megspórolt fél óra.

Az IKT-eszközök használatakor nem lehet elégszer hangsúlyozni, hogy a szabályzatok elkészítése és oktatása mellett elengedhetetlen a tanultak gyakorlatba történő átültetése. Itt jelenhetnek meg a gyakorlati, mint például az eszközhasználatra vonatkozó, személyes tapasztalatra épülő képzések vagy egy-egy IKT-eszközhöz kapcsolódó incidens bekövetkezésének, esetleg a humán alapú támadásokról szóló esettanulmánynak a szimulációja.

A kérdőív és az interjúk eredménye az IKT-eszközök használatának relációjában

A vizsgált vállalatoknál eltérések mutatkoznak az eszközhasználat területén. Egyes szervezeteknél munkacélra szigorúan csak a cég által biztosított eszközt szabad használni, míg másoknál, bár ugyanilyen körülmények uralkodnak a munkavégzés során, technikailag saját eszközt is igénybe lehet venni. Fordítva viszont előfordulhat, vagyis a munkavállalók használhatják magáncélra a munkavégzésre kapott eszközt, de csak szigorított feltételekkel, például a gép korlátozza bizonyos oldalak látogatását. Ezzel együtt a szervezetek egyetemlegesen tartják magukat ahhoz, hogy válasszuk ketté a magánügyeket és a munkavégzést, így ehhez meg is teremtik a megfelelő körülményeket.

A munkavállalók részére bocsátott vállalati IKT-eszközökre információvédelmi megoldásokat is alkalmaznak a vizsgált szervezetek. Ilyen például a saját belső hálózat használata, adott weboldalak blokkolása, vírusvédelmi rendszer, tűzfal, sandbox,[69] DLP[70] monitorozó rendszer. Nemcsak a számítógépre telepítenek védelmi rendszereket, ugyanolyan fontos, hogy a mobilkészülékek és a rajtuk tárolt adatok is biztonságban legyenek. A kérdőívek eredményéből kiderül, hogy a munkavállalók – intézménytől függetlenül – kockázatosnak ítélték meg az IKT-eszközökön használt szoftverek és hardverek régebbi verzióit, továbbá a talált ismeretlen pendrive-hoz kapcsolódó magatartásuk is biztonságtudatosságról árulkodik.

Fontos megjegyezni a biztonságtudatossághoz kapcsolódó oktatás eredményének kérdőívből is kinyerhető következtetéseit, ugyanis a munkavállalók által adott válaszok alapján azok, akik az utóbbi két évben részt vettek információbiztonsággal kapcsolatos képzésen, sokkal óvatosabbak. Abból is látszik ez, hogy a munkaeszközök saját célú használatát a kitöltők elég nagy része – több mint 7%-a – korlátozná a kockázatok miatt.

Összegzés

Összességében elmondható, hogy napjainkra az infokommunikációs technológiák használatát illetően kialakult egyfajta kultúra, de a kapcsolódó kockázatok kezelésére még most sem vagyunk eléggé felkészültek, annak ellenére, hogy viszonylag régóta az életünk részei ezek az eszközök. Használjuk őket a közlekedési járműveken, otthon, a munkahelyen, hol magánügyek intézése, hol pedig munkavégzés céljából. Az átlag munkavállalók nagy része nem törődik azzal, hogy ki látja a képernyőt, ki tudja megszerezni fájljait a nyílt wifin keresztül, esetleg ki tud odamenni a géphez vagy a nem zárolt laptophoz, amíg annak jogos tulajdonosa/használója nincs a közelben.

A vizsgált vállalatok mindegyike fontosnak tartja a biztonságtudatosságot az IKT-eszközök használatakor. Ennek eredménye egyértelműen látszik,

[69] Sandbox: a homokozónak is nevezhető biztonsági mechanizmus azért hasznos, mert olyan programokat tudunk vele futtatni, amelyek ellenőrizetlen gyártóktól származnak, vagy amelyeket nem megbízhatónak tituláltak.

[70] Data loss prevention: adatszivárgás-megelőzés.

hiszen az incidensek bekövetkezési valószínűsége ehhez köthető mulasztások miatt – kutatásunk alapján – kimondottan alacsony.

3.2.5. A közösségi média használata

Napjainkra a hétköznapi életünk részévé váltak a közösségi oldalak, emiatt kortól, nemtől, munkahelytől függetlenül mindenkit érint az általuk generált sérülékenység is. Az innen érkező támadások is jellemzőek manapság, ezért fontos hangsúlyozni azokat a magatartásformákat, amelyek révén a közösségimédia-használatból eredő kockázatok csökkenthetőek. A következő rész azt a célt szolgálja, hogy egyértelműen értelmezhető legyen a közösségi média mint fogalom, illetve az általa jelentett veszélyek. Elsőként tisztázni kell, hogy mit is nevezünk közösségi médiának. Tulajdonképpen a web 2.0[71] azon képességét értjük ez alatt, amely lehetőséget teremt az online tartalommegosztásra és együttműködésre.[72] Ezen belül a közösségi oldalak olyan „virtuális közösségek, ahol a felhasználók egyedi nyilvános profilokat készíthetnek, kapcsolatba léphetnek a valós barátokkal és más emberekkel találkozhatnak, például a közös érdeklődési körük alapján".[73] Ilyenkor még az sem fontos, hogy személyesen ismerjük az illetőt, hisz online kapcsolatteremtésre is lehetőségünk van. A közeg fontos tulajdonsága a felhasználók aktív részvétele, a folytonos interakció.[74] A legnépszerűbb közösségi oldal a nagyjából 2,7 milliárd aktív felhasználójával továbbra is a Facebook, amelyet a YouTube (2 milliárd) és a WhatsApp (2 milliárd) követ.[75]

A közösségi média veszélyei

A közösségi médiának számos előnye, pozitív hatása van. Megkönnyíti a kapcsolattartást, az információ megosztását, lehetőséget teremt, hogy kapcsolatokat építsünk *(networking).* Általa óriási információbázist érhetünk el csupán pár

[71] A web 2.0 a világháló jelenlegi állapotát jelenti, amelyben a tartalomgyártók nagyobb részt már maguk a felhasználók, ellenben a web 1.0-val. Nem technológiai változásról van szó, hanem ez csupán az internet használati módjának átalakulására utal. PETERS 2021.

[72] KUSS–GRIFFITHS 2017: 311.

[73] KUSS–GRIFFITHS 2017: 311. Az idézet a szerzők fordítása.

[74] MANNING 2014: 1158–1162.

[75] YOUNGBLOOD 2020.

kattintással. Felületeit használhatjuk önreklámozásra vagy az „énmárka" építésére *(self-branding),* fejlesztésére is, megoszthatjuk másokkal gondolatainkat, életünk, személyiségünk bármely szegmensét. Ám tagadhatatlan előnyei mellett számos negatív hatást, veszélyt is rejt, amelyet érdemes figyelembe venni, és ennek megfelelően minél tudatosabb felhasználóként viselkedni.

Számtalan tanulmányban rámutattak már arra, hogy kapcsolat van a közösségimédia-használat és a depresszió, magány, rossz alvásminőség és szorongás között.[76] Ráadásul ezeket a felületeket kifejezetten úgy fejlesztették ki, hogy minél több időt töltsünk a képernyő előtt (például értesítések, jutalmazó rendszerek stb.). Ezt segíti továbbá, hogy olyan algoritmusokat is kifejlesztenek, amelyek figyelik online tevékenységünket, és aszerint személyre szabják a nekünk megjelenő híreket, hirdetéseket. Ezzel azonban egyfajta „buborékba" zárnak minket mint felhasználókat, hiszen egy idő után nem találkozunk ellenvéleménnyel, és kialakul körülöttünk egy alternatív valóság. Ez különösen fel tudja gyorsítani az álhírek[77] terjedését, hisz a megosztások révén olyan emberekhez fog elérni az információ, akik az adott témában érdekeltek, anélkül hogy az ezeket cáfoló tartalmak előfordulnának a hírfolyamban. Mindez szintén komoly veszélyforrása a közösségi médiának. Ugyanakkor – különösen a bejegyzések kommentszekciójában – kiberagresszió, online zaklatás áldozatává is válhatunk, de veszélyt jelenthet az is, ha túl sok információt osztunk meg magunkról, mert ez sebezhetővé tesz minket a számos támadási formát használó kiberbűnözőkkel szemben.

Hasznos tippek a tudatos felhasználáshoz

Ahhoz, hogy a felmerülő veszélyek mértékét csökkentsük, érdemes néhány tanácsot megfogadni a közösségi oldalak használatával kapcsolatban:

1. Megfontoltan posztoljunk! A legfontosabb, hogy kellő figyelemmel és óvatossággal kezeljük, mit osztunk meg magunkról, a munkahelyünkről, illetve milyen tartalmakat továbbítunk privát üzenetben. Egy rólunk készült, ártatlannak tűnő kép is hordozhat olyan információkat (például nem publikus, számunkra értékes információt tartalmazó post-it

[76] Lis 2020.

[77] Az álhírek *(fake news)* szándékosan és igazolhatóan hamis hírek, amelyek célja a megtévesztés. Lim 2020.

a háttérben a parafa táblán), amelyeket felhasználhatnak ellenünk. Nem szabad figyelmen kívül hagyni a tényt, hogy az általunk megosztott tartalmak még tíz év múlva is előkerülhetnek, akár kellemetlen pillanatokat okozva nekünk. Fontos továbbá tisztában lenni azzal, hogy a közösségimédia-oldalak azokról is rengeteg információt gyűjtenek, akik sosem regisztráltak a felületre.[78]

2. Ne kattintsunk gyanús linkre! Legyünk mindig kritikusak az ismeretlen e-mail-címről vagy telefonszámról érkező üzenetekkel. Ha adataink megadására, alkalmazás letöltésére kérnek, mindig érdeklődjünk hivatalos csatornákon keresztül, applikációt pedig kizárólag Google Play áruházból/App Store-ból töltsünk le. Gyanús linkeket akár ismerőseinktől is kaphatunk, mert gyakran előfordul, hogy feltörik a gyenge jelszóval védett profilokat, amelyeket aztán adathalászoldalak linkjének továbbítására (poszt, privát üzenet, csoportos üzenet formájában) használnak. Ezeket könnyen álcázhatják ártatlan videómegosztó portáloknak, ismert oldalak bejelentkezési felületére hasonlító linkeknek is. Érdemes rákérdezni ismerősünknél, milyen tartalmat osztott meg, mielőtt rákattintunk.
3. Legyünk körültekintőek az átirányított oldalon történő bejelentkezés során! Mindig ügyeljünk arra, hogy a közösségimédia-felületre való belépés céljából a hivatalos oldalt látogassuk. Ha egy másik oldal irányított át minket a bejelentkezéshez, amennyiben lehet, ne éljünk a lehetőséggel. A támadók képesek a hivatalos oldallal szinte teljesen megegyező felületet létrehozni, amivel megtévesztik a felhasználót, és a bejelentkezést követően megszerzik a felhasználónevet és a jelszót.
4. Éljünk a privát mód beállításaival! Amennyiben van lehetőség rá, az ismerőslistánál állítsunk be privát megtekintést. A támadók információgyűjtés révén kapcsolatainkat (például *social engineering*[79] során) felhasználhatják az akció előkészítéséhez.
5. Alkalmazzunk széles körű biztonsági beállításokat! Állítsuk be, hogy a fényképeken csakis az engedélyünkkel jelölhessenek meg minket, ezzel elkerülve a nem kívánt tartalmak megosztását.

[78] Ingram 2018.

[79] A *social engineering* olyan technika, amely pszichológiai manipulációt, csalást vagy más tisztességtelen módszert használ arra, hogy az embereket személyes vagy vállalati információk nyilvánosságra hozatalára, illetve egy adott intézkedésre kényszerítse. Lásd: *Social Engineering* és a *Trükkös csalás* alfejezet.

6. Aktualizáljuk adatvédelmi beállításainkat! Figyeljünk oda ezekre, és rendszeresen vizsgáljuk felül őket, hisz időközben változhatnak (így ami eddig nem volt publikus tartalom, az azzá válhat). Számos lehetőségünk van már arra, hogy gondoskodjunk adataink biztonságáról, például célszerű beállítani a kétfaktoros hitelesítést (lásd *A biztonságos jelszó ismérvei* című alfejezetben), illetve azt is, hogy e-mailes értesítést kapjunk, ha idegen helyről, eszközről jelentkeznek be a profilunkba. Ezzel megnehezítjük, hogy feltörjék azt, és személyes üzenetváltásaink rossz kezekbe kerüljenek.
7. Mindig használjunk megfelelő erősségű jelszót![80]
8. Törekedjünk digitális lábnyomunk csökkentésére! Alkalmazzunk a privát szférát erősítő technológiákat (például anonimitást biztosító böngészők használata), mert így a digitális lábnyom jelentős csökkentése mellett védekezhetünk a techcégek már említett, felhasználókat érintő adatgyűjtése ellen is.

A kérdőív és interjúk eredménye a közösségimédia-használat relációjában

A kérdőíves felmérésünk a közösségimédia-használatra, ahhoz való viszonyulásra is kiterjedt. A kutatás során megállapítottuk, hogy van olyan partnerszervezet, ahol nagyobb az egyetértés azt illetően, hogy kirúghatják a munkavállalókat a közösségi médiában megosztott posztjuk miatt. Érdekes különbség figyelhető meg ugyanakkor a korosztályok között. A 18–25 évesek a többi csoporthoz képest másképp ítélték meg annak a kockázatát, hogy valaki a munkahelyéről posztol a közösségi oldalakon. A kitöltők 1-től 5-ig terjedő skálán 4,69-re, tehát igen valószínűnek értékelték ennek a kockázatát. Fontos hangsúlyozni ezzel kapcsolatban, hogy az ún. vélt biztonságtudatosság is befolyásoló tényezőként értelmezhető. Azon csoportok, akik biztonságtudatosnak tartják magukat adatvédelmi szempontból, illetve azok között, akik nem tudják, hogy azok-e, érdemi különbség mutatkozik arra vonatkozóan, hogy szerintük a munkahelyéről azt posztolhat-e valaki a közösségi médiára, amit csak akar. Ugyancsak e két tábor között figyelhető meg eltérés azon állítás kapcsán, hogy nincs jelentősége annak, ha valaki olyat posztol a közösségi médiában, amit nyilvánosan nem mondana ki. Ennek a kérdésnek a megítélését befolyásolja az, hogy az illető részt vett-e

[80] Részletek a *Jelszó* alfejezetben.

információbiztonsági képzésen, és az eredmények mind az ilyen oktatás szükségességét támasztják alá. Láthatóvá vált továbbá az is, hogy aki olvasta a szervezete informatikai biztonsági szabályzatának legfrissebb verzióját, másképp vélekedik arról, hogy kirúghatják a közösségi médiában megjelent posztjaiért.

Az interjúkból kiderült, hogy mindhárom szervezet segíti a munkavállalókat a közösségi média megfelelő használatában, főként képzésekkel, beleépítve ezt a biztonságtudatosító tananyagba, illetve hírlevelek formájában. Egyes vállalatok etikai kódexszel is rendelkeznek, amellyel általános iránymutatást adnak a tudatos felhasználáshoz. Néhány megkérdezett szakértő azonban úgy véli, van még mit tenni a biztonságtudatosság növelése érdekében, hisz nem olyan régen kezdtek el foglalkozni a közösségi médiával mint potenciális fenyegetéssel, illetve konkrét szabályozókat hiányolnak, amelyekben pontosan lefektetnék, hogy mit lehet és mit nem lehet posztolni.

Összegzés

A közösségi média olyan a 21. században, mint az alapvető szolgáltatások: észre sem vesszük, hogy az életünk része. A kutatásban közreműködő vállalatok felismerték az ebben rejlő biztonsági kockázatokat, és folyamatos képzéssel, tájékoztatással igyekeznek támogatni a munkavállalókat, de még így is tapasztalható hiányosság a felhasználói oldalról. Kiemelendő ugyanakkor, hogy ez a kockázat az oktatással, a jó gyakorlatok folyamatos hangsúlyozásával jelentősen csökkenthető.

3.2.6. Adathalászat

Meglátásunk szerint az eddigi alfejezetek alapján teljes mértékben helytálló kijelentés, hogy napjaink technológiaorientált társadalmában adataink védelme kiemelten fontos. Az előzőekben kifejtettük, milyen negatív és káros oldalai lehetnek a közösségi média alkalmazásának, amelyek nem utolsósorban az adathalászat kockázati tényezőit is nagymértékben növelni tudják. Az általunk széles körben használt portálok javarészt ingyenesek, ám a valóságban a szolgáltatók profitjukat adataink értékesítésével, illetve a reklámbevételekkel maximalizálják. Ez egy „belső munka" ugyan, amely mellett az oldalak üzemeltetői igyekeznek megvédeni minket a különböző „külső" támadóktól. Mégis szinte kivédhetetlen,

hogy valamilyen formában kapcsolatba kerüljünk az adathalászattal, amely a felhasználók hiszékenységét, figyelmetlenségét és sokszor leterheltségét kihasználva igyekszik rávenni a célpontokat bizonyos cselekmények elvégzésére. Az évről évre egyre nagyobb anyagi károkat okozó kiberbűnözés, ezen belül pedig az adathalászat mára az online élet minden szegmensébe beköltözött.[81] Éppen ezért elengedhetetlen, hogy ebben a tanulmányrészben annak gyakorlati aspektusán túl a védekezési lehetőségekkel is foglalkozzunk.

Az adathalászat definiálása igen nehéz feladat. Ennek oka, hogy számos megjelenési formája ismert, ezért egységes fogalomról nem beszélhetünk. Maga a szó a *password harvesting fishing,* azaz jelszóhalászás kifejezésből származik.[82] Olyan eljárást jelent, amelynek keretében internetes csalók különböző lehetőségeket kihasználva, látszólag ártatlannak tűnő módszerekkel személyes adatokat vagy pénzt próbálnak szerezni a gyanútlan felhasználóktól. Habár a csalók igen sokféle technikát alkalmaznak, leggyakrabban mégis e-mailekkel, esetleg SMS-alapú üzenetekkel veszik célba a felhasználókat, de tipikus elkövetési forma a megbízható webhelyek látszatát keltő oldalak üzemeltetése is. Napjainkra az adathalászat gyakorlatilag önálló iparággá nőtte ki magát, hiszen a begyűjtött adatokat megszámlálhatatlan formában tudják felhasználni és értékesíteni. Nem véletlen, hogy a 2019-es évben ez volt az egyik leginkább növekvő tendenciát mutató online támadástípus Magyarországon, az incidensek 23%-a tartozott ide.[83]

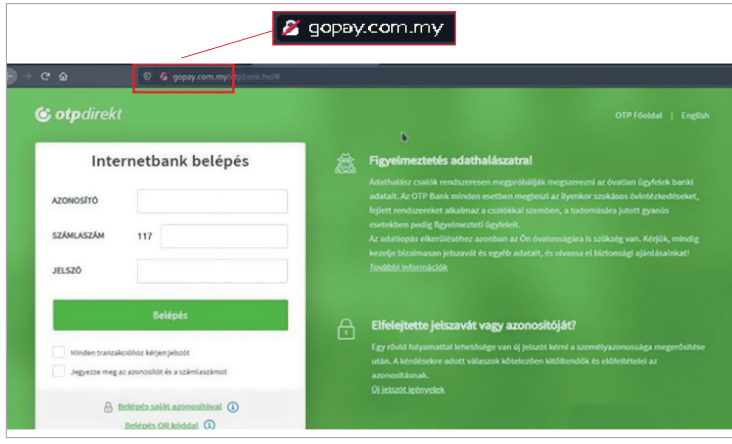
Az adathalászat formái

Az adathalász-támadások egyik leggyakoribb formája a cselekvésre késztető e-mail. A csalók nemritkán valamilyen közbizalmat élvező vállalatnak vagy szolgáltatónak adják ki magukat. Ezeknek a leveleknek a célja az, hogy a címzett letöltse a mellékletet, amely révén valamilyen káros programot juttatnak az infokommunikációs eszközére, illetve az általa használt hálózatba, vagy kattintson rá a csatolt weblapra, ahol megadhatja személyes adatait. Az utóbbi esetben ezek az oldalak közel sem a felhasználó által vélelmezett eredeti honlapok.[84]

[81] Kovács 2018: 124–125.
[82] Muha–Krasznay 2018: 57–58.
[83] ORFK Kommunikációs Szolgálat 2020.
[84] ORFK Kommunikációs Szolgálat 2018.

A csalók tipikusan a közismert szolgáltatók internetes belépési oldalainak látszó felületekkel próbálnak a felhasználók bizalmába férkőzni, amelyek valójában a támadók által üzemeltetett weblapok az eredeti honlap logójával, arculati elemeivel, az 1. ábrán is látható módon.

Az OTP Bank valós internetbanki szolgáltatására épülő felület, valamint a fenti ábrán látható adathalász-weboldal között csupán az URL-cím mutat különbséget. A hasonlóság azonban pont elég arra, hogy a gyanútlan felhasználó hajlandó legyen megadni a kért adatokat (személyes vagy banki, illetve egyéb azonosításhoz használt adatok), és ezt követően azok máris hozzáférhetővé válnak a csalók számára, amiről a becsapott személyek valószínűleg egyáltalán nem, vagy csak jóval később szereznek tudomást.



1. ábra: Adathalászoldal
Forrás: www.otpbank.hu

Szintén tipikus módszer a mobiltelefonon, SMS-ben történő adathalászat *(smishing),* amely gyakorlatilag megegyezik az e-mailes verzióval. A különbség abban rejlik, hogy a megnyitásra szánt mellékletek mobiltelefonon érkeznek, nem e-mailben. Ennek azért van kiemelt jelentősége, mert míg az e-mailes átverésekkel sokan tisztában lehetnek, a „régi és elavult" SMS-re kevésbé gyanakodnánk.

Egy következő szint az ún. szigonyozás *(spear phishing),* amely egy-egy kiválasztott személy ellen irányul, ellentétben az e-maillel és SMS-sel, ahol a célközönség nagyobb tömeg. A csalók ez esetben munkatársként, partnerként

vagy más hasonló formában keresik fel a felhasználót, hogy érzékeny adatokat kérjenek tőle.[85] Ez azért lehet veszélyesebb, mert a csalók névre szólóan, személyes jelleggel veszik fel a kapcsolatot az áldozattal, ezáltal sokkal bizalmasabb körülményeket teremtve. Minél hivatalosabb vagy személyesebb a levél, annál nagyobb eséllyel lesz sikeres az adatszerzés.

Ismert kategória a hangalapú adathalászat (*voice phishing* vagy *vishing*) is,[86] amely főleg VoIP-csatornán keresztül terjed. A módszert az a bankok által közzétett javaslat ihlette, hogy ha az ügyfél gyanúsnak tartja a banki értesítőt, akkor telefonon bizonyosodjon meg róla, hogy az üzenet tartalma valóban hiteles-e. Ilyenkor az adathalászok tömeges tárcsázást hajtanak végre, és ha valaki felveszi a telefont, azt állítják, hogy valamilyen gond van a számlájával, ezért egy megadott telefonszámon érdeklődjön a további teendőkről. A gyanútlan áldozat ha felhívja a számot, és megadja az azonosításhoz szükséges adatait, máris támadás áldozatává vált.[87] E módszer kevésbé ismert, mint a fentebb taglaltak, éppen ezért meglehetősen sikeresnek mondható.

Nem ritka a „bálnavadászat" *(whaling)* jelensége sem. Az elnevezés onnan származik, hogy ezen akciók célpontja az egyes vállalatok felső vezetői köre. Az ilyen üzenetek rendszerint valamilyen partner nevében érkeznek, és céljuk a támadási stratégiától függetlenül igen változó lehet, leggyakrabban azonban megegyezik a már leírt tényezőkkel.

Végül szót kell ejteni a közbeékelődéses támadásról *(man-in-the-middle attack).* E módszer lényege, hogy a támadó úgy hallgatja le a felek közti kommunikációt, hogy a csatornát eltérítve mindkettőjük számára a másik félnek adja ki magát, ezáltal a felek azt hiszik, a másikkal beszélnek, valójában viszont a csalóval, aki így minden adathoz hozzáfér.[88]

„Megérkezett a csomagja" – FluBot-esettanulmány

2021. március második felében jelent meg Magyarországon a FluBot nevű kártékony program, amely pénzügyi adatok ellopásával került be a köztudatba.

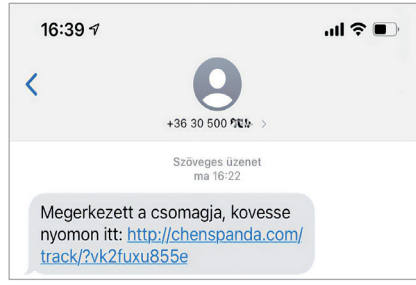
[85] Pšenáková 2020: 56–58.

[86] A beszélgetés ebben az esetben nem hagyományos telefonos hálózaton, hanem az interneten vagy esetleg más IP-alapú adathálózaton keresztül történik.

[87] Muha–Krasznay 2018: 57.

[88] Kovács 2013: 201.

Az érintettek egy futárcég oldalához hasonlító honlapra mutató linket kaptak SMS-ben, amelyre kattintva „csomagkövető” alkalmazást lehet letölteni és telepíteni. Az SMS a 2. ábrán látható módon jelent meg a felhasználók készülékén.



2. ábra: Malware által küldött üzenet
Forrás: https://kiber.blog.hu/

Amennyiben a címzett végrehajtja az üzenetben leírtakat, a készüléke megfertőződik. Az így telepített *malware* folyamatosan monitorozza a futtatott alkalmazásokat, és ha pénzügyi, esetleg kriptovalutához kapcsolódó tevékenységet észlel, akcióba lendül: begyűjti a pénzügyi szolgáltatásokhoz használt azonosítókat a csalók számára, sőt, a megfertőzött készülékről akár több ezer ilyen SMS-t is elküldhet, ezáltal jelentős kárt okozva az érintetteknek.[89] Ezt úgy tudja megtenni, hogy a telefonkönyvben lévő számokat ellopja és egy adatbázishoz rendeli, majd olyan címzetteknek küld SMS-t a készülék gazdájának nevében, akik nem is szerepelnek az áldozat kontaktjai között. Mindezeken túl a csalók hozzáférést szereznek az SMS-ek tartalmához, ami azért is különösen kockázatos, mert észlelik a lemásolt pénzügyi szolgáltató alkalmazását a telefonokon: ha a felhasználó megnyitja az adott applikációt, akkor valójában az adathalász-alkalmazás indul el. Ezen a ponton nyer igazán értelmet az SMS kérdése, hiszen ha a kétfaktoros hitelesítés[90] arra van beállítva, akkor a csalók akár a fiókba is könnyedén bejuthatnak.

[89] Nemzeti Kibervédelmi Intézet 2021.

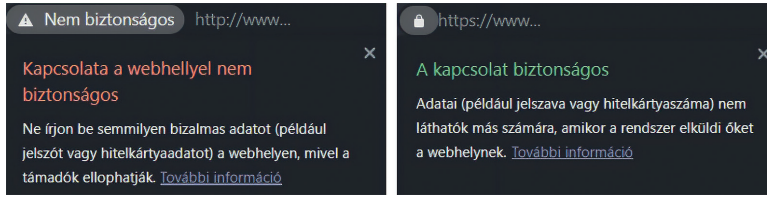
[90] A kétfaktoros hitelesítés *(two-factor authentication)* olyan biztonsági funkció, amely a bejelentkezési kísérlet megerősítéséhez szükséges. Azon túl, hogy a felhasználó megadja bejelentkezési adatait, a fiókhoz való hozzáférés érdekében szükséges egy belépőkód beírása is, amelyet leggyakrabban SMS, e-mail, esetleg valamilyen alkalmazás formájában lehet igényelni.

A FluBot adathalász-tevékenysége pusztán a felhasználók figyelmessége és tudatossága révén kivédhető. Sajnos saját környezetünkben is tapasztaltuk, hogy többen annak ellenére kattintottak a weblapra, hogy nem, vagy nem az SMS feladójától vártak csomagot, de az ismeretlen alkalmazás letöltésére és telepítésére vonatkozó kérés sem riasztotta vissza őket.

Védekezési lehetőségek, prevenció

Néhány általános szabályt betartva jó eséllyel felismerhető, ha adathalász-tevékenységgel állunk szemben. Hangsúlyozzuk, hogy a bankok vagy közszolgáltatók e-mailben vagy SMS-ben soha nem kérnek személyes vagy belépési adatokat, így ezeket semmiképp nem szabad megadni egy levélben érkező linkre kattintva.

Kifejezetten fontos a biztonságos weblapok használata is. Ezzel kapcsolatosan megemlítendőek az adatok továbbításáért felelős http és https protokollok. A https a TSL *(Transport Layer Security)* vagy az SSL *(Secure Sockets Layer)* titkosítótanúsítványra épül, amely arra szolgál, hogy a weboldalon megadott adatok titkosított csatornán juthassanak el a szerverhez. Ezeket az adatokat csak a megcélzott webszerver képes lefordítani, ez biztosítja, hogy azok ne kerüljenek illetéktelenek kezébe. Ha idegen, vagyis „nem biztonságos" (http) jelölésű weboldalra látogatunk, gondoljuk végig, hogy feltétlenül meg szeretnénk-e adni személyes adatainkat.



3. ábra: Adattovábbításért felelős protokollok megjelenése
Forrás: a szerzők saját felvétele

Legtöbb esetben a csalók nem rendelkeznek személyes adatainkkal, ezért általános megszólításokat alkalmaznak megkereséseikben. Gyanakvásra adhat okot, ha a levél hangneme erőszakos, sürgető, vagy valamilyen visszautasíthatatlan ajánlattal, esetleg örökölt vagy elnyert vagyonnal kecsegtet. Kifejezetten

árulkodó a tegeződés vagy annak keveredése a levélben a magázódással vagy személytelen megszólítással, valamint a hosszú magánhangzók ékezeteinek pontatlansága, amelyek fordítása még mindig nem teljesen megfelelő, fordítóprogramok segítségével sem. Ahhoz, hogy az érintett szervek mihamarabb léphessenek, és csökkenteni tudják az esetek számát az olyan ügyekben, mint a FluBot tevékenysége, a sértetteknek jelezniük kell a történteket szolgáltatóiknak bejelentés formájában, valamint – ha szükségesnek érzik és káruk indokolja – rendőrségi feljelentést is tehetnek.

A kérdőív és az interjúk eredménye az adathalászat relációjában

A kérdőíves kutatás egy fontos fejezete az adathalászattal kapcsolatos ismereteket vizsgálta. Az eredményekből leszűrhető, hogy az ismeretlen személyek által küldött e-mail-csatolmányokat a többség nem nyitja meg, azokat kockázatosnak tartja. Hasonlóan megnyugtató eredmény, hogy a kitöltők nagy része mindig meggyőződik arról, hogy az egyes információk után érdeklődő személy valóban jogosult-e az adat tartalmának megismerésére.

Általánosságban az is elmondható, hogy nem jellemző a kitöltőkre az érzékeny adatok nyilvános wifihálózaton keresztül való továbbítása. Ugyanakkor összefüggés van aközött, hogy megteszik-e ezt, és hogy részt vettek-e információbiztonsággal kapcsolatos képzésen az utóbbi időben – aki részt vett, arra ez kevésbé vagy egyáltalán nem jellemző.

A kérdőíves kutatás mellett az interjúk során is megjelent az adathalászat mint fő vizsgálati terület. Az egyik kérdésben arra kerestük a választ, hogy az illető vállalata milyen megoldásokat alkalmaz az adathalászat ellen. Majdnem minden interjúalany említette a levélszűrő rendszer vagy az e-mail-címek tiltásának lehetőségét. Szintén gyakori volt a felvilágosítást szorgalmazó módszerek, valamint az oktatás és az ezzel kapcsolatos folyamatos kampányolások fontosságának hangsúlyozása. Az egyik válaszadó szervezetén belül pedig az informatikai cég éjjel-nappali helpdesk szolgáltatást nyújt, vagy éppen automatikus mechanizmusokkal védekezik az ilyen tartalmak ellen.

Egy másik kérdés arra irányult, hogy az interjúalanyok milyen intézkedések, szabályozók révén képzelik el az efféle támadások megelőzését. Tipikus válaszként itt is megjelent a tudatosítás, az oktatás, valamint a gyakorlati esetekből való tapasztalatszerzés és tudásbővítés vagy éppen az egyes hatóságokkal való együttműködés szorgalmazása. A leírtak mellett volt, aki a mesterséges

intelligenciára alapozott rendszerekben, míg mások az információtechnológia jellegű szabályozókban és technikai kontrollerekben látják a probléma megoldásának kulcsát.

Összegzés

Láthattuk, hogy az adathalászat – módszereit tekintve – a kiberbűnözés egyik legalattomosabb formája. A támadások elleni védekezés első lépcsője annak a felismerése, hogy mi is lehetünk célpontok. Minél több személyes adatot osztunk meg magunkról az internet világában, annál kiismerhetőbbek és támadhatóbbak leszünk.[91] Ugyanakkor igazán komoly eredményeket csak a megfelelő kiberbiztonsági eszközök és módszerek támogatásával, kellő éberséggel és tudatossággal érhetünk el. Bizakodásra adhat okot, hogy mind a kérdőívre válaszolók, mind pedig az interjúalanyok esetében pozitív, tudatos válaszok érkeztek, ami arra enged következtetni, hogy esetükben az adathalász-támadások jelentős mértékben visszaszorulhatnak, megelőzhetők. Ettől függetlenül a leírtakon túl elengedhetetlen eszközeink naprakészen tartása, a rendszeres frissítések, az operációs rendszer és a tűzfal állapotának figyelemmel kísérése, az internetes fiókok és a hitelesítési adatok ellenőrzése, valamint a szervezetek dolgozóinak folyamatos képzése, az őket körülvevő, kiberbiztonság területén jelentkező kockázatok bemutatása. Ha adataink biztonsága valóban fontos – legyen szó adathalászatról vagy bármely más, az online biztonságot fenyegető veszélyről –, mindez nélkülözhetetlen.

3.2.7. Trükkös csalás

A korábbi alfejezetek alapján kijelenthetjük, hogy az infokommunikációs technológiák rohamos terjedésével, a közösségi média napról napra történő térhódításával, illetve az egyre szofisztikáltabb adathalász-kísérletek okán napjaink egyik legjelentősebb biztonsági kockázataként a kiberteret azonosíthatjuk. A kibertámadások ellen rendkívül nehéz védekezni, és ahogy a védelmi megoldások, úgy az incidensek is egyre kifinomultabbak, komplexebbek, ezért a csalók elsősorban a leggyengébb láncszemen, a nem kellően biztonságtudatos felhasználón

[91] Klein–Szabó 2018: 148–150.

keresztül igyekeznek hozzáférni a védett rendszerekhez. A szakirodalom az ilyen jellegű támadásokat *social engineering* akcióként definiálja, ennek rövid ismertetésével zárjuk az alapvető ismeretek körét.

A *social engineering,* avagy trükkös csalás egy olyan támadási technika, amelyet személyek, szervezetek, bűnözők, terroristák, hírszerzők egyaránt használnak céljaik elérése érdekében. E cél rendkívül eltérő lehet: vonatkozhat információszerzésre, az informatikai rendszer befolyásolására, dezinformálásra, zsarolásra, üzleti titkok megszerzésére és számos egyéb tevékenységre is. Összességében tehát a *social engineering* mint incidens maga az eszköz, amelyet az online és az offline térben, közvetlen és közvetett módon egyaránt alkalmazhatnak a csalók. A megszerzett információkhoz hozzájuthatnak többek között akár a 3.2.6. alfejezetben részletezett adathalász-támadások útján is, amelyet mint technikát a támadók implementálhatnak a *social engineering* akcióba, és az adatokat a saját céljaik elérése érdekében hasznosíthatják.

A *social engineering* fogalmának legjobb meghatározása Kevin Mitnick nevéhez köthető, aki szerint:

„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."[92]

Vagyis a támadó egy személy vagy szervezet olyan adataihoz akar hozzájutni, amelyek számára nem elérhetőek, és amelyekhez magán a személyen vagy a szervezet munkatársain át vezet az út. Egy támadás főbb lépései közé tartozik az információgyűjtés, a kapcsolat kiépítése és kihasználása, valamint az akció végrehajtása is.

A *social engineering* támadások modellje

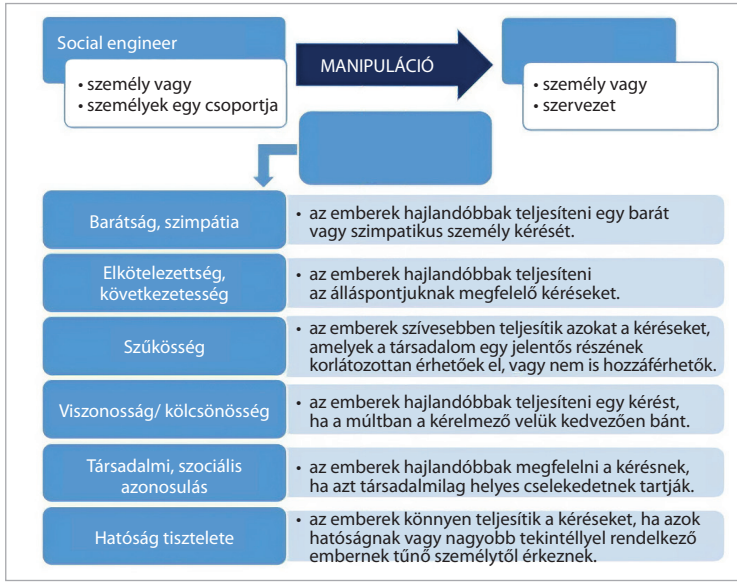
Az elkövető a támadás végrehajtása során a célpontról személyes információkat gyűjt, személyes kontaktusba kerül, beszélget, és bizalmat, illetve számára kedvező hangulatot teremt. Összességében tehát a célpont emberi magatartására (empátia, segítségnyújtás) építve kezd el tevékenykedni. A *social engineer* a kommunikációja szempontjából használhat direkt és indirekt modellt. Meg

[92] Kevin D. Mitnick és William L. Simon *A legendás hacker. A megtévesztés művészete* című könyvének fülszövegét idézi Oroszi 2008: 28.

kell határoznia a célpontot, a közeget, a célt, valamint a manipuláció alapját és a technikákat, emellett el kell döntenie, hogy a támadás egy vagy több lépcsőben valósuljon-e meg. A 4. ábrán azokat az alapvető és leggyakrabban problémát okozó emberi magatartásformákat láthatjuk, amelyeket az elkövetők a különböző humán alapú támadások alkalmával (így a *social engineering* esetében is) rendszerint kihasználnak, és amelyekre az otthoni és a munkahelyi környezetünk védelme szempontjából egyaránt fokozottan ügyelnünk kell.

Technika tekintetében beszélhetünk:

– adathalászatról *(phishing);*
– ürügyről, amely alapul szolgál a támadó számára értékes információk megszerzéséhez *(pretexting);*
– „beetetésről", vagyis az áldozat mohóságának, kíváncsiságának kihasználásáról *(baiting).*



4. ábra: A manipuláció eszközei humán alapú támadásokkor

Forrás: Dub Máté szerkesztése Mouton–Leenen–Venter 2016: 186–189. alapján

Ezek mellett meg kell említenünk az úgynevezett „valamit valamiért" technikát, amelynek értelmében a *social engineer* váltságdíjat követel például személyes

adat vagy belépési azonosító visszajuttatásáért cserébe. Mindezen tevékenységek elsődleges célja az anyagi haszonszerzés, az illetéktelen hozzáférés biztosítása vagy éppen a szolgáltatás megzavarása. A megvalósításhoz alkalmazott közeg pedig lehet:

- e-mail, weboldalak,
- személyes kapcsolatfelvétel,
- telefon/SMS,
- levél, röpirat, adathordozó stb.

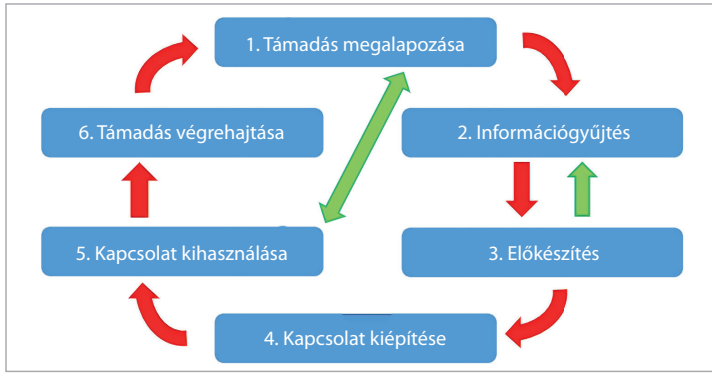
A támadó és a célpont közötti kommunikáció jellege alapján három nagy kategóriát különböztethetünk meg:

1. Direkt, kétirányú kommunikációról akkor beszélhetünk, ha közvetlen kapcsolat van a támadó és a célpont között. Ez a kommunikációs forma jár a legnagyobb kockázattal a lebukást illetően, ugyanis ilyenkor mindkét fél aktívan részt vesz az offline térben, például egy személyes kapcsolatfelvétel során. Ugyanakkor idetartozik például az online levelezés, az e-mailezés is.
2. Direkt, egyoldalú kommunikáció alatt az olyan helyzetekre gondolunk, amikor a célpontnak nincs lehetősége felvenni a kapcsolatot a támadóval. Ezzel például egy, a feladó címét nem tartalmazó levél esetében találkozhatunk.
3. Indirekt kommunikációnak tekintjük azokat a támadási formákat, ahol közvetett kapcsolat van a támadó és a célpont között, a közvetítő közeg pedig egy harmadik „fél". A fél azért került idézőjelbe, mert az indirekt kommunikáció tekintetében beszélhetünk például fizikai adathordozó elhelyezéséről egy bizonyos helyen, amelynek rendszerbe történő csatlakoztatásával juttathatnak kártékony programot a célpont rendszerébe. Ebben az esetben például a támadó az áldozat személyes indíttatására támaszkodik, aki a megtalált adathordozót akár kíváncsiságból, akár a visszajuttatáshoz szükséges információ megtalálásának reményében csatlakoztatja a számítógépéhez.

A *social engineering* támadások keretrendszere

A *social engineering* támadások keretrendszerének hat fő lépcsőfoka van, ezt mutatja be az 5. ábra.

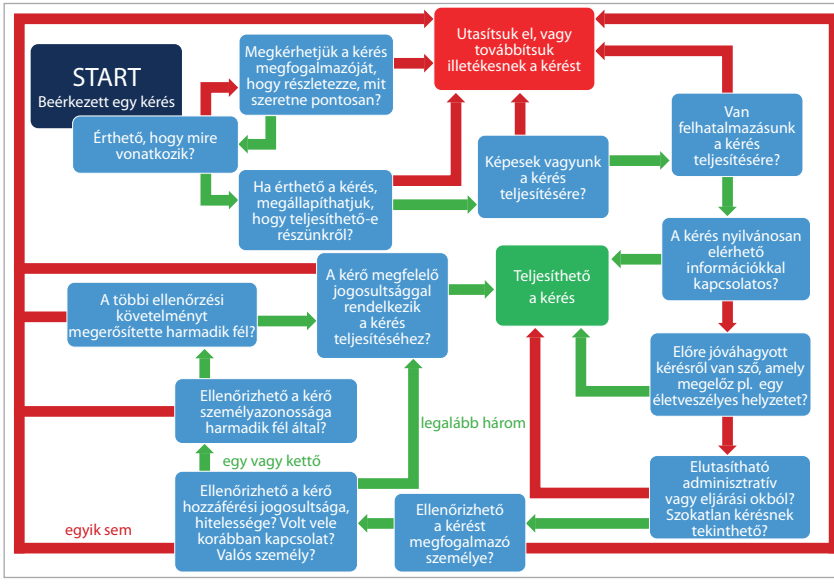
1. Támadás megalapozása: cél és célpont specifikus meghatározása.
2. Információgyűjtés: valamennyi, potenciális forrásból származó információ összevetése és elemzése a cél és a célpont vizsgálatának implementálásával.
3. Előkészítés: a begyűjtött információk kombinált elemzése, majd ennek alapján a támadási módszertan kiválasztása. Új információk megszerzésére is szükség lehet.
4. Kapcsolat kiépítése: a módszertan meghatározását követően kerül sor a kommunikáció kialakítására a célponttal, amely során a fő szempont egy bizalmi kapcsolat kiépítése.
5. Kapcsolat kihasználása: mértékét és módját az elérni kívánt cél határozza meg.
6. Támadás végrehajtása: a kiépített kapcsolat kihasználása egy ideig és egy bizonyos mértékig folyamatos, mert így érhető el a kitűzött cél.



5. ábra: A social engineering támadások általános keretrendszere
Forrás: Dub Máté szerkesztése Mouton–Leenen–Venter 2016: 196–206. alapján

Az incidensek elkerülése, kiküszöbölése érdekében figyelni kell arra, hogy amennyiben a támadónak nem sikerült elsőre elérnie a célját, előfordulhat, hogy más módszerekkel, új információk tudatában újra próbálkozik, így egymást követő – adatszerzésre, belépésre, hozzáférés megszerzésére stb. irányuló – próbálkozásokra is számítani kell.

A 6. ábrán a *social engineering* támadások felismerését segítő modell látható, amely tartalmazza az akció során nekünk szegezett kérdésekre adandó, a tudatosság szempontjából megfelelő válaszlépéseket. Ezzel kapcsolatban le kell szögeznünk néhány fontos részletet, amelyről sosem szabad megfeledkezni, amelyet a biztonságos otthoni és munkahelyi környezetben egyaránt alkalmaznunk kell.



6. ábra: A social engineering támadások felismerésének modellje

Forrás: Dub Máté szerkesztése Mouton–Leenen–Venter 2016: 196–209. alapján

Megjegyzés: Az egyes kérdésekre adott válaszok esetén az „igen” a zöld, míg a „nem” a piros nyilak szerinti továbbhaladást mutatja. A start után az első kérdés, hogy érthető-e, mire vonatkozik a beérkezett kérés.

– Csak és kizárólag azokról a kérésekről adjunk felvilágosítást, amelyek esetében erre felhatalmazásunk van!
– Ha nem vagyunk illetékesek az adott kérés teljesítésében, vonjuk be a megfelelő hozzáféréssel rendelkező kollégánkat, felettesünket!

– A kérés megfogalmazójához intézett kérdéseinkre mindenképp szerezzünk válaszokat!
– Soha ne engedjük, hogy a kérés megfogalmazója akár csak a legkisebb mértékben is presszió alá helyezzen minket a folyamat során, ugyanis a támadó számára megfelelő hangulat és a stresszhelyzetben jelentkező emberi tulajdonságok kihasználása a sikeres támadás egyik alapvető eleme!

A kérdőív és interjúk eredménye a trükkös csalás típusú támadások relációjában

A vizsgált partnerszervezetektől beérkezett információk elemzését követően megállapíthatjuk, hogy munkatársaik a közösségi médiában érkező megkereséseket, illetve a kapott linkeket, csatolmányokat fenntartásokkal kezelik, többségében nem kattintanak rájuk, nem nyitják meg azokat. Ugyanez vonatkozik azokra a technikákra, amikor a támadó egy kollégával folytatott korábbi megbeszélésre hivatkozik.

A fő probléma, hogy a *social engineering* veszélye akkor a legnagyobb, amikor – állítólagos – felső vezetői megkeresés történik, ugyanis ekkor a munkavállalók hozzáállása megváltozik a levélben szereplő kérésekkel kapcsolatban, hajlandóbbak az együttműködésre. A szervezetekről összességében megállapítható továbbá, hogy az információbiztonsággal kapcsolatos képzések elősegítették a *social engineering* támadásokat illető tudatosság növekedését.

Az érintett vállalatok a *social engineering* incidenseket kiemelt fontosságúnak tekintik, van köztük olyan, amely saját szervezésű vizsgálatokat is rendszeresen végez. A különböző képzések, kampányok, gyakorlatok, tudatosítási események folyamán külön foglalkoznak ezzel a technikával, és igyekeznek a legalaposabban felkészíteni a munkatársakat, ideértve a különböző kapcsolódó támadási területeket, például az adathalászatot.

Összegzés

A *social engineering* támadási technika az alapvető emberi magatartásokból adódó biztonságtudatossági hiányosságokat használja ki. Az elkövetők a munkatársak manipulációjával próbálják elérni céljaikat. A figyelem, a megfelelő kiberbiztonsági tudatosság, a belső szabályzók követése, a folytonos éberség, a kérések fenntartással kezelése, illetve a több helyről történő megerősítés a kulcs, amellyel

ez a technika a legegyszerűbben kivédhető, és amely által a munkahelyünk és magánéletünk biztonságos környezete könnyebben kialakítható és fenntartható.

Felhasznált irodalom

10 Rules for Creating a Hacker-Resistant Password. *PrivacyRights.org,* 2009. július 30. Online: https://privacyrights.org/resources/10-rules-creating-hacker-resistant-password

A Magyar Nemzeti Bank 12/2020. (XI. 6.) számú ajánlása a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről. Online: www.mnb.hu/letoltes/12-2020-tavmunka-ajanlas.pdf

A weboldal jelszavainak tárolásának 4 módja – előnyök és hátrányok. Online: https://hu.elobservadorgt.com/479-how-and-where-is-better-to-store-passwords-from-websites

Adatvédelmi kihívások az otthoni munkavégzés során. *Biztonságportál,* 2020. december 2. Online: https://biztonsagportal.hu/adatvedelmi-kihivasok-az-otthoni-munkavegzes-soran.html

Adelmann, Frank – Gaidosch, Tamas [é. n.]: Cybersecurity of Remote Work During the Pandemic. Online: www.imf.org/~/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx

Authentikáció. *Egészségtudományi fogalomtár.* Online: https://fogalomtar.aeek.hu/index.php/Authentikáció

Biztonságtudatos szemlélet kialakítása. *Computerworld.hu,* 2018. május 2. Online: https://computerworld.hu/biztonsag/biztonsagtudatos-szemlelet-kialakitasa-247149.html

Burnett, Mark (2005): *Perfect Passwords. Selection, Protection, Authentication.* Rockland: Syngress Publishing.

Curran, Kevin (2020): Cyber Security and the Remote Workforce. *Computer Fraud & Security,* (6), 11–12. Online: https://doi.org/10.1016/S1361-3723(20)30063-4

Felhőtárolás jelszó kezelőkhöz – ellene vagy mellette? *TMSI Kft. – Tőzsér és Máriás Szoftver Iroda,* 2017. november 27. Online: www.tmsi.hu/2017/11/27/felhotarolas-jelszo-kezelokhoz-ellene-vagy-mellette/

Forgó Sándor – Komló Csaba (2015): *Blended learning, tudásszervezés, hálózatalapú tudásmegosztás.* Eger: Eszterházy Károly Főiskola.

Horváth Gergely Krisztián (2013): *Közérthetően (nem csak) az IT biztonságról. Információ és IT biztonsági kultúra fejlesztése a közigazgatásban*. Budapest: KIFÜ. Online: https://kifu.gov.hu/wp-content/uploads/2022/03/IT_brosura_v7.pdf

How IT Can Get Employees to Engage With Your Company's Security Awareness Program. *Inspired eLearning,* 2020. október 13. Online: https://inspiredelearning.com/blog/how-it-can-get-employees-to-engage-with-your-companys-security-awareness-program/

Ingram, David (2018): Facebook Fuels Broad Privacy Debate by Tracking Non-Users. *Reuters,* 2018. április 15. Online: www.reuters.com/article/us-facebook-privacy-tracking-idUSKBN1HM0DR

Internet Organised Crime Threat Assessment (IOCTA) 2020. *Europol,* 2021. december 7. Online: www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Interpol Report Shows Alarming Rate of Cyberattacks During COVID-19. *Interpol,* 2020. augusztus 4. Online: www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Itt az idő, hogy mindenki, mindenhol bekapcsolja a kétlépcsős azonosítást! Mutatjuk hogyan. *Webshark.hu,* 2017. november 16. Online: https://webshark.hu/hirek/ketlepcsos-azonositas-beallitasa/

Jelszó. *A magyar nyelv értelmező szótára.* Online: https://mek.oszk.hu/adatbazis/magyar-nyelv-ertelmezo-szotara/kereses.php?kereses=jelszó

Kárász Balázs (2019): Biztonságtudatossági tréningek hatékonyságának vizsgálata. *Hadmérnök,* 14(2), 313–324.

Klein Tamás – Szabó Aliz (2018): A cybercrime, mint infokommunikációs jogi probléma. In Klein Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről.* Budapest: Nemzeti Média- és Hírközlési Hatóság, 123–159. Online: https://nmhh.hu/dokumentum/194190/MK30web.pdf

Kovács László (2018): *A kibertér védelme.* Budapest: Dialóg Campus Kiadó.

Kovács Zoltán (2013): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. *Hadmérnök,* 8(3), 198–210.

Kuss, Daria J. – Griffiths, Mark D. (2017): Social Networking Sites and Addiction: Ten Lessons Learned. *International Journal of Environmental Research and Public Health,* 14(3), 311.

László Gábor (2014): Kockázatértékelés, kockázatmenedzsment. Budapest: Nemzeti Közszolgálati Egyetem.

Lazányi Kornélia (2016): A biztonsági kultúra szerepe a vezetői döntések támogatásában. The Role of Safety Culture in Supporting the Leaders' Decision Making. *Taylor,* 8(1), 143–150.

Lengyelné Molnár Tünde – Kis-Tóth Lajos (2015): *IKT innováció.* Eger: [k. n.]. Online: http://okt.ektf.hu/data/szlahorek/file/kezek/05_ikt_02_27/index.html

Lim, Sook (2020): Academic Library Guides for Tackling Fake News: A Content Analysis. *The Journal of Academic Librarianship,* 46(5).

Lis, Lea (2020): Does Social Media Cause Depression? *Psychology Today,* 2020. november 16. Online: www.psychologytoday.com/intl/blog/the-shameless-psychiatrist/202011/does-social-media-cause-depression

Manning, Jimmie (2014): Definition and Classes of Social Media. In Harvey, Kerric (szerk.): *Encyclopedia of Social Media and Politics.* Thousand Oaks: Sage Publications, 1158–1162.

Michelberger Pál – Lábodi Csaba (2012): Vállalati információbiztonság szervezése. In *Vállalkozásfejlesztés a XXI. században II.* Budapest: Óbudai Egyetem Keleti Károly Gazdasági Kar, 241–302. Online: https://docplayer.hu/3431306-Vallalati-informacio-biztonsag-szervezese.html

Mouton, François – Leenen, Louise – Venter, Hein S. (2016): Social Engineering Attack Examples, Templates and Scenarios. *Computers & Security,* 59, 186–209.

Muha Lajos – Krasznay Csaba (2018): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem.

Nádasi András – Racskó Réka (2013): *IKT erőforrás-menedzsment.* Eger: Eszterházy Károly Főiskola.

Nemzeti Kibervédelmi Intézet (2021): Rendkívüli tájékoztató SMS üzenetek útján terjesztett FluBot kártevővel kapcsolatban. *Nemzeti Kibervédelmi Intézet,* 2021. március 25. Online: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-sms-uzenetek-utjan-terjesztett-flubot-kartevovel-kapcsolatban/

Nyikes Zoltán (2017): A biztonságtudatosság fejlesztésének egyes lehetőségei. *Műszaki Tudományos Közlemények,* (7), 327–330. Online: https://doi.org/10.33895/mtk-2017.07.74

ORFK Kommunikációs Szolgálat (2018): Egy hónap – egy téma: adathalászat. *Police.hu,* 2018. január 26. Online: www.police.hu/hu/hirek-es-informaciok/bunmegelozes/aktualis/egy-honap-egy-tema-adathalaszat

ORFK Kommunikációs Szolgálat (2020): Csalók az interneten és a való világban – a rendőrség fokozott óvatosságra int. *Police.hu,* 2020. február 26. Online: www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/csalok-az-interneten-es-a-valo-vilagban-a

Oroszi Eszter Diána (2008): *Social Engineering. Az emberi erőforrás, mint az információbiztonság kritikus tényezője.* BSc-szakdolgozat. Budapesti Corvinus Egyetem. Online: https://docplayer.hu/3827943-Social-engineering-az-emberi-eroforras-mint-az-informaciobiztonsag-kritikus-tenyezoje.html

Peters, Katelyn (2021): *„Web 2.0".* Online: www.investopedia.com/terms/w/web-20.asp

Policy tiszta asztal, tiszta képernyő. Online: http://hu.tutkrabov.net/articles/policy-tiszta-asztal-tiszta-kepernyo.html

Póserné Oláh Valéria (2007): IT kockázatok, elemzésük, kezelésük. *Hadmérnök,* 2(3), 206–214. Online: http://hadmernok.hu/archivum/2007/3/2007_3_poserne.html

Pšenáková, Ildikó (2020): Ne hagyd magad becsapni! *Lélektan és Hadviselés,* 2(1), 55–65. Online: http://doi.org/10.35404/LH.2020.1.55

Remote Work Monitoring. *Black Cell.* Online: https://blackcell.io/remote-work-monitoring-whitepaper/

Seymour, Hunter (2020): A Pandemic and Remote Working: Cyber Security Under the Microscope. *IFSEC Insider,* 2020. augusztus 25. Online: www.ifsecglobal.com/cyber-security/a-pandemic-and-remote-working-cyber-security-under-the-microscope/

Social Engineering. *Dictionary.com.* Online: www.dictionary.com/browse/social-engineering

Souppaya, Murugiah – Scarfone, Karen (2016): *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.* Online: https://doi.org/10.6028/NIST.SP.800-46r2

Strong Password. Online: www.sciencedirect.com/topics/computer-science/strong-password

United Security Incorporated (2020): 5 Reasons Your Business Should Have Security Awareness Training. *Usisecurity.com,* 2020. július 6. Online: https://inbound.usisecurity.com/blog/5-reasons-your-business-should-have-security-awareness-training

Waksman, Michael (2013): 'Open Sesame!' – Is Your Password So Easy to Guess? *Jetico.com,* 2013. június 11. Online: www.jetico.com/blog/open-sesame-your-password-so-easy-guess

Youngblood, James Everett (2020): 15 Top Social Media Sites & Platforms. *Smart Blogger,* 2020. október 8. Online: https://smartblogger.com/social-media-sites/

Jogszabályok

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

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

Ajánlott irodalom

Bányász Péter – Bóta Bettina – Zágon Csaba (2019): A social engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 12–37.

Edwards, Matthew – Larson, Robert – Green, Benjamin – Rashid, Awais – Baron, Alistair (2017): Panning for Gold: Automatically Analysing Online Social Engineering Attack Surfaces. *Computers & Security.* 69, 18–34.

Harley, David (1998): *Re-Floating the Titanic: Dealing with Social Engineering.* London: Imperial Cancer Research Fund.

Heartfield, Ryan – Loukas, George (2016): A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys,* 48(3), 1–38.

Mitnick, Kevin D. – Simon, William L. (2003): *The Art of Deception. Controlling the Human Element of Security.* Hoboken: John Wiley & Sons.

Mitnick, Kevin D. – Simon, William L. – Wozniak, Steve (2012): *Ghost in the Wires. My Adventures as the World's Most Wanted Hacker.* New York: Back Bay Books.

Köszönetnyilvánítás

Az előző oldalak tartalma alapján talán bebizonyosodott, hogy nem lehet eléggé hangsúlyozni a kiberbiztonsági tudatosság fontosságát. Tanulmányunkkal azoknak a munkáját szeretnénk támogatni, akik egy cégnél vagy szervezetnél felelősek a tudatosság erősítéséért, bízva abban, hogy az általunk összeállított minimumismeretek révén a munkavállalók felkészültsége javítható.

Mindehhez jelentős segítséget nyújtott nekünk partnerszervezeteink közreműködése, a dolgozók, akik kitöltötték a kérdőívet, valamint a biztonsági területek szakértőinek alázatos és támogató hozzáállása. Köszönetünket fejezzük ki a Szerencsejáték Zrt. és a Vodafone Magyarország Zrt. szakértőinek, valamint az MVM Services Zrt. és az MVM Biztonsági Szolgáltató Központ Zrt. kollégáinak, hogy időt és energiát áldoztak az interjúkban való részvételre, és tudásukkal, tapasztalatukkal hozzájárultak tanulmányunk elkészítéséhez.

Vákát

Melléklet

A biztonságtudatosságot felmérő kérdőív

Tisztelt Válaszadó!

A Nemzeti Közszolgálati Egyetem és az MVM Energetika Zártkörűen Működő Részvénytársaság között kötött együttműködési megállapodás keretében, az MVM Csoport, a Szerencsejáték Zrt. és a Vodafone Magyarország Zrt. aktív közreműködésével szakmai kutatást indítottunk, amellyel arra keressük a választ, hogy a részt vevő szervezetek kollégái milyen szintű biztonságtudatossággal, illetve milyen, e képesség fejlesztéséhez szükséges tapasztalatokkal rendelkeznek. A válaszadás természetesen anonim, mindössze 10 percet vesz igénybe, és nem célja a meglévő ismeretek értékelése. A kérdőív teljes kitöltését pedig egy kis jutalommal díjazzuk, amely a kérdéssor végén válik majd elérhetővé.

Kérjük, amennyiben problémát észlel, szíveskedjen jelezni a tudatossag.kutatas@uni-nke.hu címen. Az adatvédelmi irányelvekben a LimeSurvey szabályzata a releváns: www.limesurvey.org/privacy-policy

Közreműködését és a kitöltésre szánt idejét köszönjük!

Felvezető kérdések:

1. *Melyik szervezet alkalmazottjaként tölti ki a kérdőívet?*
   a) MVM Csoport
   b) Szerencsejáték Zrt.
   c) Vodafone Magyarország Zrt.

2. *Korcsoport:*
   a) 18–25
   b) 26–35
   c) 36–45
   d) 46–55
   e) 56 felett

3. *Munkavégzés területe:*
   a) adminisztráció (valamennyi irodai tevékenység)

b) üzemeltetés (nem IT-vonatkozású üzemeltetési tevékenység)
c) IT-üzemeltetés (minden olyan üzemeltetési és fejlesztési tevékenység, amely IT-rendszerekkel/-eszközökkel kapcsolatos)
d) vezető/döntéshozó

4. *Biztonságtudatosnak tartja-e magát adatvédelmi szempontból?*
Igen/nem/nem tudom megítélni

5. *Biztonságtudatosnak tartja-e magát információbiztonsági szempontból?*
Igen/nem/nem tudom megítélni

6. *Részt vett-e a munkahelye által szervezett, információbiztonsággal kapcsolatos képzésen az elmúlt 2 évben?*
Igen/nem

7. *Mennyire ismeri Ön a szervezete informatikai biztonsági szabályzatát?*
a) Sosem hallottam róla.
b) Volt valamikor oktatás ezzel kapcsolatban.
c) Olvastam a legfrissebb verziót, amikor megjelent.

8. *Magáneszközeit szokta-e munkavégzési céllal használni?*
Igen/nem

A kérdőív további része tudatossággal kapcsolatos állításokat tartalmaz, amelyeket 1–5-ig terjedő skálán tud értékelni a kitöltő, ahol 1 = egyáltalán nem jellemző, 5 = teljes mértékben jellemző.

1. *kérdéscsoport: Jelszóhasználat*
Tudom, hogy lehet ugyanazt a jelszót használni több profil esetében (akár munkahelyen is).
Biztonságosnak tartom ugyanannak a jelszónak a használatát a különböző profilok esetében (akár munkahelyen is).
Eltérő jelszavakat használok a különböző profiljaim esetében.
Tisztában vagyok vele, hogy bizonyos esetekben megengedhető a jelszavak megosztása másokkal.
Nem tartom jó ötletnek megosztani a jelszavaimat másokkal, akkor sem, ha kérdezik is.

Megosztom a jelszavaim másokkal.

2. *kérdéscsoport: E-mail-használat*
   Tisztában vagyok vele, hogy meg lehet nyitni az ismerősöktől kapott linkeket.
   Biztonságosnak tartom az ismerőstől kapott linkek megnyitását.
   Nem minden esetben nyitok meg ismerősöktől kapott linkeket.
   Tisztában vagyok vele, hogy egy ismeretlen által küldött e-mailben meg lehet nyitni a csatolmányt.
   Kockázatosnak tartom egy ismeretlentől kapott e-mail csatolmányának megnyitását.
   Sosem nyitok meg ismeretlenek által küldött e-mailben csatolmányt.

3. *kérdéscsoport: Közösségimédia-használat*
   Tisztában vagyok azzal, hogy kirúghatnak amiatt, amit a közösségi médiában közzéteszek.
   Azt gondolom, nincs jelentősége, ha olyasmit posztolok a közösségi médiában, amit egyébként nem mondanék ki nyilvánosan.
   Semmit nem osztok meg a közösségi médiában anélkül, hogy ne fontolnám meg az esetleges negatív következményeket.
   Tudom, hogy azt posztolhatok a közösségi médiában a munkahelyemről, amit csak akarok.
   Kockázatosnak tartom bizonyos, a munkahelyemmel kapcsolatos információk posztolását a közösségi médiában.
   Azt posztolok a közösségi médiában a munkahelyemről, amit csak akarok.

4. *kérdéscsoport: Infokommunikációs eszközök használata*
   Tudom, hogy érzékeny információ továbbítása nyilvános wifihálózaton nem jelent problémát.
   Kockázatosnak tartom érzékeny információk továbbítását nyilvános wifihálózaton.
   Továbbítok érzékeny információt nyilvános wifihálózaton.
   Tisztában vagyok vele, hogy a munkahelyen vagy környékén talált pendrive-ot nem szabad a számítógépemre csatlakoztatni.
   Úgy vélem, semmi rossz nem történhet, ha a munkahelyen vagy környékén talált pendrive-ot a számítógépemhez csatlakoztatom.
   A munkahelyen vagy környékén talált pendrive-ot csak addig csatlakoztatom a gépemre, amíg megtudom, kié, hogy visszaadhassam neki.

5. *kérdéscsoport: Tiszta asztal*

Tisztában vagyok vele, hogy a munkámhoz szükséges dokumentumokat őrizetlenül hagyhatom.

Kockázatosnak tartom a munkámhoz szükséges dokumentumok őrizetlenül hagyását.

Őrizetlenül hagyom a munkámhoz szükséges dokumentumokat.

Tudom, hogy a képernyő bizonyos idő után lezár, ezért nyugodtan őrizetlenül hagyhatom a gépem.

Azt gondolom, hogy mindig zárolnom kell a képernyőt, ha bármilyen okból otthagyom a munkaállomásom.

Általában le szoktam zárni a képernyőt, ha valamiért el kell hagynom az irodát.

6. *kérdéscsoport: Otthoni munkavégzés*

Tisztában vagyok azzal, hogy a munkahelyi eszközeim biztonsági frissítéseit a szervezetem rendszergazdája intézi.

Kockázatosnak tartom, ha az általam használt infokommunikációs eszközökön a szoftvereknek és hardvereknek nem a legfrissebb verziója fut.

Mindig beállítom a saját eszközeimen az automatikus frissítést.

Tisztában vagyok azzal, hogy a munkavégzés céljából kapott eszközök magáncélú használata kockázatot jelent a szervezetemre nézve.

Azt gondolom, hogy szükséges korlátozásokat bevezetni a munkavégzés céljából kapott eszközök magáncélú használatát illetően.

A munkavégzés céljából kapott eszközeimet ugyanúgy, mindenre használom, mintha a sajátjaim lennének.

7. *kérdéscsoport: Pszichológiai eszközökkel és módszerekkel történő megtévesztés, manipuláció (social engineering)*

Tudom, hogy megválaszolhatom azokat a kérdéseket, amelyeket a felső vezetők nevében küldenek nekem.

Úgy vélem, hogy ha valaki egy kollégámra hivatkozva kér tőlem információt, előzetesen egyeztetett is vele.

Mindig meggyőződöm arról, hogy ha valaki feltesz egy kérdést, akkor az a személy jogosult-e a válasz megismerésére.

II. RÉSZ

A villamosenergia-rendszer egyes szervezeteinek OSINT-tudatossága és aktuális védelmi képességei

Vákát

Bevezetés

Az elmúlt időszakban számos kibertámadás ért villamosenergia-rendszereket, az egyik legjelentősebb az ukrán villamosenergia-rendszer elleni 2016. decemberi támadás volt. Az elemzések azt valószínűsítik, hogy a támadókat nyílt forrású információk is jelentősen segíthették tevékenységük végrehajtásában. Ennek megfelelően a biztonságos villamosenergia-ellátás összetett feltételrendszerét szükséges egy új elemmel bővíteni, mégpedig a nyílt forrású információk körével.

A nyílt forrású információszerzés (*open source intelligence,* OSINT) alapvetően a nyílt forrású információk gyűjtését jelenti. A nyílt forrású információk kifejezésre számos különböző fogalmat találunk, ezek közül az egyik legpontosabb megfogalmazás az Információs Hivatal honlapján érhető el. E szerint

> „a nyílt forrású információk a bárki számára hozzáférhető, nyilvános és legális eszközökkel megszerezhető információk, amelyeknek forrásai az elektronikus média, az írott sajtó, az internetes oldalak, az ingyenes és kereskedelmi adatbázisok lehetnek. Ezek szisztematikus gyűjtése és feldolgozása révén hírszerzési szempontból releváns információk keletkeznek."[1]

A *NATO Open Source Intelligence Handbook*ban szintén megfogalmaztak egy OSINT-fogalmat. Ez a 2001-ben publikált könyv a nyilvánosság számára szabadon elérhető, célja, hogy a nyílt forrású hírszerzés tárgyában alapvető oktatási segédlet legyen az egyesített és a szövetséges képzések alkalmával. A könyv megfogalmazása szerint

> „az OSINT olyan információ, amelyet tudatosan megszereztek, kiválasztottak, kivonatoltak és felterjesztettek egy kiválasztott felhasználói körnek, általában a parancsnok és közvetlen beosztottja számára, speciális kérdések megvizsgálása céljából. Az OSINT más szóval a hírszerzés bevált eljárási módszereit alkalmazza a sokféle nyílt forrású információ gyűjtése során, ami értesülések megszerzéséhez vezet."[2]

[1] Információs Hivatal.

[2] „OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence." NATO 2001: 2–3. Az idézet a szerzők fordítása.

A nyílt forrású információszerzés definícióját hazánkban először Lévay Gábor határozta meg a hírszerzéstől és a katonai felderítéstől elkülönített formában. E definíció szerint az *OSINT*

> „[a] *katonai felderítés és hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti*".[3]

Jelen tanulmányban bemutatjuk azokat az eredményeket, amelyeket az MVM Energetika Zártkörűen Működő Részvénytársaság, valamint a Nemzeti Közszolgálati Egyetem között kötött együttműködési megállapodás alapján végrehajtott kutatások szerint állítottak fel a résztvevők. A kutatás során a szakértők és a hallgatók a villamosenergia-rendszerek kiberbiztonsági képességének fokozása érdekében azt vizsgálták, hogy az OSINT, vagyis a nyílt forrású információszerzés tekintetében milyen tapasztalatok jellemzőek a magyar villamosenergia-rendszerre. A tanulmányban bemutatjuk a jelenleg rendelkezésre álló, hatályos uniós és hazai szabályozói környezetet, valamint az interjúk alapján a hazai villamosenergia-szektor szereplőinek OSINT-tudatossági szintjét, illetve képességeit.

A tanulmány 2021-ben készült, ám csak megerősíthetjük, hogy a nyílt forrású információszerzés mint tevékenység vizsgálata az azóta eltelt mintegy két évben még relevánsabb terület lett. A jelenleg is zajló orosz–ukrán háború okán a villamosenergia-rendszerek védelmével különösen érdemes foglalkozni a lehető legtöbb nézőpontból. Ezért is ajánljuk jó szívvel az Olvasónak gondolatainkat.

Tóth András

[3] Lévay 2006: 6.

1. A nyílt forrású információszerzés eszközei

A nyílt forrású információszerzés során számos különböző eljárást alkalmazhatnak a gyűjtési tevékenységet folytató személyek. A legjellemzőbb eljárási módszereket Deák Veronika *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* című cikkében foglalta össze. Ezek a következők:

- telefonos információgyűjtés;
- hagyományosan publikált anyagok;
- megfigyelés;
- internetes információgyűjtés;
- kukaátvizsgálás;
- rádió- és televíziós adások, médiahírek;
- személyes megkeresés.[4]

A fenti felsorolásból is látható, hogy nem feltétlenül az interneten keresztül történő információgyűjtés az egyetlen módszere a nyílt forrású információk gyűjtésének. Erre hívja fel a figyelmet Solti István is *Az OSINT információgyűjtő eszközeiről* című cikkében, amelyben azt írja, hogy

> „az internet alapvető OSINT-forrásként való megjelölése nem vitatható, azonban az online térben automatikusan nem alkalmazható minden információgyűjtő eszköz az OSINT során. Nem tartoznak az OSINT területére azok az információgyűjtő tevékenységek, amelyeknél
> • hackingeszközök felhasználásával,
> • megszerzett jogosultságok felhasználásával vagy
> • szándékolt, az érintett megtévesztését célzó magatartás tanúsításával történik információszerzés."[5]

Szintén ő mutatja be azokat a személyeket, szolgáltatókat és módszereket, amelyek hozzájárulhatnak az információk megszerzéséhez. Az első ilyenek az online kereskedelmi szolgáltatók, akiknél alapvető lehetőségként merül fel, hogy az általuk létrehozott, gyűjtött, feldolgozott és tárolt tartalmakat és adatbázisokat ellenszolgáltatás fejében biztosítják partnereik számára. Ebben az esetben

[4] Deák 2018: 391–402.
[5] Solti 2019: 11.

sem feltétlenül játszik szerepet az internet, nagyon sok esetben előfordul, hogy a szükséges információkat valamilyen adathordozón vagy például nyomtatott formában osztják meg. A következő lehetséges módszer a szürke irodalom előállításának és megszerzésének köre. A szürke irodalom olyan dokumentumokat takar, amelyek nyílt információkat tartalmaznak, azonban csak egy jól meghatározott szűk kör számára készülnek, a széles nyilvánosság számára nem feltétlenül publikálják őket. Idesorolhatók az akadémiai értekezések, disszertációk, bizottsági beszámolók, konferenciaanyagok, technikai jelentések és technikai szabványok, vitairatok, előnyomatok, kormányzati beszámolók, hírlevelek, üzleti vagy piaci előrejelzések, kutatási beszámolók, fordítások, úti beszámolók, munkaanyagok stb. A szürke irodalmat legtöbbször előállító szervezetek és intézmények:

- a nemzeti kormányok és kormányzati szervek;
- a politikai pártok;
- a kutatóintézetek;
- az egyetemek;
- az akadémiák;
- a kereskedelmi társaságok.[6]

A szürke irodalom minden esetben nyilvános adatokat tartalmaz, a minősített adatok ebbe a körbe semmiképpen nem vonhatók be, és magának az OSINT-tevékenységnek sem képezik részét.

A különböző OSINT-technikákon keresztül végzett, folyamatos iterációkat elemezni és értelmezni kell, hogy értékes információkat nyerjenek. A szakirodalomban egyre több elemzési technika létezik ennek a feladatnak a végrehajtására.[7] Az alábbiakban kiemeljük a nemzetközi szakirodalomban feldolgozott technikákat és csoportosításokat:

- Lexikai elemzés: A nyers adatokat meg kell vizsgálni, hogy az információt és az összefüggéseket ki lehessen vonni a szövegből. Alapvető fontosságú, hogy ha többnyelvű forrásokat használunk, azokat lefordítsuk az OSINT-vizsgálatban használt nyelvre,[8] és szűrjük.
- Szemantikai elemzés: Az adatok megértésének céljából manapság természetes nyelvfeldolgozó algoritmusokat alkalmaznak.[9] Ezenkívül

[6] Lévay 2006: 8.
[7] Liu–Zhang 2012: 415–463.
[8] Ranade et al. 2018: 238–243.
[9] Noubours–Pritzkau–Schade 2013: 1–7.

a hangulatelemzési technikák lehetővé teszik a szubjektív hozzászólások vagy vélemények kontextusba helyezését a szerző érzelmi állapotának osztályozásával (például pozitív, negatív vagy semleges). Végezetül az igazságfeltáró eljárások azzal a kihívást jelentő feladattal foglalkoznak, hogy feloldják a konfliktusokat a több forrásból származó adatok között, amelyek ugyanabban a témában ellentétes álláspontokat képviselnek.[10]

– Földrajzi elemzés: A közösségi médiából, eseményekből, érzékelőkből vagy IP-címekről gyűjtött adatokat érdemes helyalapú szempontból elemezni. Ebben az értelemben a térképek vagy grafikonok használata megkönnyíti az adatok ábrázolását és megértését, valamint értelmes összefüggések feltárását az események vagy személyek között.[11]
– Közösségimédia-elemzés: A modern közösségi média által nyújtott szolgáltatások lehetővé teszik a kutatók számára, hogy mélyreható elemzést végezzenek a felhasználókról. Ilyen helyzetben a közösségimédia-adatok elemzése lehetővé teszi a téma körüli kapcsolatok, interakciók, helyek, viselkedések és ízlések hálózatának létrehozását.[12]

A fent említett technikák bevezetésének eredményeit kimeneti információnak tekintjük, és három fő csoportba soroljuk:

– A személyes adatok összegzik azon személyazonossági adatokat, amelyek főként a valódi névből, e-mail-címből, felhasználónévből, közösségi médiából és keresőmotorokból származnak.
– A szervezeti információkat azon személyek adatai alkotják, akik egy csapatban vagy vállalatnál vannak. Lényegében a közösségi média, keresőmotorok, helyadatok, domainnév és IP-cím-adatok segítségével határozzák ezeket meg.
– A hálózati információk a rendszerek és a kommunikációs topológiák technikai adatait tartalmazzák, amelyeket általában hely-, tartománynév- és IP-cím-információval valósítanak meg.

[10] Li et al. 2015: 1–16.
[11] Vopham et al. 2018.
[12] Stieglitz et al. 2018: 156–168.

2. Az OSINT előnyei és kihívásai

Az OSINT alkalmazási területei sokfélék, és az e paradigma alapján fejlesztett megoldások köre egyre bővül. A módszertan mögött azonban sokszor olyan kompromisszumos lehetőségek állnak, amelyekkel a fejlesztőknek és a mérnököknek meg kell birkózniuk. Amint az első táblázatban láthatjuk, az OSINT számos előnnyel jár, de néhány kihívással is foglalkozni kell, amennyiben ezt a technológiát szeretnénk használni. Ezeket az előnyöket, illetve kihívásokat a következőkben részletezzük.

1. táblázat: Az OSINT előnyei és kihívásai

Előnyök	Kihívások
Hatalmas mennyiségű rendelkezésre álló információ	Az adatkezelés összetettsége
Nagy számítási kapacitás	Strukturálatlan információk
Big data és gépi tanulás	Téves információk
Kiegészítő adatok	Az adatforrások megbízhatóságának kérdésköre
	Erős etikai/jogi kérdések

Forrás: a szerzők szerkesztése Bányász 2015: 22–24. alapján

2.1. Az OSINT előnyei

A nyílt forrású információszerzés alkalmazásának számos előnye létezik, amelyek közül jelen tanulmányban csak az alábbiakat elemezzük:

- hatalmas mennyiségű rendelkezésre álló információ;
- nagy számítási kapacitás;
- *big data* és gépi tanulás;
- kiegészítő adatok.

2.1.1. Hatalmas mennyiségű rendelkezésre álló információ

Jelenleg nagy mennyiségű értékes nyílt forrású adat áll rendelkezésre, amely elemezhető és összekapcsolható.[13] Idetartoznak többek között a közösségimédia-platformok, a kormányzati dokumentumok és jelentések, az online multimédiás tartalmak, az újságok, sőt a deep és dark web tartalmai is.[14] Valójában mind a *deep web,* mind a *dark web* (utóbbi az előbbin belül található) még több információt tartalmaz, mint a *surface web* (azaz a legtöbb felhasználó által ismert internet).[15] Ahhoz, hogy hozzáférhessünk ezekhez a hálózatokhoz, speciális eszközöket kell használni, mivel tartalmukat a hagyományos keresőmotorok nem indexelik.

2.1.2. Nagy számítási kapacitás

A számítógépes architektúra, a processzorok és a GPU-k (*graphics processing unit:* grafikus feldolgozóegység) fejlődése lehetővé teszi az erőforrás biztosítását a gyűjtésre, feldolgozásra, elemzésre és tárolásra egyaránt. Ezeknek az eszközöknek a segítségével lehetőségünk van az OSINT alkalmazására, tekintettel arra, hogy nagy mennyiségű nyilvános információt kell feldolgozni, és ezen információk kapcsolatát és mintáit is kezelni kell.

2.1.3. Big data és gépi tanulás

Az adatelemzési és adatbányászati technikák, valamint a gépi tanulási algoritmusok növekvő elterjedése is elősegíti az OSINT használatát. A gépi tanulás automatizálhatja és intelligensebbé, továbbá hatékonyabbá teheti a vizsgálati és döntéshozatali folyamatokat.[16] Lehetővé teszi olyan összetett összefüggések észlelését, amelyek az emberek számára kiszámíthatatlanok. Ez a pont kiemelt jelentőségű lesz az OSINT jövőbeni használatában, mivel meg fognak jelenni az emberi és a mesterséges intelligencia által vezetett kutatások közötti különb-

[13] Wong 2016: 167–185.
[14] Kalpakis et al. 2016: 111–132.
[15] Bergman 2001.
[16] Gandomi–Haider 2015: 137–144.

ségek. E technikák beépítésével a gyűjtés és elemzés folyamata végérvényesen javulni fog, ezáltal pontos, célunkhoz közeli vizsgálatokat eredményezve.[17]

2.1.4. Kiegészítő adatok

Lehetőség van az OSINT-vizsgálatok kiegészítésére más forrásból származó adatokkal, ezáltal tovább pontosítva e műveletek eredményeit. A legtöbb OSINT-rendszer belső felépítése kellően nyitott ahhoz, hogy olyan adatokat is feldolgozzon, amelyeket valójában nem nyílt forrásból szereztek be. Ez a tény azt jelenti, hogy az OSINT még hatékonyabb lehet, ha képesek vagyunk külső információkat hozzáadni a vizsgálatok kiegészítéséhez.[18]

2.2. Az OSINT kihívásai

Az OSINT-nak az előnyök mellett természetesen számos kihívása is van, amelyek közül jelen tanulmányban az alábbiakat elemezzük:

- az adatkezelés összetettsége;
- strukturálatlan információk;
- téves információk;
- az adatforrások megbízhatóságának kérdésköre;
- erős etikai/jogi kérdések.

2.2.1. Az adatkezelés összetettsége

Az adatok mennyisége óriási, következésképpen nehéz őket hatékonyan és eredményesen kezelni. Előnyös, ha az OSINT-folyamatok a lehető legtöbb információt feldolgozzák. Ehhez azonban fejlett technika és jelentős erőforrások kellenek, hogy a magas színvonalú gyűjtés, feldolgozás és elemzés biztosítva legyen.[19]

[17] Barnea 2019: 433–447.
[18] Day–Gibson–Ramwell 2016: 133–152.
[19] Fleisher 2008: 852–866.

2.2.2. Strukturálatlan információk

Az interneten elérhető nyilvános információk eredendően tömegesen strukturálatlanok. Ez azt jelenti, hogy az OSINT által gyűjtött adatok annyira heterogének, hogy ez megnehezíti a releváns kapcsolatok és ismeretek kinyerése érdekében történő osztályozásukat, összekapcsolásukat és vizsgálatukat. Ebben az értelemben az OSINT a strukturálatlan információk homogenizálásához, annak érdekében, hogy fel tudják használni azokat, olyan mechanizmusokat igényel, mint az adatbányászat, a természetesnyelv-feldolgozás (*natural language processing,* NLP) vagy a szövegelemzés.

2.2.3. Téves információk

A közösségimédia-platformokat és a kommunikációs médiumokat elárasztják a szubjektív vélemények, az álhírek.[20] Ezért az OSINT-mechanizmusok használatakor figyelembe kell venni a pontatlan információk meglétét. Az OSINT-tevékenységnek mindig megbízható információkon kell alapulnia, és megbízható kutatási irányokat kell követnie a pozitív és meggyőző eredmények biztosítása érdekében.[21]

2.2.4. Az adatforrások megbízhatóságának kérdésköre

Az információk megbízhatósága és valódisága valóban a sikeres OSINT-vizsgálatok kulcsa.[22] Ideális esetben az összegyűjtött adatoknak hiteles, ellenőrzött és autentikus forrásokból (hivatalos dokumentumok, tudományos jelentések, megbízható kommunikációs médiumok) kell származniuk. A gyakorlatban az OSINT-folyamatok szubjektív vagy nem hiteles forrásokat is fel fognak használni, például a közösségimédia-platformok tartalmát. Annak ellenére, hogy az ilyen típusú források hajlamosabbak a félretájékoztatásra, valójában sok tudást lehet kinyerni belőlük az emberek, csoportok vagy vállalatok vizsgálatához.[23]

[20] Bello-Orgaz–Jung–Camacho 2016: 45–59.
[21] Mármol–Pérez–Pérez 2014: 32–40.
[22] Gong–Cho–Lee 2018: 5428–5435.
[23] Zago et al. 2019: 98–104.

2.2.5. Erős etikai/jogi kérdések

Az OSINT fejlesztésével számos aggály merül fel a magánélet tisztelete és a személyes integritás tekintetében. Egyrészt, bár nyilvánosan hozzáférhető a felhasznált adatok köre, az OSINT képes olyan információkat felfedni, amelyek nincsenek kifejezetten közzétéve az interneten. A feltárt eredményeknek tiszteletben kell tartaniuk a felhasználók magánéletét, és nem szabad felfedniük intim és személyes adatokat, figyelembe véve a vonatkozó szabályozásokat (például GDPR). Ebből a szempontból az internetről kikövetkeztethetők olyan adatok, mint a szexuális irányultság, a vallási meggyőződés, a politikai hovatartozás. Másrészt az OSINT-alapú keresések hatókörét értelemszerűen a nyílt adatforrásokra kell korlátozni. A tudás kinyerése érdekében semmilyen körülmények között nem lehet megkerülni a hozzáférés-vezérlést vagy a hitelesítési módszereket.[24]

3. Jogszabályi háttér

Ebben a fejezetben a nyílt információszerzés jogszabályi hátterét ismertetjük. A felhasznált módszerektől függetlenül, általánosságban elmondható, hogy minden tevékenység, amely adatszerzéssel, adatfeldolgozással vagy adatelemzéssel kapcsolatos, meg kell feleljen a jogszabályi alapoknak. A nyílt jellegű információszerzés esetén nem szabad abba a tévedésbe esni, hogy csupán azért, mert az adat nyíltan elérhető, a gyűjtése, felhasználása jogszerű. E fejezetnek ez a kulcskérdése, a jogszabályi elemzéseinkkel erre a kérdésre kívánunk választ adni. Számos információ nyíltan, ráadásul a közösségi médiával átszőtt világunkban relatíve könnyen és olcsón hozzáférhető. Ugyanez igaz a telefonos applikációkon belül történő adatgyűjtésre. Viszont amennyiben ez az adat személyes adatnak minősül, hiába nyílt, egyértelmű hozzájárulás nélkül nem felhasználható. Ez nem csupán a jogkövetkezmények, hanem a szervezet jó hírneve miatt is kifejezetten fontos. A közelmúltban a legjelentősebb botrány a Cambridge Analyticához kapcsolódott, pedig a felhasználók adatait a közösségi médián

[24] Kandias et al. 2013: 98–110.

keresztül és hozzájárulással gyűjtötték és dolgozták fel. A szervezetet ebben az esetben azért érte komoly médiakritika, mert ugyan a felhasználók engedélyt adtak az adataik kezelésére, de nem volt egyértelmű, hogy mit gyűjtenek, és azt mire használják fel.

A jogszabályi háttér bemutatása során az Európai Unióban és Magyarországon releváns jogszabályokat elemezzük. Az Európai Unióban legjelentősebb az Európai Parlament és a Tanács (EU) 2016/679-es rendelete (GDPR), Magyarországon pedig az Alaptörvény és a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.).

Elemzésünk kulcskérdése a személyes adat kérdésköre lesz, mivel mindkét jogforrás abban az esetben válik hatályossá, ha személyes adat kezelése történik. A GDPR esetében először egy keretszerű tájékoztatást adunk, majd pedig a személyes adatok jogszabályi definícióját tisztázzuk. A magyar jogforrásoknál a GDPR vonatkozásában releváns azonosságokat és jogszabályi szűkítéseket mutatjuk be, szintén a személyes adat kérdésével kapcsolatban. A jogszabályi háttér ismertetésének így az a célja, hogy segítsen a szervezetnek mérlegelni, érdemes-e személyes adatokat kezelnie (tisztázva azt, hogy ténylegesen mi is a személyes adat) és a következő lépcsőben megvalósítania a jogszabályoknak való megfelelést, vagy sem.

3.1. Az Európai Parlament és a Tanács (EU) 2016/679-es rendelete (GDPR)

Az Európai Parlament és a Tanács (EU) 2016/679-es rendelete (más néven: GDPR, adatvédelmi rendelet) számos változást hozott az adatkezelők számára. Ez a nyílt információ szerzése (és ezen adatok feldolgozása, elemzése) szempontjából is kifejezetten időszerű. A GDPR-t az OSINT vonatkozásában nem úgy kell kezelni, hogy ez egy jogszabály, amely ellehetetleníti a nyílt információból történő adatszerzést, hanem szigorú szabályozásként, amely az egyének védelme érdekében szűkíti vagy bizonyos esetekben engedélyhez köti az adatokkal kapcsolatos tevékenységet. Az OSINT alkalmazásában a GDPR hozott érezhető változásokat,[25] viszont a tényleges hatása szervezettől és OSINT-jellegtől függő. Az adatvédelmi rendeletnek alapvetően nem az a célja, hogy lehetetlenné tegye a személyes adatok feldolgozását, hanem sokkal inkább az egyensúly

[25] Shere 2020: 429–448.

megteremtése az adatcsere szükségessége, valamint a polgárok magánélethez való alapvető joga között. A GDPR egyensúlyt teremt e jog és más jogok között azáltal, hogy a személyes adatok feldolgozását olyan esetekre korlátozza, amikor erre jogalap van (6. cikk). Hat különböző jogalapot sorol fel, amelyek közül három potenciálisan releváns az OSINT-tevékenység szempontjából, ezek: a hozzájárulás [6. cikk (1) bekezdés *a)* pont], a jogi kötelezettség [6. cikk (1) bekezdés *c)* pont] és a jogos érdek [6. cikk (1) bekezdés *f)* pont].

A rendelet tisztázza a jogszabály célját:

> „A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog. Az Európai Unió Alapjogi Chartája (Charta) 8. cikkének (1) bekezdése és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdése rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez."[26]

A fentiek alapján a cél a személyes adatok védelme, amely vonatkozásában OSINT-szempontból két részre szükséges bontani az adatgyűjtést. Az egyik rész a személyes adat, a másik rész a személyekhez nem köthető adatok köre. A GDPR csak a személyes adatok gyűjtésére vonatkozik, így az adatkezelőnek csupán ezek esetében kell a jogszabályban foglaltakat betartania. A személyes adatok nyílt információból való gyűjtése nem kizáró ok, viszont e tevékenység végzéséhez megfelelő tájékoztatás és hozzájárulás szükséges. Ez az OSINT szempontjából egy erős limitációt jelent: egy szervezet – még ha jó szándékkal is (például saját biztonságának növelése érdekében) – az érintettek hozzájárulása nélkül nem gyűjthet személyes adatot nyílt forrásokból. Ez fundamentálisan viszont alá tudja ásni egy szervezet OSINT-céljait, hiszen amennyiben az érintett dolgozók tudnak arról, hogy mit és miért fognak gyűjteni róluk, maga az adatgyűjtés okafogyottá és értelmetlenné válhat. Az idézett első bekezdés kiemelten fontos, mivel egyértelműsíti, hogy a jogszabály elsődleges célja leszögezni, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. Nem az adatgyűjtők, hanem az egyének szemszögéből közelíti meg a kérdést, és így elsődlegesen az érintettek érdekeit védi és képviseli. A jogszabály alapelveit tiszteletben kell tartani a természetes személyek lakóhelyétől és állampolgárságától függetlenül – mondja

[26] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (1) bekezdés.

ki az Európai Unió –, mivel ez az alapja a közösség gazdasági és társadalmi fejlődésének. Ellensúlyként megfogalmazza a rendelet, hogy:

> „[a] személyes adatok kezelését az emberiség szolgálatába kell állítani. A személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal."[27]

Az OSINT-tevékenységek során a megismert kutatásban a fő cél a szervezet biztonságának növelése, amely így része az energiabiztonság növelésének. Ezáltal a felmerülő jogviták elkerülhetőek, és az is egy relatív kérdés, hogy milyen az arányosság mértéke a személyes adat korlátozása és felhasználása esetén, továbbá ez hogyan viszonyul a társadalmi érdekhez. Kiegészítésként meg kell állapítanunk, hogy bizonyos szabadságelveket még így sem lehet megsérteni. Ezek a következők:

- a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához,
- a személyes adatok védelméhez,
- a gondolat-, a lelkiismeret- és a vallásszabadsághoz,
- a véleménynyilvánítás és a tájékozódás szabadságához,
- a vállalkozás szabadságához,
- a hatékony jogorvoslathoz és a tisztességes eljáráshoz,
- a kulturális, vallási és nyelvi sokféleséghez való jog.

Értelmezésünkben ez azt jelenti, hogy ha még a biztonság érdekében történik is nyílt információszerzés, és ez arányos a társadalmi érdekekkel, a személyes adatok védelméhez való jog akkor sem sérthető meg. Tehát ha a felhasználó védeni kívánja a személyes adatait, ezt a jogot nem lehet korlátozni, és a nyílt információszerzés szempontjából ez egy erős limitáció. Előzetesen megismertük azt, hogy amennyiben nyílt forrásból szerzünk információt, és ebben személyes adatok érintettek, akkor a felhasználónak erről előzetesen tudnia kell, és bele kell egyeznie. Ezzel a ponttal együtt értelmezve a szervezet nem kényszerítheti olyan helyzetbe az érintettet, hogy az a személyes adatok védelmének jogáról lemondjon. Azaz ha nem járul hozzá, hogy az adatai OSINT tárgyává váljanak, akkor az ő esetében még társadalmi érdekre hivatkozva sem korlátozható ez.

[27] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (4) bekezdés.

Továbbá a (6) bekezdés lehetővé teszi a személyes adatok cseréjét (a nemzetek között), és a hatóságok tevékenységét is elismeri.

> „A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és a társadalmi életet, és egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását és a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását, biztosítva egyúttal a személyes adatok magas szintű védelmét."[28]

OSINT-tevékenységek szempontjából ez az egyik legfontosabb és legkiemelkedőbb rendelkezés. A kérdéskört a rendelet nem a szolgáltatók vagy az állam, hanem az érintettek, egyének szemszögéből közelíti meg, és az is érezhető, hogy az ő érdekükben fogalmazták meg, az ő döntéseiket is figyelembe véve. A biztonság növelése céljából folyamatosan az aktuális technológiai kihívásokra kell választ adnunk: a felhasználók új platformokon élnek virtuális életet, illetve folyamatosan új eszközöket használnak. A rendeletet úgy érdemes értelmeznünk, hogy az figyelembe veszi, hogy egyre több személyes adat válik elérhetővé. Ez a nyílt információból történő adatszerzés kulcsa, ami kapcsán ugyanakkor a rendelkezés védelmet kíván nyújtani. Az információszerzés szempontjából ez nem kibővíti a lehetőségeket, hanem leszűkíti. Ha a két kiemelt rendelkezést együtt értelmezzük (a személyes adatoknak az emberiség szolgálatába állítása és a személyes adatok megosztása), akkor érezhető, hogy a védelem sokkal erősebben jelenik meg, mint a társadalmi érdek. Ebből eredően egy szervezetnek nem elegendő csakis önmagában a (4) bekezdésben foglalt társadalmi érdekre hivatkoznia. A GDPR a címében[29] tartalmaz olyan ellensúlyt, amely megerősíti azt, hogy ez egy adatvédelmi rendelet. Más érdekek alárendelődnek az adatvédelemnek. Bármiféle nyílt információgyűjtést, adatfeldolgozást (személyes adatokra vonatkozóan) csak arra alapozni, hogy az a későbbiekben társadalmi érdeket fog szolgálni, nem szabad, mivel a jogszabály ezt az opciót ellensúlyozza

[28] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (6) bekezdés.

[29] Cím alatt nem a jogszabály tényleges címét, hanem a bevezető rendelkezéseket értjük a szövegben.

erősen. Országok közötti diverzifikációra[30] pedig nincs sok lehetőség, az adatvédelmet az unió egész területén biztosítani és érvényesíteni szükséges.

Kutatásunkban egy másik kérdéskör az automatizáció szerepe. A GDPR az automatizált és a manuális adatgyűjtést is taglalja:

> „A komoly szabály-kerülési kockázat veszélyének elkerülése érdekében a természetes személyek védelmének technológiailag semlegesnek kell lennie és nem függhet a felhasznált technikai megoldásoktól. A természetes személyek védelme a személyes adatok automatizált eszközök útján végzett kezelése mellett a manuális kezelésre is vonatkozik, ha a személyes adatokat nyilvántartási rendszerben tárolják vagy kívánják tárolni. Olyan iratok, illetve iratok csoportjai, és azok borítóoldalai, amelyek nem rendszerezettek meghatározott szempontok szerint, nem tartoznak e rendelet hatálya alá."[31]

Gyakorlati szempontból ez azt jelenti, hogy nem releváns maga az adatgyűjtés módja, ha az automatizáltan vagy manuálisan történik. Nem szabad abba a tévedésbe esnünk, hogy csupán azért, mert automatizált és nagy mennyiségű az adatgyűjtés, nem esik a GDPR hatálya alá. Ez nem képez kivételt a törvény alól, mondván, hogy a nyílt adatok az automatizáltságból és a nagy mennyiségből eredően személytelenné válnak. A GDPR ezt a kiskaput itt bezárja: a rendeletet nem lehet és nem is érdemes úgy megkerülni, hogy a szervezet a technológiai megoldáson keresztül hoz létre jogalapot az OSINT-tevékenységének, mivel a jogszabály technológiasemlegességet mond ki. Az automatizáltságról továbbá meg kell jegyezni, hogy amennyiben az érintett igényli, gépi formátumban kell rendelkezésére bocsátani az adatot, és joga van azt más adatkezelőnek is továbbítani.[32] Az adatkezelés helye sem releváns ilyen szempontból, amit a (22) bekezdés taglal: azzal sem kerülhetőek meg a rendelkezések, hogy az adatkezelés és -tárolás az EU-n kívül történik. Amennyiben az alanyok az EU állampolgárai, akkor az adatkezelőnek a rendeletben foglaltakat be kell tartania.

Technológiai szempontból felmerülő kérdés a személyes adat személytelenítése vagy álnevesítése. Álnevesítésre viszont lehetőséget nyújt a rendelet, amely ezt szintén az egyén szemszögéből közelíti meg, és nem az adatgyűjtő érdekeit veszi figyelembe. Ennek a célja az, hogy az egyéneknek pluszvédelmet nyújthasson a szolgáltató, nem pedig az, hogy a meglévő személyes adatokat álnevesítsék, majd felhasználják. Továbbá a (30) bekezdés a technológiai

[30] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (10) bekezdés.
[31] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (15) bekezdés.
[32] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (68) bekezdés.

aspektust és a személyeket összekapcsolja: a rendelet elismeri, hogy technológiai szempontból egy egyén beazonosítható az eszköze adatain keresztül is (például IP-cím, cookie-azonosító). OSINT-tevékenység során erre kifejezetten figyelnie kell a szervezetnek, hogy ha egyedi eszközadatokat gyűjt be, amelyek alapján a felhasználó beazonosítható, akkor szintén hozzájárulás szükséges. Egyedi azonosítók akár nyílt információból (például nyílt wifihálózaton látható eszközök) való begyűjtése és elemzése, ahogy az ezekkel kapcsolatos adatoké is, így hozzájáruláshoz kötött. Az adatkezelőnek ezért létre kell hoznia olyan technológiai megvalósítást, amely lehetővé teszi azt, hogy az érintettek jogainak és szabadságainak érvényesülését bizonyítani tudja.[33] Ennek érdekében nyilvántartást is kell vezetnie, illetve az adatvédelmi incidens bekövetkezése esetén megfelelő tájékoztatást kell adnia.

A nemzetbiztonsággal kapcsolatos teendők a GDPR hatályán kívül esnek,[34] így a szervezet akkor gyűjthet személyes adatokat nyílt forrásokból, ha tevékenysége ugyanebbe a halmazba tartozik. De ez esetben, amennyiben nemzetbiztonsági alapja van az adatgyűjtésnek, az egész jogszabályi kérdéskör megváltozik. Ezt a speciális esetet itt, a jogszabályi háttér elemzésénél nem kívánjuk feltárni, mivel nem kapcsolódik szorosan a nyílt információszerzéshez. Hasonlóan mentesülést határoz meg a rendelet hatósági, bűnmegelőzési és bűnfelderítési tevékenység végrehajtása esetén is.

Az adatkezeléssel kapcsolatosan szigorú szabályokat fogalmaz meg a törvény:

> „Az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez. Ilyen hozzájárulásnak minősül az is, ha az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés ezért nem minősül hozzájárulásnak. A hozzájárulás az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre kiterjed. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni. Ha az érintett hozzájárulását elektronikus felkérést követően adja meg,

[33] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (77)–(78) bekezdés.
[34] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (16) bekezdés.

a felkérésnek egyértelműnek és tömörnek kell lennie, és az nem gátolhatja szükségtelenül azon szolgáltatás igénybevételét, amely vonatkozásában a hozzájárulást kérik."[35]

A rendelet egyértelműen kimondja: ahhoz, hogy személyes adatot gyűjtsenek vagy dolgozzanak fel, az érintett konkrét tájékoztatás birtokában adott hozzájárulása szükséges. Ennek a módja lehet digitális is, viszont az egyértelműségnek ott is meg kell jelennie. Egy applikáció esetében például lehetőség van arra, hogy a felhasználó hozzájáruljon az adatkezeléshez, de önmagában egy hozzájárulás gomb nem elegendő, megfelelő tájékoztató tartalmat kell megjeleníteni. Ez az applikációkból történő nyílt információszerzést elő tudja segíteni, és így a felmerülő jogviták elkerülhetők. Továbbá, mivel a jogszabály a gyermekek személyes adatait kifejezett védelem alá helyezi, amennyiben feltételezhető, hogy gyermekek is alanyaivá válhatnak az adatgyűjtésnek, ennek elkerülése érdekében érdemes életkor szerinti ellenőrzést elhelyezni az applikációban. Az adatkezelőnek emellett tudnia kell bizonyítani azt a későbbiekben, hogy az érintett hozzájárult az adatkezeléshez. Digitálisan így nem elegendő csupán egy „ellenőrző pont" felállítása, hanem ténylegesen rögzíteni kell a felhasználó engedélyét. Az önkéntes hozzájárulást illetően jogakadályként jelenik meg a közhatalmi aszimmetria esete. A (43) bekezdés egyértelműen kimondja, hogy még ha az érintett engedélyt is adott, azonban az adatkezelő és az érintett között egyenlőtlen viszony áll fenn, akkor a hozzájárulás nem tekinthető önkéntesnek. Erre kifejezetten oda kell figyelni azért, hogy ne legyen esély arra, hogy a felhasználó az egyenlőtlen viszonyból eredő helyzete miatt adja beleegyezését. A hozzájárulás ebből következően nem köthető más tevékenységek elvégzéséhez, kivéve, ha szorosan kapcsolódik ahhoz. Általánosságban így elmondható, hogy a szervezet biztonságának növelése mint cél nem tartozik szorosan ide. Jogalap szempontjából tehát az adatkezelést külön hozzájárulással szükséges intézni, mert a munkakörhöz, pozícióhoz kapcsolása jogszerűen nehezebb, és így nem merülhet fel a hatalmi aszimmetria kérdése.

Összességében kijelenthető, hogy a hozzájárulás kulcsszerepet játszik az adatgyűjtés esetében. A hozzájárulásnak:

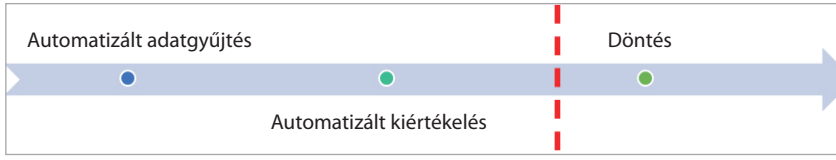
- az egyén szempontjából
  - önkéntesnek,
  - egyértelműnek,
  - hatalmi pozíciótól függetlennek, míg

[35] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (32) bekezdés.

– a szervezet szempontjából
  - arányosnak,
  - etikusnak,
  - szükségesnek,
  - tisztességesnek,
  - átláthatónak kell lennie.

A hozzájárulástól függetlenül az egyénnek joga van az elfeledéshez, azaz az egyén kérése esetén a kifejezetten az online környezetben szerzett adatokat is törölni kell.[36] Az applikációkban erre a felmerülő jogviták elkerülése és a felhasználók GDPR-ban rögzített jogai biztosítása érdekében érdemes lehetőséget biztosítani.

Az OSINT-on alapuló adatgyűjtés a biztonság növelése céljából felveti a teljes automatizálás kérdését. Teoretikusan nézve nyílt információból való adatszerzéskor előfordulhat olyan eset, hogy az érintett nyíltan olyan adatokat ad meg magáról, amelyek a szervezeten biztonsági rést ütnek. Ezt akár egy automatizált OSINT-alapú rendszer ki tudná szűrni, és ez alapján releváns döntéseket lehetne hozni. Viszont erre ilyen tisztán a GDPR-ban foglaltak fényében nincs lehetőség: a megfogalmazás szerint ha személyes jellemző érintett, akkor nem lehet ez a folyamat döntéssel együtt automatizált.[37] Első olvasatra úgy tűnhet, hogy ellenkező esetben azonban engedélyezett ez a megoldás. Viszont (később ismertetjük, hogy) a személyes adat személyes jellemzőkből áll össze. Gyakorlati szempontból így elmondható, hogy ha a GDPR alapján történik a személyes adatok kezelése, akkor (főszabály szerint) teljes automatizmus nem valósulhat meg.



1. ábra: GDPR és a személyes adatok kezelése

Forrás: a szerzők szerkesztése Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (1)–(68) bekezdése alapján

[36] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (66) bekezdés.
[37] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (71) bekezdés.

Az előbbiekben bemutatott rendelkezések a cím részét képezik és a jogalkotó szándékát fejezik ki. Összességében keretet adnak a GDPR-ban foglalt határozatoknak, viszont a jogszabályi elemzés szempontjából nem eshetünk abba a hibába, hogy ezeket a bevezető pontokat átugorjuk, mert ezek prezentálják igazán a jogalkotó szándékát. A tényleges elbírálásban és értelmezésben ez jelentős szerepet játszik.

Röviden megfogalmazva érdemes az OSINT vonatkozásában egymással szembehelyezni a korlátozó és erősítő tényezőket.

2. táblázat: Az OSINT-tevékenységeket erősítő és korlátozó tényezők

Erősítő tényezők	Korlátozó tényezők
Társadalmi érdekből végzett tevékenység	Személyes adatok védelméhez fűződő jog
Nemzetbiztonsággal kapcsolatos tevékenységek	Személyes adatok védelméhez fűződő jog védelme
Digitális hozzájárulás lehetősége	Automatizált adatgyűjtés esetén azonos védelem
	Technológiai semlegesség elve
	Személyek készülékazonosítókhoz kapcsolásának alapelve
	Közhatalmi aszimmetria esete
	Teljes automatizáció (a döntést is beleértve) tilalma
	Részletes nyilvántartás vezetése az adatkezelés módjáról

Forrás: a szerzők szerkesztése Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I–III. fejezetének egésze alapján

A rendelet a bevezetőt követően összesen 11 fejezetre tagozódik, ebből OSINT-szempontból az első három a releváns: az Általános rendelkezések, az Elvek és az Érintettek jogai. Az általános rendelkezésekben a törvény tárgyát, tárgyi hatályát, területi hatályát és a releváns fogalmak meghatározását taglalják. A rendelet tárgya röviden megerősíti a címben foglalt célokat:

> „(1) Ez a rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.
> (2) Ez a rendelet a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.

> (3) A személyes adatok Unión belüli szabad áramlása nem korlátozható vagy tiltható meg a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból."[38]

A tárgy jelentése számunkra az, amit a címben lefektetett alapvetéseknél is értelmeztünk. A rendelet célja az érintettek személyes adatainak védelme, és ezt az érintettek szemszögéből kívánja érvényesíteni. Így az OSINT-tevékenység szempontjából elmondható, hogy ha a GDPR alapján személyes adatokat fog kezelni, akkor azt úgy érdemes felépíteni, hogy figyelembe vegye a felhasználó nézőpontját. A jogszabállyal való hasonulás érdekében előnyös, ha a szervezet az ilyen nyílt információgyűjtésen alapuló tevékenységét úgy fogalmazza meg és hajtja végre, hogy az nem csupán az ő, hanem az egyének adatainak védelmében is történik.

A második cikk a rendelet tárgyi hatályát rögzíti. Röviden négy pontban taglalja azokat a fő eseményeket (kritériumokat), amelyek során az adatkezelőnek a rendeletben foglaltakat kötelező érvényűen be kell tartania.

> „(1) E rendeletet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni."[39]

A kulcsfogalom a tárgyi hatály értelmezésénél a személyes adat, erre épül a tárgyi hatály. Ha nem személyes adat kezelése történik, akkor a rendelet nem kötelező érvényű. Ezt a gondolatot a címben foglalt alapvetésekből már megismertük. A nyílt információszerzés szempontjából azt kell értelmeznünk, hogy személyes adatot kezelünk, vagy sem. A címben rögzített alapvetések itt is visszaköszönnek, tehát maga a technikai mód, hogy automatizált (és, mondjuk, ebből eredően nagy mennyiségű), nem jelent kibúvót a jogszabály tárgyi hatálya alól.

A rendelet területi hatálya komplexebb, és értelmezéséhez szükséges a teljes szövegét látnunk:

[38] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 1. cikk (1)–(3) bekezdés.

[39] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 2. cikk (1) bekezdés.

„(1) E rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem.
(2) E rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:
a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy
b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó.
(3) E rendeletet kell alkalmazni a személyes adatoknak a nem az Unióban, hanem olyan helyen tevékenységi hellyel rendelkező adatkezelő által végzett kezelésére, ahol a nemzetközi közjog értelmében valamely tagállam joga alkalmazandó."[40]

A területi hatálynál is megerősíti a rendelet azt, hogy nem az adatkezelők szemszögéből közelíti meg az adatvédelmi kérdést, hanem az érintettek felől. Mindhárom pontban előjön az, hogy ha az alany egy bizonyos kritérium alá tartozik, és személyes adatot gyűjtenek, akkor a területi hatály érvényes. Ez a technikai kiskapu kihasználásának lehetőségét kizárja, azaz lényegtelen, hogy az adatkezelőnek jelen esetben nincs európai székhelye, hogy az adatokat nem egy EU-s ország területén kezeli és tárolja, amennyiben a tevékenységi hely uniós. Ez az érintettek jogvédelme szempontjából előnyös, viszont ha az OSINT-tevékenység felől nézzük az egészet, akkor elmondhatjuk, hogy a területi hatály érvényesül. A kulcskérdés itt is az, hogy személyes adatnak minősül-e az adat, de arra, hogy mi számít annak, később tér ki a rendelet.

Az első bekezdés azt mondja ki, hogy ha az adatkezelőnek vagy -feldolgozónak az Európai Unió területén tevékenységi helye van, akkor függetlenül attól, hogy az érintettek uniós állampolgárok, vagy sem, személyes adat kezelése esetén érvényes a rendelet. Ami itt hiányosság, az az, hogy a tevékenységi helyet mint fogalmat nem tisztázzák. A tevékenységi központot viszont igen, amely a rendelet szerint a központi ügyvitele a tevékenységi helyeknek. Így utóbbit ebből a fogalomból tudjuk csak levezetni: bármilyen tevékenység, amely az EU érintettségi területén történik, az itteni tevékenységi helynek minősül. A második bekezdés szerint szintén ha személyes adatot kezelnek, akkor az érintett uniós területen belül való tartózkodása területileg hatályossá teszi a rendeletet. A b) pont pedig megerősíti azt, hogy nem csupán szolgáltatás nyújtása esetén érvényesül a jogszabály, az is elegendő, hogy a tevékenység megfigyelési célt szolgáljon, ebben

[40] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 3. cikk.

az esetben azonban az érintett megfigyelendő viselkedésének az unió területén belül kell jelentkeznie. Arra a kérdésre, hogy a tevékenységi hely telefonos applikációból gyűjtött nyílt információk esetén elkülöníthető-e, akkor „nem" a válasz, ha az érintett, akinek a viselkedését megfigyelik, már nem az EU területén tartózkodik, és ezt egy szoftver geolokációs adatok alapján felismeri, mert akkor sem gyűjthető személyes adat az érintettről GDPR-kompatibilitás hiányában, ha az első pont szerinti tevékenységi területe változatlan.

Az egész rendelet kulcskérdését, azaz a személyes adat fogalmát a fogalommeghatározásoknál ismertetik:

> „1. »személyes adat«: azonosított vagy azonosítható természetes személyre (»érintett«) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;"[41]

illetve a címben foglalt alapvetés szerint

> „[a] természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, valamint egyéb azonosítókkal, például rádiófrekvenciás azonosító címkékkel".[42]

Az eddigi jogszabály-értelmezésben visszatérő elemként nevezik meg a személyes adat kifejezést, és az OSINT-tevékenységek szemszögéből általánosan úgy értékelik, hogy valószínűleg személyes adat lesz a gyűjtött információ. Ez a címben megismert tág értelmezésből következik. A legegyszerűbb megfogalmazás ez esetben az, hogy minden olyan egyedi azonosító vagy akár jellemző információ, amelyből egy személy kiléte levezethető, személyes adatnak minősül. Ami a konkrét behatárolást jelentősen megnehezíti, az az, hogy a jogszabály példálózó jellegű. A „különösen" szó azt jelenti, hogy ezekben az esetekben kifejezetten érvényesül, de nem kizárólag ezekben az esetekben. Emiatt nagyon nehéz arra a kérdésre választ adni, hogy mi minősül személyes adatnak, mert az kimondottan függhet a szervezetnél dolgozók sajátosságaitól is. Így olyan jellemzők

[41] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 4. cikk.
[42] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (30) bekezdés.

(gyűjtött adatok) is személyes adattá tehetik az adathalmazt, amelyekről elsőre nem gondolnánk. Például ha a vállalat nyílt információt gyűjt az applikációba való bejelentkezési időről, azaz arról, hogy a felhasználó milyen gyorsan adja meg a jelszavát (hogy így határozzák meg a megfelelő időzárhosszt a biztonság növelése érdekében), az elsőre nem tűnhet személyes adatnak. De ha van egy érintett a csoporton belül, akiről tudják, hogy lassan gépel, akkor így már beazonosíthatóvá válik, és személyesadat-kezelésnek minősül a tevékenység. Az egész kérdéskör nagyon komplex, és a tág fogalommeghatározás jelentősen megnehezíti annak egyértelmű meghatározását, hogy mi nem minősül személyes adatnak. Ez nagymértékben szervezet- és személyfüggő, és ahogy az a rendelet kulcseleméből is látható („bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon"),[43] maga a személyes adat nagyon sok esetben konkrétan nem meghatározható.

A tényleges kihívás az OSINT-tevékenység szempontjából az, hogy ne minősüljön személyes adatnak a gyűjtött információ. De a rendelet szerint bármilyen információ annak számíthat, ha akár közvetett módon is beazonosítható általa az érintett. Nem magyarázzák meg, hogy a közvetlenség alatt mit ért a törvény, így még nehezebb egyértelmű behatárolást megfogalmazni a kérdéskör értelmezésénél. A legegyszerűbb köznyelvi szinten úgy lehetne ezt kifejezni, hogy bármilyen adat, amelyből az érintett személye kikövetkeztethető – módtól, tevékenységtől, adatmennyiségtől – függetlenül a személyes adatok halmazába esik.

Az is igen lényeges elem, ha az eszközök azonosítóit a személlyel kapcsolják össze. Tehát ha egy eszköz azonosító adatát kezelik, és ebből beazonosítható az érintett, akkor az is személyes adatnak minősül. A „különösen" határozószóval bevezetett részben ezeket taglalja a rendelet, amelyek közül számunkra a helymeghatározó adat és az online azonosító a releváns és hangsúlyos. A helymeghatározó adat mint kifejezés erősen függ az értelmezéstől, így az, hogy ezt nem definiálják, szintén megnehezíti a személyes adat fogalmának szűkítését. Ez utóbbi definíciójának első feléből az szűrhető le, hogy a helymeghatározó adatot is a közvetett identifikáció lehetősége teszi személyessé. Az online azonosító aránylag egyértelműnek hangzik, viszont ezt sem határozza meg a rendelet, ami szintén tágítja a fogalom értelmezését. Az online azonosító nemcsak a felhasználónév és a hozzá kapcsolódó jelszó lehet, hanem bármilyen adat, amely az adott személyt beazonosítja. A bevezető cím teszi egyértelművé

[43] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 4. cikk.

azt, hogy ezeket az azonosítókat tágan kezeli a rendelet, ezért kiemelten fontos a címben foglaltakat is értelmezni. Itt megnevezik az IP-címet (amely akár több érintett/eszköz esetében is azonos lehet[44]) és a cookie-azonosítókat is, szintén példálózó jelleggel.

Összefoglalva: ha OSINT-tevékenység során bármilyen olyan eszközadatot is rögzítünk, amely alapján az érintett identifikálható, akkor a GDPR szabályai érvényesek. A személyes adat definíciója így igen tágan értelmezhető, és ez jelentősen szűkíti az OSINT-lehetőségeket. De nem zárható ki az ilyen tevékenység, hiszen a címben (és később szabályozásban is) taglaltak alapján hozzájárulás esetén végezhető. Ugyanakkor ha az érintett értesül az adatgyűjtésről, akkor maga az OSINT-tevékenység gyengülhet. A személyes adatoknál esetenkénti értelmezés szükséges, hogy az adott információ alapján beazonosítható-e ténylegesen valaki. Lényegében az adat jellege, mennyisége, minősége, akár átfedés az adatokban nem releváns, csak az, hogy ha hozzárendelhető egy érintett, akkor az személyes adatnak minősül.

Amennyiben személyes adatot kezelünk, az alábbi elveket szükséges követnünk:[45]

- jogszerűség,
- tisztességes eljárás,
- átláthatóság,
- célhoz kötöttség,
- adattakarékosság,
- pontosság,
- korlátozott tárolhatóság,
- integritás és bizalmas jelleg elve.

Ezek az alapelvek kötelező jelleggel érvényesek a személyesadat-kezelés teljes egészére. Fontos eleme a rendeletnek, hogy nem az adatkezelésre mint tevékenységre vonatkozóan határozza meg ezeket az elveket, hanem a személyes adatok kezelésére. Ez a különbség azt jelenti, hogy az egyenkénti információknak, amelyek személyes adatnak minősülnek, kell megfelelniük ezeknek a kritériumoknak. Ez például az adattakarékosság elvénél jelenik meg igazán, amely azt jelenti, hogy csak a releváns és szükséges adatokat lehet gyűjteni. Tehát az OSINT-tevékenység vonatkozásában nem felel meg az adattakarékosság elvének az, ha

[44] IPv4 esetén.

[45] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) II. fejezet 5. cikk.

különféle, nagy mennyiségű adatot gyűjtenek (hozzájárulás birtokában), és azt ténylegesen nem használják fel, nem elemzik. A „később még jól jöhet" mint cél a személyes adatok esetében nem jöhet szóba, mert az ilyen tevékenység sem az adattakarékosság, sem pedig a célhoz kötöttség elvének nem tesz eleget. A korlátozott tárolhatóság elve is ezt erősíti meg, amelynek értelmében az adat csak a cél eléréséig őrizhető meg. Ezeknek az alapelveknek csak akkor lehet megfelelni, ha a tervezett tevékenységet előzetesen konkrétan tisztázták, a gyűjteni kívánt adatfajtákat egyértelműen meghatározták, és mindegyikhez világosan hozzákapcsolható a kezelési cél, illetve a szükséges tárolási idő. „Szórt" jellegű nyílt információ (személyes adat) gyűjtésére nem ad lehetőséget a rendelet, még akkor sem, ha az érintett hozzájárul.

Az adatkezelés jogszerűségét mint alapelvet a 6. cikkben taglalják részletesen. Hat esetet határoz meg a rendelet, amelyek közül ha csak egy is érvényesül, az adatkezelés jogszerűnek minősül. Ezektől eltérésre lehetőség nincs. Az esetek röviden és egyszerűen a következők:

- az érintett hozzájárult;
- a szerződés teljesítéséhez szükséges;
- az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- létfontosságú érdek védelme miatt történik;
- közérdekű vagy közhatalmi adatkezelés;
- harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

Számunkra a releváns ezek közül az érintett hozzájárulása, amelynek feltételeit a 7. cikk taglalja, és a címben is tesznek említést erre vonatkozóan. A hozzájárulással kapcsolatban négy esetkört fogalmaz meg a rendelet:

- az adatkezelés alapja a hozzájárulás, amelynek meglétét tudnia kell igazolni az adatkezelőnek;
- összevont hozzájárulások esetén egyértelmű elkülönítés szükséges;
- a hozzájárulás bármikor visszavonható;
- az önkéntes hozzájárulás esete.

A címben taglalt jelölőnégyzetes módot itt nem említik, de az (1) bekezdés nem zárja ki ennek a lehetőségét, ha összevetjük az alábbi, címben foglalt gondolatokkal:

> „Ilyen hozzájárulásnak minősül az is, ha az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat

> hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi."[46]

A cím és a rendelkezés összevetése során világossá válik, hogy a rendelet maga a hozzájárulás módját tágan kezeli, a hangsúly azon van, hogy a felhasználó egyértelműen tájékozódhasson arról, mihez járul hozzá, illetve a hozzájárulását később visszavonhassa. A technikai megoldás nem releváns, ami jelentősen egyszerűsítheti a nyílt információs adatgyűjtési eszközök viszonyát. Felmerül, hogy technikai megoldás keretében lehet-e álnevesíteni és így megkerülni a hozzájárulás és a személyes adat komplex kérdéskörét. Ebben a rendelet címében megismert eset az irányadó, külön fejezet nem tárgyalja az álnevesítés lehetőségét. Ezt egyébként egy biztonsági lépésnek titulálja a GDPR, nem pedig egy lehetőségnek, amellyel megkerülhető a rendelet. A gyakorlatban ez azt jelenti, hogy az adatkezelő a birtokában lévő személyes adatokat álnevesíti, így biztosítva azt, hogy ha később történne egy adatvédelmi incidens, és az adatok részben vagy egészben elérhetővé válnának, akkor az érintettek ne legyenek azonosíthatóak. Arra viszont, hogy olyan technikai megoldással, amelynek keretében a gyűjtött adatot automatikusan álnevesíti a rendszer, megkerülhető-e a hozzájárulás, a válasz az, hogy nem. Azért nem, mert személyes adatnak minősül minden olyan adat, amely alapján az érintett közvetlenül vagy közvetetten identifikálható, az adott szervezeten belül pedig így a közvetett beazonosítás lehetősége fennáll.

Az érintettnek továbbá joga van a helyesbítéshez és a törléshez is:

> „Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését."[47]

Hat esetben jogosult az érintett kérni a róla rögzített személyes adatok törlését:

- az adatgyűjtési cél már nem áll fenn;
- az érintett visszavonta a hozzájárulását, és nincs más jogalap;
- személyes ok miatt;
- jogellenes az adatkezelés;

[46] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (32) bekezdés.
[47] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) III. fejezet 16. cikk.

– más jogszabály miatt törölni kell;
– online térben gyűjtött adatról van szó.

A rendelet azt nem határozza meg, hogy ezt miként kell megvalósítania az adatkezelőnek, és erre hogyan kell lehetőséget nyújtania. Viszont az átláthatóság alapelvének érvényesülése érdekében ezt érdemes a hozzájáruláshoz hasonló módon biztosítani. Tehát egy applikáció, egy eszköz esetében célszerű azon az opción belül, ahol a személyes adatok gyűjtéséről szóló tájékoztatás olvasható, megadni a lehetőségét (vagy megnevezni a módját) annak, hogy a felhasználó az adatokat pontosíthassa, vagy az adatkezeléshez való hozzájárulást visszavonhassa.

Automatizált döntéshozatalra, ahogy a címben is említik, nincs lehetőség:

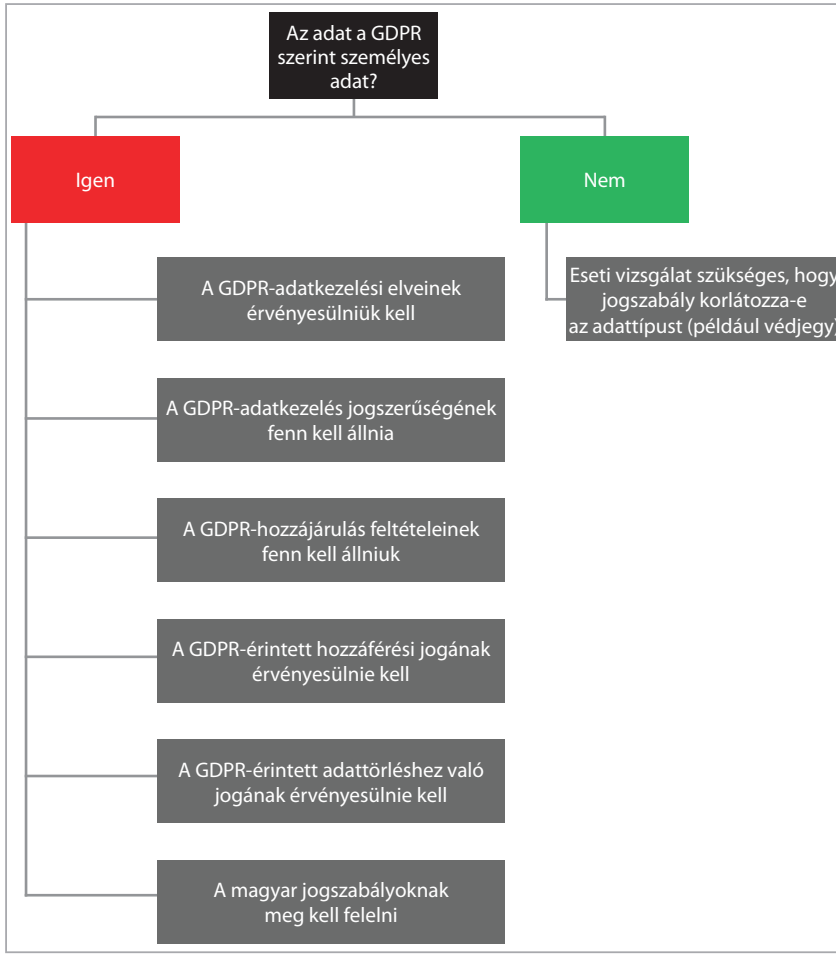
> „Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené."[48]

Főszabály szerint nem lehet nyílt információból személyes adatot gyűjteni, és ennek alapján egy automatizált rendszer révén hátrányos döntést hozni még bizonyos kritériumok fennállása esetén sem szabad. A címben megismertek fényében a döntésnek magának egyedinek kell lennie.

Az adatkezelőre és adatfeldolgozóra vonatkozó szabályokat ebben a tanulmányban nem taglaljuk, mivel túlzottan szervezetspecifikus az értelmezésük. Jogszabályelemzésünk során bemutató jelleggel értelmeztük a GDPR vonatkozásait, amelyek az OSINT-tevékenység megkezdése előtt relevánsak a jogszabályi megfelelés szempontjából.

Az OSINT-tevékenységgel kapcsolatosan így első lépésként minden esetben azt kell megvizsgálnunk, hogy az adatvédelmi rendelet szerint a gyűjteni kívánt adatok személyes adatnak minősülnek-e. Amennyiben igen, lépcsőzetes keretszerű megfelelést kell előzetesen végrehajtanunk.

[48] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) III. fejezet 22. cikk (1) bekezdés.



2. ábra: Lépcsőzetes keretszerű megfelelés

Forrás: a szerzők szerkesztése Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) alapján

Összességében elmondható, hogy az OSINT-tevékenységet elsődlegesen az előzi meg, hogy az annak során gyűjteni kívánt adat az Európai Parlament és a Tanács (EU) 2016/679-es rendelete szerint személyes adatnak minősül-e, vagy sem.

Az, hogy az adat nyíltan elérhető, vagy automatizált gyűjtéssel szerzik, nem releváns a rendelet szempontjából. Az viszont kifejezetten fontos, hogy először meg kell vizsgálnunk, az érintett adatok személyes adatnak számítanak-e. Ezen jogszabályi elemzésünkkel ennek a kérdésnek a tisztázását kívánjuk megalapozni. Az, hogy milyen adattípusok esnek pontosan ebbe a kategóriába, erősen személy- és szervezetfüggő. Ugyanakkor elmondható, hogy a megszerezni kívánt információ nagy eséllyel személyes adatnak minősül, így a szabályozás összetettségéből eredően olyan tényezők gyűjtését javasoljuk, amelyekből egy személy még közvetett módon sem azonosítható be egyértelműen. Ez a gyakorlatban azt jelenti, hogy általános jellegű OSINT-tevékenység valósítható meg, így az egyén nem tud fókuszba kerülni. Az általános jellegre egy példa az értelmezés vonatkozásában: az érintett szervezet fel kívánja mérni azt, hogy a szolgálati okostelefonokon a felhasználók milyen alkalmazásokhoz (például névjegyzék, kamera, üzenetek, naptár) milyen mértékű hozzáférést adnak más applikációknak. Ez egy biztonsági kockázat, amely legitimálni tudja a nyílt információs felmérés célját. Amennyiben ezeket az információkat egy applikáció csak mennyiségileg továbbítja, nem minősülnek személyes adatnak, azonban ha ezekhez eszközadatot is hozzárendel, akkor már igen. Ez pedig egy nagy dilemmát vet fel, amelyet a szervezetnek kell eldöntenie az OSINT-tevékenység előtt: érdemes-e a személyes adatok kezelésének útjára lépnie, vagy sem. A tevékenység akkor is hatékony lehet, ha megmarad az általános jelleg, a vállalat kiberhigiéniájának felméréséhez és oktatási anyagok létrehozásához nagyon nagy segítséget tud nyújtani. A súlyos, kiugró végletek, amelyek tényleg veszélyeztetik az intézmény biztonságát, azonban így nem beazonosíthatóak és nem szankcionálhatóak. Ha pedig a szervezet a személyes adatok kezelése mellett dönt, akkor a megismert jogszabály alapján neki kell mérlegelnie, hogy megéri-e a plusz jogi lépéseket a biztonsága. Még egy óriási hátulütője a rendelet alkalmazásának, hogy a benne foglalt adatkezelési szabályoknak meg kell felelni, de ezt a specifikussága miatt a jogszabály-értelmezésünkben nem taglaljuk.

3.2. A Magyarországon releváns jogszabályi háttér

Ebben a fejezetben a Magyarországon releváns jogszabályokat mutatjuk be és értelmezzük a nyílt információs adatgyűjtés szempontjából. Számunkra két jogforrás az, amely kulcsfontosságú: Magyarország Alaptörvénye és a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

Az Alaptörvény nem taglalja részletesen a kérdéskört, a VI. cikkében szól a személyes adatokról:

> „(1) Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák. A véleménynyilvánítás szabadsága és a gyülekezési jog gyakorlása nem járhat mások magán- és családi életének, valamint otthonának sérelmével. […]
> (3) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.
> (4) A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi."[49]

Az Alaptörvény is a GDPR-ból megismerthez hasonló nézőpontot képvisel az adatkezelést illetően: szintén az egyén felől közelíti meg a kérdéskört. A számunkra releváns adatkezelés kérdésével csak a VI. cikkben foglalkozik, tehát itt sem valósul meg az, hogy szervezeti szempontokból vizsgálják a tevékenységet. Ez sem előnyös a nyílt információból történő adatgyűjtés esetében. Az első bekezdésben megfogalmazott kritérium először nem tűnik relevánsnak, de fontos, mert esetünkben azt fejezi ki, hogy maga a tevékenység, azaz az adatok gyűjtése, feldolgozása, kielemzése, értékelése során nem fordulhat elő olyan helyzet, amely az egyénre nézve sértő. A harmadik pontban az Alaptörvény meghatározza azt, hogy mindenkinek joga van a személyes adatai védelméhez. Ez a kifejezés kulcsfontosságú: az egyéneknek nem egyszerűen az adataik, hanem a személyes adataik védelméhez van joguk. Ez nagyon hasonlít az európai adatvédelmi rendelet szemléletéhez, és a magyar jogszabályi háttér esetében itt rajzolódik ki, hogy a személyes adatnak minősülés irányából kell megközelíteni a kérdéskört.

Az Alaptörvény VI. cikkéhez kapcsolódik a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.). Ezt maga a törvény is megerősíti a bevezetőjében:

„Az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, a személyes adatok védelmét, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog érvényesülését szolgáló alapvető szabályokról, valamint az ezen szabályok ellenőrzésére hivatott hatóságról az Alaptörvény végrehajtására, az Alaptörvény VI. cikke alapján a következő törvényt alkotja".[50]

[49] Magyarország Alaptörvénye VI. cikk (1), (3)–(4) bekezdés.
[50] 2011. évi CXII. törvény.

E törvény bevezetőjének értelmezése is releváns számunkra, igaz, hogy a magyar jogban ez jóval rövidebb, de ez mutatja meg a jogalkotó tényleges szándékát és célját a jogszabállyal. A hazai törvény célja pedig teljesen azonos az EU adatvédelmi rendeletéével: mindkettő a személyes adatok védelmére irányul. Ezért a magyar jogszabályok esetében is az egyén felől kell megközelítenünk a kérdést, mert így tudjuk biztosítani a megfelelést. Az első szakasz megismétli a törvény célját:

> „E törvény célja a hatálya alá tartozó tárgykörökben az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák […].”[51]

Gyakran felbukkanó gondolat, és már lassan önismétlő hatást is kelt, de ennyiszer visszatérő elem és ennyire nyomatékos adatkezelési szempontból, hogy ez a jogszabály az érintettek szemszögét érvényesíti. Itt újra megerősítik azt a feltevést, hogy a cél az, hogy a természetes személyek magánszféráját tiszteletben tartsák az adatkezelők. Semmi olyat nem fogalmaznak meg, hogy bizonyos kivételes esetekben (például a biztonság növelése) az érintettek szféráját akár egy vállalat érdekei alá kell rendelni. A nyílt információs adatgyűjtésnél és adatkezelésnél mindig ezt kell szem előtt tartanunk, de még előnyösebb, ha a tevékenységbe belevonható az egyének érdekeltsége is.

A jogszabályi megfelelés kiemelt célja a párhuzamos tevékenység létrehozása. Az Infotv. hatálya szintén nagyon hasonló a GDPR hatályához: „[…] minden olyan adatkezelésre kiterjed, amely személyes adatra, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik”[52]. A magas szintű hasonulás a jogszabályi megfelelésből ered: az adatvédelemmel kapcsolatos magyar jogszabályoknak is eleget kell tenniük az uniós szabályozásnak, így az abban foglaltakhoz hasonló feltételeket szabnak. Az adatkezelőknek ettől függetlenül mind a hazai, mind az uniós rendeleteket be kell tartaniuk. A kulcskérdés az előbbinél is a személyes adat fogalma, hiszen a jogszabály csak arra az esetre vonatkozik, amikor személyes adatot kezelnek. A törvény hatályánál ezt definiálják, és egy az egyben a GDPR-ban használt meghatározást veszik át, illetve megerősítik azt, hogy a GDPR-ban foglaltak kötelező érvényűek attól függetlenül, hogy az Infotv. hatályos-e, vagy sem. Ez azt jelenti, hogy ha egy kérdéskör az adatvédelem

[51] 2011. évi CXII. törvény 1. §.
[52] 2011. évi CXII. törvény 2. §.

vonatkozásában nem szabályozott a hazai jogrendben, de a GDPR-ban igen, akkor az ott rögzített meghatározás kötelező érvényű. Ez nem előírt része egy jogszabálynak, viszont számunkra azt jelenti, hogy a magyar jogalkotó megerősíti és elismeri a felettes jogforrásban foglaltakat.

Az értelmező rendelkezésekben egy kicsit eltérően újra megfogalmazza a jogszabály a személyes adat definícióját, illetve bevezet egy új fogalmat, a különleges személyes adatot.

> „2. személyes adat: az érintettre vonatkozó bármely információ;
> 3. különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,
> 3a. genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;
> 3b. biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;”[53]

A GDPR értelmezéséhez képest a személyes adatot itt egyszerűbben fogalmazzák meg, viszont ez jelentésbeli eltérést nem hozott a képbe. A különbség a különleges adat megjelenésénél érződik. Ez semmivel sem más, mint a GDPR-ban rögzített személyesadat-fogalom, valójában nem bővült a definíció, csupán két részre bontották. A különleges adatok közül számunkra az egyedi azonosítást célzó biometrikus adat válhat relevánssá. A gyakorlatban OSINT-tevékenység során nagyon kevés esetben, esetleg telefonos applikációnál a képernyőzár módjának és adatainak gyűjtésekor merülhet fel a kérdéskör. Egy későbbi értelmezésben kiemeljük, hogy ez miért nem megvalósítható jogi szempontból. Ezek a definíciók viszont csupán magyarázóbb leírásai a GDPR személyesadat-kritériumának.

Az Infotv. is megfogalmaz személyes adatok kezelésére vonatkozó alapelveket:[54]

– jogszerű és tisztán meghatározott célú kell hogy legyen;

[53] 2011. évi CXII. törvény 3. §.
[54] 2011. évi CXII. törvény 4. §.

– csak az adatkezelés céljával összefüggő személyes adatok kezelhetők;
– adatkapcsolat elve – mindaddig személyes adat marad az információ, ameddig kapcsolódik az érintetthez;
– adatok pontosságának elve;
– adatok védelmének elve.

Ezen alapelvek szintén követik az európai uniós jogszabályban foglaltakat, és általánosságban elmondható, hogy az észszerű és jóhiszemű adatkezelést biztosítják. Itt is kirajzolódik, hogy az érintettek érdekét képviseli a jogszabály, nincs olyan pont és lehetőség, amely az adatkezelő szemszögéből közelíti meg a jogosultságot. Az alapelveknél is szem előtt kell tartani ezt, hogy nem a szervezet érdeke a létfontosságú, sőt, az semmilyen módon nem jelenik meg mint személyesadat-kezelésre feljogosító esetkör. Emiatt itt is csak a hozzájárulás függvényében történhet személyesadat-kezelés, amelynek jogalapja (és általános feltételei) a jogszabály szerint a következők:[55]

– ha törvény elrendeli;
– ha az adatkezelő törvényben meghatározott feladataihoz szükséges, és az érintett hozzájárult;
– létfontosságú érdek védelméhez kapcsolódik, és ezzel arányos;
– az érintett a személyes adatát kifejezetten nyilvánosságra hozta, és az adatkezelés ezzel arányos.

A különleges adatok kezelését illetően pedig a törvény még szigorúbb kritériumokat fogalmaz meg: azok lényegében törvényben meghatározott érdekek esetén használhatók. Az automatizált adatkezelés vonatkozásában szintén keményebb feltételeket szab a jogszabály: döntéssel együtt csak akkor engedélyezett, ha azt az érintett kifejezetten kéri, vagy az adatkezelőnek európai uniós jogi aktust kell végrehajtania. Az általános követelményekből sokkal szigorúbb kritériumrendszer rajzolódik ki, mint a GDPR-ban. A GDPR hozzájárulással lehetőséget ad az adatkezelésre, de ezt az Infotv. jelentősen szűkíti. A beleegyezés itt önmagában nem elegendő, hanem az is szükséges, hogy valamilyen egyedi feltétel fennálljon. Ez lehet az adatkezelő törvényi kötelezettsége vagy speciális létfontosságú érdek (például testi épség, vagyoni javak védelme). A különleges adat kezelésének lehetőségei pedig így még korlátozottabbak.

[55] 2011. évi CXII. törvény 5–7. §.

A nyílt információs személyes adatok kezelését, gyűjtését a jogszabály ezzel erősen visszaszorítja. Hogy az megvalósítható legyen, kritikus érdeknek és hozzájárulásnak kell mögötte állnia, amelyet a szervezetnek kell mérlegelnie és megvizsgálnia az esetkör előtt. Ez az OSINT-tevékenységre nézve nagy érvágás, de küzdeni ellene nem érdemes, mert abból később jogviták lehetnek. Ha személyes adatát kezelik, az érintettnek számos joga van, ezeknek az érvényesülését is biztosítani kell. A jogok röviden:[56]

- előzetes tájékozódáshoz való jog: az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről tudomást szerezzen;
- hozzáféréshez való jog: az adatkezelőnek az illető kérelmére rendelkezésére kell bocsátania a tárolt személyes adatait;
- az adatok helyesbítéséhez való jog;
- az adatkezelés korlátozásához való jog;
- az adatok törléséhez való jog.

Ezek szintén hasonlítanak a GDPR-ban megfogalmazottakhoz, ahogy a jogok érvényesülésének biztosításáról szóló rész is, amelynek értelmében az adatkezelő:

- mind műszakilag, mind szervezéssel biztosítsa, hogy az érintett jogai érvényesüljenek;
- ingyenesen lássa el az érintett jogaival kapcsolatos tevékenységét;
- előzetesen tájékoztassa az érintettet az adatvédelemmel kapcsolatos releváns információkról (például az adatkezelő, az adatvédelmi tisztségviselő személye, az adatkezelés célja és időtartama, az adatkezelés jogalapja);
- segítse elő az érintett adatokhoz való hozzáférését;
- biztosítsa a helyesbítéshez való jogot az érintettnek.

Ezek a jogok megerősítik azt, hogy az egyén van a törvény középpontjában, és az ő érdekében történik az adatkezelés. A jogszabály „hatalmat" ad az érintettnek az adatai fölött, így bármikor kérhet törlést, helyesbítést vagy módosítást. Ez szintén szűkíti az OSINT-tevékenységek lehetőségeit, mivel így a háttérben történő, felmérő jellegű személyesadat-kezelést nem lehet megvalósítani. Az adatkezelés szervezetre vonatkozó szabályait nem elemezzük ebben a tanulmányban, mivel azok túlzottan szervezetspecifikusak, hanem az OSINT-tevékenység jogi alapjára kívánunk itt választ adni.

[56] 2011. évi CXII. törvény 14–24. §.

Összességében elmondható, hogy a magyar jogszabály is szigorú a személyes adat kezelését illetően, sőt, a GDPR-hoz képest tovább szűkíti annak lehetőségeit. A megismert jogszabályi háttér fényében a ténylegesen hatékony és megvalósítható OSINT-tevékenységek alapja a nem személyes adatok kezelése. Arra kell kifejezetten figyelnie a szervezetnek, hogy az információk ne minősüljenek személyes adatnak, mert ha annak minősülnek, akkor az Infotv. és a GDPR szabályainak szigorúan meg kell felelniük, és ez a két rendelet jelentősen csökkenti bármilyen személyes adat kezelésének lehetőségét. A megismert szabályozás alapján szerintünk érdemesebb ezt a tevékenységet általános jelleggel folytatni és a személyspecifikus adatgyűjtést, személybeazonosíthatóságot mellőzni, mert abban az esetben jogszabályi felhatalmazásra van szükség a hozzájárulás mellett, ami a ténylegesen végezhető cselekvések körét jelentősen szűkíti.

4. A villamosenergia-vállalatok OSINT-tudatossága és képességei

Ebben a részben a mellékletben vázolt interjúkérdésekből leszűrt eredményeket tekintjük át. Az egyes témaköröket a kapott válaszok alapján külön ismertetjük az általános jellemzők és az alkalmazott gyakorlatok bemutatásával.

4.1. Miért van szükségük a vállalatoknak a nyílt forrású információszerzésre?

A nyílt forrású hírszerzés legnagyobb előnyei közé tartozik a korai adatszivárgás észlelése, ugyanis az OSINT-elemzők a keresőmotorok, weboldalak eltemetett adatai navigálásának szakértői, így hihetetlen gyorsasággal össze tudják szedni a szükséges információkat. A szivárgások korai detektálása és megállapítása a vállalat márkájának és hírnevének védelmére is szolgálhat, amely védelem az ügyfelek, vevők véleményének eldugott fórumokon vagy akár a *surface* vagy *deep weben* való felkutatásával is megvalósítható. Mindezek mellett a hírszerzés a gyors közvélemény-kutatással elősegítheti a kríziskommunikációt, és akár egy

felbecsülhetetlen értékű eszköz lehet a megalapozottabb döntések meghozatalához, ráadásul alacsony költséggel jár.

4.1.1. Az általános ismeretek felmérése

Kutatásunk során először a vállalatok OSINT-ról való általános ismereteit mértük fel, továbbá egy átfogó képet alkottunk a folyamataikról. Ezeket az alábbi kérdések tették lehetővé:

1. *Hogyan definiálja az OSINT-ot?*

2. *Véleménye szerint az OSINT a szervezetére nézve inkább lehetőség vagy kockázat?*

3. *Milyen, az OSINT-tal kapcsolatos normatív szabályzókat ismer?*

4. *Végeznek-e nyílt forrású információgyűjtést?*

Minden válaszadó tisztában volt az OSINT fogalmával, vagyis azzal, hogy az legális keretek között végzett, nyílt, bárki által hozzáférhető adatokból való információgyűjtés. A válaszadók feltűnően az OSINT támadó oldalát vették figyelembe a kitöltés során, vagyis azt a típusú hírszerzést, amellyel más cégekről gyűjthetnek össze a saját vállalatukat valamilyen kompetitív előnyhöz juttató információkat. A válaszokból rendre kihagyták az OSINT elleni védekezést, azaz a vállalatról kikerülő információk figyelését és kontrollálását.

A lehetőség és kockázat témakörében kettős kép rajzolódott ki: megközelítőleg azonos gyakoriságúnak tartották a pozitív és a negatív kimeneteleket. A képet azonban árnyalja, hogy bár látták a lehetőségeket, ezeket nem tartották teljes mértékben kihasználhatónak, különböző hiányosságokra hivatkozva. A kockázatok között megjelent a reputációs és az informatikai kockázat is, míg a lehetőségeket a válaszadók nem pontosították.

Normatív szabályzóknál a vállalati belső kommunikációs szabályzat és a magyar törvények jelentek meg, de több válaszadó üresen hagyta ezt a területet. Általánosságban kijelenthető, hogy a szervezet életében nincsen kiemelt szerepe az OSINT-műveletek során a különböző szabályzatoknak és törvényeknek. Árnyalja a képet, hogy minden válaszadó tudott példát mondani cégcso-

porton belüli informatikai biztonsági tudatosságnövelő képzésekre, valamint vállalati titkokat érintő és védő szabályokra. Ezek nem kizárólag az OSINT-tal foglalkoznak, de mindenképpen érintik a területet.

Összességében megállapítható, hogy a kitöltő vállalatok szisztematikus, folyamatkövető nyílt forrású hírszerzést akár anyagi, akár humánerőforrás-hiány miatt nem folytatnak. Sokkal elterjedtebb az eseti megkeresések alapján történő információgyűjtés. Ellenben nagy eltérés tapasztalható a vállalatok között: van olyan, amely ezt kizárólag csoportszintű feladatnak tartja, de olyan is, amely munkája során ennek a területnek stratégiai fontosságú szerepet adna, és a jövőbeli terveinek is része a képesség további fejlesztése. Ez nagyjából egybeesik a várakozásainkkal, miszerint a legtöbb piaci szereplő jelenleg nem foglalkozik operatív szinten OSINT-tal. A válaszok között megjelenik a sajtófigyelés is, amely manapság az ilyen hírszerzés legelterjedtebb típusa. A reputációs veszteségek megelőzése külső szolgáltató segítségével vagy megvásárolható szoftver útján könnyen definiálható és számszerűsíthető eredményt hoz, épp emiatt a vállalati szintű OSINT egyik népszerű formája. Ugyanakkor a cégcsoport dolgozói által a közösségi oldalakon végzett tevékenységek és a megosztott tartalmak figyelése, a támadások kivédése céljából nem jelenik meg. Pedig az így nyilvánossá tett adatok és információk elősegítik mind a *social engineering,* mind a tradicionális hackertámadások kivitelezését.

A vállalatok OSINT-ról való általános ismeretének szintje válaszaik alapján megnyugtató. Ideális esetben cégcsoportra vonatkozóan kell létrehozni szabályzatokat és folyamatokat, amelyekkel minden vállalatnak tisztában kell lennie, így közösen magasabb szintű tevékenységet tudnak végezni, és a kinyert információ jobban áramolhat a tagok között.

4.1.2. A kapacitás felmérése

A második kérdéskör a vállalatok jelenlegi és tervezett OSINT-kapacitását járja körül. Választ kerestünk rá, hogy amennyiben nem, miért nem végeznek információgyűjtést, továbbá mi hiányzik ahhoz, hogy széles körű és mélyebb hírszerzést folytassanak.

Ezt a területet az alábbi négy kérdés fedte le a kérdőívben:

5. *Ha nem végeznek, akkor szeretnének-e kialakítani ilyen képességet?*

6. *Ezen képesség kialakításában mely tényezők jelentik a legfőbb kihívást az alábbiak közül:*
   a) *szükséges technológiai erőforrás beszerzése;*
   b) *szükséges humán erőforrás biztosítása;*
   c) *szükséges szaktudás biztosítása?*

7. *Lát-e egyéb tényezőt, amely kihívást jelenthet ezen képesség kialakításában?*

8. *Ha végeznek nyílt forrású információgyűjtést, annak lépései mennyire dokumentáltak?*

Mindössze egy kitöltő állította, hogy kétséget kizáróan végeznek OSINT-tevékenységet, egy másik vállalat pedig, bár nem lát el ilyet, a jelenlegi eljárásaival teljesen elégedett volt. A többi cégnél nincsen folyamatban a képesség kialakítása, bár akár csoportszintű kérés, akár lehetőség esetén érdeklődőek és nyitottak lennének rá.

A kitöltők egyhangúlag a szükséges humán erőforrás biztosítását jelölték meg mint kritikus hiányzó tényezőt. A válaszokból az derül ki, hogy vagy pluszfőt igényelnének a csapatukba, vagy azt szeretnék, hogy a kollégák kapjanak időt erre. Továbbá többen is megjelölték a szaktudás hiányát. Mivel az ilyen jellegű feladathoz szükséges a vállalatcsoport működésének ismeretén túl a specializált technológiai szaktudás, új munkatárs felvétele vagy egy meglévő átképzése esetén jelentős időt vesz igénybe, hogy az megtanulja a helyi működést vagy megszerezze az OSINT-ismereteket.

Egy kivételével semelyik kérdőív nem fogalmaz meg további akadályt a képesség kialakítását illetően. A humán erőforrás biztosításán kívül az egyetlen felmerülő tényező az erre a területre fordítható keret lehet: költséghatékonyság miatt jelenleg nem opció a folyamattal való kísérletezgetés, és nincs szabad befektetési tőke új technológiák megvásárlására. Erre a problémára megoldást jelenthet az olyan eszközökbe való csoportszintű befektetés, amelyek mindegyik vállalat számára segítséget tudnak nyújtani.

A korábbi válaszoktól függetlenül az OSINT-tevékenység nem dokumentált módon működik. Elsősorban ad hoc projektek, kérések és megkeresések a jel-

lemzőek, már ahol egyáltalán van ilyen tevékenység. Ezeket előzmény alapon (a múltban nyilvánosan megjelent információkat kutatva) végzik el, a szerzett információkat pedig külön nem tárolják vagy dolgozzák fel. A módszertan nem egységes, inkább célorientáltan történik a keresés.

Az világos, hogy új kollégák felvételére, új ismeretek elsajátítására és technológiák, eszközök megvásárlására mindenképp költeni kell. Azonban, ahogy a többi kérdésből látszik, ezt meg kell hogy előzze a célok és módszerek pontos definiálása és dokumentálása. Természetesen a jelenlegi állapotban is vannak még rejtett tartalékok, elsősorban vállalati szinten, azonban a vállalatcsoport esetében ez kizárólag úgy tud érvényesülni, ha a kitöltők egy csoportszintű, definiált és strukturált folyamat részesei, ami lehetővé teszi a tevékenység visszakövetését, reprodukálását és a kinyert eredmények többszöri és több célból történő felhasználását.

A kérdőíveket kiegészítő szóbeli interjún elhangzottak alapján két terület tovább nehezíti a gyors kiépítést. Az egyik a kizárólagos hosszú távra tervezés, ami megakadályozza, hogy egy-egy projektet indítsanak ezen a téren a vállalatok. A másik pedig a feladatkiosztás megváltozása a vállalatstruktúra átalakulása során: korábbi központi feladatok eltűntek, a cégek pedig nem tudják beépíteni a képességet a szolgáltatásportfólióba. Erre a konkrét példa a különböző akvizíciókat vagy üzleti döntéseket megelőző vezetői összefoglaló készítése volt, amely korábban nagymértékben támaszkodott OSINT-technikákra, azonban jelenleg már semelyik kitöltő vállalat nem foglalkozik ilyen területtel.

4.1.3. Hol és mivel végeznek OSINT-tevékenységet?

A következő kérdéscsoport azt mérte fel, hogy pontosan hol, tehát milyen felületeken, honlapokon, nyílt adatbázisokban keresnek a kitöltők elérhető információkat, továbbá hogy amikor ilyen kutatást végeznek, akkor azt milyen eszközökről teszik. Alapvetően az OSINT definíciója miatt nem feltétlenül szükséges ezeket az eszközöket túlságosan korlátozni, mivel nyíltan hozzáférhető és legálisan gyűjtött információról beszélünk. Azonban az adatok felhasználása, tárolása és osztályozása miatt, megfelelve a GDPR-nak és további informatikai biztonsághoz köthető szabályozásoknak, szabványoknak és törvényeknek, senki nem lehet elég óvatos, így OSINT-tevékenység végzése esetén mindenképpen javasolt a hétköznapi felhasználásúnál zártabb rendszerek használata.

9. Milyen felületeken, platformokon végeznek nyílt forrású információgyűjtést?

A válaszadók közül felületszinten az OSINT mindössze egy vállalatnál jelent meg széleskörűen, amelyre hagyományos webes keresőmotorok (például Google), közösségi oldalak (például Facebook) és még a célzottan OSINT-tevékenységre specializálódott Maltego[57] használata is jellemző volt. A Maltego egy nyílt forráskódú hírszerző és grafikus kapcsolatelemző eszköz, egy Java-alkalmazás, amely Windows, Mac és Linux rendszereken fut, és nyomozati feladatokhoz szükséges információk gyűjtésére és összekapcsolására szolgál. Sokan használják, a biztonsági szakemberektől kezdve a törvényszéki nyomozókon át az oknyomozó újságírókig és kutatókig.

Ezenkívül mindössze egy kitöltő jelezte, hogy a cége valamilyen szinten formalizáltan céloz különböző platformokat. Ők a nyomtatott és az online sajtóból szereznek információkat. A többi vállalat elmondása alapján feladatfüggően, ad hoc folytat gyűjtést, olyankor pedig inkább célorientáltan, bármilyen felületet felhasználva.

10. Külön rendszeren végzik a nyílt forrású információgyűjtést, vagy ugyanazt a rendszert használják, mint amelyet a napi munkavégzésre is?

Egy kitöltő használ a hétköznapi munkavégzéstől elkülönülő rendszert információgyűjtésre, mindenki más az ügyviteli rendszerüket alkalmazza erre. A korábbi megállapítással azonosan igazából nem elképzelhetetlen az OSINT működése, de mindenképpen könnyebb a formalizált munkavégzés és a szabályzóknak való megfelelés, ha az OSINT-ot végző rendszerek elkülönülnek a többitől, legalább eszköz-, de akár hálózati szinten is.

11. Virtualizációt használnak?

Semelyik válaszadó nem használ virtualizációt.

„A virtualizáció olyan technológia, amely egyesíti vagy felosztja a számítási erőforrásokat, hogy egy vagy több operációs környezetet hozzon létre, olyan módszerek segítségével, mint a hardver- és szoftverparticionálás vagy -összevonás, részleges vagy teljes gépszimuláció, -emuláció, időmegosztás stb. A virtualizációs technológiáknak számos területen vannak fontos alkalmazásai, mint például

[57] Lásd: www.maltego.com.

a szerverkonszolidáció, biztonságos számítási platformok, több operációs rendszer támogatása, rendszermag-mentesítés, szerver- és szerveralapú kiszolgálás, hibakeresés és fejlesztés, rendszermigráció stb. Legtöbbjük hasonló működési környezetet kínál a végfelhasználónak, azonban nagymértékben különböznek az általuk alkalmazott absztrakciós szintek és a mögöttes architektúra terén."[58]

Az OSINT esetében azért használunk virtualizációt, hogy csökkentsük a saját rendszereink megfertőzésének veszélyét. Akár kézi, akár automatizált eszközöket alkalmazunk munkánk során, nem tudjuk elkerülni azt, hogy a talált és megnyitott dokumentum potenciálisan fertőző legyen, esetleg kifejezetten kibervédelmi mézesbödönként álljon előttünk.

Amennyiben virtualizációt használunk, jelentősen, szinte nullára csökkenthetjük annak az esélyét, hogy az ilyen fenyegetések elérjék az éles rendszereinket, és kárt tudjanak tenni bennük. A virtualizált rendszer ugyanis hálózatilag is elkülönülten tud futni, és ideális esetben egy kártevőnek köszönhetően kizárólag az aznapi munkát lehet elveszíteni.

12. Automatizáltan vagy manuálisan folytatnak információgyűjtést?

Felmérésünkben megvizsgáltuk, hogy a vállalatok az információgyűjtés folyamatát manuálisan vagy pedig automatizációs szoftverek segítségével végzik. Az interjúk során megállapítottuk, hogy ahol nyílt forrásból szereznek adatokat, azt manuálisan teszik. Ugyan túlnyomórészt így gyűjtik össze az információt, alkalmanként használják a Maltego nevű alkalmazást. De számos más program és szoftver is segíti és gyorsítja az adatgyűjtés folyamatát, például az OSINT Framework[59] vagy a Shodan[60]. A Google a legismertebb és legnépszerűbb böngésző, azonban a Shodan, más keresőmotorokkal ellentétben, a biztonsági szakemberek számára sokkal érthetőbb és könnyebben értékelhető eredményeket biztosít. Az OSINT Framework pedig a nyílt forrású hírszerzésre használt eszközök összegyűjtésére készült keretrendszer, amelynek célja, hogy segítsen az embereknek megtalálni az ingyenes OSINT-forrásokat.

[58] Nanda–Chiueh 2005: 1. Az idézet a szerzők fordítása.
[59] Lásd: https://osintframework.com.
[60] Lásd: www.shodan.io.

13. Amennyiben manuálisan folytatják a nyílt forrású információgyűjtést, milyen gyakorisággal teszik? Mennyi humánerőforrás-időt igényel naponta/hetente?

Vizsgálatunk során megállapítottuk, hogy a folyamat formalizálatlansága, valamint a projektszerű és megrendelésalapú működés következtében a kérdésre nem tudtak a vállalatok pontos válasszal szolgálni.

14. Milyen keresőmotort használnak jellemzően?

Az interjúk során kapott válaszok alapján a vállalatok által használt egyetlen keresőmotor a Google, amelynek számos hasznos kiegészítő funkciója van. Ezek között szerepel például a *deep web search,* amelynek segítségével a *deep weben* is kereshetünk. Ez a funkció a Google Chrome megnyitása után az Alt + Shift + F billentyűkombináció lenyomásával érhető el és használható. Továbbá talán egyik legismertebb előnye a Google Dorks és a Google Hacking Database, amelyekkel szűkíthetjük és pontosíthatjuk, irányíthatjuk a keresést. A Google Dorks segítségével kereshetünk fájlkiterjesztésekre, URL- és weblapcímekre is. A Google Hacking Database elérhető az exploit.db nevű oldalon, valamint folyamatosan frissítik. Ezenfelül a Google-nak létezik képkereső funkciója, amellyel hasonló képeket lehet keresni, vagy felkutathatjuk az eredetit is, de egy adott személyről készült felvételekre is rátalálhatunk. Erre a legalkalmasabb, bár kevésbé ismert oldal a PimEyes[61] arcfelismerő eszköz, amelynek felületén napi 10 keresés ingyenesen lefuttatható.

15. Használnak-e rejtett kommunikációt?

Vizsgálatunk során megállapítottuk, hogy a vállalatok egyike sem használ rejtett kommunikációt. Annak érdekében, hogy értelmezni tudjuk az információgyűjtés és -szerzés célját, módszereit, lépéseit, illetve a folyamatok elleni védekezést, vagyis az információk védelme érdekében tett intézkedéseket, elengedhetetlen, hogy tisztában legyünk az alapvető fogalmakkal és jelenségekkel. A hírszerzés típusától függetlenül elsőként szükséges tisztázni, hogy mire irányulnak ezek az információs tevékenységek, tehát mi a művelet tárgya. Konkrétan az általunk vizsgált témakörben a lényegi kérdés az információk és adatok gyűjtése, majd azok felhasználása.

[61] Lásd: https://pimeyes.com/en.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rögzíti, hogy az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. A jogszabály leszögezi, hogy az információ bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában közölt tapasztalat, megfigyelés vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét átalakítja, megváltoztatja, illetve befolyásolja, továbbá bizonytalanságát csökkenti vagy megszünteti.

Az említett források közé tartoznak a nyilvánosan elérhető adathordozók, ilyenek az általános módon publikált anyagok, kötetek, könyvek, folyóiratok, konferencia-előadások, közösségimédia-tartalmak. Az OSINT tárháza szinte végtelen, viszont manapság az internet fejlődésének és a globalizációnak köszönhetően ez a módszer mondható a legjobbnak a cél elérése érdekében.

16. Milyen elérhető források között keresnek?

A kérdőívet kitöltő vállalatoknál az elérhető források kihasználtsága széles skálán mozog. Az erre a kérdésre adott válaszokból is tisztán látszik, hogy melyek azok a cégek, amelyek jelenleg is használnak OSINT-eszközöket, vagy legalább a közeljövőben kívánják kihasználni a tevékenység nyújtotta lehetőségeket.

17. Mire keresnek jellemzően?

A kutatásban érintett szereplők a tevékenységüktől függően jelölik ki azokat a témaköröket, amelyekben adatokat, jobb esetben pedig információt kívánnak gyűjteni.

18. Melyek azok a kulcsszavak, információk, amelyek az OSINT szempontjából lényegesek a vállalata számára?

A kérdésre adott válaszok eltérőek voltak. Itt is megjelent a vállalatokra jellemző profil, amely az egyes válaszadóknál megegyezett a keresett témakörrel. Ezzel szemben láthattunk példát a versenytársakra, illetve olyan nyíltan elérhető adatokra történt irányított, kulcsszavas keresésekre, amely információk magukban foglalják a cégekhez köthető e-mail-címeket, más esetben vállalati felhasználóazonosítókat, informatikai rendszereket és azok elérhetőségeit.

19. Igénybe veszik-e külső, harmadik felek (beszállítók, alvállalkozók, tanácsadók) segítségét az OSINT bármelyik állomása során?

Három érintett adott igenlő választ, akik közül kettő ugyanazt a médiafigyelő szolgáltatót nevezte meg mint harmadik felet, a harmadik pedig egy, az adott vállalaton belül működő szervezeti egységet jelölt meg mint támogató elemet. A többiektől nemleges választ kaptunk.

20. Hogyan dolgozzák fel a találatokat? Használnak-e szabadszavas keresőt?

Két esetben használnak szabadszavas keresőt az érintettek, egy szereplő pedig a manuális adatfeldolgozást preferálja.

21. Hogyan és meddig tárolják az információgyűjtés során szerzett nyers adatokat?

Egy válaszadó konkrét törvényi szabályozásra (Infotv.) hivatkozott, míg a többiek úgy nyilatkoztak, hogy az információgyűjtés témájától függően tárolják az adathalmazokat (például intranet). Egy kirívó esetben az adatgyűjtést végző munkatársra bízták az adatok megőrzésének időtartamát, ami egy kevésbé kötött belső szabályozási környezetre utal.

22. A mobilalkalmazások adatait felhasználják-e nyílt információszerzéshez?
A kérdésre az összes kitöltő nemleges választ adott.

23. A nyílt információgyűjtésbe bevonják-e az alkalmazottak közösségimédia-profiljait is, és ha igen, milyen mélységben?

Napjainkban egyre népszerűbb és hangsúlyosabb a közösségimédia-portálokon történő aktivitás, kommunikáció, jelenlét, azonban sokan nem ismerik fel az ezekben a felületekben rejlő veszélyeket. A koronavírus miatt a mindennapos kommunikáció is eltolódott az online térbe, hiszen annak egyik elsődleges forrását a karantén alatt a közösségimédia-oldalak jelentették, ami jelentősen növelte a felhasználók digitális lábnyomát. Ez azon nyomok, információk összessége, amelyeket az internetezők online tevékenységük és jelenlétük után hagynak, és amelyek alapján aktivitásukról következtetéseket lehet levonni. Az online térben történő nyílt forrású hírszerzés is felhasználja ezeket a nyomokat, hogy

átfogó, részletes és informatív profilt alkosson egy adott személyről. Az ilyen eredetű információkkal visszaélve küldhetnek célzott adathalászleveleket, vagy egy kibertámadáshoz használhatják fel az adatokat. Ezért egyre több vállalat bővíti ki információbiztonság-tudatosítási tréningjét a közösségimédia-portálok megfelelő használatával.

Vegyük például a LinkedInt, a világ legnagyobb professzionális hálózatát. Segítségével a felhasználók megtalálhatják a megfelelő állást vagy szakmai gyakorlatot, szakmai kapcsolatokat alakíthatnak ki és ápolhatnak, valamint elsajátíthatják a karrierjükhöz szükséges készségeket. A LinkedIn elérhető asztali számítógépről, mobilalkalmazásból, mobil webes élményből vagy a LinkedIn Lite Android-applikációból. Számos előnye mellett viszont nagyon sok veszélyt is rejt magában, hiszen e felületen keresztül megkereshetőek egy adott szervezet alkalmazottai, az ő profiljukból, képességeikből pedig kiszűrhetőek a cég által használt technológiák, vagy a vállalat álláshirdetéséből, a szükséges technikai készségek révén. Ezenfelül képek megosztására is van lehetőség, ami szintén veszélyes lehet, ha a fotót a belépőkártyával a nyakában készíti a felhasználó, vagy egy olyan monitorral a háttérben, amelyen érzékeny adatok olvashatóak, esetleg egy ráragasztott cetlire írva a dolgozó jelszava.

Az interjú során megfigyeltük, hogy a vállalatok gyűjtenek-e információt nyílt forrásból az alkalmazottaikról. A felmérés keretében elsősorban a közösségimédia-portálokon keresztül történő adatgyűjtést vizsgáltuk. Az első kérdés ez volt: A nyílt információgyűjtésbe bevonják-e az alkalmazottak közösségimédia-profiljait, és ha igen, milyen mélységben? Az interjú eredményeit három csoportba soroltuk: a vállalat nem végez, csak mérsékelten végez, illetve végez ilyen adatgyűjtést.

Az első csoport esetében a cégek nem folytatnak semmiféle információgyűjtést. A második kategóriába tartozó szervezetekre jellemző bizonyos mértékű nyílt forrású adatgyűjtés. Itt az elsődleges közösségimédia-portálok a Facebook, LinkedIn, Instagram, Twitter, YouTube, valamint társkereső oldalak. A harmadik csoport tagjai a leírtak szerint is végeznek nyílt forrású információgyűjtő tevékenységeket, nemcsak passzív módon, hanem akár aktív interakcióba is kezdenek az alkalmazottakkal, egy baráti felkérés vagy üzenetküldés által. Ennek oka a biztonságtudatosság felmérése, továbbá a jövőbeli oktatási anyagok összeállításához történő információgyűjtés. Az ilyen interaktív vizsgálatot végző szervezetek viszont az adatokat semmilyen más módon nem használják fel.

24. Végeznek-e profilalkotást a kinyert információk alapján? Ha igen, ezt hogyan és meddig tárolják?

Ezt az előző kérdéshez szorosan kapcsolódva az ott felosztott csoportok közül csupán a második és harmadik esetében vizsgáltuk. A második kategóriába tartozó vállalatok nem csinálnak profilalkotást, csupán szűrő jelleggel végzik ezeket a tevékenységeket, az információkat nem is tárolják. A harmadik csoport tagjai csak a *social engineering auditok* keretében, közösségimédia-fókusszal összegyűjtött információk alapján készítenek anonim – azaz konkrét természetes személyhez nem köthető – értékeléseket és elemzéseket a későbbi oktatási anyagok összeállításához. Így profilalkotás ebben az esetben sem történik.

25. Történt-e a szervezetükben olyan információbiztonsági incidens, amelynek hátterében OSINT-tevékenység állhatott?

A támadóképességek mellett a védekezőképességeket is felmértük kutatásunk során, és ez volt az első erre vonatkozó kérdésünk. A vállalatokat, mint ahogy minden céget vagy magánszemélyt, szintén érték adathalász-támadások, amelyek a nyílt forrású hírszerzés felhasználási lehetőségeinek egyikét jelentik. Ezenfelül a szervezetek úgy vélik, hogy az ügyfélszolgálati honlapjukon történő visszaélések hátterében is OSINT-tevékenység állhat, ez azonban nehezen bizonyítható. Tehát a vállalatokat is érintik a ma már mindennaposnak számító adathalászkampányok, ugyanakkor más OSINT-akcióból származó incidensről nem tudnak.

26. Ha igen, ezt hogyan követték vissza?

A következő kérdésünk az előzőben megfogalmazott, OSINT-tevékenységből eredő incidensek visszakövetésére vonatkozott, ami a biztonsági terület feladata. Mivel az adathalász-támadásokon kívül más nyílt forrású hírszerzéssel kapcsolatban álló incidens nem történt, nem vizsgáltuk tovább ezt a kérdést.

27. Az egyes incidenseket besorolják-e veszélyességi szintek szerint?

Kitértünk egy kérdés erejéig az egyes incidensek biztonsági szintbe sorolására, amelyet a társaságok információbiztonsági szabályzataiban rögzítenek, és amely az ott meghatározott szintek alapján történik. A vállalatoktól kapott

válaszok szerint minden esetben az információbiztonsági szabályzatban foglaltak szerint járnak el.

28. Milyen jogi lépéseket tettek az incidenskezelést követően?

A támadásokra vonatkozóan az adott jogi lépésekre kérdeztünk rá. Ezek megtétele a biztonsági és jogi terület feladat- és hatáskörébe tartozik. A vállalatok legjobb bevett gyakorlata, hogy az incidens okozóját a feltárt és általa előidézett kockázat megszüntetéséről szóló nyilatkozattételre kérik fel. Azonban nyílt forrású hírszerzési tevékenység nyomán történt incidens esetében jelen állás szerint nem került sor jogi lépésekre. Ennek oka az előzőleg leírtak alapján az, hogy a villamosenergia-rendszer vállalatait ért egyetlen OSINT-tevékenységből származó támadástípus, amely igazolhatóan bekövetkezett, az adathalászat volt.

29. Lehetséges-e Ön szerint az OSINT-ot alkalmazni a reputációs veszteségek csökkentésére?

E kérdés esetében is az előzőleg kialakított három csoport alapján értékeltük az interjúk eredményét. Az első csoportnál, ahol a vállalatok nem végeznek semmiféle információgyűjtést, a válasz semleges volt, míg a második tagjai, amelyek aktív adatgyűjtést folytatnak, úgy vélik, hogy lehetséges a reputációs veszteség. Ugyanígy gondolják a harmadik kategória cégei, amelyekre szintén jellemző a nyílt forrású információgyűjtés és azon túl az aktív kapcsolatfelvétel is. Elképzelhetőnek tartják azt, hogy ha egy megfelelően konfigurált, automatizált OSINT-eszköz a vállalatcsoportot érintő, negatív tartalmú információról ad riasztást, akkor a kommunikációs területtel együttműködve – az információ széles körű elterjedése előtt – megelőző intézkedéseket lehet hozni. (A válaszadók minden esetben a vállalatról a közösségi platformokon megjelent hírek, bejegyzések, hozzászólások vizsgálatát tartották szem előtt, nem az alkalmazottakra vonatkozó kereséseket.)

30. Milyen megelőző intézkedéseket tesznek, hogy a vállalat működése során a dolgozókról gyűjtött adatok ne legyenek nyíltan elérhetőek?

31. Ha nem tesznek ilyen megelőző intézkedéseket, akkor szeretnének-e a jövőben ilyen képességet kialakítani?

A vállalatok a tudatosítást tartják a legjobb módnak arra, hogy biztosítsák, a dolgozókról gyűjtött adatok ne legyenek nyíltan elérhetőek. Ha a munkavállalók megértik, milyen kockázatai vannak a nyilvános adatmegosztásnak, akár a magánéletük tekintetében, maguk is érdekeltté tehetőek az adatok védelmében. A jövőre nézve pedig fontos a tananyagok folyamatos modernizálása, aktualizálása, ezzel tovább segítve a megelőzést. A témakört szabályozó adminisztratív intézkedések meghozatalát is jó módszernek vélik.

32. Ezen képesség kialakításában mely tényezők jelentik a legfőbb kihívást az alábbiak közül:
a) *szükséges technológiai erőforrás beszerzése;*
b) *szükséges humán erőforrás biztosítása;*
c) *szükséges szaktudás biztosítása?*

33. Lát-e egyéb tényezőt, amely kihívást jelenthet ezen képesség kialakításában?

A képességek kialakítása esetében a legnehezebbnek a szükséges humán erőforrás megtalálását tartják, ezt pedig a szükséges szaktudás és technológiai erőforrás biztosítása követi.

34. Szerveznek-e rendszeres sérülékenységvizsgálatot? Ennek a fingerprinting/reconnaissance, vagyis a teszteket megelőző információgyűjtési fázisának része-e a vállalatukról online hozzáférhető információk vizsgálata? Ha igen, hogyan kezelik az esetleges találatokat?

Arra is kíváncsiak voltunk, hogy a megkérdezett cégek szerveznek-e sérülékenységvizsgálatot. Erre többféle válasz érkezett, de általánosságban elmondható, hogy többféle információbiztonsági tesztet végeznek. Egy válaszadó úgy nyilatkozott, hogy szolgáltatásként is nyújtanak sérülékenységvizsgálatot, majd javaslatokat tesznek a megrendelőnek a feltárt kockázatok kezelését illetőleg. Ezek a javaslatok minden partner esetében vállalatspecifikusak, a kockázat

mértékéhez igazodnak. Náluk *social engineering auditra, social media reconra, rubber duckyra* (billentyűzetet emuláló pendrive), illetve *phishingre* is lehetőség nyílik. A kitöltők közül volt, aki *black box* jellegű sérülékenységvizsgálatot szokott kérni, azonban a rendszerelemzések mindig célzottak, sosem általános behatolási kísérletek. Egy válaszadó nyílt forrású információgyűjtést is végez, amelynek eredményeit a vállalat későbbi vizsgálatai során is felhasználják.

35. Ön szerint OSINT-támadások elleni védelem esetén meddig tud eljutni egy támadó, azaz van-e olyan pont (és azt lehetséges-e meghatározni) a szervezetben, amelyen semmilyen esetben sem hatolhatnak át?

Összességében elmondható, hogy nem definiálható ilyen pont. A válaszadók véleménye szerint ha a munkavállalók betartják az előírásokat, akkor nem juthat be a támadó, valószínűleg elakad vagy felderítik.

36. A szervezetre irányuló, felderítő célú OSINT-tevékenységek naplózási adatait elemzik-e?

37. Védekezés és támadás tekintetében használnak AI-alapú módszert, vagy van-e tervben ilyesmi alkalmazása a jövőben?

38. Foglalkoznak-e nyílt információgyűjtésre alkalmas szoftver fejlesztésével? Ha igen, mikor kezdték meg ezt, illetve milyen hatékonysággal működik?

A megkérdezettek közül csak egyetlenegynek vannak információi a szervezetre irányuló, felderítő célú OSINT-tevékenység naplózásáról. Továbbá védekezés és támadás esetén nem használnak AI-alapú technológiát, és nem is foglalkoznak nyílt forrású információgyűjtésre alkalmas szoftver fejlesztésével.

39. Rendelkezik-e a terület valamilyen szabályozással? Van-e eljárásrend releváns találat esetén esemény eszkalálására?

A megkérdezetteknél nincs ilyen, vagy nem foglalkoznak esemény eszkalálásával kapcsolatos eljárásrenddel. Egy válaszadó említette az információbiztonsági szabályzatot, amelyben szerepel eszkalációs rend, azonban nyílt forrású információgyűjtésre vonatkozót nem tartalmaz.

40. Milyen jogi akadályokba ütköznek, amelyek a hatékony és szükséges információgyűjtést gátolják?

41. Ön szerint milyen hazai és/vagy nemzetközi jogi szabályozásra vagy változtatásra lenne szükség?

Az interjú során kitértünk a nyílt forrású hírszerzés jogi korlátaira is. Ilyeneket nem azonosítottak a vállalatok, azonban egy megkérdezett pont a normatív eszközök hiányát említette mint legnagyobb akadályt. A kitöltők szerint szükség lenne egy hazai és/vagy nemzetközi szabályozásra, amely meghatározza az OSINT-tevékenység kereteit és határait, főleg az internet mint információforrás tekintetében. Itt ugyancsak fontos a nagyobb közösségi oldalak és keresőmotorok (például Facebook, Google, Twitter, Instagram) részletesebb szabályozása.

42. Hogyan értékeli szervezete OSINT-képességét (1–10-es skálán, ahol az 1-es a leggyengébb, a 10-es a legjobb)?

Erre a kérdésre eltérő válaszokat kaptunk. Az egyik megkérdezett 2-esre értékelte magukat, mert a szervezetükben maximum egy terület végez ilyen jellegű tevékenységet.

43. Önnek milyen javaslatai lennének szervezete OSINT-fejlesztésére?

Végezetül pedig kíváncsiak voltunk, milyen ötleteik vannak arra, hogy szervezetük OSINT-tevékenységét javítsák. Egy válaszadó szerint ezt célszerű lenne a központi biztonsági terület által meghatározott és végrehajtott formában végezni. Egy másik egy olyan automatizált OSINT-eszköz beszerzését javasolta, amely nemcsak a biztonsági, hanem az üzleti folyamatok támogatására is alkalmas (például üzleti hírszerzés).

4.2. Javaslatok

Az interjúk alapján javasoljuk a felhasználói jogosultságokkal és felelősségi körökkel arányos oktatás és a biztonságtudatosság fenntartását, valamint a közösségi média megfelelő használatának e tananyagokba való integrálását. Azért tartjuk fontosnak az optimális közösségimédia-használat oktatását,

hogy a vállalatok a lehető legkevesebbre csökkentsék az interneten fellelhető olyan információk számát, amelyeket a támadók felhasználhatnak egy későbbi adathalász-kísérletre vagy a cég hírnevének károsítására.

Tanácsoljuk továbbá az automatizált eszközök bevezetését, valamint a jelenleg használt keresőmotorok kibővítését, a kutatásunk során korábban említett programok alkalmazását. Például ajánljuk az OSINT Framework használatát, amely az ingyenes eszközökből vagy forrásokból történő információgyűjtésre összpontosít. A célja az, hogy segítsen az embereknek megtalálni az ingyenes nyílt információs forrásokat. Előfordulhat, hogy egyes webhelyek regisztrációt igényelnek, vagy további adatokat kínálnak magas áron, azonban a keretrendszer segítségével a vállalatok képesek lehetnek arra, hogy a rendelkezésre álló információk legalább egy részét hatékonyan és díjmentesen szerezzék be. Javasoljuk továbbá a Shodan platform használatát, amely révén nemcsak az ismert hálózat figyelhető meg, hanem hálózati eszközök megtalálására is alkalmas az interneten. Észlelheti az adatszivárgásokat a felhőben, adathalászwebhelyeket detektálhat, és veszélyeztetett adatbázisokat tárhat fel, ami elősegíti a vállalatok hírnevének védelmét, valamint lehetőséget biztosít az internethez csatlakoztatott összes eszköz megfigyelésére. Természetesen a listáról nem maradhat le a Paterva fejlesztette Maltego sem, amely mára már a Kali Linux – sérülékenységvizsgálatokra, külső és belső hálózati betöréstesztekre és biztonsági auditokra fejlesztett operációs rendszer – beépített eszközévé vált, de Windows operációs rendszerre is elérhető. A Maltego számos beépített transzformáció lefuttatásával segít jelentős és átfogó felderítést végezni (valamint lehetővé teszi egyedi módosítások implementálását is). Van egy úgynevezett *community,* azaz közösségi verziója, amelynek használata ingyenes, de funkcióiban korlátozott a fizetős verzióhoz képest.

Az előbb említett két pont mellett fontosnak tartjuk az információgyűjtés formalizálását, dokumentálását egy kidolgozott szabályzat elkészítésével, amely tartalmazza a folyamat lépéseit, hatályát, alkalmazott és releváns jogszabályi környezetét, valamint a vállalatok által használt módszertanokat és eszköztárat. Végezetül pedig javasoljuk az I-Intelligence-től az *Open Source Intelligence Tools and Resources Handbook 2020,* valamint Heather J. Williams és Ilana Blum *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* című tanulmányának feldolgozását az OSINT-képességek fejlesztése és fontosságának megértése érdekében.

Felhasznált irodalom

Bányász Péter (2015): A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3(2), 21–36.

Barnea, Avner (2019): Big Data and Counterintelligence in Western Countries. *International Journal of Intelligence and CounterIntelligence,* 32(3), 433–447. Online: https://doi.org/10.1080/08850607.2019.1605804

Bello-Orgaz, Gema – Jung, Jason J. – Camacho, David (2016): Social Big Data: Recent Achievements and New Challenges. *Information Fusion,* 28, 45–59. Online: https://doi.org/10.1016/j.inffus.2015.08.005

Bergman, Michael K. (2001): White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing,* 7(1). Online: https://doi.org/10.3998/3336451.0007.104

Day, Tony – Gibson, Helen – Ramwell, Steve (2016): Fusion of OSINT and Non-OSINT Data. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser (szerk.): *Open Source Intelligence Investigation. From Strategy to Implementation.* Cham: Springer, 133–152. Online: https://doi.org/10.1007/978-3-319-47671-1_9

Deák Veronika (2018): A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során. *Hadmérnök,* 13(3), 391–402.

Fleisher, Craig S. (2008): Using Open Source Data in Developing Competitive and Market Intelligence. *European Journal of Marketing,* 42(7–8), 852–866. Online: https://doi.org/10.1108/03090560810877196

Gandomi, Amir – Haider, Murtaza (2015): Beyond the Hype: Big Data Concepts, Methods, and Analytics. *International Journal of Information Management,* 35(2), 137–144. Online: https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gong, Seonghyeon – Cho, Jaeik – Lee, Changhoon (2018): A Reliability Comparison Method for OSINT Validity Analysis. *IEEE Transactions on Industrial Informatics,* 14(12), 5428–5435. Online: https://doi.org/10.1109/TII.2018.2857213

Információs Hivatal: *A hírszerzés forrásai.* Online: www.mkih.hu/a-hirszerzes-forrasai.html

Kalpakis, George – Tsikrika, Theodora – Cunningham, Neil – Iliou, Christos – Vrochidis, Stefanos – Middleton, Jonathan – Kompatsiaris, Ioannis (2016): OSINT and the Dark Web. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser (szerk.): *Open Source Intelligence Investigation. From Strategy to Implementation.* Cham: Springer, 111–132. Online: https://doi.org/10.1007/978-3-319-47671-1_8

Kandias, Miltiadis – Mitrou, Lilian – Stavrou, Vasilis – Gritzalis, Dimitris (2013): Which Side Are You On? A New Panopticon vs. Privacy. In *Proceedings of the*

10th International Conference on Security and Cryptography (SECRYPT). Setúbal: SciTePress, 98–110. Online: https://doi.org/10.5220/0004516500980110

Lévay Gábor (2006): *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem.

Li, Yaliang – Gao, Jing – Meng, Chuishi – Li, Qi – Su, Lu – Zhao, Bo – Fan, Wei – Han, Jiawei (2015): A Survey on Truth Discovery. *ACM SIGKDD Explorations Newsletter,* 17(2), 1–16. Online: https://doi.org/10.1145/2897350.2897352

Liu, Bing – Zhang, Lei (2012): A Survey of Opinion Mining and Sentiment Analysis. In Aggarwal, Charu C. – Zhai, ChengXiang (szerk.): *Mining Text Data.* Boston: Springer, 415–463.

Mármol, Félix Gómez – Pérez, Manuel Gil – Pérez, Gregorio Martínez (2014): Reporting Offensive Content in Social Networks: Toward a Reputation-Based Assessment Approach. *IEEE Internet Computing,* 18(2), 32–40. Online: http://dx.doi.org/10.1109/MIC.2013.132

Nanda, Susanta – Chiueh, Tzi-cker (2005): *A Survey on Virtualization Technologies.* Online: www.computing.dcu.ie/~ray/teaching/CA485/notes/survey_virtualization_technologies.pdf

NATO: *NATO Open Source Intelligence Handbook* (2001): Norfolk: [k. n.]. Online: https://archive.org/details/NATOOSINTHandbookV1.2/mode/2up

Noubours, Sandra – Pritzkau, Albert – Schade, Ulrich (2013): NLP as an Essential Ingredient of Effective OSINT Frameworks. In *2013 Military Communications and Information Systems Conference (MCC 2013).* Piscataway: IEEE, 1–7.

Ranade, Priyanka – Mittal, Sudip – Joshi, Anupam – Joshi, Karuna (2018): Using Deep Neural Networks to Translate Multi-Lingual Threat Intelligence. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI 2018).* [H. n.]: IEEE, 238–243. Online: https://doi.org/10.1109/ISI.2018.8587374

Shere, Anjuli R. K. (2020): Now You [Don't] See Me: How Have New Legislation and Changing Public Awareness of the UK Surveillance State Impacted OSINT Investigations? *Journal of Cyber Policy,* 5(3), 429–448. Online: https://doi.org/10.1080/23738871.2020.1832129

Solti István (2019): Az OSINT információgyűjtő eszközeiről. *Nemzetbiztonsági Szemle,* 7(2), 3–18.

Stieglitz, Stefan – Mirbabaie, Milad – Ross, Björn – Neuberger, Christoph (2018): Social Media Analytics – Challenges in Topic Discovery, Data Collection, and Data Preparation. *International Journal of Information Management,* 39, 156–168. Online: https://doi.org/10.1016/j.ijinfomgt.2017.12.002

Vopham, Trang – Hart, Jaime E. – Laden, Francine – Chiang, Yao-Yi (2018): Emerging Trends in Geospatial Artificial Intelligence (GeoAI): Potential Applications for Environmental Epidemiology. *Environmental Health,* 17(1). Online: https://doi.org/10.1186/s12940-018-0386-x

Wong, B. L. William (2016): Fluidity and Rigour: Addressing the Design Considerations for OSINT Tools and Processes. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser (szerk.): *Open Source Intelligence Investigation. From Strategy to Implementation.* Cham: Springer, 167–185. Online: https://doi.org/10.1007/978-3-319-47671-1_11

Zago, Mattia – Nespoli, Pantaleone – Papamartzivanos, Dimitrios – Pérez, Manuel Gil – Mármol, Félix Gómez – Kambourakis, Georgios – Pérez, Gregorio Martínez (2019): Screening Out Social Bots Interference: Are There Any Silver Bullets? *IEEE Communications Magazine,* 57(8), 98–104. Online: https://doi.org/10.1109/MCOM.2019.1800520

Jogszabályok

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) 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)

Magyarország Alaptörvénye

Ajánlott irodalom

Bielska, Aleksandra – Kurz, Noa Rebecca – Baumgartner, Yves – Benetis, Vytenis (2020): *Open Source Intelligence Tools and Resources Handbook.* [H. n.]: I-intelligence. Online: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

Burns, Matt (2020): Open Source Intelligence: What Social Media Can Tell Us. *CameraForensics,* 2020. február 14. Online: www.cameraforensics.com/blog/2020/02/14/open-source-intelligence-what-social-media-can-tell-us/

Echosec Systems Ltd. (2019): 5 Reasons Why Every Organization Needs an OSINT Team. *Flashpoint,* 2019. május 31. Online: www.echosec.net/blog/-5-reasons-why-every-organization-needs-an-osint-team

g0tmi1k (2021): *What is Kali Linux?* Online: www.kali.org/docs/introduction/what-is-kali-linux

Mckay, Dave (2020): How to Use OSINT to Protect Your Organization. *How-To Geek,* 2020. november 27. Online: www.cloudsavvyit.com/8214/how-to-use-osint-to-protect-your-organization/

Social Media and Cybersecurity – Navigating the risks. *Sophos Home,* 2020. november 5. Online: https://home.sophos.com/en-us/security-news/2020/social-media-and-cybersecurity.aspx

What is a Digital Footprint? *Netsafe,* 2021. április 22. Online: www.netsafe.org.nz/digital-footprint/

Williams, Heather J. – Blum, Ilana (2018): *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.* Santa Monica: RAND Corporation.

Vákát

Melléklet

A vizsgálat során feltett interjúkérdések

Az alábbiakban ismertetjük azokat a kérdéseket, amelyek alapján a Nemzeti Közszolgálati Egyetem hallgatói elkészítették az interjúkat, továbbá meghatározták a tudatossági és készségi eredményeket a megkérdezett vállalaton belül. A kérdések négy fő témakör köré összpontosultak, ezek az általános ismeretek, a kapacitás felmérése, az OSINT-tevékenységek típusai és a javaslatok.

Az interjúkérdések a következők voltak:

1. *Hogyan definiálja az OSINT-ot?*

2. *Véleménye szerint az OSINT a szervezetére nézve inkább lehetőség vagy kockázat?*

3. *Milyen, az OSINT-tal kapcsolatos normatív szabályzókat ismer?*

4. *Végeznek-e nyílt forrású információgyűjtést?*

5. *Ha nem végeznek, akkor szeretnének-e kialakítani ilyen képességet?*

6. *Ezen képesség kialakításában mely tényezők jelentik a legfőbb kihívást az alábbiak közül:*
   a) *szükséges technológiai erőforrás beszerzése;*
   b) *szükséges humán erőforrás biztosítása;*
   c) *szükséges szaktudás biztosítása?*

7. *Lát-e egyéb tényezőt, amely kihívást jelenthet ezen képesség kialakításában?*

8. *Ha végeznek nyílt forrású információgyűjtést, annak lépései mennyire dokumentáltak?*

9. *Milyen felületeken, platformokon végeznek nyílt forrású információgyűjtést?*

10. *Külön rendszeren végzik a nyílt forrású információgyűjtést, vagy ugyanazt a rendszert használják, mint amelyet a napi munkavégzésre is?*

11. *Virtualizációt használnak?*

12. *Automatizáltan vagy manuálisan folytatnak információgyűjtést?*

13. *Amennyiben manuálisan folytatják a nyílt forrású információgyűjtést, milyen gyakorisággal teszik? Mennyi humánerőforrás-időt igényel naponta/hetente?*

14. *Milyen keresőmotort használnak jellemzően?*

15. *Használnak-e rejtett kommunikációt?*

16. *Milyen elérhető források között keresnek?*

17. *Mire keresnek jellemzően?*

18. *Melyek azok a kulcsszavak, információk, amelyek az OSINT szempontjából lényegesek a vállalata számára?*

19. *Igénybe veszik-e külső, harmadik felek (beszállítók, alvállalkozók, tanácsadók) segítségét az OSINT bármelyik állomása során?*

20. *Hogyan dolgozzák fel a találatokat? Használnak-e szabadszavas keresőt?*

21. *Hogyan és meddig tárolják az információgyűjtés során szerzett nyers adatokat?*

22. *A mobilalkalmazások adatait felhasználják-e nyílt információszerzéshez?*

23. A nyílt információgyűjtésbe bevonják-e az alkalmazottak közösségimédia-profiljait is, és ha igen, milyen mélységben?

24. Végeznek-e profilalkotást a kinyert információk alapján? Ha igen, ezt hogyan és meddig tárolják?

25. Történt-e a szervezetükben olyan információbiztonsági incidens, amelynek hátterében OSINT-tevékenység állhatott?

26. Ha igen, ezt hogyan követték vissza?

27. Az egyes incidenseket besorolják-e veszélyességi szintek szerint?

28. Milyen jogi lépéseket tettek az incidenskezelést követően?

29. Lehetséges-e Ön szerint az OSINT-ot alkalmazni a reputációs veszteségek csökkentésére?

30. Milyen megelőző intézkedéseket tesznek, hogy a vállalat működése során a dolgozókról gyűjtött adatok ne legyenek nyíltan elérhetőek?

31. Ha nem tesznek ilyen megelőző intézkedéseket, akkor szeretnének-e a jövőben ilyen képességet kialakítani?

32. Ezen képesség kialakításában mely tényezők jelentik a legfőbb kihívást az alábbiak közül:
   a) *szükséges technológiai erőforrás beszerzése;*
   b) *szükséges humán erőforrás biztosítása;*
   c) *szükséges szaktudás biztosítása?*

33. Lát-e egyéb tényezőt, amely kihívást jelenthet ezen képesség kialakításában?

34. Szerveznek-e rendszeres sérülékenységvizsgálatot? Ennek a fingerprinting/reconnaissance, vagyis a teszteket megelőző információgyűjtési fázisának

része-e a vállalatukról online hozzáférhető információk vizsgálata? Ha igen, hogyan kezelik az esetleges találatokat?

35. *Ön szerint OSINT-támadások elleni védelem esetén meddig tud eljutni egy támadó, azaz van-e olyan pont (és azt lehetséges-e meghatározni) a szervezetben, amelyen semmilyen esetben sem hatolhatnak át?*

36. *A szervezetre irányuló, felderítő célú OSINT-tevékenységek naplózási adatait elemzik-e?*

37. *Védekezés és támadás tekintetében használnak AI-alapú módszert, vagy van-e tervben ilyesmi alkalmazása a jövőben?*

38. *Foglalkoznak-e nyílt információgyűjtésre alkalmas szoftver fejlesztésével? Ha igen, mikor kezdték meg ezt, illetve milyen hatékonysággal működik?*

39. *Rendelkezik-e a terület valamilyen szabályozással? Van-e eljárásrend releváns találat esetén esemény eszkalálására?*

40. *Milyen jogi akadályokba ütköznek, amelyek a hatékony és szükséges információgyűjtést gátolják?*

41. *Ön szerint milyen hazai és/vagy nemzetközi jogi szabályozásra vagy változtatásra lenne szükség?*

42. *Hogyan értékeli szervezete OSINT-képességét (1–10-es skálán, ahol az 1-es a leggyengébb, a 10-es a legjobb)?*

43. *Önnek milyen javaslatai lennének szervezete OSINT-fejlesztésére?*

Kötetünket a kiber- és információbiztonsági kérdések iránt érdeklődőknek ajánlunk. A tudatosság mint eszköz és képesség kulcsfontosságú egy szervezet biztonság-orientált működése során. Első tanulmányunkban partnereink jó gyakorlatai segítenek a biztonságtudatosság jelentőségét hangsúlyozni. A kötet másik tanulmánya a villamosenergia-rendszerek kiberbiztonsági képességfokozása érdekében vizsgálja meg, hogy az OSINT (open source intelligence), azaz a nyílt forrású információszerzés terén milyen tapasztalatok jellemzik Magyarországot. Bemutatjuk a hatályos uniós és hazai szabályozói környezetet, valamint (interjúkra alapozva) elemezzük a magyar villamosenergia-szektor szereplőinek OSINT-tudatossági szintjét, illetve képességeit.

9 786156 598684