

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

A nyílt forrású információszerzés szerepe a kibertámadások tükrében

Jelige: Aki bújt, aki nem

Pályamunka lezárásának időpontja: 2022. május 12.

Tartalom

Bevezetés.....	4
Téma aktualitása	4
Tudományos probléma megfogalmazása	5
Kutatási célkitűzések	6
Hipotézisek	6
Kutatási módszertan	7
Az ötlépcsős információbiztonsági modell.....	7
I. A Cyber Threat Intelligence területén nagyon vékony a jég.....	9
1. OSINT a Cyber Threat Intelligence területén.....	10
2. Vizsgálati szempontok és kitettséget jelentő tényezők.....	13
3. Informatikai infrastruktúra	13
4. Az emberi tényező	14
5. Harmadik fél és ellátási lánc.....	15
6. Metodológiai és eszközök.....	15
7. Informatikai infrastruktúra	16
8. Az emberi tényező	21
9. Etikusság kérdésköre	22
10. Megrendelő és Végrehajtó kapcsolata.....	23
Összegzett következtetés	25
II. OSINT az adathalászattal szemben.....	26
1. A Cyber Kill Chain® modell.....	26
2. Kontextuális összehasonlítás	27
3. Eltérő célpont, eltérő technika?	28
4. Az adathalászat, mint az OSINT kiszolgálója?	30
5. Adathalászattal sakk-matt.....	30
Összegzett következtetés	31
III. A fenyegetettség mértéke a digitális lábnyom méretében gyökerezik.....	32
1. A védekezés lehetőségei	33
2. A tudatos lábnyomcsökkentés	34
3. Dezinformáció	35
4. Defenzív technikák	36
5. Fájl-hash vizsgálat	36
6. Adatszivárgások ellenőrzése.....	38
7. Többfaktoros azonosítás	39
8. Meta és EXIF adatok	39
9. Magánszemélyek illetve kis- és középvállalatok esete.....	43

Összegzett következtetés	44
IV. Eredmények.....	46
1. Trendelemzés.....	48
2. Klaszterelemzés	54
Felhasznált irodalom	59
V. Mellékletek.....	63
1. Annotáció.....	63
2. Rövidítések jegyzéke	64
3. Ábrák jegyzéke	65
4. Interjúkérdések	66
5. A klaszterelemzés Python kódja.....	68

Bevezetés

A nyílt forrású információszerzést (Open Source Intelligence, továbbiakban: OSINT) a kiberbiztonság és más kutatási területek, valamint számos kapcsolódó iparág területén egyaránt alkalmazzák. A kiberbiztonságot illetően az OSINT-ra elsősorban talán a kiberfenyegetésekre irányuló hírszerzés (Cyber Threat Intelligence, továbbiakban: CTI) keretein belül kerül a legnagyobb hangsúly. A CTI az egyes fenyegetésekről és a fenyegetést jelentő aktorokról, entitásokról szerzett információ gyűjtő-elemző tevékenység, amely segít a kibertérben bekövetkező káros események hatásainak mérséklésében, még mielőtt bekövetkezne az incidens. Azonban a végfelhasználói szinten sem marad el jelentősége, mivel a szó szoros értelmében mindenki rendelkezésre álló eszközökről beszélünk. Ez a kompetitív előnyöket és erőt jelentő lehetőség, képesség, az érme másik oldalán könnyen egy ránk leselkedő veszéllyé alakulhat, amennyiben nem rendelkezünk megfelelő szintű információbiztonsági tudatossággal. Hétköznapi internet felhasználóként ugyanis gyakran a hamis biztonság tudatos önpercepció érzetében nem gondoljuk végig azt, hogy mit és mennyit oszthatunk meg biztonságosan magunkról, valamint azt, hogy azoknak milyen következményei lehetnek. Megragadva a gondolatot szeretném szemléltetni, hogy a „támadó oldalon” is kiemelten nagy szerepet kap a nyílt forrású információszerzés. Ugyanis a kibertámadások legtöbbségét – a spam adatbázisok felállításra irányuló adathalászatától kezdve a jellemzően egy nemzetállam vagy államilag támogatott hacker csoportok (APT, vagyis Advanced = Célzott, összehangolt, céltudatos; Persistent = Elhúzódó ideig tartó, hónapok-évek; Threat = Szándékokkal, lehetőségekkel és képességekkel rendelkező entitás(ok)) összehangolt, nagy volumenű kibertámadásaiig – e folyamatok mentén készítik elő a hackerek és kiberbűnözők. Azonban kibertámadásokra való reagálásul az állami igazságszolgálató, bűnüldöző szervek, valamint a részükre segítségét nyújtó informatikai biztonsági cégek és egyszemélyi entitások is előszeretettel alkalmazzák OSINT technikákat a kiberbűnözők kilétének felderítésére.

Téma aktualitása

Napjainkban a kibertér felértékelődéséből keletkező lehetőségekkel, veszélyekkel és fenyegetettségekkel lépést tartani nagy kihívást jelent. Az információ birtoklása a mostanra kialakult információs és a digitalizáció irányába rohanó társadalomban kulcsfontosságú, és rendkívüli értékkel bír, továbbá az internet megjelenésétől számított 30 év tapasztalata kiválóan statuuálja az okos eszközökre és magára az internetre való ráutaltságunkat. Ebből következően mindenkinek egyéni felelőssége áll fent a tekintetben, hogy mennyit oszt meg privátszférájából,

karrierútjából és munkájából. Egyes képzési és foglalkoztatási területek vonatkozásában indokoltabb lehet, hogy a felhasználó egy bizonyos fokú titkosság jegyében elővigyázatosabban járjon el, hiszen esetlegesen magára, vagy szervezetére irányíthatja ártó szándékú hackerek figyelmét, így például ha közigazgatási vagy egyéb közszolgálati ágazat munkatársa a tárgyalt felhasználó. A nyílt forrású információszerzés egy sokoldalú lehetőséget hordoz magában az online térben végzett törvényes és engedélyekhez nem kötött információgyűjtéshez, azonban a mérleg másik oldalán ugyanez a lehetőség veszélyként jelenik meg, ugyanis a hackerek közkedvelt eszközéről is beszélünk. Ebből fakadóan kiemelten fontosnak tartom a nyíltforrású információszerzésből eredeztethető veszélyek szélesebb körben való ismertetését. Továbbá témaválasztásom személyes motivációjaként tudom be azt, hogy érdeklődési köröm és jövőképem a kiberbiztonság köré orientálódnak, az alapszak elvégzését követően a Nemzeti Közszolgálati Egyetem kiberbiztonsági mesterképzésén tervezem folytatni tanulmányaimat. Karrierutamat kizárólagosan a kiberbiztonsági iparágban képzelem el, egyes ágazatainak elsajátítására egyetemi tanulmányaim során, önképzés, valamint keresőtevékenység keretein belül egyaránt törekszem. Mára az ezirányba folytatott folyamatos tanulás a szenvedélyemmé vált. Kutatásom egy olyan témát dolgoz fel, amivel hosszútávon tervezek foglalkozni, s a várható eredmények kiemelkedő fontosságot jelentenek az elmélyülésben és a szakmai tudásom minőségi megalapozásában.

Tudományos probléma megfogalmazása

A nyílt forrású információszerzésnek számos alkalmazási területe van, belefoglalva civil, katonai és nemzetbiztonsági tartományokat, de kiváltképpen megjelenik a vállalatbiztonság egyes részeit tekintve is. Azonban az OSINT technikákkal és módszerekkel végzett munka mélysége, összetettsége és elfogadottsága területtől függően látványos és olykor kifogásolható eltéréseket mutat. Ennek oka elsősorban, hogy a feladat természetéből ered, hogy az eredményesség érdekében milyen eszközökhöz és forrásokhoz kell nyúlni, milyen adatokat, információt kell megszerezni, elemezni majd értékelni. Egyes esetekben a folyamat kimerülhet egyszerűen a sajtótermékek vizsgálatában, azonban vannak területek, ahol mélyebbre kell menni a nyúlüregben. Dolgozatom keretein belül végzett kutatásom a Cyber Threat Intelligence szakterületén jelentkező úgynevezett szürke zónát hivatott feltárni. Szürke zónának minősítem mindazon tények és körülmények alkotta halmazt, mely szerint bizonyos eljárások, adott nézőpontból már túlmutatnak az OSINT eszköztárán, kimeríthetnek egyes erkölcsi-etikai és jogi kereteket, már-már összemosódnak a hacker-tevékenységtől elválasztó határral, azonban továbbra is szilárdan őrzik legitimitásukat. A vizsgált szakterületen végzett munka során előnyt

jelent a zóna létezése, mivel a „kiterjesztett” tevékenységi kör nagyobb hatásfokú megelőzést és biztonságot garantálhat. Szentesíti a cél azonban az eszközt?

Kutatási célkitűzések

A dolgozatom elkészítése során végzett kutatásom célja megvizsgálni az OSINT tevékenységek körét, mint a Cyber Kill Chain® (továbbiakban: Kill Chain) (A kill chain kifejezést eredetileg a támadás felépítésével kapcsolatos katonai fogalomként használták, amely a cél azonosításából, a cél megközelítésből, a cél megtámadásának elhatározásából és parancsából, végül a cél megsemmisítéséből áll. A koncepciót a Lockheed Martin adaptálta az információbiztonsághoz, módszerként használva a behatolások modellezéséhez egy számítógépes hálózaton) első láncszemét. Mivel a kibertámadások alapos megtervezése minden esetben információgyűjtéssel indul és az adathalászat egyes módszerei mellett kiemelt szerepet játszik az OSINT, hiszen a megfelelő technikákkal és szoftverekkel meglepően sok értékes, bizalmas adat gyűjthető össze. Vizsgálatom során fel kívánom tárnai az eddig legerősebbnek bizonyult metodológiákat, illetve az eljárások esetleges akadályait, annak érdekében, hogy bizonyítsam az OSINT adathalászattal szembeni fölényét. Továbbá kiemelt fontossággal szeretnék kitérni arra a kérdéskörre, miszerint összemosódik-e a határ az etikus információszerzés és a hacker-tevékenység között. Végül kutatásom rámutat majd a digitális lábnyom mérete és a fenyegetettség mértéke közötti összefüggésre is.

Hipotézisek

A kutatásom és dolgozatom elkészítését megelőző szakirodalom gyűjtés és elemzés elvégeztével az alábbi három hipotézist vázoltam fel, melyeket cáfolni vagy igazolni kívánok.

H1: Bizonyos alkalmazási területeken célhoz kötötten összemosódnak a határok az OSINT, az etikus információgyűjtés és a hackertevékenység között.

H2: Az OSINT nagyobb megbízhatóságot és eredményességet biztosít a támadások előkészítésében, mint az adathalászat.

H3: A digitális lábnyom szándékos és tudatos minimalizálásával kivédhető, hogy kizárólag nyílt forrásokból egy támadás kivitelezéséhez elegendő információt gyűjtsenek össze rólunk.

Kutatási módszertan

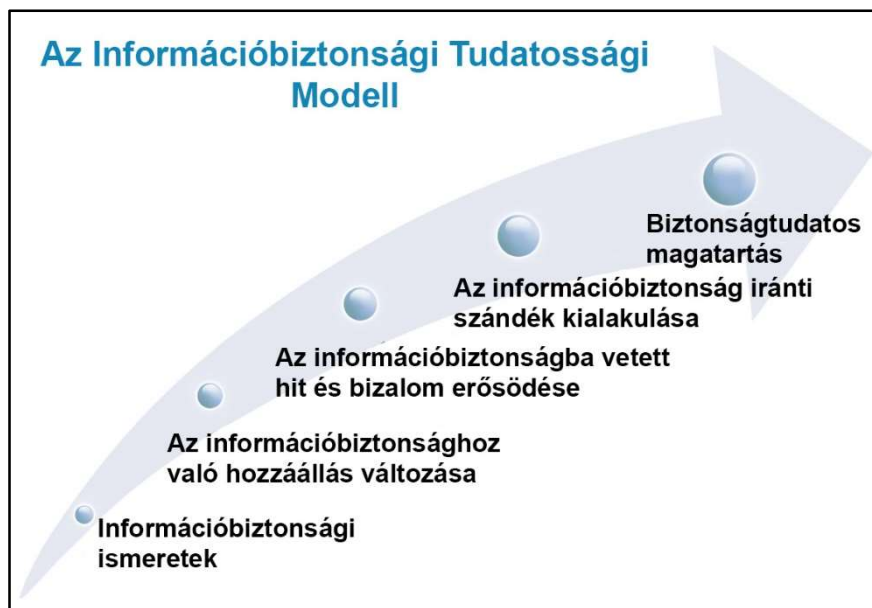
A fent tárgyalt kérdések megválaszolásának érdekében a Scopus és SciVal adatbázisaiban kulcsszó analízissel tervezem megállapítani, hogy mely releváns kiberbiztonsági vonatkozású témakörökben esik említés az OSINT-ről és a Cyber Threat Intelligence-ről. A fellelt és meghatározó jellegű dokumentumokat részletesen elemzem, majd belőlük levezetve trendelemzést végzek, miképp változott az OSINT-al és a CTI-al kapcsolatos publikációk iránya, fejlődése. Ezt követően a kutatás időtartama alatt fókuszcsoportos interjúsorozatot tervezek lefolytatni a kiberbiztonság egyes ágazataiban dolgozó szakemberek részvételével, többek közt etikus hackerekkel, behatolástesztelőkkel és információbiztonsági szakértőkkel, miszerint mindennapi munkájuk során milyen szempontokból jelentkezik az OSINT, továbbá a jogi vonatkozás oldaláról egy GDPR szakjogász közreműködésére is támaszkodom. Az interjú kérdéseit az ötlépcsős információbiztonsági modellre építem. Ezen túlmenően az átfogóbb képalkotás érdekében vizsgálom meg az érintett szakértők motivációját, különös tekintettel a pályaválasztásukkal kapcsolatos attitűdre, figyelembe véve a bemenetet, az előmenetet, illetve a pályaelhagyás kérdéseit. Végül az interjúsorozatból befolyó eredményekből egy klaszterelemzést készítek a Python programozási nyelv segítségével.

Az ötlépcsős információbiztonsági modell

A SANS Institute¹ eredetileg öt lépcsőből álló Információbiztonsági Tudatossági Érettségi Modelljét először Lance Spitzner, a szervezet egyik vezető oktatója publikálta egy blogbejegyzésben 2012. május 22.-én. A modellt eredeti elgondolás alapján az információbiztonsági tudatosító programok érettségi szintjének értékelésére céljából alkották meg. Társául a szintén ötlépcsős információbiztonsági tudatossági modellt tartják, amely nem szervezetekre, hanem személyekre fókuszál, de annak megközelítése, kialakítása és eszköztára² megfelel interjúkérdéseim alapjának is.

¹ A SANS Institute egy 1989-ben az Egyesült Államokban alapított magáncég, amely információbiztonságra, kiberbiztonsági képzésekre és tanúsítványok értékesítésére specializálódott.

² Tarján Gábor: Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben. Budapesti Corvinus Egyetem, 2020



1. ábra: Az Információbiztonsági Tudatossági Modell (Saját fordítás, forrás: sans.org)

I. A Cyber Threat Intelligence területén nagyon vékony a jég

A Cyber Threat Intelligence legfőbb forrásai közé tartoznak a nyílt forrású információszerzés, a közösségi médián alapuló hírszerzés (SOCMINT), az emberi kapcsolatokon alapuló hírszerzés (HUMINT), a napjainkban megjelenő ötvözet az úgynevezett „virtuális ügynök” által folytatott emberközpontú hírszerzés (VHUMINT), a műszaki hírszerzés, továbbá a Deep és Dark Web³ tartományokból történő információgyűjtés. Az imént felsoroltak közül a CTI munka során talán a legrelevánsabb intelligenciaforrás az OSINT, míg a Threat Hunting domain-t tekintve pedig a honeypot és honeynet⁴ rendszerek hálózatba történő telepítése, valamint a különböző biztonsági információ- és eseménykezelő (Security Information and Event Management, továbbiakban: SIEM⁵) architektúrák használata. A SIEM rendszereket széles körben alkalmazzák hatékony eszközként a kibertámadások megelőzésére, észlelésére és az ellenük való reagálásra. A SIEM megoldások átfogó rendszerré fejlődtek, amely széles rálátást biztosít a magas kockázatú területek azonosítására, proaktívan összpontosít a mérséklési stratégiákra, amelyek célja a költségek és az incidensre adott válaszidő csökkentése.⁶ Jelen fejezetben egy általános bevezetést követően áttekintést készítek az egyes vizsgálati szempontokról. Majd esetpéldákkal kiegészítve górcső alá veszem a hozzájuk rendelt metodológiákat, annak szemléltetése céljából, hogy kizárólag egy nagyon vékony vonal választja el az etikus információszerzést és a fenyegetettségeket-sebezhetőségeket feltáró információszolgáltatást a hacker-tevékenységtől, melyeket a jelenleg hatályos Büntető törvénykönyv többek közt az alábbi tényállásokkal rögzít: Az információs rendszer felhasználásával elkövetett csalás⁷, a tiltott adatszerzés⁸ és az információs rendszer vagy adat megsértése⁹.

³ Az internetnek olyan tartományai, melyeket hétköznapi keresőmotorok nem indexálnak, elérésük speciális szoftvert és tudást igényel.

⁴ A honeypot egy hálózathoz csatlakoztatott rendszer, amely csaliként van beállítva a támadók odavonzására, valamint a hackelési kísérletek észlelésére, elhárítására és tanulmányozására.

⁵ A biztonsági információ- és eseménykezelés az informatikai biztonság olyan területe, ahol a szoftvertermékek és -szolgáltatások egyesítik a biztonsági információkezelést és a biztonsági eseménykezelést.

⁶ G. González-Granadillo, S. González-Zarzosa, és R. Diaz, „Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures”, *Sensors* 21, sz. 14 (2021), <https://doi.org/10.3390/s21144759>.

⁷ 2012. évi C. törvény 375. § (1) Aki jogtalan hasznoszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, büntetett miatt három évig terjedő szabadságvesztéssel büntetendő.

⁸ 2012. évi C. törvény 422. § (1) d) elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti. e) információs rendszerben kezelt adatokat titokban kifürkész, és az észlelteket technikai eszközzel rögzíti.

⁹ 2012. évi C. törvény 423. § (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit

1. OSINT a Cyber Threat Intelligence területén

Mint említettem dolgozatomban bevezető szekciójában, a nyílt forrású információszerzés bizonyos alkalmazási területein nagy eltérések fedezhetők fel a rétegzettség és a mélység vonatkozásában. Ennek szemléltetését három esettanulmány segítségével végzem el. Elsőként, OSINT folyamatok mentén lehetséges társadalmi vélemény- és hangulatelemzést is végezni. Az online közösségi hálózatok fellendülése lehetővé teszi a felhasználók interakcióinak, üzeneteinek, érdeklődési köreinek és preferenciáinak összegyűjtését a nem explicit tudás kinyerésére. A közösségi médiából felhalmozódott információk kiértékelést követően messzemenő és széles körű előnyökhöz vezethet, például egy ilyen gyűjtés és elemzés alkalmazható akár marketing vagy politikai kampánnyal összefüggő célokra. Azonban bűnüldözési és nemzetbiztonsági érdekeket is sokoldalúan kiszolgálhat egy erős OSINT képesség. A múlt század végétől napjainkig a fogyasztók egyre inkább az online térben élik életüket. Manapság a világon az átlagember ideje jelentős részét online kapcsolattartással tölti több platformon keresztül. Nincs ez másképp a profitorientált vállalatok esetében sem, melyek saját weboldal üzemeltetése helyett gyakorta a közösségi média egyes felületeit (például LinkedIn, Instagram és Twitter) veszik igénybe marketing, PR és HR célokra, azonban egyúttal bűnözői személyi körök melegágyát is képezhetik ezek a hálózatok. Ez az online tevékenység azt is eredményezi, hogy az emberek egyre nagyobb mennyiségben osztanak meg szabadon személyes adatokat. A bűnüldözés szempontjából már évtizedekkel ezelőtt megjelent az igény, miszerint a hagyományos bizonyítási eszközök mellett nyílt forrásosokból gyűjtött információkkal is ki kell egészíteni a fegyvertárat. Megragadva a lehetőséget, ez a fejlődés rengeteg új digitális bizonyítékforrásnak felel meg. A bűnüldöző szervek munkáját természetesen segítik még azon folyamatok, melyekre bírósági engedélyek útján nyílik lehetőségük, így például sarkalatosak lehetnek még a digitális törvényszéki (Digital forensics) vizsgálatok, amikor a lefoglalt elektronikus eszközt, vagy annak teljes rendszeréből készített digitális lemezkép fájlt vetik elemzés alá a szakemberek bizonyítékok után kutatva. Ötvözve a rendfenntartó erők tevékenységét a nyilvánosan elérhető adatok proaktív és folyamatosan elemzésével, lehetségessé válik egyes entitások bűnözői szándékainak korai előrejelzése is, valamint a megfelelő források igénybevételével nyomon követhető a terrorista szervezetek tevékenysége is, melyek egyre nagyobb aktivitást mutatnak a digitális térben. Nem utolsósorban természetesen a kiberbiztonság és kibervédelem területén is megmutatkoznak az OSINT

túllépve vagy azt megsértve bent marad. Továbbá a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl, vagy hozzáférhetetlenné tesz.

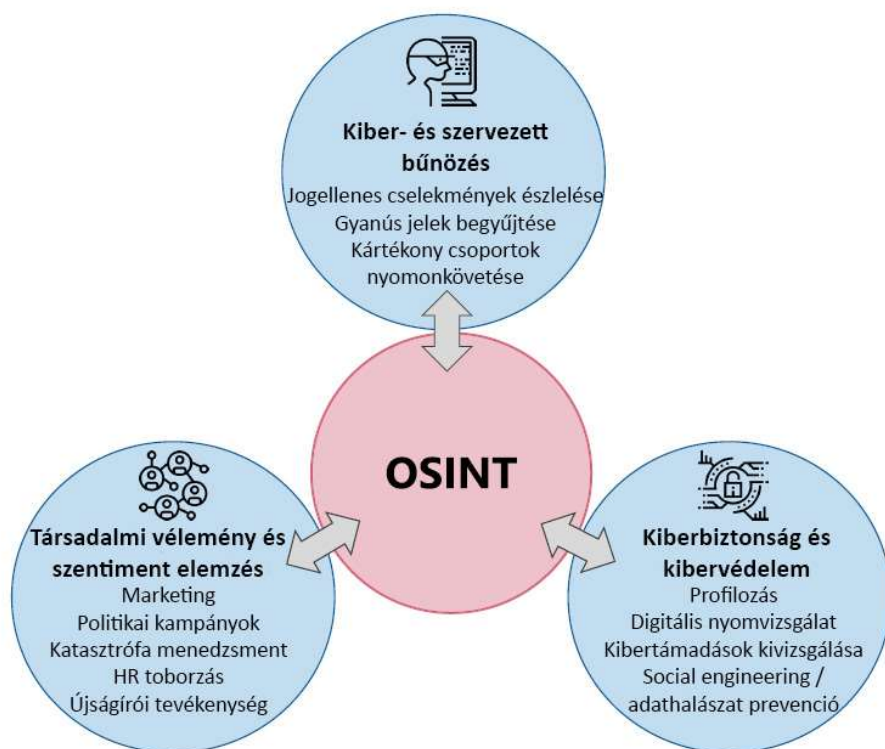
sokrétű lehetőségei. Az információs és kommunikációs technológiai rendszerek (továbbiakban: IKT) térnyerése jelentős függőséget eredményezett mind az egyének, mind az államok részéről, amely függőség a technológia fejlődésével és további terjedésével a jövőben vélhetően csak erősödni fog.¹⁰ Az IKT rendszerek folyamatos fenyegetettségnek vannak kitéve olyan támadók által, akiknek célja többek közt az adott rendszer rendelkezésre állásának (Availability¹¹) megzavarása. Ebben a kontextusban az adatok elemzését nem csak a digitális lábnyom méretének meghatározására használják, hanem a rendszerek megelőző védelmére is. Összefoglalva tehát erre a rétegzettséget statuáló jelenségre a feladat sajátossága nyújthat magyarázatot, hiszen másképpen kell megközelíteni például egy oknyomozás jellegű újságírói célt és egy digitális kitettségvizsgálatot. A CTI szakterületén többek közt az utóbbi merül fel, mint az OSINT munka célkitűzése. Ahhoz tehát, hogy megfelelő mértékben fel lehessen mérni egy kis- és középvállalat, vagy egy létfontosságú rendszerelem jogállása alá sorolható intézmény kiberbiztonsági felkészültségét és ellenállóképességét – melynek garantálása nemzetstratégiai érdek¹² – olyan eszközökhöz és forrásokhoz kell nyúlni, melyek erkölcsi és etikai legitimitása szükségesség hiányában vitatottak más alkalmazási területeken. Példának okáért, a fentebb említett újságírói tevékenység során indokolatlan volna adatsértésekből származó adatbázisokat elemezni, majd nyilvánosságra hozni – akár korlátozott terjesztésben is – a valóságnak megfelelő email és jelszó párosokat. Azonban, ha ugyan ebben a kontextusban vizsgálunk egy energetikai szektorban elhelyezkedő, monopolhelyzetben lévő létfontosságú rendszerelemet, így például egy földgázszolgáltató szervezetet, más dimenziókat üt meg az elemzés. Szükségessége abszolút mértékben indokolható, azonban etikai vonatkozásban ugyan azon folyamat. Továbbá jellemző a szakterületen végzett munkára a Dark Web releváns részeinek automatizált legyűjtése és monitorozása, mivel a kiberbűnözők tevékenységeit – mint a napjainkban egyre növekvő gyakorisággal elforduló zsarolóvírusos támadások – is lekövethetővé teheti bizonyos mértékben. A későbbiekben felvázolom ennek ütközését az Európai Unió Általános Adatvédelemről szóló rendeletével (General Data Protection Regulation, továbbiakban: GDPR). Ezen műveletek az átlagos, laikus felhasználó perspektívájából kétes erkölcsi hovatartozásúak lehetnek. Hipotézisem abban gyökerezik tehát,

¹⁰ „Kiberbiztonsági incidensek a magyar közigazgatásban (MTMT)”, elérés 2022. február 20., <https://m2.mtmt.hu/gui2/?mode=browse¶ms=publication;30867893>.

¹¹ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról – A kiberbiztonság három alapelvének, az ún. CIA hármas egységének egyike (Confidentiality, Integrity, and Availability, vagyis Bizalmasság, Sértetlenség és Rendelkezésre állás).

¹² A. Cartagena and mtsai., „Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework for Critical Infrastructure Owners”, in *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, szerk. Paul R. Chakrabarti S. (Institute of Electrical and Electronics Engineers Inc., 2020), 494–99, <https://doi.org/10.1109/CCWC47524.2020.9031172>.

hogy mivel egyedi alkalmazási területéből kifolyólag „támadólag” – vagyis egy ártó szándékú kibertámadás előkészítéséhez szükséges módon – kell nyílt forrású információszerzést és elemzést végezni egy érdembeli kiberbiztonsági átvilágítás lefolytatása céljából, az igénybe vett eszközök és források mentén összemosódik a határ az etikus információszerzés és a hacker-tevékenység között. Mivel a valódi szolgáltatás e mögött nem maga a vizsgálat lefolytatása és az azt követően eredménytermékként átadott jelentés, hanem sokkal inkább egy jövőbeni kibertámadás megelőzése, így ennek keretein belül bizonyos mértékben legitim lehet túlmutatni az OSINT eszköztárán. Ettől a ponttól fogva beszélhetünk a Privacy Violating OSINT-ről (továbbiakban: PV-OSINT), vagyis a nyílt forrású információszerzés olyan eszközeiről, melyek szembe mehetnek például a személyes adat- és magánszféravédelem egyes erkölcsi és jogi normáival. Természetesen a túllépés nem terjed ki egy behatolási tesztelés jogköréig, hanem csak megközelítő mértékben súrolja annak alsó határait, azonban az összemosódás már tetten érhető. A PV-OSINT valódi szükségességére és belőle eredeztethető veszélyekre dolgozatom harmadik fejezetében bővebben kitérek, azonban alább egyes magában foglalt módszertanait prezentálom.



2. ábra: Az OSINT főbb használati esetei (Saját fordítás, forrás:¹³)

¹³ J. Pastor-Galindo és mtsai., „The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends”, *IEEE Access* 8 (2020): 10282–304, <https://doi.org/10.1109/ACCESS.2020.2965257>.

2. Vizsgálati szempontok és kitettséget jelentő tényezők

Jelen bekezdésben nagy vonalakban szeretném ismertetni azon tényezők összességét, melyekkel a CTI elsősorban foglalkozik egy kitettségvizsgálat során, mivel azok számos fenyegetést hordozhatnak magukban és veszélyt jelenthetnek vállalatbiztonsági szempontokból. Vizsgálatuk mind elvégezhető, s jellemzően is OSINT forrásokból történik. Az áttekintést követően kerülnek majd szemléltetésre az egyes célok teljesítése vonatkozásában talán leghatékonyabbnak bizonyuló módszertanok és technikák.

3. Informatikai infrastruktúra

Az első és talán legkritikusabb szempont, az informatikai infrastruktúra összetételének és sajátosságainak vizsgálata, mivel egyfajta gerincoszlopát képezi a digitális biztonság. Ugyanis bárminemű hiátus vagy hiba, melyek természetesen előfordulnak emberi figyelmetlenség, mulasztás okán vagy a szükséges szakértelem hiányában, azonban gyakori az is, hogy egyszerűen nem a megfelelő implementáció kerül alkalmazásra, könnyen biztonsági rést képezhet az agilis ellenállóképesség pajzsán. Fontos, hogy a megfelelő eszközökkel beazonosítsuk az adott célponthoz tartozó egyes entitásokat, melyek jelen kontextusban IP címek, a hozzájuk kapcsolt domain-ek és aldomain-ek¹⁴, a nyitott portok¹⁵ és rajtuk futó szolgáltatások, illetve azok verziószáma. Lehetőség szerint célszerű felkutatni a lehető legtöbb használatban lévő eszközt (belefoglalva minden informatikai, hálózati eszközt a nyomtatótól és egyéni munkaállomásoktól kezdve az ipari és logikai vezérlőegységekig). Egy analízis jellemzően a hibák kereséséről szól, nagyvonalakban olyan tények, s körülmények ellenőrzése szükséges, melyek biztosítanak arról, hogy a kirakós minden darabja a megfelelő helyen van a megfelelő módon. Az olyan hibák, mint a nem szükségesszerű portok nyitottsága, az elavult verziójú szolgáltatások (például open-source webserverek: Apache, nginx) használata, lejárt SSL tanúsítványok, vagy a tanúsítványok teljes hiánya, a gyári- alapbeállításként használt hozzáférések (továbbiakban: default credentials) – például: admin/admin – alkalmazása és az egyéb hozzáférés-kontrollbeli hiányosságok mind alááshatják a digitális biztonságot.

¹⁴ A tartománynév az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés. Az aldomain az elsődleges domainnév kiegészítője. Lényegében az aldomain a webhely különálló része, amely ugyanazon az elsődleges domain néven működik.

¹⁵ A számítógépes hálózatban a port kommunikációs végpont. Szoftver szinten az operációs rendszeren belül a port egy logikai konstrukció, amely egy adott folyamatot vagy hálózati szolgáltatás típusát azonosítja.

4. Az emberi tényező

Mint azt számos vonatkozó szakirodalomban is olvasni lehet, jó okkal, a kiberbiztonságban a másik legkritikusabb pont, s egyben rizikó faktor, az emberi tényező. Mivel lehet egy szervezet bármennyire is fejlett biztonságtechnika terén, illetve rendelkezhet nagy határfokú biztonságot képviselő informatikai infrastruktúrával, ha a mögötte lévő felhasználó információbiztonsági tudatossági szintje nem konvergál. Az emberi tényező jelen szövegkörnyezeti középpontja természetesen a munkavállaló, pontosabban a szakmai személyzet, mely halmazban elsősorban az informatikával és a biztonsággal ötvözött munkakörök szerepelnek. Azonban nyilvánvalóan nem elhanyagolhatók az egyéb, alsóbb és felsőbb szinteken elhelyezkedő munkavállalók jelentette sebezhetőségek sem. Mind ezek vonatkozásában elsősorban az egyének biztonsági felkészültségét, szakmai hozzáértését kell vizsgálni, továbbá fel kell tárni az esetlegesen fellépő veszélyeket személyenkénti lebontásban, úgy, mint a vállalati email címek szakszerű és szükséges használata, a célzott adathalásztámadás (spear-phishing) és social engineering¹⁶támadások valószínűsége, valamint a zsarolhatóság lehetőségének fennállása. Nem nézhetünk el továbbá azon kérdéskör mellett sem, ami a munkavállaló szervezetéhez való lojalitását és megbízhatóságát tárgyalja. Ennek értelmében olyan körülményeket kell vizsgálni, mely arról biztosít, hogy a tárgyalt személy betartja-e a munkaköré vonatkozó elvárásokat, nem szegi meg az esetleges titoktartási szerződést és nem szivárogtat információt (üzleti titkokat, technikai részleteket) akár gondatlanul akár szándékosan. A gyakorlatban sajnos nagy esetszámmal érhető tetten, hogy a munkavállalók nem képesek elhatárolni egymástól a vállalati és magánéleti identitásukat, ezáltal felelőtlenül használják a munkavégzéshez rendelkezésükre bocsátott eszközöket (vállalati email cím, laptop, telefon, belépőkártya és igazolvány stb.), egyáltalán nem vagy csak hiányosan tartják be az egyes szabályzatokat, előírásokat, ezzel tovább növelve szervezetük digitális kitettségét. Valamint meg kell említeni még az emberi tényező kapcsán egy további threat aktort, vagyis fenyegetettséget jelentő entitást, a szakirodalom által úgynevezett malicious insider-t vagy insider threat-et. A fogalmat a tükrörfordításban vett értelmében kell venni, vagyis a szervezeten belüli kártékony szándékú dolgozókat.

¹⁶ Pszichológiai manipuláción alapuló támadás, amikor egy jogosultsággal rendelkező felhasználó jogosulatlan személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít a rendszerbe történő belépésre a másik személy megtévesztő viselkedése miatt.

5. Harmadik fél és ellátási lánc

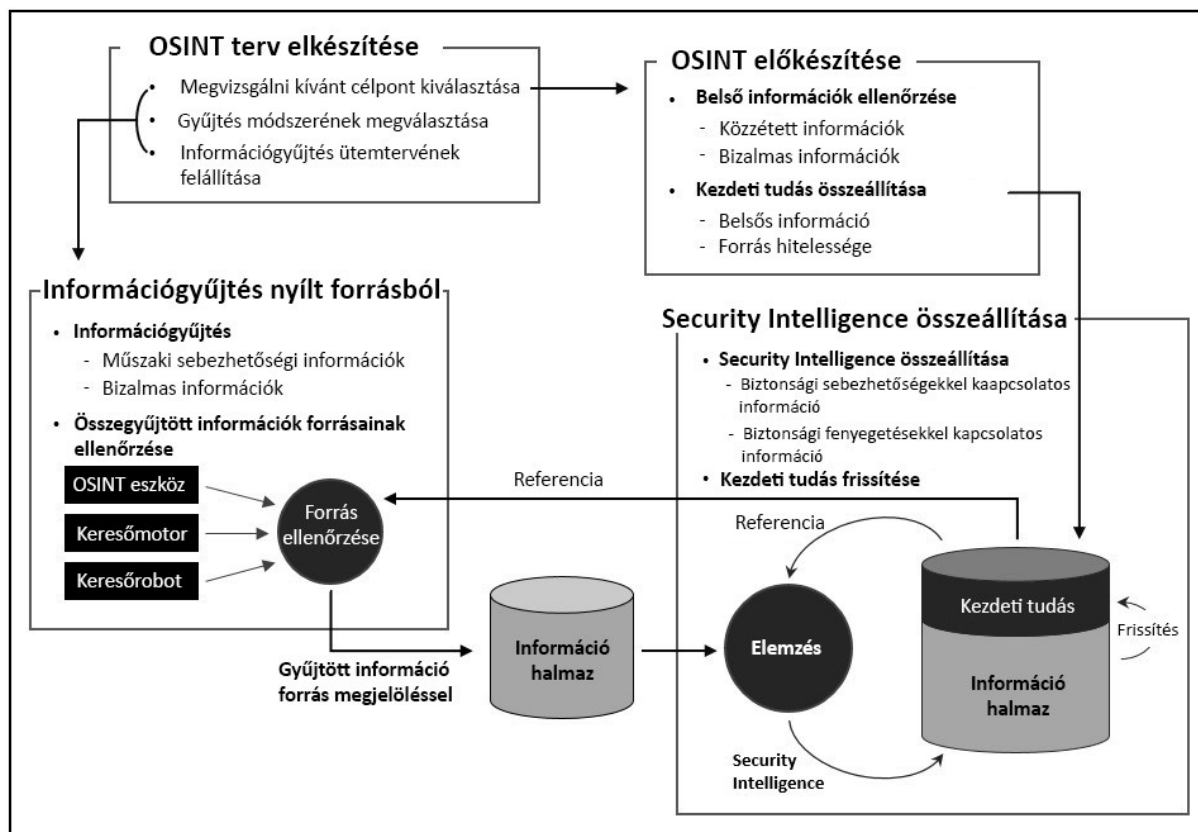
A harmadik fél (Third-party) olyan magánszemély vagy szervezet, amely részt vesz egy ügyletben, de nem tartozik a megbízók közé, és így kevésbé érdekelt az ügyletben. Az ellátási lánc (Supply chain) pedig általánosságban azon a tevékenységek összessége, melyekre az adott szervezetnek szüksége van ahhoz, hogy árukat vagy szolgáltatásokat szállítson a fogyasztónak. A vizsgált témám értelmében a harmadik fél és ellátási láncon belül a külső beszállítók, tárhelyszolgáltatók, illetve szoftver és hardver fejlesztő-szolgáltató partnerek igénybevételevel összefüggésben álló kitétségeket értem. Elmondható ugyanis, hogy ha a fentebb említett valamennyi hiba, hiányosság vagy veszélyforrás fent áll a külső partnereknél, az közvetett sebezhetőséget jelent az őket megbízókra, s beárnyékolhatja a védekezésének képességeit és törekvéseit. Ebből kifolyólag a teljes kép érdekében ugyanazon séma szerint ebben a körben is el kell végezni az ellenőrzés folyamatát.

6. Metodológiák és eszközök

Egy bevezetőt követően olyan módszertanokat és eszközöket szemléltetek, melyek hipotézisem vonatkozásában alátámasztó erővel bírnak, miszerint vitatott hovatartozású eljárások kerülhetnek alkalmazásra legitim módon egy nyílt forrásból történő kiberbiztonsági átvilágítás során.

A lépésekre lebontott OSINT vizsgálat folyamata egy előzetes koncepció felállításával kezdődik meg, amikor is meghatározzuk magát a célpontot, amely a példa esetében lehet egy vállalat informatikai infrastruktúrája, munkavállalói hálója és külső partnerei. Ezt követően a feladatszabással összhangban egy predikció állítással – mely szerint mi jelenthet kifejezetten nagy kitétséget, kockázatot és veszélyt – körül határoljuk azokat a tartományokat, melyekből majd információt gyűjtünk, s elkészítjük a munka menetrendet. Célszerű rétegzetten haladni a szemmel látható felszíntől a mélyebb tartományokig, s először a tudatosan, nyilvánosan közzétett és elérhető tartalmak (például saját weboldal, álláshirdetések, publikált dokumentumok, kontaktszemélyek – jellemzően HR és sales beosztású dolgozók, telephelyek, céginformáció stb.) elemzésével kezdeni, ez menetközben is elősegítheti az átfogóbb képalkotást a célpontról. A megfelelő előkészületek után megkezdődhet a felderítés és információgyűjtés, amely egyidőben manuálisan és automatizáltan zajlik különféle technikák és eszközök segítségével. Fontos kritérium a forrás megbízhatóságának és az információ validáltságának folyamatos ellenőrzése. A beszerzett információ elemzését és kiértékelését

követően eredménytermékké strukturáljuk a tudást, egy főképp sérülékenységeket, vonatkozó fenyegetettségeket szemléltető jelentés formájában.



3. ábra: Egy OSINT művelet általános lépései

Az általános szemléltetőt követően most rátérek azon módszertanok bemutatására, melyek alátámasztják dolgozatom első hipotézisét. Előre bocsátom, hogy dolgozatom jellegéből és terjedelmének megkötéseiből fakadóan nincs lehetőségem részletesen szemléltetni az egyes eszközök használatát és működését, valamint irományom erre nem is hivatott.

7. Informatikai infrastruktúra

Fontos leszögezni, hogy az információgyűjtés fázisban megkülönböztetünk aktív és passzív felderítési módokat (active and passive reconnaissance), melyek abban térnek el egymástól, hogy az aktív folyamat során a behatoló kapcsolatba lép a célrendszerrel, hogy információkat gyűjtsön a sebezhetőségekről, míg a passzív folyamat szigorúan a rendszerrel való interakció nélkül, „kívülről” történik. Azonban valahol a kettő közt helyezném el a szkennelésen alapuló felderítést, vagyis a scanning reconnaissance fogalmát. Ez alatt legjellemzőbben a portszkennelési eljárásokat kell érteni, melyeket többféle eszköz igénybevételel is végre lehet hajtani. Érvem amellet, hogy a portszkennelés a két fogalom között helyezkedik el az, hogy

mivel támadás előkészítő folyamatnak van címkézve, így az ilyen felderítést végző személy is az illegális tevékenység határait súrolja¹⁷, azonban Magyarországon ezt konkrét törvényi tényállás nem rögzíti, valamint, passzív folyamatok mentén is elérhető ugyanazon eredmény. Továbbá, a vonatkozó szakkönyvek és témában született releváns tudományos elemzések sem tekintik törvénybeütközőnek a szkennelést¹⁸, ameddig azt nem követi támadó célzatú tevékenység. Ezen a ponton állítanám szembe a két talán legnépszerűbb és leghatékonyabb eszközt a Shodan-t és az Nmap-et. A Shodan lényegében egy olyan keresőmotor, amely lehetővé teszi a felhasználók számára, hogy különböző szűrők segítségével különböző típusú, az internethez csatlakozó szervereket és egyéb hálózati eszközöket keressenek. Egyesek úgy is jellemezték, mint a szolgáltatás bannerek keresőmotorját, amelyek olyan metaadatok, amelyeket a szerver visszaküld az ügyfélnek. Az Nmap pedig egy olyan hálózat szkennelő szoftver, amely a gazdagépek és szolgáltatások felderítésére szolgál egy számítógépes hálózaton csomagok küldésével és a válaszok elemzésével. Utóbbit meglehetősen széleskörűen lehet alkalmazni, mivel egy ingyenes és nyílt forráskóddal rendelkező szoftver, melynek szkript motorját a szükséges programozási ismeretek birtokában bárki szabadon bővítheti céljainak megfelelően. A Shodan kínál ugyan ingyenes regisztrációs lehetőséget, de az azzal járó lehetőségek köre limitált, az átfogóbb használati jogosultság havidíjas szolgáltatásként vehető igénybe. A lényeg tehát abban gyökerezik, hogy a portszkennelés köré fűjt jogi kétely kódét, egyszerűen meg lehet kerülni egy keresőmotorral, mely legalább ugyan olyan pontos eredménnyel szolgál például a nyitott portok, illetve a használt eszköz- és szoftververziók vonatkozásában, mely információk birtoklása megalapozhat egy kibertámadást. Továbbá felmerül azon nézőpont is, hogy ami a szó szoros értelmében „kint van” a nyilvános interneten (portok, eszközök), a róluk valamilyen formában szerzett tudás, ismeret nyílt forrásnak bizonyul. Példának okáért, az alábbi ábrán egy Shodan keresési eredményt láthatunk, amely az adott IP címen egy nyitott 102-es számú portot mutat, amit gyári beállításként alapértelmezetten használ egy Siemens típusú programozható logikai vezérlőegység (Programmable Logic Controller, továbbiakban: PLC). Ezen túlmenően információt kapunk még az eszköz nevről, sorozatszámáról és a használt firmware¹⁹ verzióról is. Azonban szkennelési technikával is elvégezhető a felderítés a megfelelő parancsok futtatásával. Ezt szintén egy ábrán keresztül

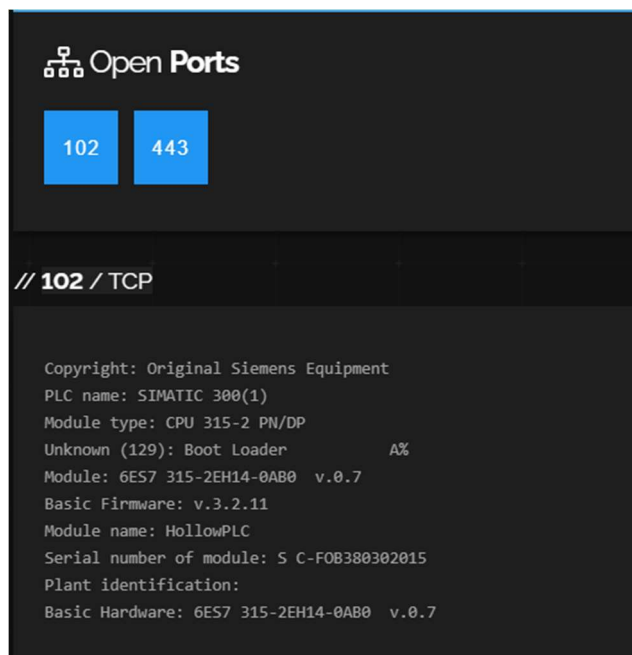
¹⁷ Gányi Sándor: Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem.

Zrínyi Miklós Nemzetvédelmi Egyetem, Hadtudományi Kar, Katonai Műszaki Doktori Iskola, Budapest, 2011

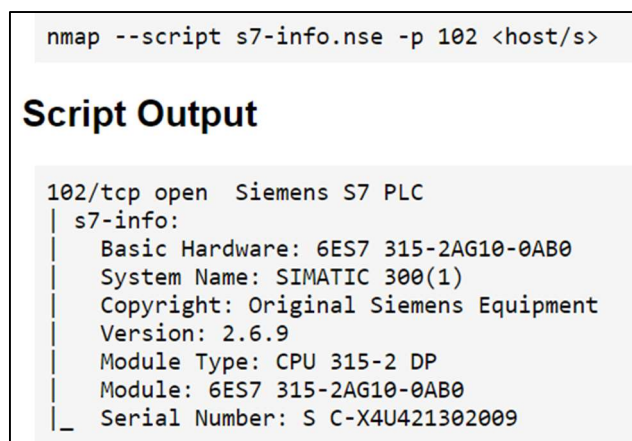
¹⁸ Cartagena és mtsai., „Privacy Violating Open source Intelligence Threat Evaluation Framework: A Security Assessment Framework for Critical Infrastructure Owners”.

¹⁹ Az elektronikai rendszerekben és a számítástechnika területén firmware alatt azokat a rögzített, többnyire kisméretű programokat és/vagy adatstruktúrákat értjük, melyek különböző elektronikai eszközök vezérlését végzik el.

szemléltetem. Említőlegesen, az ilyen ipari vezérlőegységeknek és logikai vezérlőknek soha nem szabadna kint lenniük a nyilvánosan interneten, mivel használatuk jellemzően valamilyen ipari környezetben történik – magában foglalva a kritikus infrastruktúrák, mondjuk egy víztisztító üzem esetét is – így kifejezetten nagy veszélynek vannak kitéve. Sok APT csoport specializálódik kimondottan ilyen eszközök támadására.



4. ábra: Shodan keresési eredmény. (saját képernyőmentés, forrás: shodan.io)



5. ábra: Nmap parancs használatának példája. (saját képernyőmentés, forrás: nmap.org)

Mivel a CTI egyik rendeltetése a megelőző védelem így nagy hangsúlyt kell fektetni a tényleges gyengepontok legteljesebb feltárására. Így a felelősségvállalás okán ebbe kiegészítőleg beletartozhatnak a valamilyen védelmi mechanizmussal ellátott rendszerek biztonságának oly módú tesztelése, próbára tétele, mely még nem csap át a klasszikus értelemben vett behatolási

tesztelésbe (Penetration testing). Előfordul ugyanis, hogy egyes hálózati elemekhez (például egy router vagy switch, IP kamera, hálózathoz kapcsolt adattároló stb.) beüzemelését követően továbbra is a gyári alapbeállításként biztosított hozzáférési adatok maradnak alkalmazásban (jellemzően admin/admin vagy root/root). Ezek a hozzáférések típus specifikusan nyilvánosan elérhetők, hiszen termékhasználati útmutatók és egyéb dokumentációk mind fellelhetők a gyártók weboldalain is. Továbbá gyakori esetszámmal fordul elő az is, hogy valamilyen teszt vagy fejlesztési felület HTML forráskódjában, kommentben gondatlanul hozzáférést tüntet fel és felejt ott egy fejlesztő. Egy OSINT elemzés során jó technika a HTML forráskód alapján összeállított szöveglista készítése a célpont specifikus keresések végzése érdekében. Tehát ha gyári jelszavak vannak alkalmazásban, vagy ilyen jellegű hibák érhetők tetten, az szemmel láthatóan nem bizonyul egy nagy védelmet biztosító eljárásnak, s ez által szükségtelen kitettséget eredményez. Egy ilyen forgatókönyv esetben egy OSINT elemző, aki a kiberbiztonsági átvilágítást végzi, vélhetően jogosulatlan hozzáférést fog szerezni az adott rendszerhez és megvalósítja az információs rendszer vagy adat megsértése bűncselekmény törvényi tényállását, mivel teljesülnek a konjunktív feltételek, miszerint az adott rendszeren aktív védelmi eljárás kell legyen eszközölve, s a hozzáférés szerzés azt kijátszva történjen meg. Sarkaltos pont, hogy a nyílt forrású eszközökkel történő vizsgálatokhoz elvégzéshez nem szükségesek előzetes engedélyek, így a felhatalmazás híján merülhetnek fel kételyek. Azonban nagy tekintettel a megelőző védelmi célzatra, a kártékony szándék és a társadalomra veszélyesség hiányára, valamint a megrendelő és a szolgáltató közötti bizalmon alapuló kapcsolatra azt lehet mondani, hogy e tevékenység a szürke zónán belül marad.

Ugyan ez a mintázat húzható arra az esetre is, amikor például egy webszerveren hozzáférés-szabályozási hiányosságok okán olyan könyvtárak is bejárhatók, melyeket eredetileg nem szántak annak (például /uploads, /assets, /admin), s azok bizalmas adatokat tartalmaznak. Elemzéskor ezekhez a tartalmakhoz a vizsgálatot végző hozzá fog férni, és annak érdekében, hogy érdemben meg tudja ítélni a hiba jelentőségét, súlyosságát, a „kint hagyott” fájlokat fel kell mérni. Bizonyos formátumú, például a PHP vagy JSON fájlokat egyszerűen a böngészőben is meglehet vizsgálni, azonban van, amit csak letöltést követően. Lényegesen nagy különbséget képez ugyanis, ha csak web-design célra használt tartalmakról van szó (például .css és java script állományok) vagy bizalmas információkat tartalmazó SQL adatbázisokról. Az említett könyvtárak bejárhatóságának vizsgálatát el lehet végezni manuálisan, ha a célzott webszerver URL-jének felkeresésekor begépeljük azok neveit, illetve automatizáltan, egy a teljes

kipróbálás módszerén (brute force²⁰) alapuló szoftver segítségével, mely azonban már az aktív felderítés módszerei közé tartozik. Fontos megjegyezni, hogy ami bármilyen okból is nyilvánosan elérhető, arról az elemzőnek nem feladata megítélni, hogy szándékos-e vagy sem, maga a kint lét ténye már a szándékosságra utaló tényező lehet. Ezen a ponton ismét felmerül egy jogi akadály kérdésköre, miszerint az így hozzáférhető tartalmak nyílt forrásnak minősülnek-e. Amennyiben nem, letöltésükkor az elemző megvalósíthatja a tiltott adatszerzés bűncselekményét. Jelen példában a célzat nem a magán vagy üzleti titok megsértése, hanem a biztonsági rések feltárása, valamint figyelembe kell venni azt, hogy a magyar jogi szabályozás elmarad a technológia fejlődési üteme mellett, így, az precedensek hiányában nem egyértelmű. Valamint a célzathoz levezetve e tekintetben is minimális szintű társadalomra való veszélyességről lehet beszélni.

Erkölcsei kétség jelentkezik továbbá egyes automatizált információgyűjtő szoftverek használatát illetően, mivel azok bizonyos esetekben olyan forrásokból is hozhatnak adatokat a célpontról, melyek már nem minden tekintetben minősülnek klasszikus OSINT-nak. Ez alatt jellemzően azokra a tartományokra kell gondolni, melyek nem mindenki számára hozzáférhetők, és szembe mehetnek egyes személyes adatvédelmi regulációkkal. Automatizált passzív felderítő szoftverből számos változat létezik, azonban jelen esetben a Spiderfoot névre keresztelt programot emelném ki. Használati eseteit tekintve a Spiderfoot-ot többnyire eszközfeldezésre, biztonsági értékelések készítésére és támadásfelszín figyelésére alkalmazzák, mely feladatköröket több mint 100 integrált forráson keresztül szolgál ki. Azonban az információgyűjtési tartományok spektruma tovább bővíthető egyéb szolgáltatások API²¹ kulcsait felhasználva. Ilyen kiegészítő beköthető forrás a DeHashed²² is, amely lényegében egy feltört adatbázis-keresőmotor, amelyet biztonsági elemzők, újságírók, biztonsági cégek és hétköznapi emberek számára hoztak létre, hogy segítsenek a fiókok védelmében, és betekintést nyújtsanak az adatbázis-feltörésekbe és a fiókszivárgásokba. Erkölcsi aggályok ezzel kapcsolatban abból a megközelítésből merülhetnek fel, hogy az egyes szivárgott regisztrációk vizsgálata a személyességből kifolyólag már-már a levéltitok megsértésének határát súrolják. Azonban minden ilyen jellegű erkölcsi határ semmisnek tekinthető, ha az elemzés a kitérttség mérésére, a biztonsági szint megállapítására és annak

²⁰ Egy, a valamilyen titkosítást alkalmazó rendszerekkel szemben elkövetett támadási mód. Működésének lényege, hogy az adott rendszer ismeretében előre összeállított szólista segítségével az összes lehetséges kulcsot kipróbálva határozza meg az alkalmazott kulcsot.

²¹ Az API-kulcs egy egyszerű, titkosított karakterlánc, amely az adott alkalmazás azonosításáért felelős, valamint nyilvános adatok anoním elérését teszi lehetővé.

²² <https://www.dehashed.com/>

fejlesztésére irányul, ugyanis szakmai mulasztásnak minősíthető, ha az ilyen és hasonló információ tartományok figyelmen kívül hagyásával vagy mellőzésével történik a vizsgálat. A támadók nem fognak megállni az adott erkölcsi vonalakon, ebből eredően, ha az elemző megáll, akkor nem tud naprakész információt szolgáltatni ügyfelének.

8. Az emberi tényező

A munkavállalók személyenkénti online aktivitásának, illetve annak biztonságosságának vizsgálatakor sarkalatos pont a hackerek körében is nagy értéket képező, különböző adatszivárgások és adatsértésekből származó tartalmak elemzése, mivel azokból pontos képet alkothatunk arról, hogy az adott személy az elvárásoknak megfelelően használja-e a rendelkezésére bocsátott vállalati email címet, telefonszámot és egyéb eszközöket. Ennek leghatékonyabb módja minél több forrás automatizált legyűjtése valamilyen kereső robot (továbbiakban: web crawler) segítségével. A web crawler az olyan speciális programok gyűjtőneve, amelyek képesek az interneten fellelhető publikus, illetve a robots.txt²³ és a robots metatag által engedélyezett tartalmak letöltésére, és ezek valamilyen formában való elemzésére és az adatok eltárolására. A gyűjtést követően a tartalmakat egy tetszőleges adatbázisba kell rendezni és kereshetővé kell tenni. Lehetőségekhez mérten a gördülékeny munkavégzés érdekében célszerű egy különálló back-end²⁴ és front-end²⁵ környezet kifejlesztésével társítani az összeállított adatbázist. Jóllehet, hogy az ilyen kétes forrásokból származó tartalmak használatáról megosztó vélemények vannak, valamint a GDPR aspektusából is vethet fel kételyeket. A szivárgott vagy szivárogtatott listák ugyan nyilvánosan elérhetők, de megszerzésüket követően mi magunk leszünk tulajdonképpen az adatkezelők. Azonban figyelembe kell venni azon tényezőt, hogy egy kiberbiztonsági átvilágítás keretében nem magáncélra történik az adatkezelés, hanem sokkal inkább egy kockázatelemzési célból, aminek az információszolgáltatás a vonzata. Egy vállalat, ha pontos képet kap magáról a kitettségei tükrében, a rendelkezésére bocsátott ismereteket be tudja építeni például munkavállalóinak információbiztonságtudatossági képzésébe, ezzel akár hozzásegítve őt egy tanúsítvány megszerzéséhez szükséges szint eléréséhez.

²³ Egy egyszerű szöveges fájl, amely instrukciókat tartalmaz a robotok számára, hogy az azt tartalmazó weboldal mely oldalait érhetik el.

²⁴ Informatikai rendszereknél back end-nek hívjuk egy adott alkalmazás szerver oldali "háttér/kiszolgáló" logikáját vagy kódrészt.

²⁵ A programoknak, weboldaloknak az a része, amelyik a felhasználóval közvetlenül kapcsolatban van. Feladata az adatok megjelenése, befogadása a felhasználó (vagy ritkábban egy másik rendszer) felől.

Amennyiben tehát egy profitorientált entitás, egy piaci kiberbiztonsági hírszerző cég dolgozik a fentebb említett koncepció szerinti adatbázisokkal, az a sajátos kontextusból kifolyólag védhető a GDPR rendelkezéseivel szemben. Ugyanis a szabályozás fogalomtárában is megjelenő jogos érdek lehetővé teszi ezt. A cég jogos érdeke ezesetben az anyagi haszonszerzés mellett az ügyfelei biztonságának garantálása, melyet a naprakész információszolgáltatás útján képes ellátni, amihez elengedhetetlen szükség van az adatbázisokban szereplő adatok felhasználására. A GDPR rendelkezései szerint ehhez szükséges egy úgynevezett érdekmérlegelési teszt elkészítése, melyben az adatkezelő részletesen szemlélteti az adatok forrását, az adatszerzés és felhasználás körülményeit, valamint egy logikai érvelés láncolat útján bizonyítja, hogy az ő jogos érdeke miért való előrébb, mint az adatkezeléssel érintett személy, vagy személyek érdekei, Ennek jellemző és egyszerű példája az egyes kereskedelmi egységekben üzemeltetett biztonsági kamerák és azok felvételei. A tulajdonos jogos érdeke, hogy üzletét és annak árucikkeit a megfelelő biztonságban tudhassa, és megelőzze az őt esetlegesen megkárosító eseményeket, vagy azok megtörténte esetén meg tudja tenni a szükséges jogi lépéseket. Ezzel szemben ésszerűen hátrébb sorolhatók azon személyek érdekei, akiket az adott biztonsági kamera rögzít.

9. Etikusság kérdésköre

Társadalmi szinten elmondható, hogy bizonyos esetekben az erkölcsi vonatkozásban alkotott ítéletek egyerősebbek, mint a törvényi ítéletek. Nem kifejezetten jogkövetkezmény tekintetében, de morálisan biztosan. A következőkben annak kérdéskörében vizsgálódok, milyen nézőpontból és mennyire etikus, vagy éppen etikátlan az alkalmazott eljárás. Milyen szerződési megkötések és engedélyek mellett indulnak el az egyes vizsgálatok, továbbá milyen akadályok jelentkezhetnek akár jogi szinteken. Különös tekintettel arra, miképp tekint a GDPR az adatsértésekből származó tartalmak elemzésére, illetve milyen társadalmi megítélés alá esik az egyének személyes, mondhatni intim mélységben történő vizsgálata a szakemberek szemében. Utóbbi tagmondat esetében azt értem, hogy vannak olyan speciális esetek, mikor egyrészt az Oversharing²⁶ és adatszivárgások, másrészt a kétes aktivitás (például Dark Web fórumok tisztázatlan célú használata) következtében lehetséges – és célhoz kötötten szükséges – az adott célszemély magánéletét is olyan részletekig megvizsgálni, mely már kifogásolhatónak tűnhet egy kívülálló és laikus ember számára. Mindezt természetesen a

²⁶ Az a jelenség, mikor egy felhasználó túlzott mélységben oszt meg tartalmakat magánéletéről, tálcán kínálva fel értékes információkat az ártó szándékú támadók számára, s ez által veszélybe sodorja saját online biztonságát.

veszélyforrások legteljesebb mértékig történő detektálása és mitigálása érdekében. A kérdéskör vizsgálata tervezetten kiterjed mindkét, vagyis a megrendelői és végrehajtói oldalra egyaránt. A szöveggörnyezetbe helyezésként az alábbi két eshetőséget vázolnám fel. Egyes vállalatok-szervezetek esetében (például a közigazgatás egyes egységei, vagy ipari gyártással foglalkozó nagyvállalatok) talán kételyek nélkül merülhet fel annak eshetősége, hogy egy idegen ország titkosszolgálatának, például ipari kémkedés céljával beépített ügynöke az adott munkavállaló. Kevésbé szélsőséges esetben azonban felmerülhet azon forgatókönyv is, miszerint egy befolyásos pozícióban lévő munkavállalóval kapcsolatban merül fel gyanúja adott vállalat vezetőségének, azonban a munkajogi gyakorlatok nem teszik kézenfekvővé közvetlen elbocsátását. Mivel nem törvényi erővel bíró bizonyíték beszerzése a cél, hanem kizárólag ráutaló kontextuális jelek gyűjtése szükséges, így a nem nyomozati jogkör révén a rendőrség helyett a vezetőség egy Intelligence szolgáltató céget bíz meg. E tekintetben vizsgálom a két oldalon megjelenő erkölcsi-etikai korlátok jelentkezését, valamint azok esetleges átlépését.

10. Megrendelő és Végrehajtó kapcsolata

Mivel a munkáltatónak a vállalata vagy szervezete biztonságának érdekében tudnia kell, kivel dolgozik együtt, milyen munkavállalókat alkalmaz, így fontos kérdéskörként merül fel az ellenőrzés. Természetesen minden munkahelynek meg van a saját belső szabályzói környezete, beleértve a szervezeti és működési szabályzatot, a vonatkozó információbiztonsági és minőségbiztosítási tanúsítványokat, szabványokat (például ISO 27001²⁷, NATO AQAP²⁸ stb.), titoktartási szerződéseket és az egyéb protokollokat. Továbbá a sajátos ökoszisztéma részét képezik az egyes vállalati tulajdon alá tartozó eszközök, melyek jelen kontextusban, az információbiztonságban, a számítógépbiztonságban és a hálózati biztonságban minden olyan adat, eszköz vagy a környezet egyéb eleme, amely támogatja az információval kapcsolatos tevékenységeket. Az eszközök általában hardvert, szoftvert és bizalmas információkat tartalmaznak. Ide sorolhatók a vállalati email címek is, melyek használatával kapcsolatban a munkavállalók felelősséggel és elszámolási kötelezettséggel tartoznak a munkáltató irányába. Az ellenőrzés folyamatának tehát összhangban kell állnia a belső szabályzókkal, valamint tényének a munkaszerződésekben is meg kell jelenniük, ezen felül szervezet specifikus, hogy mire és hogyan terjedhet ki. Példának okáért, a hivatásos szolgálati jogviszonyban állók teljes

²⁷ Az ISO 27001 vagy ISO/IEC 27001 egy információbiztonsági szabvány, amelyet a Nemzetközi Szabványügyi Szervezet és a Nemzetközi Elektrotechnikai Bizottság együttesen tesz közzé.

²⁸ Allied Quality Assurance Publications a minőségbiztosítási rendszerek szabványai, amelyeket a NATO fejlesztett ki. Az AQAP megállapodás célja a védelmi termékek minőségbiztosításának szabványainak meghatározása.

tudtában vannak annak, hogy őket szolgálatellátásuk során bármikor megbízhatósági vizsgálatnak vethetik alá. Hasonló minta alapján történhet a titoktartási szerződések betartásának vizsgálata is, melyhez az adott szervezet külső cégtől megrendelhet CTI szolgáltatásként egy digitális kitettségvizsgálatot. A vizsgálat keretein belül meghatározható bizonyos munkavállalók online térbeli tevékenységének nyílt forrásból történő vizsgálata. Ilyenkor személyenkénti lebontásban történik meg a biztonsági rések feltárása, melyek jellemzően gondatlan vagy szándékos információszivárogtatásban, illetve a vállalati email címek nem megfelelő használatában gyökereznek. Sok esetben ugyanis a munkavállalók magáncélú regisztrációkhoz is felhasználják a munkavégzésükhöz rendelkezésükre bocsátott email címet – például társskereső oldalakon és ételszállító szolgáltatásokhoz – újra hasznosítva ugyan azt a jelszót, amit a belső rendszerekhez is használnak. Egy ilyen forgatókönyvben, ha adatsértési incidens éri az adott szolgáltatót, az közvetett veszélyt jelent a vállalatra, mivel kiszivárgott egy lehetséges hozzáférés. Gyakori jelenség még, hogy a kevésbé biztonság tudatos dolgozók a különböző közösségi média felületeken olyan tartalmakat osztanak meg, melyek szükségtelen kitettségeket eredményeznek, például az irodában a munkaállomások közelében készített portrék, képernyőfotók, a belépőkártyákról készített fényképek. Ezek mind olyan hasznos információkat fedhetnek fel (például használt szoftverek), amelyeket később egy támadó fel tud használni a támadási stratégiájának megtervezésekor. Továbbá az informatikai személyzet, például szoftverfejlesztők részéről szokott előfordulni, hogy különböző szakmai fórumokon teszik fel az éppen aktuális projekttel kapcsolatos kérdéseiket, gyakran felfedve kódrészleteket vagy pontos elérési utakat. Fontos kritérium a személyiségi jogok tiszteletben tartása mellett, hogy az ellenőrzés kizárólag az adott munkavállalóra terjedhet ki, és csak a munkavégzéssel összefüggésben álló tényezőkre. Ennek értelmében a munkáltató nem kérheti olyan adatok szolgáltatását, melyeket nem rögzít a munkaügyi nyilvántartás (így például egészségügyi adatok), továbbá összeférhetetlenség vagy összefonódás hiányában nem lehet indokolt a magánéleti tényezők, a családi és ismeretségi kör vizsgálata sem. További no-go zónát alkothat még a sok vállalatnál népszerű és előszeretettel alkalmazott úgynevezett „Hozza magával saját készülékét” eszközmenedzsmenti modell (angolul BYOD, vagyis Bring Your Own Device), amikor is a munkavégzéshez nem a cég biztosítja az eszközöket a munkavállalók számára, hanem azok a saját tulajdonú eszközeiket használhatják. Ilyenkor ugyanis az alkalmazottak nem tartoznak teljeskörű elszámolási kötelezettséggel, amíg tevékenységükkel nem veszélyeztetik a munkavégzés érdekeit. Azonban ilyen esetben sem kérheti a megrendelő, hogy az elemző bármilyen értelemben ellenőrzést hajtson végre az adott munkavállaló saját tulajdonú eszközét illetően.

Összegzett következtetés

Az OSINT-ot érintő számos akadály közül az egyik, az adatkezelési szabályozások terén megmutatkozó földrészenkénti eltérés. Másképp állnak e kérdés tekintetében az egyes adatnagy hatalmak, tehát az Egyesült Államok, Kína és Európa. Az Egyesült Államokban minden személyes adat az adott személy vagy cég tulajdonát képezi, míg Kína esetében az állam a kizárólagos tulajdonos, Európát pedig az egységes szabályozás miatt kollektíven kell említeni, s esetében a GDPR az irányadó. Ebből kifolyólag nehezítő tényező lehet a jogszabályi környezet széttagoltsága, melynek egységesítése, vagy szimplán a határok bizonyos mértékben átjárhatóvá tétele megkönnyítené a hatékony információszerzést, azonban minden hírszerzés egy alkalmazkodó folyamat, tehát nem lehet arra támaszkodni, hogy ennek elősegítése érdekében hozzanak törvényeket vagy eszközöljenek módosításokat. Továbbá az eltérő államformák és jogrendszerek révén ez nem kivitelezhető. A jogszabályi korlátok kapcsán szűkebb körben, tehát hazai viszonylatban sem kedvezőbb a helyzet, ugyanis a CTI szakmai elismertsége és legitimitása nem éri el azt a szintet, melyet el kellene érniük, nincsenek meg azok a szilárd jogszabályi keretek, melyek lehetővé tennék a szakma számára a biztonságérzetben történő működést. Ebből kifolyólag egyfajta piaci korlát is képződik, mivel szerencsésebb a helyzet, ha az ügyfélkör eleve egy bizalmon alapuló ismeretség útján alakul ki. Továbbá ez forrásbeli akadályokat is felvet, mivel Magyarországon jellemző az adatbázisok transzparenciájának teljes hiánya. Például a közadatoknak és a közpénzből keletkezett adatoknak mind kereshetőnek kellene lennie, továbbá a magyar cégjegyzék is könnyen rejt el a historikus adatokat, melyek hozzáférhetőségéért fizetni kell.

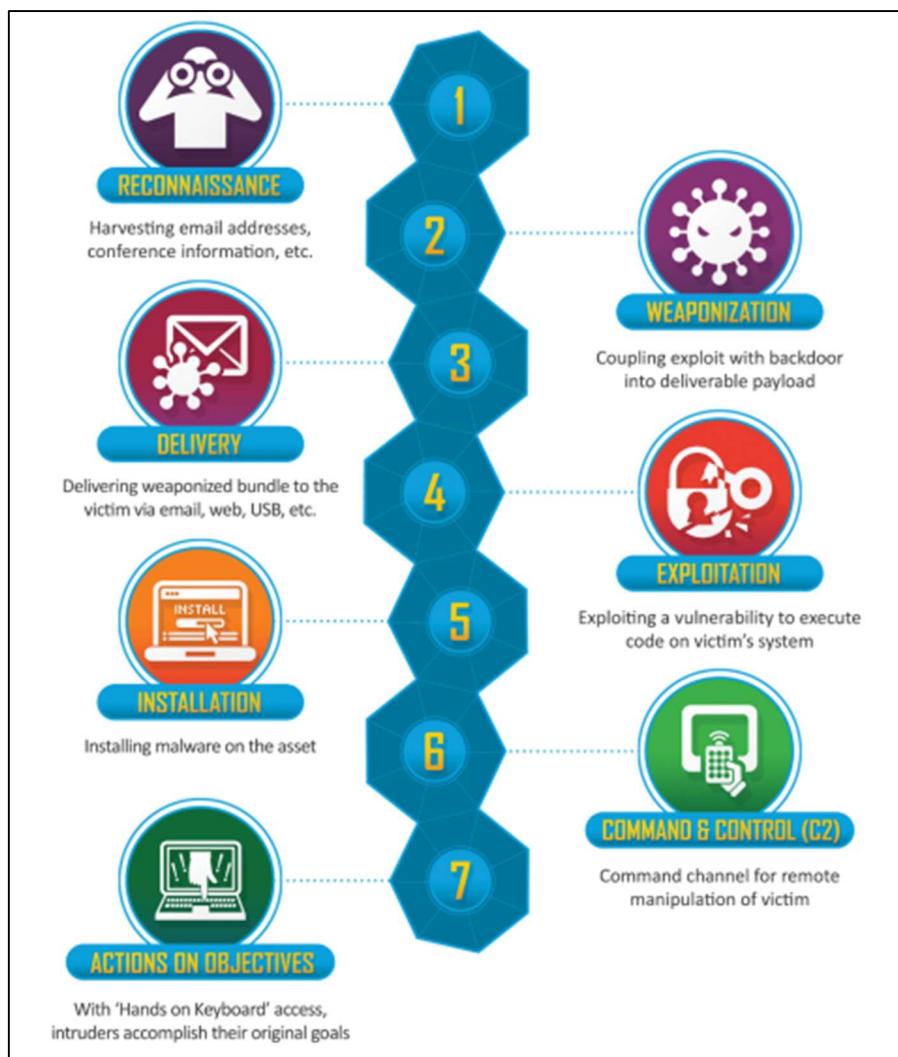
II. OSINT az adathalászattal szemben

A Lockheed Martin által kifejlesztett és az információbiztonsághoz adaptált Cyber Kill Chain® keretrendszer az Intelligence Driven Defense® modell része a kiberbehatolások azonosítására és megelőzésére. A modell meghatározza, hogy a támadónak milyen lépéseket kell megtennie, céljának elérése érdekében. A Kill Chain hét lépése javítja a támadások láthatóságát, és hozzájárul az elemzők látóterének-megértésének gazdagításához az ellenfél taktikájával, technikáival és eljárásaival (Tactics, techniques and procedures továbbiakban: TTP-k) kapcsolatban. A modellt egyébként elsősorban az APT csoportok tevékenységével hozták összhangba. Dolgozatom jelen fejezetében a Kill Chain első láncszemének, tehát a felderítés perspektívájából vizsgálom meg az OSINT kompetitív hatékonyságát az adathalászattal szemben.

1. A Cyber Kill Chain® modell

Az informatikai biztonságban széleskörűen alapul vett, hét lépésből álló Kill Chain modellt az amerikai gyökerű, elsősorban repülőgépgyártással foglalkozó – majd a későbbiekben már haditechnikai és űrkutatási irányba is terjeszkedő – Lockheed Martin elnevezésű cég adaptálta az információbiztonsághoz, melyen keresztül kívánták szemléltetni a számítógépes hálózatokba történő behatolásokat. A folyamat lépései egymásra épülően a mindent megalapozó felderítés, melyen belül a célponttól történő mély és részletes információgyűjtés történik, az email címeiktől kezdve a fizikai eszköztípusokig bezárólag. Második fázisban kezdődik meg a felfegyverkezés, amikor a fellelt sebezhetőségekről szóló információk alapján a támadók összeállítják a célra legmegfelelőbb támadóeszközt, malware-t. Ezt követően kártékony kód bizonyos módon zajló célba juttatása következik, mely történhet például email-ben vagy digitális adathordozón keresztül. A negyedik és ötödik fázisban a támadók elműködtetve a támadóeszközt kihasználják a cél rendszer sérülékenységeit, hozzáférést szereznek és megvetik lábukat. Folytatásul a kommunikációs csatorna (Command & Control, továbbiakban: C2) felállítása következik, a távoli és perzisztens hozzáférhetőség kialakítása érdekében. Miután már a támadók eljutottak erre a szintre, a megtámadott rendszeren intenciójuknak megfelelően cselekedhetnek. Az OSINT technikák a modellben való elhelyezkedésüket tekintve az első és legfontosabb lépcsőfokot alkotják, vagyis felderítés és „lenyomatképzés” (reconnaissance és fingerprinting²⁹) folyamatokat.

²⁹ Az előzetes információgyűjtés folyamata, ami a célpont alapos megismerésén nyugszik.



6. ábra: a Cyber Kill Chain® modell lépések szerinti ábrája. (Forrás: lockheedmartin.com)

2. Kontextuális összehasonlítás

Úgy gondolom, hogy minden személy vonatkozásában – foglalkozásától és társadalmi elhelyezkedésétől függetlenül – a lélegzetvétellel megegyezően alapvető szükségletként kellene, hogy jelentkezzen a privátszféra védelme, belefoglalva személyes adatainkat és a digitális azonosítókat (az OSINT vonatkozásában ilyen értékes adat a felhasználónév, a jelszó és hash³⁰, az email és IP cím stb.) egyaránt. A megfelelő szintű információbiztonsági tudatosság hiányában tett minden digitális érintkezés nem csak az adott egyén számára jelenthet veszélyt, aki áldozatul eshet egy támadásnak, hanem a közvetett és közvetlen ismeretségi körére, továbbá munkahelyére, szervezetére is. Elképzelhető ugyanis, hogy nem mi vagyunk az elsődleges célpont, csupán egyfajta kulcsként, egy ugródeszkeként szolgálunk a célpont eléréséhez (Pivoting). Ebből kifolyólag amennyiben nem alkalmazunk bizonyos biztonsági eljárásokat,

³⁰ Egy kriptográfiai algoritmussal titkosított jelszó. Ilyen algoritmus például az MD5.

nem építünk be cselekvéseinkbe a biztonsági szint növelésére irányuló szokásokat és jó gyakorlatokat, mi képezzük a biztonsági rést a pajzson. A kiberbiztonságban javarészt az emberi tényező kínálja a legnagyobb biztonsági kockázatot, éppen ezért is örvend nagy sikernek valamennyi social engineering és adathalász támadás. Azonban napjainkra az tapasztalható, hogy a kis- és középvállalatok időszerűen szerveznek tudatosító és oktató kampányokat a támadások kivédésére. Jóllehet tehát, hogy az adathalászzal szembeni védekezés már nagyobb hatásfokot képvisel, mivel titka a felismerésben és az aktív cselekvő magatartás megtagadásában rejlik. Ezzel ellenkezőleg a támadólagos OSINT folyamatok javarészt passzív folyamatok, ügyfél-oldalról nem igényelnek tevőleges érintkezést, ezért jelentősen nehezebb őket kiszűrni, felismerni, illetve védekezni velük szemben. A legnagyobb nehézséget a hatékonyság megítélésében a befolyó adatok valódiságának ellenőrzése jelenti. Az adathalászat eredményessége és megbízhatósága mellett szól azon érv, hogy a social engineeringgel átfedésben a célszemély jóhiszeműségét, óvatlanságát és konfliktuskerülési természetét targetálja, így amennyiben célt ér a folyamat, például ha egy átlagos felhasználó ismeretekkel rendelkező személyt valamilyen közműszolgáltató vagy pénzintézet nevében ér támadás, nagy eséllyel a valóságnak megfelelő adatokat ad meg. Azonban számolni kell azzal a lehetőséggel, hogy a legkisebb gyanú felmerülése esetén is megghiúsulhat a támadás, és az egyén figyelmen kívül hagyja azt, esetleg hamis adatokat szolgáltat. Ellentétet képezve, az OSINT vonatkozásában a felhasználók alapesetben nem érzik úgy, hogy bármikor egy támadás potenciális áldozataivá válhatnak, ebből kifolyólag a veszély érzetének hiányában könnyelműen járhatnak el, s a nélkül oszthatnak meg támadók számára értékes információkat, hogy jelezne a képzeletbeli piros lámpa. Egy CTI szolgáltatás keretein belül a talált adatok validációját egyes esetekben a megrendelő végzi, azonban egy támadás előkészítésében nem lehet kizárólag a felhasználó veszélyérzetének hiányára hagyatkozni. Vannak olyan információk, melyeket lehet kontextuális jelekből igazolni, például egy lakcím vagy a vizsgált vállalat telephelye, adott emberek közötti kapcsolat léte, illetve bizonyos limitációkkal, de rendelkezésünkre állnak ellenőrző eszközök, mondjuk bankkártya és telefonszámok vonatkozásában. Ellenben megfelelő méretű digitális lábnyom hiányában meglehetősen nehéz igazolni egy név vagy születési hely és idő valódiságát. Ezért is lehet kifejezetten jó védekezési alakzat a dezinformáció.

3. Eltérő célpont, eltérő technika?

A következő szempont, melynek figyelembevétele szükséges a hipotézis igazolásához azon kérdéskör, miszerint a célponttól (vagyis a személy és annak életkora, szokásai, értékrendje,

valamint munkahelyének, szervezetének típusa és szektoriális elhelyezkedése) függetlenül egységesen hatékonyak-e az egyes módszerek, vagy annak függvényében finom hangolni kell őket? Tehát egyaránt működik minden célpontot illetően az OSINT vagy bizonyos esetekben az adathalászat kínál célravezetőbb eredményt?

A különböző nagy társadalmak (jellemzően nyugati, keleti és távolkeleti) online térben is megjelenő kultúrájához adaptálódni kell a megfelelő módszertan és metodológia megválasztásakor. A gyakorlatban mára megvannak a legkiforrottabb technikák, amelyekkel könnyedén lehet például csupán felhasználónevek vagy egyéb ismertető jegyek – akár billentyűzet használatból rajzolódó írásképek minták – alapján valódi személyhez kötni egyes digitális entitásokat, profilokat. Továbbá a napjainkra kialakult közösségi médiahasználati trendeknek köszönhetően meglehetősen konzekvenssé váltak a releváns források. Értem ezalatt azt, hogy kézzelfogható sarokpontok érhetők tetten, amikor egy vállalt munkavállalói hálóját kívánjuk feltérképezni, vagy éppen haditechnikai vonatkozásban vizsgálódunk. Előbbire általános gyakorlat szerint a LinkedIn közösségi platform nyújt kiváló alapot, utóbbi vonatkozásában pedig számottevően sok hazai és nemzetközi szakmai fórum áll rendelkezésünkre. Legtöbbször. Azonban akadnak a konvencionálistól teljes mértékben eltérő esetek is. Így példának okáért, Kína – feltehetőleg politikai bizalmatlansági alapon – maradéktalanul elzárkózik a nyugati eredetű technológiák, trendek használatától, s helyette főképp saját fejlesztésű implementációkat alkalmaznak függetlenül attól, hogy ez bizonyos esetekben a biztonsági szint vagy éppen az adott szolgáltatás színvonalának rovására megy. Továbbá jelentős eltérés figyelhető meg a közösségi média használatuk vonatkozásában is a nyugati társadalmakéhoz képest, amely igen nagy kihívás elé állítja az OSINT elemzőket, s nem csak az esetleges nyelvi akadályokat illetően.

Figyelembe kell venni azt, hogy a tárgyalt két információszerző és támadáselőkészítő módszer eltérő eszköztárral dolgozik, ebből kifolyólag felmerül annak gondolata, hogy hatékonyságuk önmagában nem vethető össze egymással. Tehát adja magát a következő kérdés, miszerint mire mi a leghatékonyabb. Tekintve, hogy az adathalászat jellegéből adódóan emberi felhasználókat céloz, ésszerű a feltételezés, miszerint esetükben az jobbnak bizonyul, mint az OSINT. Informatikai infrastruktúrákról azonban nem feltétlenül az adathalászat technikáit alkalmazva fogunk tudni éles képet alkotni. Azonban a felállás akkor sem ilyen egyszerű, ha ezt a két célpontot vesszük alapul, a rendszert és a felhasználót, mivel köztük számos összefonódás fedhető fel. A következőkben két ilyen összefüggést vázolok fel.

4. Az adathalászat, mint az OSINT kiszolgálója?

Az adathalászat nagy aggodalomra ad okot a közelmúltbeli adatszivárgásokban és az államilag támogatott (APT) támadásokban betöltött aktív szerepe miatt.³¹ Amint arra az előző fejezetben kitértem, a digitális kitértségvizsgálatok és a kiberbiztonsági átvilágítások során az elemzőnek olykor megkerülhetetlen feladata a különböző vállalati adatszivárgásokból, valamint javarészt a közösségi médiából eredő adatsértésekből álló adatbázisok vizsgálata, melyek olyan vitális információkat tartalmaznak, mint email cím és jelszó párosok, felhasználónevek, jelszó hash-ek, kimenő IP címek és geo-lokációs adatok, valamint telefonszámok. Továbbá az adatszivárgásokat illető melyebbre menő elemzésben nyújthat még segítséget az úgynevezett Szivárvány táblák (továbbiakban: Rainbow table³²) használata, melyet elsősorban ugyan a jelszavak feltöréséhez alkalmaznak az etikus hackerek, azonban a visszafejtett jelszó-hash-ekkel végzett keresések további eredményeket rajzolhatnak ki. A hipotézis érdemleges igazolásához vagy cáfolásához fontos megvizsgálni az említett adatbázisok keletkezésének körülményeit, ugyanis javarészüket kártékony szándékú támadók által elkövetett adathalász kampányokból tevődnek össze, melyeket aztán kritikusságuktól függően tovább értékesítenek különböző Dark Web fórumokon vagy anyagi haszonszerzés nélkül, csupán a presztízs és reputációgyarapítás jegyében nyilvánosan közzé tesznek. Másodrészt pedig az adatbázisok forrását képezhetik az egyes Third-party szolgáltatók ügyféladatbázisai ellen intézett célzott támadások (például SQL-injection³³). Az általános gyakorlat szerint az utóbbi forgatókönyv eredménytermékei kerülnek értékesítésre a zártkörű fórumokon, azonban hipotézisem vonatkozásában számomra az előbbi a mérvadó.

5. Adathalászattal sakk-matt

Fentebb említésre került, hogy az informatikai rendszerek ellen intézett támadások előkészítésében az OSINT játszhat nagyobb szerepet, mivel azok nyílt forrásokból akár a legkisebb részletekig is feltérképezhetők, viszont alacsony az életszerűsége, hogy csupán emberek által kiadott információkból tegyünk össze a képet. Az első fejezetben szemléltetett módszereket alkalmazva könnyedén juthatunk hozzá a szükséges IP címekhez, nyitott

³¹ P. Peng és mtsai., „What happens after you leak your password: Understanding credential sharing on phishing sites”, in *AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (Association for Computing Machinery, Inc, 2019), 181–92, <https://doi.org/10.1145/3321705.3329818>.

³² Egy előre kiszámított táblázat a kriptográfiai hash függvények kimenetének gyorsítótárazásához, általában jelszavak feltöréséhez alkalmazzák.

³³ Structured Query Language, a relációsadatbázis-kezelők lekérdezési nyelve. SQL-injection: Olyan kódbejuttatási technika, amelyet adat vezérelt alkalmazások támadására használnak, és amely során rosszhindulatú SQL utasításokat szűnnek be egy beviteli mezőbe végrehajtás céljából.

portokhoz és egyéb, a támadás szempontjából szükséges adatokhoz. Azonban, mindez mellőzhető, vagy akár szükségtelen is lehet, ha a megfelelő célszemélyt sikerül megütni. Az adathalászat szempontjából a legmegfelelőbb célszemély egyrésztől nem áll megfelelő információbiztonsági tudatosság birtokában, azonban rendelkezik a szükséges hozzáféréssel a célrendszerhez. Legyen az akár csak egy helyi felhasználó fiók. Az adathalászat sokszor kéz a kézben jár bizonyos social engineering támadásokkal – egyes irodalmak szerint annak részét képezi – így életképes forgatókönyv, hogy már rögtön a rendszerkompromittálásra tett kísérlet van adatszerzésre irányuló támadásnak álcázva. Ilyenkor jellemzően az adathalász email csatolmányában (például egy kitöltendő dokumentumban) kerül beágyazásra egy kártékony kód, mondjuk egy reverse shell. A shell egy felhasználói felület az operációs rendszer szolgáltatásaihoz való hozzáféréshez. A reverse shell kapcsolat során a célpont rendszer veszi fel kommunikációt a támadó rendszerrel, ezáltal a kimenő kapcsolat okán nehézséget okozva a tűzfalaknak az észlelésben és tiltásban. Ebben a példában másodlagos és irreleváns, hogy az adathalász levéllel célzott személy megadja-e a kért adatokat, azonban vitathatatlanul szükséges arra irányulóan tálni. Kulcs fontosságú azonban kiemelni, hogy egy ilyen támadás kivitelezhetőségét is nagy valószínűséggel segíti elő az OSINT, hiszen valahogyan meg kell határozni a megfelelő személy kilétét.

Összegzett következtetés

Az adathalászat az emberi tényező támadását illetően biztosít nagyobb megbízhatóságot, amíg az informatikai infrastruktúrák ellen intézett támadások előkészítését az OSINT szolgálja ki nagyobb mértékben. Azonban mindez nem elegendő ahhoz, hogy a két módszer hatékonyságát összemérve győztest lehessen hirdetni, ugyanis egy jól kivitelezett támadást megelőzően nagy eséllyel kerülnek együttes alkalmazásra. E tekintetben második hipotézisem, miszerint az OSINT nagyobb megbízhatóságot és eredményességet biztosít a támadások előkészítésében, mint az adathalászat, megdőlt.

III. A fenyegetettség mértéke a digitális lábnyom méretében gyökerezik

Attól a ponttól kezdve, hogy mindennapi életünk legegyszerűbb mozzanataiba is beszivárgott az internet, a technológia és ezzel együtt a digitális eszközök használata, ajtótól ajtóig digitális lábnyomot termelünk és hagyunk hátra, sokszor egyáltalán nem törődve az információbiztonsági aspektusokkal és kockázatokkal.

Roser szerint (2019) szerint az internethasználók száma a 2000-es években 413 millióról 2016-ra több mint 3,4 milliárdra nőtt. Másodpercenként több millió adat keletkezik, ezen felül az internet több mint kétévente megduplázza ezt az adatmennyiséget (Turner 2014). Ez egy információs aranybánya, de egyben óriási feladat ilyen mennyiségű adat átválogatása és az összegyűjtött darabokat valami értékessé alakítani. Burke (2007) szerint az intelligencia annak a végterméknek tekinthető, amely az adatok elemzéséből és szűréséből fakad, hogy valamit generáljunk egy meghatározott célra.³⁴

Az OSINT orientációja az elnevezéséből is fakadóan az adatok gyűjtése köré összpontosul, mely adatokat kontextusba helyezve információt kapunk, amit aztán alkalmazási területtől függően felhasználunk. Ezen egyszerű kijelentésből levezetve olybá tűnik, hogy minél több információ áll az elemző rendelkezésére, annál jobb. Habár ez az állítás csak félig igaz, ugyanis a nyílt forrású információszerzéssel végzett munka során az egyik legjelentősebb nehézségként jelentkezik a „zaj” leszűrése³⁵, vagyis a begyűjtött információmennyiség szelektálása a feladat szerinti relevanciaérték alapján, valamint a találatok kontextusba helyezése. Ugyanis, mint azt tapasztalhatjuk a mindennapi internethasználat során is, ha egyszerűen önmagában rákeresünk valamire egy keresőmotor használatával, másodpercek alatt kapunk vissza milliós nagyságú találatszámot, s aligha jutottunk közelebb célunkhoz. Mégis, az online térben végzett információszerzés tágabb és átfogóbb lehetőségeket kínál, mint a klasszikus források (különböző írott formában megjelenő sajtótermékek, televízió és rádióadások stb.) elemzése, mivel nagyobb és sokrétűbb tartományokból meríthetünk. Mindazonáltal a teljesértékű

³⁴ A. Kanta, I. Coisel, és M. Scanlon, „A survey exploring open source Intelligence for smarter password cracking”, *Forensic Science International: Digital Investigation* 35 (2020), <https://doi.org/10.1016/j.fsidi.2020.301075>.

³⁵ S. Lee és T. Shon, „Open source intelligence base cyber threat inspection framework for critical infrastructures”, in *FTC 2016 - Proceedings of Future Technologies Conference* (Institute of Electrical and Electronics Engineers Inc., 2017), 1030–33, <https://doi.org/10.1109/FTC.2016.7821730>.

képalkotás érdekében meg kell említeni bizonyos előnyöket és hátrányokat. Ezt az alábbi táblázatban teszem meg.

1. táblázat: Az OSINT előnyei és hátrányai. (Saját szerkesztés)

Előnyök ✓	Hátrányok ✗
Óriási mennyiségű elérhető információ	Adatkezelés összetettsége
Nagy számítási kapacitás	Strukturálatlan információhalmaz
Big Data és gépi tanulás lehetősége	Dezinformáció lehetősége
Kiegészítő adattípusok	adatforrások megbízhatóságának kétsége
Rugalmas cél és széles hatókör	Erős etikai/jogi megfontolások

Következtetéseket levonva tehát, iszonytató mennyiségű információt vagyunk képesek elérni, s a kiegészítő adattípusok hozzájárulnak az elemzésből kapott kép finomhangolásához, azonban az adatok megfelelő struktúrába történő rendezése és kezelése komoly kihívást okozhat. Ebben segítségünkre lehet a machine-learning, vagyis a gépi tanulás alkalmazásának lehetősége. Ugyanakkor nem lehet eltekinteni a szándékos dezinformációs kísérletektől, melyek hamis információk-hírek-tények közlésén alapul, emiatt elengedhetetlen a forrás hitelességének és megbízhatóságának ellenőrzése. Bizonyos esetekben az erre szükséges időráfordítás veszélyeztetheti a feladat érdekeit. A leghangsúlyosabb előny és hátrány ütközés azonban abban rejlik, hogy bár meglehetősen szerteágazó célokra alkalmazhatjuk az OSINT kínálta lehetőségeket, azok gyakran igen erős, vitatott megítélés alá esnek mind erkölcsi, mind jogi perspektívákat illetően.

1. A védekezés lehetőségei

Az OSINT-tal szembeni védekezés számos kérdést vethet fel bizonyos aspektusokból szemlélve. Eredetileg passzív jellegéből adódóan nem titulálható támadásnak, valamint a kill chain-ben való elhelyezkedését is tekintve előkészítő-felderítő folyamat, melyet legfeljebb „támadólag” lehet alkalmazni. Nagy nehézséget okoz a detektálás és visszakövetés, vagyis annak megállapítása, hogy egy adott incidens háttérében OSINT munka állhatott. Az aktív felderítési módszerekkel ellentétben, a nyílt forrásokból gyűjtő eszközök nem hagynak nyomot az adott rendszer naplófájljaiban, mivel az automatizált szoftverek java része is a megkerülés módszerével dolgozik, tehát nem interaktál például a célpont domain-nel, hanem külső adatbázisokból hoz eredményeket, vagy API kulcsokkal bekötött szkanner-szolgáltatásokat futtat. Így legfeljebb az adott támadás jellegére, és annak arculatára lehet hagyatkozni a

megítélés során. Ennek értelmében a részletekben kell keresni az ördögöt, tehát ha egy Phishing támadás során a vállalatunknál is használt szolgáltatás letükrözését kapjuk (például Microsoft vagy Jira bejelentkező felület), akkor jó okkal feltételezhetjük, hogy előzetes felderítésként az informatikai infrastruktúra esetlegesen kint lévő és nyilvánosan elérhető elemeit vizsgálták meg, szűrőpróbaszerű próbálkozás helyett. Továbbá az incidenskezelés részeként a jogi lépések megtétele is falakba ütközhet, mivel az OSINT eszköztárát bárki igénybe veheti törvényi engedélyek szüksége nélkül, továbbá felhasználásának korlátjaira sincs egyértelmű szabályozás.

A következőkben annak kérdését vizsgálom meg, mely szerint hatékony, illetve elegendő védekezési alakzatnak bizonyulhat-e a digitális lábnyom tudatos és szándékos minimalizálására irányuló törekvés, vagy a dezinformáció, amikor ugyan növeljük az online ujjlenyomatunk méretét, de azt érdekeinknek és céljainknak megfelelően torzítjuk. Továbbá röviden bemutatok néhány defenzív OSINT technikát is, melyeket alkalmazva nagyobb eséllyel garantálhatjuk magunknak online biztonságunkat.

2. A tudatos lábnyomcsökkentés

Talán az elsődleges gondolatként az merülhet fel bennünk, hogy az a legegyszerűbb és leghatékonyabb védekezési módszer az, ha teljes körűen távolmaradunk az internettel minden területétől, különösen a közösségi média használatától. Lehetséges azonban ez napjainkban? Mint említettem fentebb, életünk legegyszerűbb mozzanati során is ajtótól ajtóig digitális lábnyomokat hagyunk magunk mögött, ez a jelenség árnyékként követ minket. Egyszerűen a kényelem és a kézenfekvőség érdekében rá vagyok kényszerülve az online aktivitásra, gondoljunk csak arra, hogy a Covid-19 világjárvány ideje alatt milyen mértékben voltunk ráutalva az interneten keresztül történő élelmiszerrendelésre, mondjuk a hatósági házi karanténok elrendelése okán. Azonban egy nyaralás céljából történő utazás lefoglalása, megszervezése is jelentősen könnyebb folyamat digitálisan, nem is beszélve a hivatalos ügyintézésről, amely jelentős fejlesztési prioritás napjainkban. Magánszemélyként a közösségi médiától való elhatárolódás egy biztonságos döntés lehet, azonban ezzel együtt fel kell adnunk személyes kapcsolattartásaink bizonyos részét, és lekorlátozódni a telekommunikáció klasszikus szintjére. Erre nem mindenkinek nyílik lehetősége, mivel vannak olyan munkakörök, melyek kifejezetten az online kapcsolattartásra épülnek, például egyes kereskedelmi és marketing vonatkozású beosztások alkalmazottai esetében. Tőlük sok esetben követeli meg a munkáltató egy LinkedIn felhasználói fiók működtetését, valamint nevük, elérhetőségük sok

szerződésben és egyéb kiadott dokumentumban szerepelhet. Azok esetében, akiket nem érintenek ilyesféle kötelmek, eredményesnek bizonyulhat a védekezés e módja, eddigi tapasztalataim alapján főképp nagy befolyással rendelkező üzletemberek közkedvelt eszköze a „szellemmé válás”. Habár, nekik is számolniuk kell az elérhető források sokrétűségével, vagyis azzal, hogy nincs mindenre teljes ráhatásuk, a tőlük függetlenül keletkező források, például a nyomtatott sajtóban történő említések eliminálása küzdelmesebb folyamat lehet. A nyílt forrású információszerzés azon körforgásával dacolni, miszerint mindent meg lehet találni, ha a megfelelő helyen keressük óriási kihívás. Levonva a következtetéseket, bizonyos mértékben tehát távol lehet maradni az online tértől, de célszerűségét tekintve nem biztos, hogy a legjobb megoldás.

3. Dezinformáció

A másik védekezési alakzat, melyet meg kívánok vizsgálni, az a szándékos zajkeltés taktikája, melynek kifejezetten nagy kultúrája és kereslete van például az Egyesült Államok celebritás világában. Ilyenkor az előző módszerrel ellentétben, nem arra ügyelünk, hogy minél kisebb mennyiségű tartalom menjen ki rólunk a nyilvános internetre, hanem épp ellenkezőleg. A mindennapi és átlagos közösségi média használat mellett megpróbáljuk hihető mennyiségben növelni a digitális lábnyomunkat úgy, hogy a megosztott hamis tartalmakkal elfedjük a rólunk felfedhető valódi információkat és félrevezessük az utánunk érdeklődőket. A dezinformáció során a nyílt forrásokból begyűjthető információk igazolhatóságának nehézségét vesszük alapul és használjuk ki. Ennek értelmében a legjobb eljárás, amit alkalmazhatunk az, hogy megpróbáljuk közel nullára redukálni a digitális entitásaink hozzánk köthetőségét. Fontos leszögezni, hogy nem minden esetben ez a leghatékonyabb és legkényelmesebb védekezési alakzat, alkalmazását megelőzően mindenkinek mérlegelnie kell. Teljeskörű védelmet nem fog garantálni, hiszen csupán a rólunk nyílt forrásokból fellelhető adatokat eliminálja, értelemszerűen nem bújhatunk el vele a hatóságok elől.

A cél elérése érdekében például a következőket tehetjük:

- Ügyeljünk arra, hogy minél kevesebb valós adatot adjunk meg online, tehát
- közösségi média használatakor alkalmazzunk álprofilokat, valótlan névvel, születési adatokkal és egyébekkel,
- ha közzéteszünk valamit, adjunk meg valótlan hely adatokat, azokat használjuk szisztematikusan

- ha rendelünk valamit az interneten személyes átvétellel, adjunk meg hamis számlázási nevet és címet,
- ha regisztrációt kell SMS-ben kapott kóddal megerősíteni, használjunk online SMS fogadó szolgáltatásokat,
- legyen több olyan email címünk, melyek összetételüket illetően nem vallanak ránk, és minden regisztrációhoz használjunk eltérő címet,
- jelszóinkat illetően hasonlóképp járjunk el.

Némely technika használata bizonyos lemondással járhat, azonban ez örök dilemma, még a számunkra megfelelő vírusirtó szoftver megválasztásakor is. Ez a jelenség leginkább egy mérleg képével írható le, melynek egyik tájában a magánszféra, másikban a biztonság helyezkedik el. Ha az egyikbe beletesszünk, akkor a másikkól kiveszünk. A példák értelmében termékgarancia veszítéssel járhat, ha nem a valóságot fedő adatok szerepelnek a számlán, azonban ha esetlegesen támadás éri az adott szolgáltatót, nem kell aggódnunk amiatt, hogy adataink kiszivároghatnak. Ugyan ez a minta vonatkozik a hozzánk nem köthető email címek vonatkozásában.

4. Defenzív technikák

Annak érdekében, hogy nagyobb eséllyel tudjuk biztosítani saját digitális biztonságunkat, érdemes preaktív jelleggel bizonyos jó gyakorlatokat beépítenünk napi szintű internethasználatunkba, mivel sok esetben nyílt forrású eszközök és szolgáltatások segítségével kivédhetők egyes veszélyek. Az egyes technikák jelentőségét esetpéldákon keresztül szemléltetem, kifejezetten a metaadatok esetében.

5. Fájl-hash vizsgálat

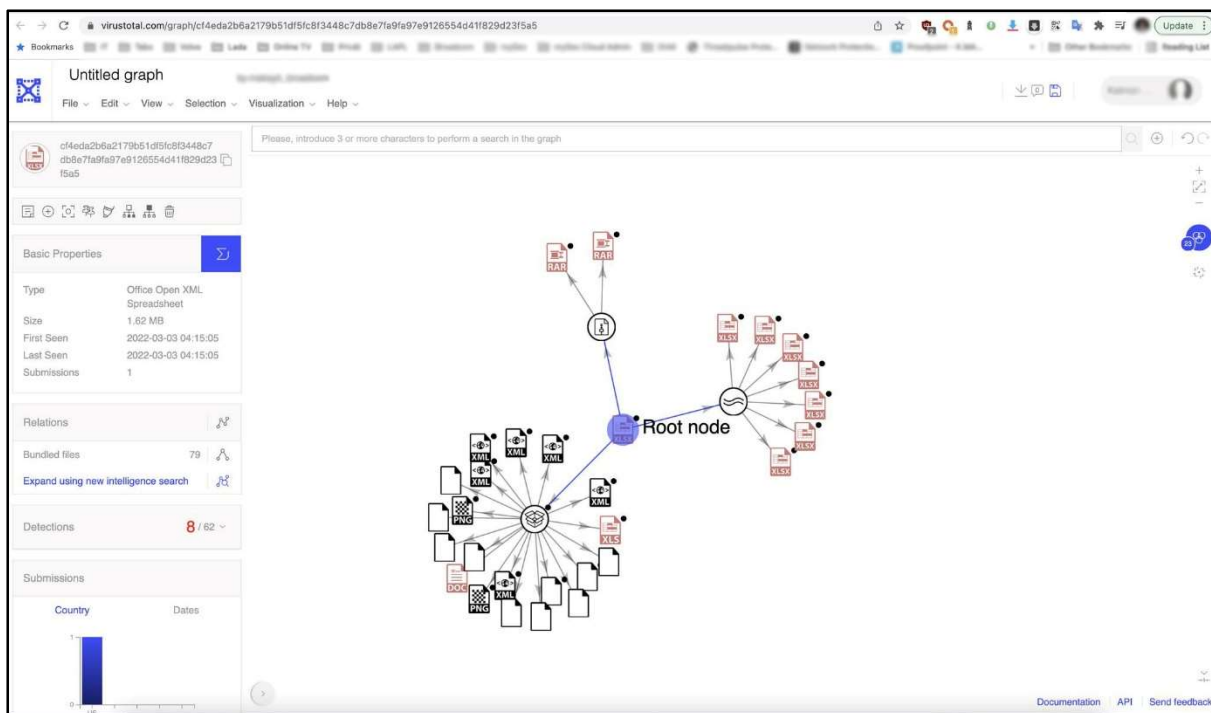
Amikor valamilyen általunk kevésbé bizalmasnak ítélt vagy teljesen ismeretlen forrásból kapunk egy csatolmánnyal kiegészített emailt, érdemes azt a szokásosnál nagyobb elővigyázatossággal kezelni. Kiemelten fontos, hogy ha a levélben található egy hivatkozás, egy link, akkor azt ne nyissuk meg azonnal, valamint legfőképpen a csatolmány ellenőrzését szükséges elvégezni. Ennek céljára használhatunk online szolgáltatásokat, mint például a VirusTotal³⁶. A VirusTotal ellenőrző mechanizmusa számos keresőmotorra és vírusirtó szoftverek integrált adatbázisaira támaszkodik. Amikor feltöltünk egy fájlt, akkor annak egyedi

³⁶ <https://www.virustotal.com/gui/home/upload>

azonosítóját veti össze a betáplált tartományok adataival, és annak fényében állapítja meg, hogy a vizsgált dokumentum tartalmaz-e valamilyen kártékony kódot, avagy megnyitása biztonságos. Fájlszkenner szolgáltatásokból sok található, célszerű az igényeinknek megfelelőt kiválasztani, ugyanis némelyik eltárolja az általunk feltöltött állományt az adatbázisok bővítése céljából. A VirusTotal is ezek közé tartozik, ebből adódóan Privacy megfontolásból nem a legmegfelelőbb. Nagyon fontos, hogy bizalmas és-vagy érzékeny adatokat (például céges dokumentációk, hozzáféréseket tartalmazó szöveges fájlok stb.) tartalmazó dokumentumokat, ne töltsünk fel vizsgálat céljából, ugyanis a prémium előfizetéssel rendelkező felhasználók – jellemzően vállalatok – számára kereshető az adatbázis, onnan szabadon letölthetnek és elemezhetnek tartalmakat. A SANS Institute vezető ICS-kezelője, Xavier Mertens 2022 márciusában végzett egy elemzést annak céljából, hogy felmérje, milyen mennyiségű hitelesítési adat lelhető fel a VirusTotal adatbázisában. Az eredmény a vizsgálat időpontjában 2 713 282 darab email cím és jelszó páros volt, melyből 2 163 756 darab volt egyedi.³⁷

Az alábbi példában egy az orosz-ukrán konfliktus körüli adatszivárogtatás során publikált orosz XML dokumentum elemzésének eredménye látható. Melynek következtében szemmel láthatóvá válik, hogy a fájlban egy olyan kártékony kód van beágyazva, mely megnyitáskor 7 darab orosz szerverrel veszi fel a kapcsolatot, a háttérben pedig elemző és adattovábbító tevékenységet folytat, természetesen észrevétlenül.

³⁷ <https://isc.sans.edu/forums/diary/Credentials+Leaks+on+VirusTotal/28426/>



7. ábra: Fáj hash vizsgálat eredménye (forrás: CyberThreat.Report Facebook csoport)

A 7. ábra forrásaként szolgáló CyberThreat.Report elnevezésű Facebook csoport 2022. február 27-én jött létre annak céljából, hogy a szakmai közösségformálás mellett naprakész betekintést nyújtson a kiberbiztonság és kibervédelem egyes szegmenseibe az aziránt érdeklődők számára. A szakértők által létrehozott csoport létszáma a létrehozásától számított 6 hetet követően már közel ezer főnél (dolgozatom írásának pillanatában 986 tag) jár. A közösség napi rendszerességgel készít összefoglalókat az aktuális kiber eseményekről, kül- és belpolitikáról, de gazdasági vonatkozású hírekről és geopolitikáról is. Tevékenységük lenyomatot képez a sajtóban is, több hírportál hivatkozott már cikkeik publikálásakor a csoportra, úgy, mint a 24.hu, a Telex és a Népszava.

6. Adatszivárgások ellenőrzése

Napi használatban lévő email címeink vonatkozásában javasolt időszerűen ellenőrzéseket lefuttatni annak céljából, hogy megbizonyosodjunk róla, érintett volt-e valamilyen adatsértésben vagy adatszivárgásban. Erre kiváló lehetőséget kínál a HaveIBeenPwned³⁸ elnevezésű szolgáltatás, amely több száz kiíratott és beillesztett adatbázist hoz egy tető alá és ez által több milliárd kiszivárgott fiókról tartalmazó információkat elemez. Találat esetén

³⁸ <https://haveibeenpwned.com/>

pontos képet kapunk arról, hogy mikor, milyen esemény következtében mely adataink szenvedtek el sérelmet.

7. Többfaktoros azonosítás

Az adatsértésekből és adatszivargásokból fakadó veszélyforrások mitigálása érdekében az egyik legjobb intézkedés, amit tehetünk az időszerű jelszóváltoztatás mellett, az a többfaktoros azonosítás alkalmazása. Mivel az ilyesféle események tőlünk és ráhatásunktól függetlenül időszerűen úgy is bekövetkeznek, érdemes további védelmi vonalakat felállítani, hogy ne eredményezzen kockázatot hozzáférési adataink kiszivargása. Többfaktoros azonosítás hiányában ugyan is egy támadó a tudtunk nélkül hozzáférhet például a levelezésünkhöz.

8. Meta és EXIF adatok

Minden digitális dokumentum és egyéb állomány tartalmaz úgynevezett metaadatokat, melyek értékes információmorzsák, amiket könnyen egy támadó kezébe szórhatunk, ha nem távolítjuk el azokat a közzétételt megelőzően. Ezek tipikusan olyan információk, mint a szerző neve, a keletkezés pontos időpontja, az eszköz típusa, a használt szoftver neve és annak verziószáma, de adott esetben GPS koordináták is eltárolásra kerülhetnek egy képfájlban. Nagyon sok példa adódott már arra, hogy kiberbűnözőket sikerült beazonosítani a gondatlanságuk okán, mivel az általuk megosztott fájlokban benne maradtak a metaadatok, így könnyű volt entitáshoz kötni az adott incidenst. Ami a digitális biztonságunkat és a magánszféránkat illeti, az alábbi példa akkor következhet be, ha okostelefonunkon a fényképező alkalmazásnak engedélyezett a helyadatokhoz való hozzáférés és a fénykép készítésekor be van kapcsolva a helymeghatározás funkció. Ez által automatikusan rögzítésre kerül a pontos GPS koordináta, ahol a kép készült. Vannak olyan közösségi média felületek, melyek fájlmegosztáskor alapértelmezetten törlik az érzékeny metaadatokat, de előfordulhat, hogy nem megfelelően megy végbe a folyamat. Továbbá az egyes, kizárólag képmegosztásra szolgáló weboldalak eredetben őrzik meg a feltöltött képfájlokat és annak minden tulajdonságát. Ha nem tesszük meg a szükséges óvintézkedéseket, könnyen az alábbi forgatókönyv áldozatai lehetünk, s csupán egy fénykép alapján meghatározható lesz a valószínűsíthető lakcímünk vagy adott esetben munkahelyünk egyik telephelye. Tovább menve a példán, képek esetében az OSINT elemzés sarkalatos pontja a háttér alapos vizsgálata. Gyakran ugyanis nem a középpontban elhelyezkedő objektum az informatív és nyomravezető, hanem ami körülötte megbújik – képernyőképek, jegyzetek, utcatáblák, egyes országok sajátos elektromos hálózati aljzat szabványai és forgalmi jelzőlámpái. Ezek az információ morzsák mind hozzásegíthetnek minket a szükséges

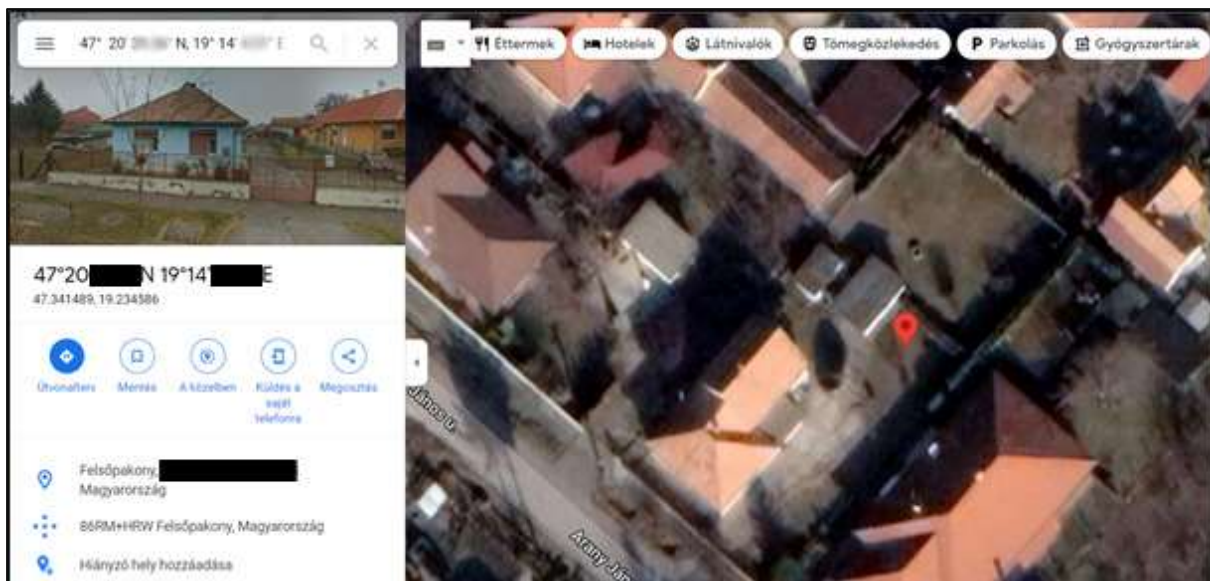
kontextuális igazolások megszerzéséhez. Természetesen ezt az elemzést is lehet manuálisan, vagyis szabad szemmel futtatni, de akár alkalmazhatunk egy megfelelően betanított mesterséges intelligencia alapú algoritmust is. Azonban legtöbb esetben a saját érzékszerveink és az analitikus gondolkodásmód a legjobb eszköz, mely rendelkezésünkre áll.



8. ábra: Ismeretlen személy portréja. (forrás: Google)

Create Date	: 2021:03:21 11:16:14.751965
Date/Time Original	: 2021:03:21 11:16:14.751965
Modify Date	: 2021:03:21 11:16:14.751965
Thumbnail Image	: (Binary data 35811 bytes, use -b option to extract)
GPS Altitude	: 0 m Above Sea Level
GPS Date/Time	: 2021:03:21 10:16:13Z
GPS Latitude	: 47 deg 20' 29.36" N
GPS Longitude	: 19 deg 14' 4.51" E
Circle Of Confusion	: 0.004 mm
Field Of View	: 69.4 deg
Focal Length	: 3.4 mm (35 mm equivalent: 26.0 mm)
GPS Position	: 47 deg 20' 29.36" N, 19 deg 14' 4.51" E
Hyperfocal Distance	: 1.45 m
Light Value	: 11.1

9. ábra: Metaadat elemzés eredménye. (saját képernyőmentés)



10. ábra: GPS koordináta alapján végzett keresés. (saját képernyőmentés, forrás: Google Maps)

A 9. ábrán látható metaadat elemzésre egy Exiftool nevű szoftvert alkalmaztam, amely a felhasználóbarát egyszerűségéből és sokoldalú alkalmazhatóságából kifolyólag nagy népszerűségnek örvend. Nem csak a fájlokban lévő adatok olvasásában nyújt segítséget, de igény szerint – például dezinformációs törekvések esetében – azok módosítására, megmásítására is szolgál, ezáltal egyfajta defenzív eszközként is alkalmazható.

A 10. ábrán látható, hogy a képfájlban lévő GPS koordináták alapján végzett keresést követően megállapítható az ingatlan pontos címe, ahol a fényképfelvétel készült. Az objektum feltételezhetően lehet a férfi magántulajdonú lakóhelye, vagy egy a Felsőpakonyi Községi Sportegyesület tulajdonában lévő ingatlan, mondjuk egy székhely. Valamint valószínűsíthető, hogy a férfinak van valamilyen kötődése a sportegyesülethez, például a labdarúgó csapat tagja. Ezen a ponton két lehetőségünk is kínálkozik a további információszerzésre. Az ingatlan esetében fordulhatunk a Földhivatalhoz, ugyanis az ingatlan nyilvántartás az ingatlan-nyilvántartásról szóló 1997. évi CXLI. törvényben meghatározottak szerint nyilvános, a tulajdoni lapok tartalma korlátozás nélkül megismerhető, azt bárki megtekintheti, arról feljegyzést készíthet, továbbá hiteles másolatot kérhet. Ehhez a település nevére és az ingatlan helyrajzi számára vagy az ingatlan közigazgatási címe van szükség. A tulajdoni lap tartalma alapján tudásunk lesz a tulajdonos bizonyos személyes adatairól (névéről, születési idejéről stb.), valamint megállapítható lesz az ingatlan hovatartozása. Azonban a procedura vitatott lehet az OSINT vonatkozásában, ugyanis nyilvánosan elérhető bárki számára az ingatlan nyilvántartás, mégis „prémium adatbázisnak” mondható, mivel igazgatási szolgáltatási díjat kell fizetni. Ez kiváló példája a korábban említett adatbázisok transzparenciájának teljes

hiányára. Másik scenárió amennyiben csak a személyre vagyunk kíváncsiak, úgy a sportegyesülettel összefüggő szálát kell vizsgálni. Labdarúgó sportolók tekintetében kézenfekvő lehetőséget kínál a Magyar Labdarúgó-szövetség adatbankja, amely nyilvánosan kereshető, és megismerhetünk belőle teljes nevet, születési adatokat, a pályafutás alatti tagsági előzményeket, valamint gyakran fénykép is szerepel a sportolói profilban. Ez által köthetőbb lesz a fellelt információ.

The image shows a sample of a Hungarian land ownership document (Tulajdoni lap - szemle) from 2000. The document is titled 'Tulajdoni lap - szemle' and includes the date '2000. 10. 25. 09:25:10'. It is issued by the 'FŐVÁROSI KERÜLETEK FÖLDHIVATALA' (Budapest, XI., Budafoki út 59. 1519 Pf. 415.). The document is divided into three main sections: I. RÉSZ (General information), II. RÉSZ (Rights and interests), and III. RÉSZ (Other rights and facts). The document is annotated with callouts explaining its parts:

- a tulajdoni lapot kibocsátó földhivatal**: FŐVÁROSI KERÜLETEK FÖLDHIVATALA, Budapest, XI., Budafoki út 59. 1519 Pf. 415.
- az ingatlan helye, fekvése, helyrajzszáma**: BUDAPEST XXII. KER. Belterület 23456/8/A/13
- az ingatlan postacíme**: 1223 BUDAPEST XXII. KER. Vadvirág utca 14. 2. emelet ajtó: 13
- széjegy: iktatószám, tartalom**: Széjegy: 23537/2000.10.05
- ingatlan megnevezése, számszerű adatai**: FŐVÁROSI ILLETÉKHIVATAL 1054 BUDAPEST V. KER. Bajcsy-Zsilinszky út 36-38. Jelszámjog törlés iránti kérelem
- tulajdonjogi adatok**: I. RÉSZ. 1. Az egyéb önálló ingatlan adatai: megnevezés, terület, eszék száma, eszmét bányád, építés/101, lakás, 51, 2, 0, 249/10000. Bejegyző határozat: 9892/1999/1999.01.18. 2. Bejegyző határozat: 740021/5/1997/1997.02.08. Társasház. Az önálló ingatlanhoz tartoznak az alapító okiratban meghatározott helyiségek.
- egyéb jogok és tények**: II. RÉSZ. 3. bányád: 1/1. Jogcím: vétel. bejegyző határozat: 10235/1999/1999.08.08. jogállás: tulajdonos. név: Gábor Áron. szül.: 1955.01.01. a. név: Kicsi Gábor. cím: 1223 BUDAPEST XXII. KER. Gábor út 252.
- aláírás, kiadó földhivatal pecsétje**: III. RÉSZ. 1. bejegyző határozat: 7690/1/1999/1999.12.01. jelszámjog: 312000 Ft. azaz háromszázötvenkettőezer Ft. tőketartozás és járulékaik erejéig. jogosult: név: FŐVÁROSI ILLETÉKHIVATAL. cím: 1054 BUDAPEST V. KER. Bajcsy-Zsilinszky út 36-38.

11. ábra: A tulajdoni lap részei és tartalma. (Forrás: foldhivatal.hu)

A 8. ábrán látható férfi egyenruháját tekintve röviden megemlíthető a példa katonai aspektusa is. Amennyiben egy szolgálati feladatát végrehajtó katona – legyen az hivatásos, szerződéses vagy valamilyen formában tartalékos – nem tartja be a rá vonatkozó előírásokat, az könnyen a műveleti biztonság aláadását eredményezheti. Ez kiváltképpen valamilyen különleges szolgálati igénybevétel alkalmával kaphat nagy hangsúlyt, így tehát egy missziós külszolgálat esetében. Tovább érzékenyíti a helyzetet, ha a fentebbi példa egy hivatali mobiltelefon használatával valósul meg, ugyanis a jelenleg hatályos a Magyar Honvédség Szolgálati Szabályzatának kiadásáról szóló 24/2005. (VI. 30.) HM rendelet erről külön rendelkezik az alábbiak szerint:

„226.2. A katonák a szolgálatteljesítési helyen honvédségi tulajdonú elektronikus eszközzel magán küldeményt (szöveget, beszélgetést, üzenetet, rajzot, képet stb.) csak a katonai szervezet parancsnokának külön engedélye alapján készíthetnek (állíthatnak elő), illetve továbbíthatnak.”

9. Magánszemélyek illetve kis- és középvállalatok esete

Az eddigiekben főképp az OSINT felhasználási lehetőségei kerültek említésre, azonban fényt kell deríteni az érme másik oldalára is, ahol veszélyforrásként jelentkezhet mindez. Amennyiben nem ügyelünk digitális lábnyomunk szerénységre, s elkövetünk olyan hibákat, mint az Oversharing, kifejezetten nagy veszélynek lehetünk kitéve. Ezen a ponton jegyzendő meg a már jól ismert mondás, miszerint „Az internet nem felejt”, tehát ami egyszer kikerül a nyilvános internetre, az jó eséllyel tovább él majd valamilyen módon, valamilyen formában. Ahogyan fentebb említettem, a magánszemélyek és a munkahelyek, szervezetek esete és az egyes kibertámadási alakzatok hálózatszerűen összefüggnek, erre kiváló példa a Cyber Torture, vagyis az internetes zaklatás és zsarolás valamennyi formáját felölelő fogalom. Ezt a következő hipotetikus, ám valóságallappal rendelkező esetpéldán keresztül szemléltetném, valamint utalnék vissza, s kötném össze a gondolatokat a PV-OSINT körül. A kibertámadások előkészítésekor a támadók az utolsó részletekig menő alaposággal térképezik fel a célpontot – a példa esetében egy vállalatot – belefoglalva a befolyásos, jellemzően C-Level (például ügyvezető igazgató) beosztásokban dolgozó munkavállalókat is. OSINT folyamatok mentén könnyedén meg lehet határozni egy adott személy szokásait, szabadidős tevékenységeit, érdeklődési köreit és személyes adatait is. Az ez alapján elkészített profil például nagyban megkönnyíti a Phishing és Social engineering támadások kivitelezését is. Vegyük tehát a következőt. Ha egy házasságban élő munkavállalóval kapcsolatban kiderül, hogy magán vagy vállalati email címén egy társskereső oldal vagy egyéb felnőtt szolgáltatásokat kínáló platformról származó adatsértési találat van, úgy a befolyással rendelkező beosztású személy zsarolhatóvá válik mind munkája, mind magánélete tekintetében. A kiberbűnözők gyakran vesznek célba hasonló módszerekkel szakmai személyzetet – főképp informatikával dolgozókat – annak érdekében, hogy közreműködjenek például biztonsági mechanizmusok deaktiválásában, vagy hozzáférések rendelkezésre bocsátásában. Az ilyen és ehhez hasonló forgatókönyvek elkerülése végett hivatott a CTI beépíteni mindennapi munkavégzésébe az adatsértésekből és adatszivárgásokból származó információkból álló adatbázisok elemzését. Ezáltal iránymutatást is tud nyújtani az érintett vállalatok részére, melyet aztán biztonság tudatosító kampányok keretein belül továbbadhatnak munkavállalóik irányába.

Fontos megvizsgálni azt a kérdéskört, miszerint vannak-e falak az OSINT folyamatokat illetően, milyen akadályokba ütközhet egy támadó az információgyűjtés során, ha van egyáltalán ilyen. A szakmában dolgozó szakértők véleménye az adott kérdéstről eltérő. Egyesek szerint nem léteznek határok a rendelkezésre álló bizonytató méretet képviselő információhalmaz okán,

mindenről alkotható érdemleges tudás, amennyiben rendelkezünk a megfelelő forrásokkal, intellektussal, képességgel és kreativitással. E gondolat életszerűségét kiválóan szemléltetik napjaink eseményei az orosz-ukrán konfliktus körül, ugyanis az egyes csapatmozgások nyomon követhetősége példátlan mértéket ütött meg, hála többek közt a közösségi médiának, a műholdkép szolgáltatóknak és a nyilvánosan hozzáférhető webkameráknak. Azonban mások szerint egy vállalat vonatkozásában meghatározhatók bizonyos falak, és lehetséges két kategóriába osztani a róla fellelhető információkat. Ennek értelmében beszélhetünk permanens, vagyis állandó jellegű adathalmazról, melynek hozzáférhetőségét nem lehet biztonsági intézkedésekkel korlátozni, így például a cégnyilvántartásban bejegyzett adatok. A GDPR bevezetését követően ez a kör ugyan szűkült, mivel a domain nevekhez köthetően már nem fedhetők fel a Whois, vagyis a tulajdonosi adatok. Így több időráfordítást igényel a megkerülés. A másik csoportba sorolhatók a mitigálható, vagyis az enyhíthető kockázatokat jelentő találatok, mint például az adatszivárgási rekordok. Ezek vonatkozásában, ha megteesszük a szükséges védelmi célzatú intézkedéseket, csökkenthetjük a fenyegetettséget.

Összegzett következtetés

Bármilyen vonatkozásban leszögezhetjük, hogy a biztonság relatív. Mihez képest vagyunk, illetve nem vagyunk biztonságban. Továbbá, sosincs száz százalékos védelem. Azonban bizonyos mértékig lehetséges védekezni az OSINT-tal szemben, de nem kizárólag elegendő az, hogy minimalizáljuk a digitális lábnyomunkat. A teljesség igényével célszerű kombinálni azt a dezinformációval, vagyis a zajkeltés taktikájával. Ennek értelmében harmadik hipotézisem, miszerint a digitális lábnyom szándékos és tudatos minimalizálásával kivédhető, hogy kizárólag nyílt forrásokból egy támadás kivitelezéséhez elegendő információt gyűjtsenek össze rólunk, megdől. Az összehangolt védekezés szigorú életmódbeli elhatározást követel meg, és hajlandónak kell viselni annak sajátosságait és következményeit. Jelentős mértékű lemondással jár, és ebből eredően megnehezítheti a mindennapi életünket, ezért a procedura nem való mindenkinek. Azonban nem lehet tudni, hogy mikor válunk érdekszférává, mikor kerülünk egy támadó látókörébe, és mi által. Sokszor igen nehéz megmondani első körben azt is, hogy egy támadásnak ki vagy mi a valódi célpontja, mondjuk a fentebb említett adathalászatból sakk-matt esetében. Éppen ezért is célszerű egyfajta preaktív online magatartásként minden esetben elővigyázatosan eljárni, és szélnek eresztetni azt a percepciót, miszerint „Én ugyan miért lehetnék áldozat?”. Magánéletünket éljük meg befelé irányulóan és kezeljük zártan. Legtöbb esetben elegendő csupán visszajára fordítani a dolgot, mielőtt cselekszünk. Ha egy ismeretlen a játszóterén kérne tőlünk egy képet gyermekünkéről, adnánk neki? Vagy ha megkérdezné valaki

az utcán, mikor és hol születtünk, esetleg hogy hol, milyen beosztásban dolgozunk, elmondanánk neki? Amennyiben a válasz egy határozott nem, akkor miért tesszük meg ugyan ezt a közösségi médiában?

IV. Eredmények

T1: Elmondható, hogy tetten érhető a határok közötti átjárhatóság, és ez által felfedhető az összemosódás. Tekintve, hogy a CTI egy meglehetősen sajátos alkalmazási területe az OSINT-nak, a benne megjelenő megelőző védelmi célzat, az abból levezetett minimális társadalomra való veszélyesség, a naprakész információszolgáltatás fontossága és a támadókkal megegyező gondolkodásmód és eszköztár használata, valamint az ügyféllel ápoltság bizalmi kapcsolat kereteit adják a túlmutatásnak. Azonban legnagyobb hangsúllyal elsősorban az etikátlanság irányába toldódnak a vektorok. Értem ezalatt azt, hogy azon források kimerítése, mely szükségessé válik a CTI munka során, egyéb OSINT alkalmazási területen indokolatlan volna, és erkölcsi aggályokat vetne fel. Amikor viszont egy megrendelő kíváncsi arra, hogy egy kártékony szándékú támadó meddig képes eljutni a róla és szervezetéről képződött információs halmazban, hogy előkészítsen egy támadást, nem léteznek ezek az etikai határvonalak. Mint említettem korábban, egy támadó nem fog megállni sem törvényi sem erkölcsi küszöbök előtt, ezért a legteljesebb veszélyforrás felderítés érdekében bizonyos mértékben hasonlóképp kell eljárnia a vizsgálatot végző elemzőnek. A másik irány, amerre kis mértékben ugyan, de mozoghat az elemző, az a hackelés egyes vetületei. Ki kell emelni, hogy mivel egy nyílt forrásból történő kiberbiztonsági átvilágítás vagy digitális kitettségvizsgálat a források nyíltsága révén nem igényel különleges engedélyt, ezért nem végezhetők beható jellegű, vertikális tesztelések. Kivételre azonban mindig adódhat lehetőség. Az első fejezetben említettekre utalnék vissza, a monopolhelyzetben lévő, valamilyen közműszolgáltatást végző kritikus infrastruktúrára, ugyanis tekintve az ügyfél szektorális elhelyezkedését, ebben az esetben nagyobb jelentősége lehet az azonnaliságnak. Ha az elemző a létfontosságú rendszerelem informatikai infrastruktúráját illetően bármely ponton olyan ráutaló körülményt talál, miszerint gyári alapbeállítású hozzáférések lehetnek használatban – melyek első körös nyílt forrásokból is felfedhetők – vagy valamilyen fejlesztési vagy tesztkörnyezet forráskódjában maradt feltüntetve hozzáférés, például egy kommentben, két dolgot tehet. Jelzi az észlelést a munkáról készült jelentésben, melyet annak végeztével átad az ügyfélnek, aki validálja majd a veszély tényét. Azonban ha a veszély valós, amit ezen a ponton még nem tudunk, az időtényező kritikus, mivel az átfutási idő alatt bárki más ugyan úgy rátalálhat a hibára és kihasználhatja azt. Mivel egy ilyen incidens nem kizárólag az ügyfél szervezetet érintené, hanem esetlegesen már állampolgárokat is, éppen ezért indokolt lehet az egyszeri manuális hozzáférés szerzés próbája az adott adatokkal. Negatív végkimenetel esetén meghatározott

ütemben folytatódik a munka, azonban sikeres autentikációt követően azonnal értesíteni kell az ügyfelet, és felszólítani a hiba elhárítására.

Ennek értelmében H1 hipotézisemet igazoltam.

T2: A vizsgált két technika nem vethető össze a természetük, az általuk nyújtott eszköztár és eltérő célokat való kiszolgálás révén. Ahogy azt a második fejezetben említtem, amíg az adathalászat egy emberközpontú tevékenység, amely aktív, tevőleges cselekvést igényel ügyféloldalról, addig az OSINT elsősorban passzív folyamatok összessége, mely csupán közvetetten követel meg aktivitást – vagyis az online térben való létezést, tartalom közzétételt – ami valamennyiben elkerülhetetlen. Ezért, ebből kifolyólag eltérő a két technika célpontválasztása. Az adathalászat az emberi tényező támadását illetően biztosít nagyobb megbízhatóságot, amíg az informatikai infrastruktúrák ellen intézett támadások előkészítését az OSINT szolgálja ki nagyobb mértékben. Így tehát, kettébontva a hipotézist, azt igaz-igaznak lehet könyvelni, mivel mindkét módozat ugyan olyan hatékonysággal képes működni, azonban a megbízhatóságuk terén mindkét esetben merülhetnek fel nehézségek. Az OSINT esetében például a dezinformáció kapcsán, az adathalászat tekintetében pedig a „try-error” vagyis a próba szerencse jelleg.

Eszerint H2 hipotézisem megdőlt.

T3: Nem feltétlen, nem minden esetben elegendő kizárólag a digitális lábnyom csökkentése annak érdekében, hogy ne gyűjthessenek össze rólunk egy támadás kivitelezéséhez szükséges mennyiségű információt. Értem mindezt magánszemélyek, valamint kis- és középvállalatok esetében egyaránt. Ez a kijelentés természetesen magában hordozza azon esetek létét is, melyekben célravezető és elégséges lehet csupán e-képp védekezni, ezért ebből az aspektusból igaznak bizonyulhat a hipotézis. Azonban a megfelelő eljárás megválasztása nagyban függ az igénybe vevő személyétől, cég vagy vállalat esetében pedig szektoriális elhelyezkedésétől, illetve tevékenységi köreitől. Ezek függvényében számottevő eltérések rajzolhatók ki. Egy átlagos internetfelhasználót tekintve – akit nem kötnek sajátos munkaköri elvárások, például sales beosztásban kötelező közösségi média profil fenntartása vagy egyéb digitális jelenlétet növelő tevékenységek, mondjuk egy szakmai aláíróval illetőleg, akinek valamennyi személyes adata nagy eséllyel fog szerepelni nyilvános szerződésekben – nem szükséges nagy volumenű dezinformációs kampányba bocsátkozni, esetében valószínűsíthetően megfelelő a lábnyomcsökkentés önmagában. Ezzel ellentétben, ha egy közszereplőt, vagy egy nagy

gazdasági, politikai befolyással rendelkező személyt veszünk alapul, vonatkozásában nem lesz elegendő az internetről való önkéntes távolmaradás. Ezesetben a magánszféra védelme érdekében fel kell venni a harcot például az oknyomozó újságírói réteggel és a nyomtatott sajtóval is. A kis- és középvállalatokra ugyanezen minta alkalmazható.

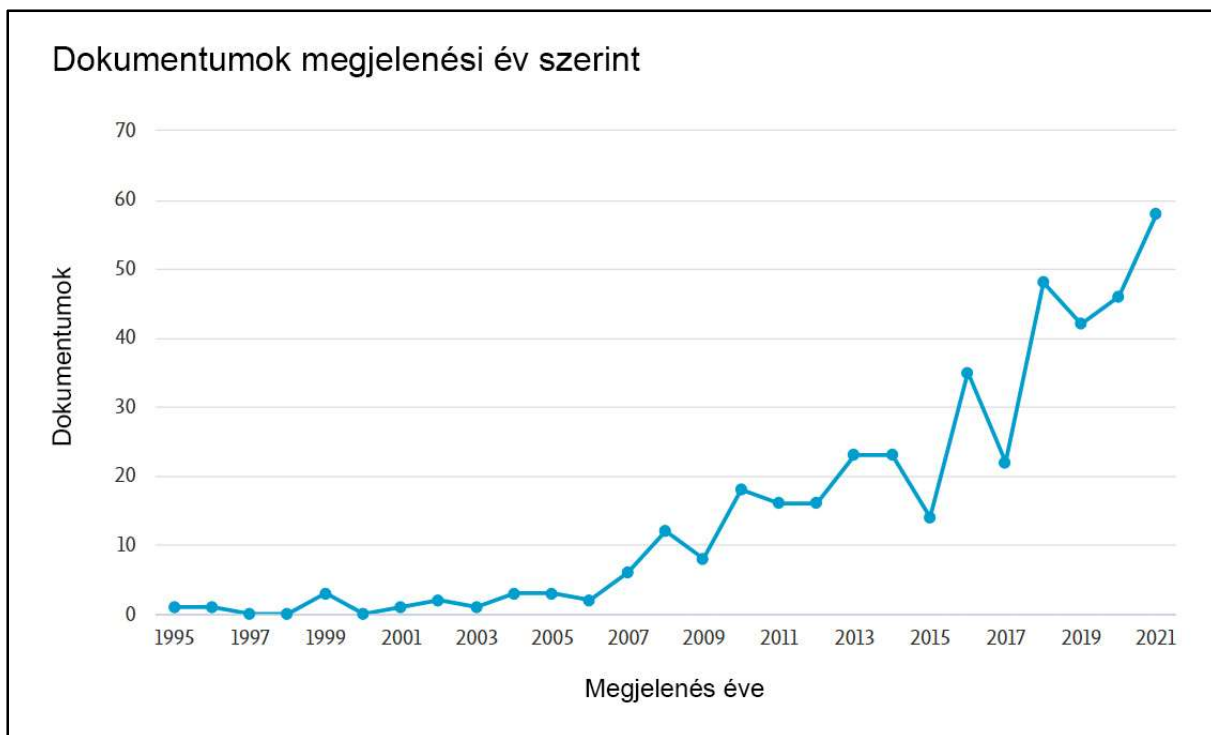
H3 hipotézisemet részben megdőltnek tekintem.

1. Trendelemzés

Kutatásom során trendelemzést végeztem az Elsevier gondozásában lévő Scopus és SciVal adatbázisában - amelyek a tudományos közlemények legnagyobb adatbázisai, ahol nem csak az ott indexált közlemények, hanem azok metaadatai is kereshetők³⁹ – fellelhető, „Open Source Intelligence” és „Cyber Threat Intelligence” kulcsszavakkal citált tudományos tartalmak vonatkozásában, hogy megállapítsam, milyen irányú változás figyelhető meg a témában íródott publikációkat illetően, illetve hogyan alakult a publikálások mennyisége az évek során. 2017-ben 69 millió rekordot, ezekhez mintegy 70 ezer hozzárendelt intézményt és 12 millió személyes szerzői profilt tartalmazott a Scopus. Az adatbázisban több mint 5000 kiadó által gondozott közlemény lett indexálva, melyek közt 24 ezer folyóirat és 150 ezer könyv volt bejegyezve. Az adatbázisban kezelt rekordok száma évente folyamatosan növekszik.⁴⁰ A két vizsgált kifejezést az adatbázisokból való lekérdezéskor idézőjelek között adtam meg annak érdekében, hogy a keresőmotor megfelelően értelmezze a szavak közötti kapcsolatot. Az OSINT esetében a Scopus adatbázisa 417, míg a Cyber Threat Intelligence esetében 465 találatot adott vissza. Mindkét esetben tudományometriát is vizsgáltam, amely egy adott entitás termékenységet adja meg, vagyis hány publikációt indexelt ez az entitás a Scopus adatbázisában. Az OSINT esetében ez az érték a vizsgálatom pillanatában 266, a CTI tekintetében pedig 435. A keresett tudományos dokumentumokat az utolsó befejezett évig, vagyis 2021-ig bezárólag elemeztem tudományterületi megoszlásuk és évenkénti megjelenési darabszámuk szerint. Elemeztem továbbá az adott témákhoz kapcsolódó 50 leggyakoribb kulcsszót is. Az eredményeket az alábbi 6 ábrán keresztül szemléltetem.

³⁹ Bányász Péter, Bóta Bettina, és Zágon Csaba, „A social engineering jelentette veszélyek napjainkban”, in *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében*, szerk. Zsámbokiné Ficskovszky Ágnes (Magyar Rendészettudományi Társaság Vám-és Pénzügyőri Tagozata, 2019), 12–37, <https://doi.org/10.37372/mrtvpt.2019.1.1>.

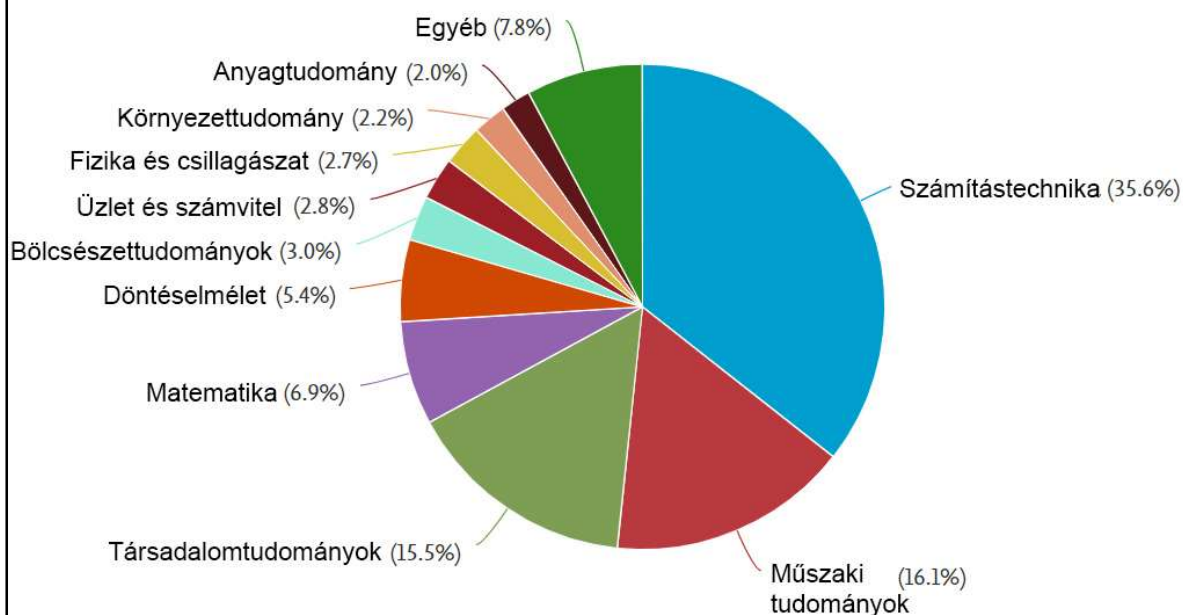
⁴⁰ URBANOVICS Anna - SASVÁRI Péter: A tudományos kutatás elixírje. Working Paper, 2019. július, DOI: 10.13140/RG.2.2.26344.83204



12. ábra: Az „Open Source Intelligence” keresőkifejezés megjelenése a nemzetközi tudományos publikációkban 1995-2021 között (Saját szerkesztés, forrás: Scopus)

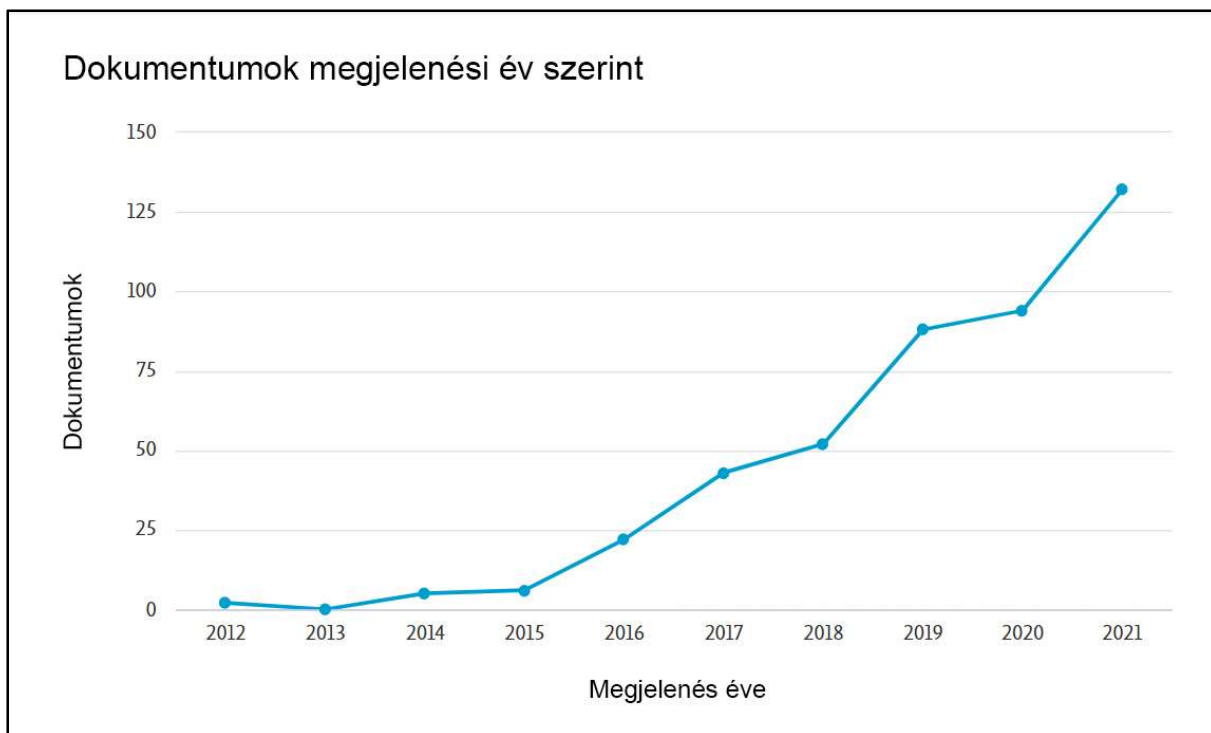
Az ábráról tisztán leolvasható, hogy az Open Source Intelligence kifejezés először 1995-ben jelent meg Scopus által indexált nemzetközi szakirodalomban. Elmondható, hogy 1999-ben egy apró kiugrást követően közel 2006-ig stagnált a téma népszerűsége és ez által a kiadott tudományos tartalmak mennyisége évenkénti lebontásban nem érte el a 10 darabot sem. 2015 és 2018 között azonban hullámzó teljesítményt láthatunk, megközelítőleg 10 és 50 közötti darabszámmal, 2021-ben született irományok száma viszont már majdnem túllépte a 60 darabot. Ebből egyértelműen megállapítható az OSINT, mint tudományos szakterület népszerűségének robbanásszerű növekedése.

Dokumentumok tudományterület szerinti megoszlása



13. ábra: Az "Open Source Intelligence" keresőkifejezés megoszlása tudományterületenként (Saját szerkesztés, forrás: Scopus)

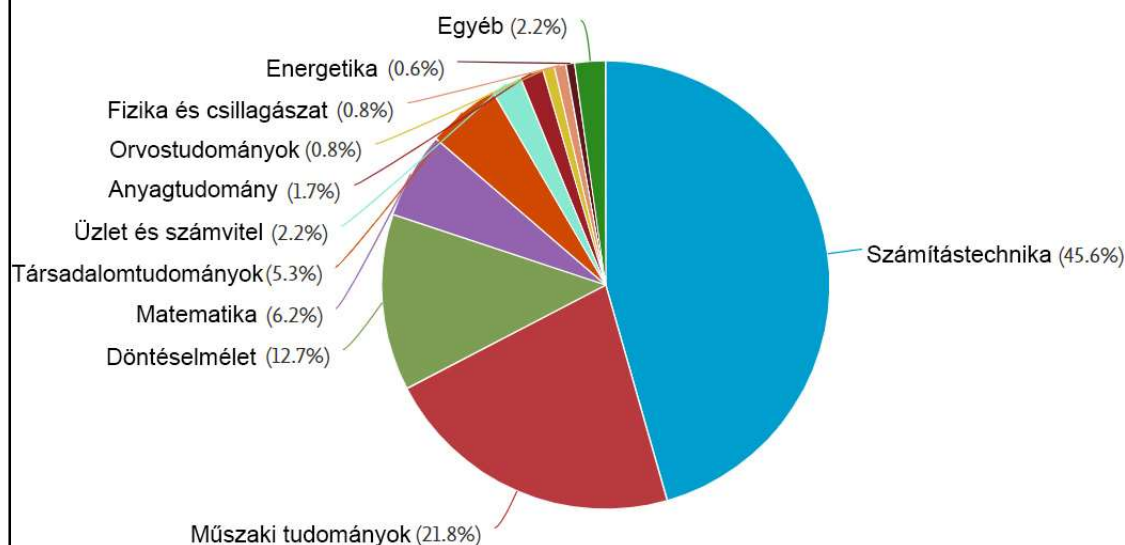
A tudományterületi megoszlást tekintve elmondható, hogy az OSINT-ot illetően a Számítástechnika képezi a súlypontot. Az eredmény azért meglepő, mivel a nyílt forrású hírszerzés az informatikától különállóan is sokrétű alkalmazásban részesül. Azonban a technológia fejlődésével olybá tűnik, hogy az információgyűjtés is dominánsan áttér a digitális területekre. Az ábra alapján szorosan egymást követik második valamint harmadik helyen a műszaki és a társadalomtudományok. Dolgozatom kontextusában azt a következtetést tudom levonni, hogy az egyes hírszerzési tartományok és források révén alakulhattak így az eredmények. A műszaki tudományokon belül helyet kaphat az általam vizsgált másik fogalmam, a Cyber Threat Intelligence, melynek közismerten az egyik legjobb eszköze az OSINT. A társadalomtudományok pedig az emberi kapcsolatokon alapuló hírszerzéssel való összefonódás kapcsán kerülhet képbe. Ami a többi szemléltetett területet illeti, úgy gondolom, hogy arányaiban igen kevés tudományos közlemény születik az OSINT meglehetősen széleskörű alkalmazási lehetőségeihez képest.



15. ábra: A „Cyber Threat Intelligence” kereső kifejezés megjelenése a nemzetközi tudományos publikációkban 2012-2021 között (Saját szerkesztés, forrás: Scopus)

Mivel a Cyber Threat Intelligence még napjainkban is egy meglehetősen újnak és fiatalnak vélt szakterület, így nem meglepő, hogy az ábra szerint a nemzetközi tudományos szakirodalomban először 2012-ben jelent meg a fogalom a Scopus adatbázisa szerint. 2015-től kezdődően egy meredek, visszaesés nélküli emelkedés figyelhető meg a témában évenként íródott irodalmak tekintetében, ami 2021-re meghaladta a 125 darabot.

Dokumentumok tudományterület szerinti megoszlása



16. ábra: A "Cyber Threat Intelligence" keresőkifejezés megoszlása tudományterületenként (Saját szerkesztés, forrás: Scopus)

Ami a CTI témában íródott publikációk tudományterületi megoszlását illeti, talán nem meglepő, hogy az első két helyen a számítástechnika és a műszaki tudományok állnak. A CTI, vagyis a kiberfenyegetettségekkel kapcsolatos hírszerzés, mint műszaki szakterület nagyobb gyakorisággal meg sem jelenhetne máshol a számítástechnikán kívül. Harmadik helyen, nagyon ésszerűen a döntéelmélet áll, mivel, minden hírszerzési forma a döntéselőkészítést, döntéshozatalt hivatott támogatni, ugyan így a CTI is.

hogy megbízhatóan támaszkodjunk rá. Továbbá magyar nyelven sajnos továbbra is jelentősen kevés releváns irodalom lelhető fel, ezáltal az egyes szakkifejezéseknek sincs még magyar nyelvű megfelelője. Az elemzéshez a Scikit-learn (közismeretebben sklearn) elnevezésű szoftveres gépi tanulási Python programozási könyvtárat alkalmaztam, amely többek közt különféle osztályozási, regressziós és klaszterező algoritmusokat tartalmaz. Jelen esetben a k-means klaszterezési algoritmust használtam. A kód lefuttatását a webalapú interaktív számítástechnikai platformként szolgáló Jupyter Notebook⁴¹-ban végeztem, amely alapvetően a nevéből adódóan a Julia, a Python és az R programozási nyelvek kezelésére hivatott, azonban mára nyelvek széleskörű spektrumát kínálja.

Az interjúalanyaim kérésére, valamint figyelembe véve az Észak-atlanti Szerződés Szervezete (NATO) által publikált OSINT Handbook-ban foglaltakat, mely szerint egy szak- vagy versenydolgozat is képezheti kiváló forrási tartományát a nyílt forrású információszerzésnek, az eredmények prezentálásakor élek a forrás anonimitásának lehetőségével. Ezért a lefolytatott interjúsorozat résztvevőit kizárólag beosztásuknál fogva nevezem meg. A kutatásom során összesen 8 személlyel folytattam le interjút, munkakörüknek fogva az alábbiakkal:

- 3 fő OSINT elemző
- 2 fő Etikus hacker
- 1 fő Ügyvezető igazgató
- 1 fő Hírszerzési üzletágvezető
- 1 fő GDPR szakjogász

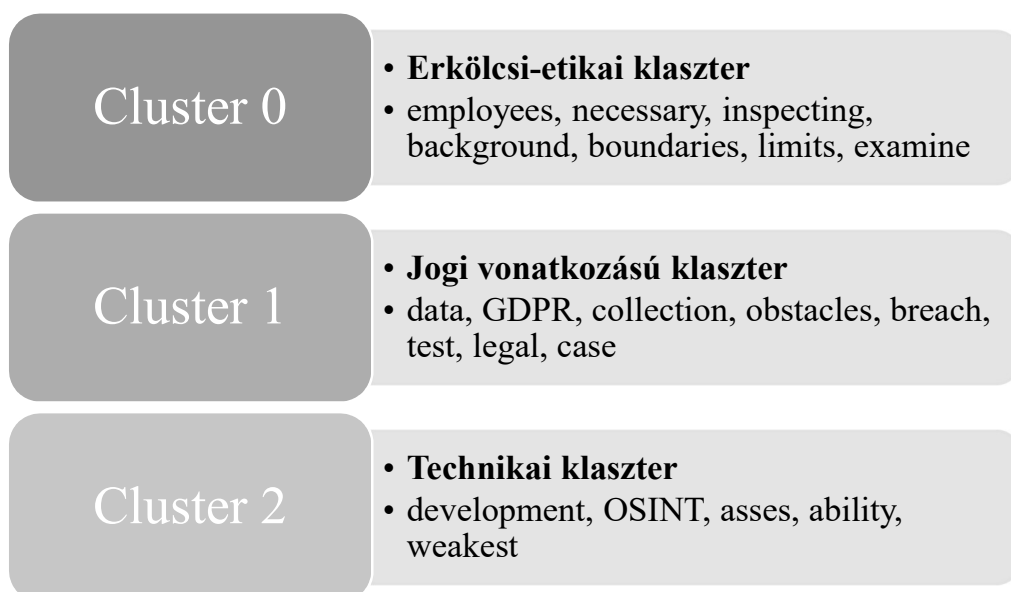
A három hipotézisemhez tartozóan összesen 35 kérdést fogalmaztam meg, melyeket egy kérdőívben foglaltam össze. Tekintve, hogy az interjúkban eltérő munkakörű és szaktudású személyek vettek részt, természetesen nem mindenki tudott minden kérdésre releváns válasszal szolgálni. Ez által a folyamat végére 151 válasszal rendelkeztem, melyekből a kérdésekkel együttesen elvégeztem a klaszterelemzést. Az interjúkérdéssorban részcélként szerepelt továbbá egy személyes kérdésblokk is, annak céljából, hogy alanyaimat közelebbről is megismerjem a témám kontextusában. Azonban magánszférájuk tiszteletben tartása és védelme érdekében ennek eredménye nem kerül ismertetésre dolgozatomban.

⁴¹ <https://jupyter.org/>

```
print('Cluster 0: ')
for ind in order_centroids[i, :10]:
    print(' %s' % terms[ind]),
print

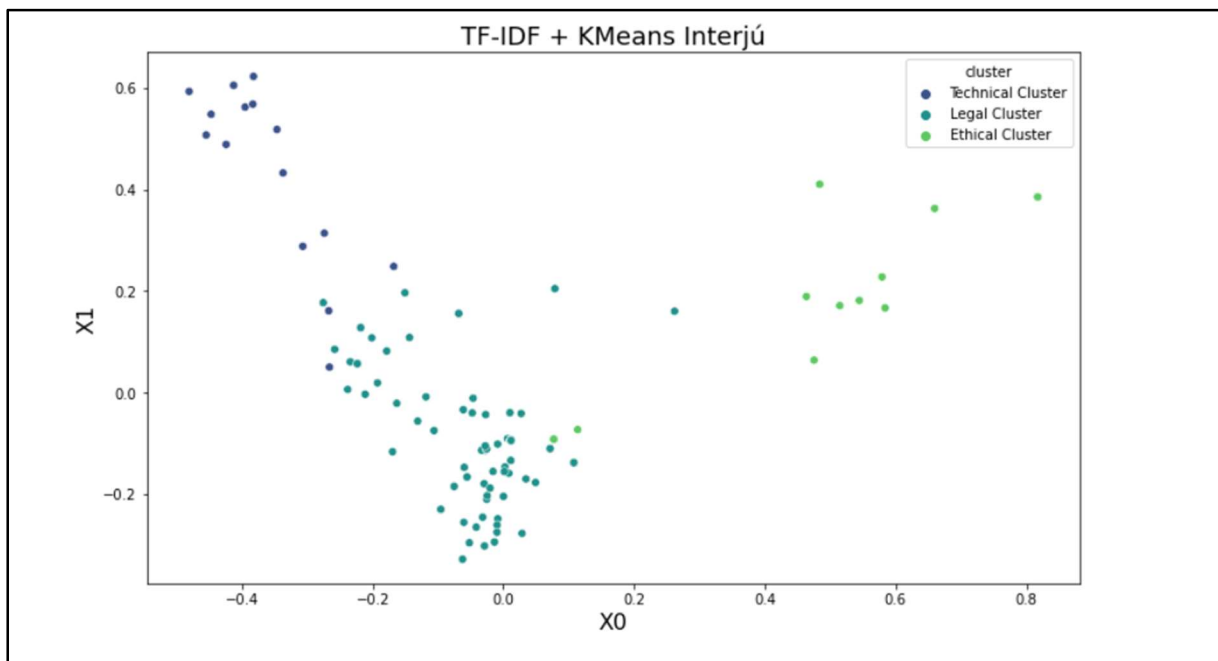
Cluster 0:
employees
cti
necessary
specific
inspecting
background
boundaries
longer
limits
examine
Cluster 1:
data
gdpr
information
collection
obstacles
breach
case
test
legal
efficient
Cluster 2:
organization
10
suggestions
development
osint
assess
ability
best
scale
weakest
```

18. ábra: A klaszterelemzési algoritmus eredménye (Saját képernyőmentés, forrás: Jupyter-Notebook)



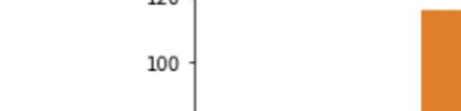
19. ábra: Az eredményként kapott három klaszter (Saját szerkesztés)

A 18. ábrán látható és a 19. ábrán szemléltetett eredmények igazolják, hogy az interjúkérdések, valamint azokra befolyó válaszok kiadják az általam előzetesen felvázolt 3 csoportot, az Erkölcsi-etikai (Cluster 0), a Jogi vonatkozású (Cluster 1), és a Technikai klasztert (Cluster 2). A hozzájuk tartozó kulcsszavakat vizsgálva elmondható, hogy talán a Technikai klaszter bizonyul első ránézésre kevésbé kifejezettnak, azonban mind a három csoportban találhatók technikai-műszaki vonatkozású vagy olyan aspektussal rendelkező kifejezések (CTI, data, breach, test, development, OSINT, asses, és weakest), tehát mindkét másik klaszter irányába szignifikáns kapcsolat állapítható meg.



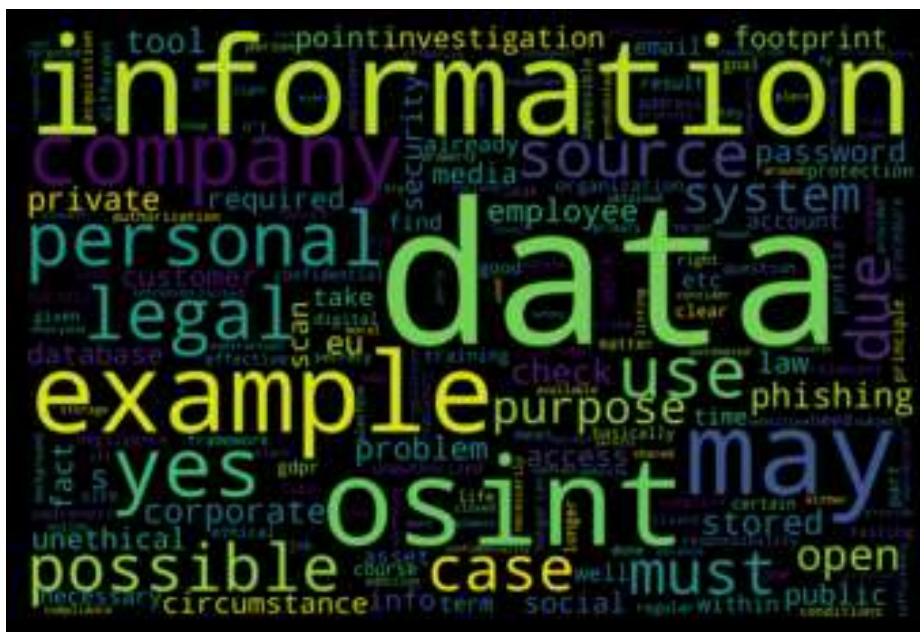
20. ábra: Klaszterek vizualizációja a centroid értékek alapján. Saját képernyőmentés, forrás: Jupyter-Notebook)

A 20. ábrán látható vizualizáció is alátámasztja a klaszterek közötti kapcsolatot. Az ábra az egyes klaszterekben található kulcsszavak középponttól számított elhelyezkedését mutatja a centroid értékek alapján. Jól megfigyelhető, hogy leszámítva néhány a jogi klaszterbe tartozó elemet, az illusztráció alján egy szorosan kapcsolódó csoport formálódik. A használt klaszterezési algoritmus a megadott szövegből alapértelmezetten klaszterenként 147 kulcsszót emel ki, ami alapján végzi a csoportosítást, azonban kevesebb „találat” esetén is sikeresen jár el. A 21. ábrán látható, hogy milyen mennyiségű adat (kulcsszavak) került rendezéskor az egyes klaszterekbe. A legnagyobb mennyiség, 100 és 120 közötti kulcsszóval a jogi vonatkozású klaszterben található, ami kiválóan szemlélteti a szakterületen vizsgált kérdésköröm jogi dependenciáit. Közel holtversenyben másodikként az erkölcsi klaszter szerepel. Utolsó helyen



Cluster	Count
Technical Cluster	16
Legal Cluster	116
Ethical Cluster	19

A látványosabb vizualizáció érdekében a wordcloud könyvtár alkalmazásával készítettem egy szófelhőt is, amit az egyes klasztereket képző kulcsszavak alkotnak. Ellenkezőleg a fentebb szemléltetett szófelhőkkel, jelen esetben nincs összefüggés az adott szó mérete és annak előfordulásának gyakorisága között, a folyamat teljesen véletlenszerűsített.



58

Felhasznált irodalom

1. 2012. évi C. törvény a Büntető Törvénykönyvről
2. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
3. 1997. évi CXLI. törvény az ingatlan-nyilvántartásról
4. 24/2005. (VI. 30.) HM rendelet a Magyar Honvédség Szolgálati Szabályzatának kiadásáról
5. „A közösségi média lehetőségei és kihívásai a védelmi szférában (MTMT)”. Elérés 2022. február 20. <https://m2.mtmt.hu/gui2/?mode=browse¶ms=publication;30682216>.
6. „A közösségi média, mint az információs hadszíntér speciális tartománya (MTMT)”. Elérés 2022. február 20. <https://m2.mtmt.hu/gui2/?mode=browse¶ms=publication;3303471>.
7. „Kiberbiztonsági incidensek a magyar közigazgatásban (MTMT)”. Elérés 2022. február 20. <https://m2.mtmt.hu/gui2/?mode=browse¶ms=publication;30867893>.
8. „Kiberbűnözés és közösségi média (MTMT)”. Elérés 2022. február 20. <https://m2.mtmt.hu/gui2/?mode=browse¶ms=publication;3313154>.
9. „Top 200 Most Common Password List 2021”. Elérés 2022. február 20. <https://nordpass.com/most-common-passwords-list/>.
10. Azevedo, R., I. Medeiros, and A. Bessani. „PURE: Generating quality threat intelligence by clustering and correlating OSINT”. In *Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019*, 483–90. Institute of Electrical and Electronics Engineers Inc., 2019. <https://doi.org/10.1109/TrustCom/BigDataSE.2019.00071>.
11. Bányász Péter, Bóta Bettina, és Zágon Csaba. „A social engineering jelentette veszélyek napjainkban”. In *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében*, szerkesztette Zsámbokiné Ficskovszky Ágnes, 12–37. Magyar Rendészettudományi Társaság Vám-és Pénzügyőri Tagozata, 2019. <https://doi.org/10.37372/mrttvpt.2019.1.1>.
12. Cartagena, A., G. Rimmer, T. Van Dalsen, L. Watkins, W.H. Robinson, and A. Rubin. „Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework for Critical Infrastructure Owners”. In *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, szerkesztette

- Paul R. Chakrabarti S., 494–99. Institute of Electrical and Electronics Engineers Inc., 2020. <https://doi.org/10.1109/CCWC47524.2020.9031172>.
13. Casanovas, P., J. Arraiza, F. Melero, J. González-Conejero, G. Molcho, and M. Cuadros. „Fighting Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project”. Szerkesztette Hoekstra R. *Frontiers in Artificial Intelligence and Applications* 271 (2014): 189–98. <https://doi.org/10.3233/978-1-61499-468-8-189>.
 14. Cha, J., S.K. Singh, Y. Pan, and J.H. Park. „Blockchain-based cyber threat intelligence system architecture for sustainable computing”. *Sustainability (Switzerland)* 12, sz. 16 (2020). <https://doi.org/10.32890/JICT2018.17.3.8260>.
 15. Chen, J., L. Zhang, X. Luo, and C. Hu. „Human-Machine Cooperation and Optimizing Strategies for Cyberspace OSINT Analysis”. Szerkesztette Taiar R. Ahram T. *Lecture Notes in Networks and Systems* 319 (2022): 634–42. https://doi.org/10.1007/978-3-030-85540-6_80.
 16. Cristiano, F. *Israel: Cyber defense and security as national trademarks of international legitimacy. Routledge Companion to Global Cyber-Security Strategy*. Taylor and Francis Inc., 2021. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85105225876&partnerID=40&md5=e3179d180fd17906ea6feef161fbadd>.
 17. Dvorak, R., and J.L. Whiteman. „A Call to Create an Open-source Project Initiative for Cybersecurity Virtual Labs”. In *ASEE Annual Conference and Exposition, Conference Proceedings*. American Society for Engineering Education, 2021. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85124517290&partnerID=40&md5=2c5fb5b91803b10975525e63dcd55bdb>.
 18. Gong, S., J. Cho, és C. Lee. „A reliability comparison method for OSINT validity analysis”. *IEEE Transactions on Industrial Informatics* 14, sz. 12 (2018): 5428–35. <https://doi.org/10.1109/TII.2018.2857213>.
 19. González-Granadillo, G., S. González-Zarzosa, és R. Diaz. „Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures”. *Sensors* 21, sz. 14 (2021). <https://doi.org/10.3390/s21144759>.
 20. Gyányi Sándor. „Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem”, 2012. <https://doi.org/10.17625/NKE.2012.008>.
 21. Hayes, D.R., and F. Cappa. „Open-source intelligence for risk assessment”. *Business Horizons* 61, sz. 5 (2018): 689–97. <https://doi.org/10.1016/j.bushor.2018.02.001>.

22. Huang, Y., C.Y. Lin, Y. Guo, K. Lo, Y.S. Sun, and M.C. Chen. „Open Source Intelligence for Malicious Behavior Discovery and Interpretation”. *IEEE Transactions on Dependable and Secure Computing*, 2021. <https://doi.org/10.1109/TDSC.2021.3119008>.
23. Kanta, A., I. Coisel, and M. Scanlon. „A survey exploring open source Intelligence for smarter password cracking”. *Forensic Science International: Digital Investigation* 35 (2020). <https://doi.org/10.1016/j.fsidi.2020.301075>.
24. Le, B.-D., G. Wang, M. Nasim, és M.A. Babar. „Gathering cyber threat intelligence from twitter using novelty classification”. In *Proceedings - 2019 International Conference on Cyberworlds, CW 2019*, 316–23. Institute of Electrical and Electronics Engineers Inc., 2019. <https://doi.org/10.1109/CW.2019.00058>.
25. Lee, S., and T. Shon. „Open source intelligence base cyber threat inspection framework for critical infrastructures”. In *FTC 2016 - Proceedings of Future Technologies Conference*, 1030–33. Institute of Electrical and Electronics Engineers Inc., 2017. <https://doi.org/10.1109/FTC.2016.7821730>.
26. Lee, S., H. Cho, N. Kim, B. Kim, és J. Park. „Managing Cyber Threat Intelligence in a Graph Database: Methods of Analyzing Intrusion Sets, Threat Actors, and Campaigns”. In *2018 International Conference on Platform Technology and Service, PlatCon 2018*. Institute of Electrical and Electronics Engineers Inc., 2018. <https://doi.org/10.1109/PlatCon.2018.8472752>.
27. Michael Bazzell - Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, ISBN-13: 979-8578577086
28. Michael Bazzell - Hiding from the Internet: Eliminating Personal Online Information, ISBN-10: 1500397814
29. Pastor-Galindo, J., P. Nespoli, F. Gomez Marmol, and G. Martinez Perez. „The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends”. *IEEE Access* 8 (2020): 10282–304. <https://doi.org/10.1109/ACCESS.2020.2965257>.
30. Peng, P., C. Xu, L. Quinn, H. Hu, B. Viswanath, és G. Wang. „What happens after you leak your password: Understanding credential sharing on phishing sites”. In *AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 181–92. Association for Computing Machinery, Inc, 2019. <https://doi.org/10.1145/3321705.3329818>.

31. Qusef, A., and H. Alkilani. „The effect of ISO/IEC 27001 standard over open-source intelligence”. *PeerJ Computer Science* 8 (2022). <https://doi.org/10.7717/PEERJ-CS.810>.
32. Samtani, S., M. Abate, V. Benjamin, and W. Li. *Cybersecurity as an industry: A cyber threat intelligence perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, 2020. https://doi.org/10.1007/978-3-319-78440-3_8.
33. Tabatabaei, F., and D. Wells. „OSINT in the context of cyber-security”. *Advanced Sciences and Technologies for Security Applications*, 2016, 213–31. https://doi.org/10.1007/978-3-319-47671-1_14.
34. Tundis, A., S. Ruppert, és M. Mühlhäuser. „A Feature-driven Method for Automating the Assessment of OSINT Cyber Threat Sources”. *Computers and Security* 113 (2022). <https://doi.org/10.1016/j.cose.2021.102576>.
35. Urban, T., M. Große-Kampmann, D. Tatang, T. Holz, and N. Pohlmann. „Plenty of phish in the sea: Analyzing potential pre-attack surfaces”. Szerkesztette Liang K. Chen L. Schneider S., Li N. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 12309 LNCS (2020): 272–91. https://doi.org/10.1007/978-3-030-59013-0_14.
36. Williams, J. „Legal and ethical issues surrounding open source research for law enforcement purposes”. In *Proceedings of the 4th European Conference on Social Media, ECSM 2017*, szerkesztette Gudeliene N. Skarzauskiene A., 398–406. Academic Conferences and Publishing International Limited, 2017. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85028540502&partnerID=40&md5=ff0fa93e7f6afbdf9fe6ab5d461b5c9>.

V. Mellékletek

1. Annotáció

Dolgozatom a „A nyílt forrású információszerzés szerepe a kibertámadások tükrében” címet viseli, s elsősorban azt hivatott feltárni, hogy az OSINT egyes alkalmazási területein, kimondottan a Cyber Threat Intelligence, vagyis a kiberfenyegetettségekkel kapcsolatos hírszerzés területén nem annyira vonalzóval rajzoltak a határok, mint az gondolható, ezért egy nem elhanyagolható jelentőségű szürke zóna képződik. Ebből kifolyólag azt szeretném szemléltetni, hogy a vékony határvonal a törvényes, engedélyekhez nem kötött információszerzés és a „hacker-tevékenység” alá eső módszerek között bizonyos esetben legitim módon átjárható, valamint szükséges is, például egy nyílt forrásból történő kiberbiztonsági átvilágítás esetében. Dolgozatomban az információszerzés jogi és etikai vetületei mellett megvizsgálom azt is, mely információgyűjtő folyamat bizonyul a leghatékonyabbnak egy kibertámadás előkészítése céljából – az adathalászat vagy az OSINT – valamint ezzel milyen összefüggésben áll az online térben tanúsított magatartásunk, a digitális lábnyomunk mérete és az információbiztonsági tudatosságunk. Továbbá górcső alá veszem még az OSINT-tal szembeni védekezési lehetőségek egyes formáit. A felvázolt kérdéskörök érdemi körül járása érdekében kutatásom a releváns hazai és nemzetközi szakirodalom, valamint szakkönyvek mellett olyan szakértők álláspontjára is támaszkodik, mint etikus hackerek, OSINT elemzők, szakmai vezetők és egy GDPR szakjogász. Ennek értelmében hipotéziseim igazolásának érdekében pályamunkám elkészítésekor olyan kutatási módszereket alkalmazok, mint a fókuszcsoporthoz tartozó interjú, az abból befolyó eredményekből végezett, arculatát tekintve a szakmába illő klaszterelemzés, valamint trendelemzés az „OSINT” és a „CTI” kulcsszavakkal citált nemzetközi szakirodalom vonatkozásában. Továbbá kontextusba helyezve szemléltetek olyan módszereket és eszközöket, melyek bizonyító erővel bírnak hipotézisem vonatkozásában, valamint bizonyos összefüggésekre esetpéldákon keresztül világítok rá.

2. Rövidítések jegyzéke

Rövidítés	Magyar meghatározás	Angol meghatározás
API	Alkalmazásprogramozási felület	Application programming Interface
AQAP	Minőségbiztosítási rendszerek szabványai	Allied Quality Assurance Publications
BYOD	Hozd a saját eszközöd	Bring Your Own Device
C2	Parancs és irányítás	Command and Control
CTI	Kiberfenyegetettségekkel kapcsolatos hírszerzés	Cyber Threat Intelligence
GDPR	Általános Adatvédelmi Rendelet	General Data Privacy Regulation
HUMINT	Emberi kapcsolatokon alapuló hírszerzés	Human Intelligence
ICS	Ipari vezérlőrendszer	Industrial Control System
IKT	Információs és Kommunikációs Technológia	Information and Communication Technology
ISO	Nemzetközi Szabványügyi Szervezet	International Organization for Standardization
OSINT	Nyílt forrású információszerzés	Open Source Intelligence
PLC	Programozható logikai vezérlő	Programmable Logic Controller
PV-OSINT	Magánszférát sértő nyílt forrású információszerzés	Privacy Violating Open Source Intelligence
SIEM	Biztonsági információ- és eseménykezelő	Security Information and Event Management
SOCMINT	Közösségi médián alapuló hírszerzés	Social Media Intelligence
SQL	Relációsadatbázis-kezelők lekérdezési nyelve	Structured Query Language
TTP	Taktikák, technikák és eljárások	Tactics, Techniques, and Procedures
VHUMINT	Ún. „virtuális ügynök” által folytatott emberközpontú hírszerzés	Virtual Human Intelligence

3. Ábrák jegyzéke

1. ábra: Az Információbiztonsági Tudatossági Modell (Saját fordítás, forrás: sans.org).....	8
2. ábra: Az OSINT főbb használati esetei (Saját fordítás, forrás:).....	12
3. ábra: Egy OSINT művelet általános lépései.....	16
4. ábra: Shodan keresési eredmény. (saját képernyőmentés, forrás: shodan.io)	18
5. ábra: Nmap parancs használatának példája. (saját képernyőmentés, forrás: nmap.org)	18
6. ábra: a Cyber Kill Chain® modell lépések szerinti ábrája. (Forrás: lockheedmartin.com) .	27
7. ábra: Fájl-hash vizsgálat eredménye (forrás: CyberThreat.Report Facebook csoport).....	38
8. ábra: Ismeretlen személy portréja. (forrás: Google).....	40
9. ábra: Metaadat elemzés eredménye. (saját képernyőmentés)	40
10. ábra: GPS koordináta alapján végzett keresés. (saját képernyőmentés, forrás: Google Maps).....	41
11. ábra: A tulajdoni lap részei és tartalma. (Forrás: foldhivatal.hu).....	42
12. ábra: Az „Open Source Intelligence” keresőkifejezés megjelenése a nemzetközi tudományos publikációkban 1995-2021 között (Saját szerkesztés, forrás: Scopus).....	49
13. ábra: Az "Open Source Intelligence" keresőkifejezés megoszlása tudományterületenként (Saját szerkesztés, forrás: Scopus)	50
14. ábra: Az "Open Source Intelligence" keresőkifejezéshez köthető leggyakoribb 50 kulcsszó (Forrás: SciVal)	51
15. ábra: A „Cyber Threat Intelligence” keresőkifejezés megjelenése a nemzetközi tudományos publikációkban 2012-2021 között (Saját szerkesztés, forrás: Scopus).....	52
16. ábra: A "Cyber Threat Intelligence" keresőkifejezés megoszlása tudományterületenként (Saját szerkesztés, forrás: Scopus)	53
17. ábra: Az "Cyber Threat Intelligence" keresőkifejezéshez köthető leggyakoribb 50 kulcsszó (Forrás: SciVal)	54
18. ábra: A klaszterelemzési algoritmus eredménye (Saját képernyőmentés, forrás: Jupyter-Notebook).....	56
19. ábra: Az eredményként kapott három klaszter (Saját szerkesztés)	56
20. ábra: Klaszterek vizualizációja a centroid értékek alapján. Saját képernyőmentés, forrás: Jupyter-Notebook).....	57
21. ábra: Klaszterek adatmennyisége kulcsszavak alapján (Saját képernyőmentés, forrás: Jupyter-Notebook).....	58
22. ábra: Szófelhő az egyes klaszterekbe tartozó kulcsszavakból (Saját képernyőmentés, forrás: Jupyter-Notebook)	58

4. Interjúkérdések

H1 Interjúkérdések

1. A munkafolyamatok során átlépnek-e bizonyos erkölcsi-etikai határokat? Olyan eszközökre igénybevételére gondolok, amelyek még nem minősülnek hackelésnek, de már nem mondhatók „Pure OSINT”-nak. Például Dark webes data breach-ek összegyűjtése és elemzése, automatizált eszközök, böngésző kiterjesztések stb., melyek akár emberi mulasztás útján elérhető bizalmas adatokat is feltárhatnak?
2. Milyen megkötésekkel, milyen engedélyek birtokában végzik az egyes CTI szolgáltatásokat az ügyfelek részére?
3. Milyen határokig mehet el egy megrendelő a munkavállalóival kapcsolatban a szervezete biztonságának vizsgálata érdekében? Mi az, amit kérhet, és amit már nem?
4. Személyes véleménye szerint etikátlannak tartja-e bármennyiben is, a személyek esetében történő részletes „háttérelmézést”? (magánélet, szokások, online térbeli tevékenységek stb.)
5. Mi az, amit már nem lehet elvégezni az adott munkavállalók ellenőrzésekor az OSINT határain belül?
6. Minősíthető-e az információs rendszer vagy adat megsértése bűncselekményének, ha az OSINT elemző egy rendszerhez default credentials próbáját követő esetleges hozzáférést szerez? Illetve ha emberi mulasztásból kifolyólag hozzáférések vannak feltüntetve egy teszt/dev felület forráskódjában és azzal próbálkozik az elemző?
7. Ha Directory listing (bejárható könyvtárak) esetén olyan bizalmas adatok is nyilvánosan hozzáférhetők, melyeket szemmel láthatóan nem szántak annak, letöltésük megvalósítja-e a tiltott adatszerzés törvényi tényállását?
8. Milyen jogi akadályokba ütköznek, amelyek a hatékony és szükséges információgyűjtést akadályozzák?
9. Van-e esetleg forrásbeli akadályuk a hatékony és szükséges információgyűjtésnek?
10. GDPR szempontjából felelősségre vonható-e egy szervezet, amiért data breach adatokkal dolgozik? Ha igen, milyen esetben?
11. Ön szerint milyen hazai és/vagy nemzetközi jogi szabályozásra vagy változtatásra lenne szükség?
12. Hogyan értékeli szervezete OSINT képességét? (1-10-es skálán, 1-es leggyengébb 10-es legjobb)
13. Önnek milyen javaslati lennének szervezete OSINT fejlesztésének irányában?

H2 Interjúkérdések

1. Végeznek-e rendszeres sérülékenységvizsgálatot? Ennek a fingerprinting / reconnaissance, vagyis a tesztek megelőző információgyűjtési fázisának része-e a vállalatokról online hozzáférhető információk vizsgálata? Ha igen, hogyan kezelik az esetleges találatokat?
2. Szerveznek-e időszerűen Adathalász-kampányokat a szervezet dolgozóinak információbiztonsági tudatosságának felmérése és fejlesztése érdekében?

3. OSINT „támadásokkal” szembeni védelem esetében, ön szerint meddig tud eljutni egy támadó, azaz lehetséges-e egy olyan pontot meghatározni a szervezetben, amin egy támadó semmilyen esetben sem juthat át?
4. Történt-e a szervezetükben olyan információbiztonsági incidens, amely háttérben adathalász tevékenység állhatott?
5. Megbízhatóságukat illetően lehetséges valamilyen módon szűrni az Adathalászatból befolyó, illetve OSINT folyamatok mentén gyűjtött adatok valódiságát?
6. Véleménye szerint melyik módszer képvisel nagyobb megbízhatóságot egy támadás előkészítését illetően?

H3 Interjúkérdések

1. Történt-e a szervezetükben olyan információbiztonsági incidens, amely háttérben OSINT tevékenység állhatott?
2. Ha igen ezt, hogyan követték vissza?
3. Milyen jogi lépéseket tettek az incidenskezelést követően?
4. Milyen megelőző intézkedéseket tesznek, hogy a vállalat működése során, dolgozókról gyűjtött adatok ne legyenek nyíltan elérhetőek?
5. Milyen védekezési lehetőséget javasolna magánszemélyek, illetve kis- és középvállalatok esetében OSINT ellen?
6. Ön szerint hatékony védekezés lehet a dezinformáció?
7. Lehetséges a digitális lábnyomunk oly mértékű csökkentése, hogy ne válhassunk OSINT támadás áldozatai? (egyfajta preaktív online magatartás)

Részcél⁴² interjúkérdések

1. Mikor és hogy (minek kapcsán) fogalmazódott meg Önben az, hogy Információbiztonsággal/etikus hackeléssel/OSINT-al szeretne foglalkozni?
2. Mi volt a pályaválasztás fő motivációja?
3. Mióta foglalkozik OSINT-tal?
4. Napi munkavégzését illetően milyen kontextusban jelenik meg az OSINT, mint feladat?
5. Hogyan jutott el jelenlegi munkaköre betöltéséig, mind képzést és gyakorlatot illetően?
6. Milyen kihívások, esetleg akadályok kerültek Ön elé az előmenetelt illetően?
7. A szakmában töltött idő alatt felmerült Önben a pályaelhagyás gondolata? Ha igen, miért?
8. Továbbá ha igen, kapcsolódó munkakörben tervezne tovább tevékenykedni?
9. Ha nem, véleménye szerint hasznára válhat még a megszerzett szaktudás az elhelyezkedésben?

⁴² Az átfogóbb képalkotás érdekében vizsgálom még az érintett szakértők motivációját, különös tekintettel a pályaválasztásukkal kapcsolatos attitűdre, figyelembe véve a bemenetet, az előmenetelt, illetve a pályaelhagyás kérdéseit.

5. A klaszterelemzés Python kódja

```
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.cluster import KMeans
from sklearn.decomposition import PCA
import pandas as pd
import numpy as np
import re
import string
import nltk
from nltk.corpus import stopwords
import matplotlib.pyplot as plt
import seaborn as sns

text = ["answer1", "answer2", "answer3", ... "answer151"]

def preprocess_text(text: str, remove_stopwords: bool) -> str:
    """This utility function sanitizes a string by:
    - removing links
    - removing special characters
    - removing numbers
    - removing stopwords
    - transforming in lowercase
    - removing excessive whitespaces

    Args:
        text (str): the input text you want to clean
        remove_stopwords (bool): whether or not to remove stopwords

    Returns:
        str: the cleaned text
    """
    if remove_stopwords:
        tokens = nltk.word_tokenize(text)
        tokens = [w for w in tokens if not w.lower() in stopwords.words("english")]
```

```

    text = " ".join(tokens)
    text = text.lower().strip()
    return text

df = pd.DataFrame (text, columns = ['corpus'])
df.shape
import nltk
nltk.download("punkt")
nltk.download("stopwords")
df['cleaned'] = df['corpus'].apply(lambda x: preprocess_text(x, remove_stopwords=True))

vectorizer = TfidfVectorizer(sublinear_tf=True, min_df=5, max_df=0.95)
X = vectorizer.fit_transform(df['cleaned'])
from sklearn.cluster import KMeans
kmeans = KMeans(n_clusters=3, random_state=42)
kmeans.fit(X)
clusters = kmeans.labels_
from sklearn.decomposition import PCA
pca = PCA(n_components=2, random_state=42)
pca_vecs = pca.fit_transform(X.toarray())
x0 = pca_vecs[:, 0]
x1 = pca_vecs[:, 1]
df['cluster'] = clusters
df['x0'] = x0
df['x1'] = x1
def get_top_keywords(n_terms):
    """This function returns the keywords for each centroid of the KMeans"""
    df = pd.DataFrame(X.todense()).groupby(clusters).mean()
    terms = vectorizer.get_feature_names()
    for i,r in df.iterrows():
        print('\nCluster {}'.format(i))
        print(', '.join([terms[t] for t in np.argsort(r)[-n_terms:]])) # for each row of the dataframe,
        find the n terms that have the highest tf idf score
get_top_keywords(30)

```

```

cluster_map = {0: "Ethical Cluster", 1: "Legal Cluster", 2: "Technical Cluster"}
# apply mapping
df['cluster'] = df['cluster'].map(cluster_map)

plt.figure(figsize=(12, 7))
plt.title("TF-IDF + KMeans Interjú", fontdict={"fontsize": 18})
plt.xlabel("X0", fontdict={"fontsize": 16})
plt.ylabel("X1", fontdict={"fontsize": 16})
sns.scatterplot(data=df, x='x0', y='x1', hue='cluster', palette="viridis")
plt.show()

sns.countplot(df["cluster"])

# Import package
from wordcloud import WordCloud, STOPWORDS
text = " ".join(title for title in df.cleaned)
word_cloud = WordCloud(width=3000,
                        height=2000,
                        random_state=1,
                        collocations = False, background_color = 'black').generate(text)
plt.imshow(word_cloud, interpolation='bilinear')
plt.axis("off")
plt.show()

```