

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

A hazai kis-és középvállalati szektor vizsgálata a nyílt forrású információszerzés aspektusából

Jelige: *biztonságOsint*

Pályamunka lezárásának időpontja:
2022. május

2023.

Tartalomjegyzék

Bevezetés.....	1
Téma aktualitása	1
Tudományos probléma megfogalmazása	1
Kutatási célkitűzések	2
Hipotézisek	3
Kutatási módszertan	3
1. fejezet: A nyílt forrású információszerzés fogalmi meghatározása	4
1.1 A nyíltforrású információszerzés fogalma	4
1.2. Történelmi fejlődésének áttekintése	6
1.3. Előnyei és árnyoldala.....	8
1.4. Az OSINT jogszabályi háttere.....	10
Következtetések.....	13
2. fejezet: Az OSINT eszköztárának áttekintése	14
2.1. Általános bevezetés.....	14
2.1.1. OSINT Framework	15
2.2. Kereső motorok és az OSINT kapcsolata.....	16
2.2.1. Meta keresőmotorok	17
2.2.2. Shodan.....	17
2.2.3. Google Hacking	18
2.3. Közösségi média, mint nyílt forrás.....	19
2.4. Legnépszerűbb alkalmazások, szoftverek	20
2.4.1. Maltego	20
2.4.2. TheHarvester.....	21
2.4.3. Spiderfoot.....	22
2.4.4. SentiOne.....	22
2.4.5. Facepager	23
2.5. OSINT eszközök felhasználási módjai	23
Következtetések.....	25
3. fejezet: A hazai kis-és középvállalkozások információbiztonsági gyakorlata	27
3.1. Mit nevezünk kis- és középvállalkozásnak?.....	27
3.2. A kis- és középvállalkozások információbiztonsággal összefüggő kihívásai	27
3.2.1 OSINT lehetőségek a kis- és középvállalati szektorban	30

3.3. Kis- és középvállalkozások nyílt forrású információszerzéssel kapcsolatos tudatossága és képessége	31
3.3.1. Kérdőív bemutatása.....	31
3.3.2. Kérdőívem kiértékelése	31
3.3.3. OSINT teszt végrehajtása egy hazai kis- és középvállalkozásra vonatkozóan.....	36
Következtetések.....	38
Összegzett következtetések	38
Kutatási eredmények	39

Bevezetés¹

Téma aktualitása

Kialakulásától kezdve az internet nagy hatással van mindennapi életünkre. Meghatározó elemmé vált a társas interakciónkban, az üzleti életben, a kapcsolattartási képességeinkben, de különösen az információhoz való hozzáférés szempontjából.² Napjainkban az információt magát egyre inkább a modern világ egyik legmeghatározóbb mozgatórugójaként, illetve társadalomszervező tényezőként tartják számon. A digitalizált világban már főképp az internetet használják az információk közlésére, megosztására, míg korábban a hagyományos nyomtatott média játszotta a főszerepet. Bár az információk közzétételének és könnyű elérhetőségnek számos előnye van, egyúttal szükséges számolni a nyílt forrásból elérhető információk információbiztonsági és adatvédelmi kockázataival. A hírszerzés mindig politikai igényből fakadt, amelynek egyik legrégebbi formája az az információk nyílt forrásból történő megszerzése. Ez egyben azt is jelenti, hogy ezt az információgyűjtési eljárást nem csak a nemzetbiztonsági szolgálatok végezhetik, hanem az egyének és szervezetek egyaránt alkalmazhatják eltérő motivációval, ami akár károkozás szándékával is történhet. A nyílt forrású információszerzés (Open Source Intelligence, továbbiakban OSINT) egyaránt jelenthet fenyegetettséget a magánszemélyeknek, felhasználóknak, valamint a szervezeteknek cégeknek, de ugyanakkor számos OSINT eszköz munkahelyi környezetbe való implementálása aktívan hozzájárulhat a vállalati biztonság vagy akár információbiztonsági irányítási rendszer kialakításában és fenntartásában.

Tudományos probléma megfogalmazása

A kis- és középvállalkozások (továbbiakban kkv) életében a szervezet szintű biztonság, valamint biztonságtudatosság megteremtése komplex feladat, különböző szakterületek összehangolt tevékenységét igényli.³ Jellemzően a cégek abban az esetben állnak neki kialakítani a céges biztonsági kultúrát, ha már előzetesen nagyobb volumenű incidens sújtotta őket, netalántán jogszabályi, szabványi megfelelésre kötelezi őket valamely hatóság vagy az ellátási lánc

¹ A dolgozat az Innovációs és Technológiai Minisztérium ÚNKP-21-2-II-NKE-87 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült

² A. Abdullah és mtsai., „OSINT Explorer: A Tool Recommender Framework for OSINT Sources”, *Communications in Computer and Information Science* 1487 CCIS (2021): 389–400, https://doi.org/10.1007/978-981-16-8059-5_24.

³ „Munk Sándor: Információbiztonság vs. informatikai biztonság”, elérés 2022. február 15., http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html.

egy szereplője.⁴ Természetesen az Információbiztonság Irányítási Rendszer (továbbiakban IBIR) kialakítása történhet szimpla vezetői elhatározás eredményeként, azonban a gyakorlatban erre jóval kevesebb példa van. Mindezek mellett az információbiztonsági szempontból kevésbé érett cégek, szervezetek, munkavállalók ugyanúgy napról napra állítanak elő hatalmas mennyiségű adatot, metaadatot, amik kikerül az online térbe és könnyen alapozhatják meg egy potenciális támadás alapját.

Az elmúlt években történő kibertámadások rámutattak arra, hogy az első lépésként értelmezett információgyűjtés alkalmas a támadás célpontjának megismerésére, ezáltal a különböző sérülékenységek, sebezhetőségek és kockázatok feltárására is, hiszen ezen hiányosságok felfedésével jelentősen növelhető a támadás eredményes végrehajtásának esélye.⁵ Ahogy már említettem az információszerzés történhet akár nyílt forrásból is. Ebben a tekintetben merülhet fel a gondolat, hogy miért ne hajtsanak végre úgynevezett „ön-OSINT-ot” a szervezetek vagy akár a magánszemélyek annak érdekében, hogy ellenőrizzék milyen mennyiségű és minőségű adat érhető el nyílt forrásból róluk.

Kutatási célkitűzések

Kutatási célomnak tekintem feltárni az OSINT előnyeit, illetve hátrányait, továbbá megvizsgálom az alkalmazási területeket és az eszközöket, amelyek rendelkezésre állnak. Feltérképezem azokat a OSINT-tal kapcsolatos bevett gyakorlatokat, amelyet egy hazai ki- és közép vállalkozás könnyen tud implementálni a mindennapi működésbe, továbbá célomnak tekintem megvizsgálni a jogszabályi hátteret. A kutatás további részében kérdőív segítségével mérem fel, a hazai kkv szektor OSINT képességeit, valamint azt, hogy van-e kapcsolat aközött, hogy egy adott kis- és középvállalkozás mennyire érett információbiztonsági szempontból és hogy alkalmaznak-e valamilyen OSINT technológiát, tevékenységet.

Végezetül pedig egy tesztet hajtok végre valamely nyílt forrású információszerzésre alkalmas szoftverrel. A teszt során azt tanulmányozom, hogy melyek azok az információ, amelyek OSINT eszközzel könnyen elérhetőek egy kkv-vel kapcsolatban, azonban a hivatalos weboldalon nincsenek feltüntetve.

⁴ „Munk Sándor: INFORMÁCIÓBIZTONSÁG VS. INFORMATIKAI BIZTONSÁG”.

⁵ Veronika Deák, „A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során”, *Hadmérnök* 13, sz. 3 (2018. szeptember 30.): 391-402-391-402.

Dolgozatomnak egyfajta figyelemfelhívó szerepet is szánok, elsősorban az hazai kis-és közép vállalati szektor figyelmét szeretném megragadni és üzenetként eljuttatni az OSINT technológiák jótékony hatását.

Hipotézisek

H1: A nagyobb (munkavállalók számában mérve) kis- és közép vállalkozások munkavállalói többször hallottak az OSINT-ről, mint azok, akik egy kisebb szervezetnél dolgoznak.

H2: Azok a kis- és közép vállalkozások, akik alkalmaznak OSINT technológiát, átlagosan nagyobb biztonsági szintre értékelik saját magukat, mint akik nem alkalmaznak.

H3: OSINT tool-ok segítségével olyan információk is megszerezhetők, amelyek nincsenek feltüntetve a vizsgált szervezet hivatalos honlapján.

Kutatási módszertan

Az adatgyűjtés során egy kérdőív segítségével elemezem ki a felmérésben résztvevő kkv-k információbiztonsági érettségét, valamint az OSINT eszközökkel kapcsolatos viszonyát. A második fázisban egy nyílt forrású információszerzésre alkalmas eszközzel tesztet bonyolítok le. A kérdőív kérdéseit az SPSS rendszerben Mann Whitney U próba segítségével elemeztem ki, a tesztet pedig bárki számára elérhető ingyenes web alapú OSINT eszközzel végzetem.

1. fejezet: A nyílt forrású információszerzés fogalmi meghatározása

Mindenekelőtt az első fejezetben az OSINT fogalmának meghatározására törekszem egyfajta történelmi áttekintés segítségével és jogszabályi háttérrel kiegészítve.

1.1 A nyíltforrású információszerzés fogalma

A nyílt forrású információszerzés fogalmára számos meghatározás létezik a hazai és nemzetközi szakirodalmakban. Az OSINT definícióját magyar vonatkozásban először Lévay Gábor alkotta meg az alábbiak szerint: „Az OSINT a katonai felderítés és a hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti.”⁶ Az sem kétséges, hogy maga az OSINT katonai igényből származik, annak érdekében, hogy releváns és nyilvánosan elérhető információkat gyűjtsön. Használatával lehetőség nyílik olyan konkrét információk megtalálására, amelyek bizonyos ismeretekkel rendelkezőknek jelentőst előnyt jelenthet.⁷

Lévay Gábor meghatározásával ellentétben számos szerző az OSINT-ot egy külön hírszerzési ágnak tekintik a kilenc adat-és információgyűjtő módszer között, sőt akad olyan értelmezés is, amely a Social Media Intelligence-el (továbbiakban SOCMINT) azaz a közösségi médiából történő hírszerzéssel kiegészülve 10 hírszerzési ágat különböztet meg. A kilenc adat- és információgyűjtő módszer közé tartoznak az alábbiak:

- ember erőforrással végzett hírszerzés;
- nyílt forrású információgyűjtés;
- elektronikai felderítés;
- kiber/digitális hálózati hírszerzés, (Cyber Intelligence/Digital Network Intelligence, CYBINT/DNINT);
- képfelderítés (Image Intelligence, IMINT);
- mérés- és jelmeghatározó hírszerzés, (Measurement and Signature Intelligence, MASINT);
- technikai hírszerzés, (Technical Intelligence, TECHINT);
- pénzügyi hírszerzés (Financial Intelligence, FININT);

⁶ Lévay Gábor: OSINT (Open Source Intelligence) – Nyílt információs hírszerzés. Egyetemi jegyzet. Zrínyi Miklós Nemzetvédelmi Egyetem, Bp., 2006. 6

⁷ João Rafael Gonçalves Evangelista és mtsai, „Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence”, *Journal of Applied Security Research* 0, sz. 0 (2020. május 7.): 1–25, <https://doi.org/10.1080/19361610.2020.1761737>.

- orvosi hírszerzés (Medical Intelligence, MEDINT).

A nyílt források tárháza alapvetően igazán sokrétű, de napjainkban az internet robbanásszerű és folyamatos fejlődésének köszönhetően a legtöbb információszerzés az interneten keresztül valósul meg. Ennek ellenére természetesen a hagyományos médiumokból származó információgyűjtést is hívhatjuk nyílt forrású információszerzésnek, azonban a gyakorlatban a hagyományos médiumok szerepe jócskán háttérbe szorult. Az OSINT fő forrásait a NATO OSINT kézikönyve a következők szerint határozza meg:⁸

- nyomtatott és elektronikus média;
- internet, beleértve a láthatatlan web információit;
- kereskedelmi (fizetős) online szolgáltatók tanulmányai, adattárjai;
- „szürke irodalom”, azaz nem publikált, de nem is minősített, szűk körben hozzáférhető,
- nyomtatott és digitális dokumentumok, tanulmányok;
- tudományos előadások, konferenciák;
- személyes tapasztalatok;
- kereskedelmi műholdak felvételei;
- tudományos-kutató szervezetek, egyetemek.

Ezek alapján tehát minden olyan adat, amelyhez külön engedély nélkül lehet hozzáférni, (tagságok vagy kapcsolatok nélkül) OSINT által megszerzett adatnak tekinthető.⁹ A nyílt jellege miatt az OSINT fejlődése rendkívül dinamikus és széles körű, külön informatikai szegmens épült ki a különböző technológiák révén.¹⁰ Napjainkban ezek a technológiák széles körben elterjedtek, gyakran alkalmazzák a szervezetek biztonsági kultúrájának kialakítása alkalmával, de akár a kibertámadások előkészítése és végrehajtása során is, azt azonban mindenképp ki kell emelni, hogy ezen módszer segítségével rengeteg információ megszerezhető, így az esetek jelentős részében nem elég csak összegyűjteni az információkat, ezt követően szűrni, szelektálni, rendszerezni, elemezni és értékelni is kell a felhasználás előtt.

Továbbá fontos látni egy lényeges különbséget abban az esetben, ha összevetjük a hazai tudományos diskurzusban előforduló OSINT fogalmat az angolszász irodalommal. Solti István értelmezésében ez a differencia annyit takar, hogy míg az angolszász irodalom

⁸ „NATO Open Source Intelligence Reader”, Military Wiki, elérés 2022. február 19., https://military-history.fandom.com/wiki/NATO_Open_Source_Intelligence_Reader.

⁹ Tony Day, Helen Gibson, és Steve Ramwell, „Fusion of OSINT and Non-OSINT Data”, 2016, 133–52, https://doi.org/10.1007/978-3-319-47671-1_9.

¹⁰ Dobák Imre, „OSINT – Gondolatok a kérdéskörhöz”, *Nemzetbiztonsági szemle* 7, sz. 2 (2019): 83–93, <https://doi.org/10.32561/nsz.2019.2.7>.

megelégszik azzal, hogy az információ nyílt forrásból származzon, addig a hazai meghatározás megköti, hogy maga az információ nem lehet semmiképpen sem minősített adat.¹¹

Deák Veronika értelmezésében pedig összességében az OSINT olyan információgyűjtő eljárás, mely során az információk megszerzése bárki által szabadon hozzáférhető forrásokból történik.¹²

1.2. Történelmi fejlődésének áttekintése ¹³

Az OSINT egy védelmi célú tevékenységként indult. Az Egyesült Államok 1941. február 26-án hozta létre a Foreign Broadcast Monitoring Service (továbbiakban FBMS) elnevezésű szervezetet, amelynek célja volt a külföldi műsorszórás és a tengelyhatalmak propaganda programjainak megfigyelése. 1942. július 26-án az FBMS-t átkeresztelték Federal Broadcast Information Service-re (FBIS), részben azért, hogy inkább háborús ügynökségnek tűnjön. A világháború végén majdnem bezárták. A második háború végén az FBIS-t 1946. január 1-jén a hadügyminisztérium vette át, egy évvel később pedig az 1947-es nemzetbiztonsági törvény értelmében átkerült a CIA-hez, és ekkor már-már egy "majdnem kiforrott, kiképzett és fegyelmezett" szervezet volt, melynek működéséhez nagy mértékben hozzájárultak a háborúból szerzett tapasztalatok. Az FBIS létrehozásától az 1990-es évekig a nyílt forráselemzés elsősorban a külföldi sajtóforrások megfigyelése és fordítása volt. Van néhány fontos és meghatározó különbség az OSINT e történelmi jellege és alkalmazása - az OSINT első generációja - és a mai technológiák használata, azaz a mai második generáció között. Az első generációs OSINT alkalmazása során jelentős hangsúlyt fektettek az anyaggyűjtésre. Az FBIS világszerte 20 irodát működtetett, hogy fizikailag anyagot gyűjthessenek. A nagykövetségek is lehetőséget biztosítottak az anyaggyűjtésre, így a diplomáciai tisztviselők feladatkörébe ez is beletartozott. Az FBIS munkája kritikus meglátásokat és döntési pontokat biztosított a hadsereg számára a hidegháború idején. A hidegháború vége a legtöbb hírszerzéssel foglalkozó intézmény költségvetésének csökkentését eredményezte, különösen az FBIS és a nyílt forrású küldetések számára. FBIS ebben az időben gyorsan veszített erőforrásaiból. 1997-ben az FBIS-t a CIA költségvetési megszorítások részeként a megszűnés veszélye fenyegette, de Federation of American

¹¹ Solti István, „Az OSINT információgyűjtő eszközeiről”, *Nemzetbiztonsági szemle* 7, sz. 2 (2019): 3–18, <https://doi.org/10.32561/nsz.2019.2.1>.

¹² Veronika, „A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során”.

¹³ Joseph E. Roop, „Foreign Broadcast Information Service. History. Part 1: 1941-1947” (Central Intelligence Agency Washington DC, 1969. április 1.), <https://apps.dtic.mil/sti/citations/ADA510770>.

Scientists (Amerikai Tudósok Szövetsége) kezdeményezésére indított nyilvános kampány megmentette a szervezetet. A FBIS-t az akadémikusok akkoriban úgy jellemezték, hogy "az amerikai hírszerző közösség legnagyobb durranása".

Az amerikai nemzetbiztonsági szervezetek vezetői felismerték, hogy a XXI. század kihívásai és dinamikája nem az OSINT iránti igény csökkenését, hanem növekedését fogja elhozni. J. Niles Riddel, az FBIS igazgatóhelyettese, az 1992-es első nemzetközi nyílt forrású intelligenciáról szóló szűkebb körű tudományos tanácskozáson elismerte a számítógépek, a nagy kapacitású digitális tárolók, a hatékony keresőmotorok és a szélessávú kommunikációs hálózatok elterjedéséből eredő változásokat. Úgy vélte mindezek a tényezők exponenciális növekedést fognak eredményezni az információ kereskedelmi hasznosításában.

Az internet fejlődése tulajdonképp elérhetővé tette az információ digitális formában való megjelenését és ez jelentős hatással volt a nyílt forrású dokumentumok, információk mennyiségének növekedésére. Másrészt, a technológiai fejlődéssel és az internet megjelenésével lehetőség nyílt arra, hogy a kívánt információkat nagyobb mennyiségben és sebességben gyűjtsék össze, függetlenül attól, hogy a tartalom az anyanyelvünkön vagy idegen nyelven jelenik meg, más szavakkal, a tudás még soha nem volt ilyen könnyen elérhető, még soha nem volt ilyen széles körben elterjedt, mint manapság.¹⁴

Jól látható, hogy a nyíltforrású információszerzési eljárások használatának dokumentált alkalmazásának gyökerei jócskán a 20. századig nyúlnak vissza, azonban fontos megemlíteni, hogy pontos dátumot vagy évet képtelenség lenne meghatározni kialakulását illetően, hiszen a szimpla szóbeszéd vagy (köznyelven kifejezve, „pletyka”) által generált információgyűjtés is a korai értelemben vett OSINT-hoz tartozhat. A nyílt forrású információszerzés legelső elismert fogalmi meghatározására 2001-ig kellett várni, mikor is a Észak-atlanti Szerződés Szervezete (NATO) publikálta az „Open Source Intelligence Handbookot”, mely a következőképp határozta meg az OSINT fogalmát: „Az Osint olyan információ, amelyet tudatosan megszereztek, kiválasztottak, kivonatoltak és felterjesztettek egy kiválasztott felhasználó körnek, általában parancsnok és közvetlent beosztottja számára speciális kérdések megvizsgálása szempontjából.”¹⁵

¹⁴ Tomislav Dokman és Tomislav Ivanjko, „Open Source Intelligence (OSINT): issues and trends”, 2020, <https://doi.org/10.17234/INFUTURE.2019.23>.

¹⁵ „OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence.” NATO Open Source Intelligence Handbook

Összességében megállapítható, hogy az internet és a legmodernebb kommunikációs és információmegosztó rendszerek megjelenéséig a nyílt forráskódú hírszerzési információkat alacsony értékűnek hírszerzési tudományágnak tartották. A nyílt forrású hírszerzés valódi értékének el nem fogadása többnyire azzal volt összefüggésben, hogy a hírszerzési termék kizárólag titkos információkból származhat, míg a nyilvánosan elérhető adatokkal végzett munkát kevésbé tartották értékesnek és kevésbé a hírszerzési tevékenység szempontjából. A jelenlegi, mindenekelőtt változó biztonsági helyzetben azonban környezetben, amikor a hagyományos fenyegetések egyre inkább szétváltak és megváltoztak a konfigurációjukban, különösen, amikor a titkos adatok gyűjtése hosszadalmas, költséges és összetett folyamattá vált, a hírszerző szolgálatok is OSINT képességek létrehozásába kezdtek. Emellett ez a gyűjtés diszciplína az állami tevékenységen kívül felbecsülhetetlen értékű ismeretforrásnak is bizonyult, ezért teljes mértékben beilleszkedett más szférákba is, így a hírszerzési tevékenység, beleértve a nyílt forrású hírszerzési információkat is, már nem csak az állam sajátossága. A releváns és felhasználható hírszerzési ismeretek gyűjtése, analitikus feldolgozása és előállítása ma már mind az állami, mind a nem állami szereplőkre jellemző. Azonban a jövőben, az OSINT-nak nagy kihívásokkal kell szembenéznie egyrészt a hatalmas mennyiségű strukturálatlan adat miatt, mivel ezek összegyűjtéséhez és megfelelő szortírozásához egyre nagyobb mértékben fejlődő kifinomult szoftverekre lesz szükség.

1.3. Előnyei és árnyoldala

Az elmúlt években a nyílt forrású információgyűjtés jelentősége és szerepe egyre nőtt mind a hírszerzés, mind a különböző gazdasági tevékenységet végző szervezetek mindennapi életében. Mára már megállapíthatjuk, hogy a nyílt forrású információgyűjtés a hírszerzési elemzők és a vállalati biztonsági elemzők által használt információk nagy részét biztosítja a potenciális rejtett kockázatok azonosításához vagy a stratégiai döntések időben történő meghozatalához. Bár az OSINT használatának számos előnye van, vannak bizonyos korlátok és gyengeségek is, amelyeket mellett nem mehetünk el említés nélkül.¹⁶

Az OSINT használatának egyik legnagyobb előnye a költség: Ha a hírszerzés oldaláról közelítjük meg, sokkal olcsóbb a hagyományos információgyűjtő eszközökhöz képest, így potenciálisan nagyobb megtérülést kínál és ez a jelleg különösen fontos a szűkös költségvetéssel rendelkező szervezetek számára. A költségelőny mellett számos előnnyel jár az információkhoz való hozzáférés és az információk megosztása terén is. Az

¹⁶ „Advantages and Disadvantages of Open Source Intelligence”, Expert.ai, 2017. február 23., <https://www.expert.ai/blog/advantages-disadvantages-open-source-intelligence/>.

információk jogszerűen és könnyen megoszthatók bárkivel; a nyílt források mindig rendelkezésre állnak és folyamatosan naprakészek bármilyen témában. Ráadásul manapság nagy mennyiségű értékes nyílt forrású adat áll rendelkezésre, amely a különböző szoftverek és eszközök segítségével könnyen elemezhető és összekapcsolható.¹⁷ Azonban fontos látni, hogy mind a Deep Webben¹⁸ mind a Dark neten¹⁹ nagyobb mennyiségben érhetőek el információk, mint a Surface Webben, azaz mindenki számára elérhető interneten.

Végül, de nem utolsó sorban, a nyilvános forrásokból gyűjtött információk nagyszerű forrást jelentenek a hírszerzéshez, de egyaránt felhasználhatók különböző üzleti célokra vonatkozó hosszú távú stratégiák létrehozásának támogatására.²⁰

A számos előnyös felhasználási mód mellett fontosnak tartom megemlíteni a kihívásokat is, amelyek felmerülhetnek az OSINT kapcsán. A rendkívüli mennyiségű információ szűrése meglehetősen időigényes munkának bizonyul, továbbá nem csak a mennyiség, de az információk minősége is nehezítő tényezőként jelenik meg. Az információk strukturátlansága megnehezíti ezen információk osztályozását, összekapcsolását és vizsgálatát a releváns kapcsolatok. Ebben az értelemben az OSINT olyan mechanizmusokat igényel, mint az például az adatbányászat.²¹ Az információk szűrését követően ellenőriznie kell, hogy azok megbízható-e. A szervezetek és egyének szándékosan hamis információkat tehetnek közzé, hogy félrevezessék az átlag fogyasztókat. Különösen a közösségi oldalak bugyraiból összegyűjtött információk esetében nehéz olykor megítélni annak valóságtartamát, egyfajta megtévesztő szerepet is betölthetnek ezek a platformok, hiszen előfordul, hogy a profilok vagy a webportálok kormányok vagy üzletemberek irányítása alatt állnak, és információik elfogultak. Ezekből könnyen következtethetünk, hogy az OSINT-eszközök egyik hátránya, hogy sokuk nem rendelkezik tényellenőrző funkcióval, így olykor nehéz feladatot jelenthet a valós hírek és az álhírek megkülönböztetése.²² Azt is

¹⁷ B.L. Wong, „Fluidity and Rigour: Addressing the Design Considerations for OSINT Tools and Processes”, 2016, 167–85, https://doi.org/10.1007/978-3-319-47671-1_11.

¹⁸ A Deep web olyan titkosított online tartalomra utal, amelyet a hagyományos keresőmotorok nem indexelnek

¹⁹ Deep web egy része

²⁰ Az MVM Zrt. és az Nemzeti Közzolgálati Egyetem együttműködési megállapodása alapján folytatott ... című projekt keretében végzett kutatás eredménye, Budapest 2021. Bányász Péter, Ináncsi Mátyás, Katona Gergő, Magas Bianka, Magyar Sándor, Mile Márió, Nimsz Vivien, Ruszkovics Patrik, Tóth András, Tóth Rebeka: A villamos-energia rendszer egyes szervezeteinek OSINT tudatossága és aktuális védelmi képességei.

²¹ A villamos-energia rendszer egyes szervezeteinek OSINT tudatossága és aktuális védelmi képességei. 2021

²² „All You Need to Know About Open Source Intelligence (OSINT)”, MUO, 2020. november 20., <https://www.makeuseof.com/all-you-need-to-know-about-open-source-intelligence-osint/>.

értelmes leszögezni, hogy az információ megtalálása nagyon keveset ér, ameddig azt nem vagyunk képesek valamilyen értelmes módon felhasználni.²³

1. táblázat Saját szerkesztés. (Forrás: <https://www.hindawi.com/journals/wcmc/2022/1290129/>)

Előnyök	Hátrányok
Gyors/valós idejű információgyűjtés	Túl nagy az információ mennyisége
Kényelem és könnyű hozzáférés	Biztonsági kérdések, technikai korlátok
Alacsony költség	Téves, struktúrátlan információk
Könnyebb megosztani a nyílt forrásokból gyűjtött információkat harmadik felekkel	Etikai/jogi kérdések

Az OSINT előnyeiről és gyengeségeiről szólva megállapítható, hogy az előnyök voltaképp felülmúlják a hátrányokat. Az összes előnye bizonyíthatóan a teljes körű hírszerzési folyamat fejlődése szempontjából, és úgy tűnik, hogy az OSINT nagyszerű képességekkel rendelkezik a versenyszférában is. A gyengeségeket azonban nem szabad alábecsülni. Ha alkalmazói még nagyobb figyelmet fordítanak az OSINT potenciáljára, akkor olyan problémák, mint a nyelvi akadályok, a dezinformáció miatti megtévesztés, a gondatlan kiszivárogtatás, vagy akár az információ túlterheltsége is kellőképpen kezelhető és csökkenthető.

1.4. Az OSINT jogszabályi háttere

A nyílt forrású információszerzés jogi szabályozása nem teljesen egyértelmű és nem egységes. Bár maga az OSINT fogalmán kívül esik az az esetkör amikor az adott információt valamilyen rendszerbe történő betöréssel szerzik meg (hiszen ekkor már nem nyílt forrásról beszélünk), azonban mégis fontosnak tartom rögzíteni azt a jogszabályt, amely az ilyen és ehhez kapcsolódó bűncselekményekről szól. Az Európai Parlament és a Tanács által Az Információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról címmel kiadott 2013/40/EU irányelv határozottan kijelenti, hogy az egyes információs rendszerekhez való jogosulatlan hozzáférés az EU területén bűncselekménynek minősül, és a tagállamok ennek megfelelően kötelesek jogrendszerüket

²³ „Open Source Intelligence: What Is OSINT & How Does It Work?”, *InfoSec Insights* (blog), 2020. július 17., <https://sectigostore.com/blog/open-source-intelligence-what-is-osint-how-does-it-work/>.

kialakítani.²⁴ Magyarország esetében ezt az irányelvet követi Büntető Törvénykönyv XLIII. fejezete is²⁵, amely szerint bűncselekményt követ el az, aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával belép.²⁶

A korábbiakban már említésre került az a fajta szemlélet, miszerint a hazai definíció hangsúlyozza az információ nyílt jellegét. Ezek alapján nem csak annak a feltételnek kell teljesülni, hogy az információ nyílt forrásból származzon, fontos, hogy minősített adat nem lehet OSINT áldozata. A minősített adat fogalmát jelenleg a minősített adat védelméről szóló 2009.évi CLV. törvény határozza meg. A törvény a minősített adat két formáját ismeri. Nemzeti minősített adatot és a külföldi minősített adatot. A nemzeti minősített adatszükséges feltétele, hogy a minősítő a minősített adat adathordozóját a törvényben előírt alakú kellékekkel lássa el.²⁷ Solti István meghatározása szerint tekintettel arra, hogy a minősítő nagy eséllyel nem biztosít megismerési jogosultságot az OSINT-tevékenységet végző magántársaságoknak, illetve törvényi szinten sem lelhető fel erre vonatkozó felhatalmazás, továbbá még a nemzetbiztonsági szervezetekről szóló 1995. évi CXXV. törvény (Nbtv). sem tartalmaz a nemzetbiztonsági szolgálatoknak szóló, erre vonatkozó általános felhatalmazó rendelkezéseket, ezért minősített adat bárki által történő megszerzése, még ha az nyílt forrásból is történik meg, jogszerűtlen magatartásnak minősül.²⁸

A jogszabályi háttér vizsgálata kapcsán továbbá lényeges kérdéseket vet fel a személyes adatok védelme. Az OSINT szinte minden tevékenysége során személyes adatokat dolgoznak fel (pl. gyűjtenek, tárolnak, elemeznek, reprodukálnak), mint például nevek, címek, felhasználói nevek, telefonszámok, IP-címek, képek. Az Európai Unióban 2018-ban bevezetett adatvédelmi jogszabály, az Általános Adatvédelmi Rendelet (továbbiakban GDPR)²⁹ szabályozza a személyes adatok kezelését. Bár az OSINT tevékenységet folytatók feltehetően nyilvánosan elérhető forrásokból gyűjtik adataikat, adott esetben meg kell felelniük a GDPR előírásainak. A GDPR alapvető célja, hogy egyensúlyt teremtsen a polgárok magánéletéhez való joga és a társadalmunk adatsere iránti igénye között. A

²⁴ 2013/40/EU irányelv (8) pont

²⁵ Solti, „Az OSINT információgyűjtő eszközeiről”.

²⁶ Btk.423 §

²⁷ A minősített adat védelméről szóló 2009. évi CLV. törvény

²⁸ Solti, „Az OSINT információgyűjtő eszközeiről”.

²⁹ Az európai parlament és a tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679>

GDPR-t OSINT esetében nem úgy kell kezelni, hogy ez egy jogszabály, ami ellehetetleníti a nyílt információkból történő adatszerzést, hanem szigorú szabályozásként, ami az egyének védelme érdekében szűkíti, vagy bizonyos esetekben engedélyhez köti az adatokkal kapcsolatos tevékenységet.³⁰ A GDPR a személyes adatok feldolgozását azokra az esetekre korlátozza, ahol ennek jogalapja van. Hat különböző okot sorol fel, amelyek közül kettő potenciálisan releváns az OSINT tevékenységek szempontjából: jogi kötelezettség (6c. cikk) és jogos érdek (6f. cikk)³¹

A személyes adatok feldolgozásának egyik lehetséges oka, amely az OSINT tevékenység szempontjából releváns lehet, az a jogi kötelezettség. Könnyen merülhet fel a kérdés, hogyan is lehet ezt a gyakorlatban elképzelni. Az Európai Parlament és a Tanács a pénzmosás ellen büntetőjogi eszközökkel folytatott küzdelemről szóló 2018/1673 irányelve³² alapján a pénzintézetek kötelesek azonosítani ügyfeleik és pénzeszközeik forrását, ezáltal előfordulhat olyan szituáció, melynek alkalmával gyanúsan nagy pénzforgalmak észlelését követően OSINT tevékenységgel is van lehetőségük utánajárni a bankjegyek eredetének, vagy egyáltalán birtokolhat-e ez adott ügyfél olyan nagy mennyiségű pénzt, amellyel a gyanús pénzforgalmat lebonyolították.

A személyes adatok kezelésének másik indoka, amely OSINT tevékenységek szempontjából releváns lehet, az ügyfelek, szervezetek jogos érdeke. Vállalkozások tevékenysége során gyakran szükség lehet személyes adatok kezelésére az üzleti tevékenységéhez kapcsolódó feladatok elvégzéséhez. Megtörténhet, hogy a személyes adatok ennek keretében történő kezelését nem indokolja jogi kötelelem vagy egy személlyel kötött szerződés feltételeinek végrehajtása. Ilyen esetben a személyes adatok kezelése indokolt lehet a „jogos érdekre” való hivatkozással. Ebben az esetben a szervezeteknek ellenőriznie kell azt is, hogy jogos érdekeinek szem előtt tartása során nem sérti-e súlyosan az érintettek jogait és szabadságait, ellenkező esetben ugyanis nem hivatkozhat vállalkozása jogos érdekeire az adatkezelés során, és egyéb jogalapot kell találnia.³³ Gondoljunk bele a következő forgatókönyvbe: Egy nagy tőzsdén jegyzett divatcég éppen új vezérigazgató

³⁰ A villamos-energia rendszer egyes szervezeteinek OSINT tudatossága és aktuális védelmi képességei 2021

³¹ GDPR 6. cikk

³² Az Európai Parlament és a Tanács (EU) 2018/1673 irányelve (2018. október 23.) a pénzmosás ellen büntetőjogi eszközökkel folytatott küzdelemről <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32018L1673> (Letöltés dátuma: 2022.03.14.)

„Mi számít »jogos érdekek«?”, Text, Európai Bizottság - European Commission, elérés 2022. március 14.,

³³ „Mi számít »jogos érdekek«?”, Text, Európai Bizottság - European Commission, elérés 2022. március 14., https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_hu.

felvételét végzi. Az adott cég egyébként az állatkínzás elleni határozott fellépésükről ismert, és számos figyelemfelkeltő kampányt támogatott ezzel kapcsolatban, már-már céges arculattá vált az éles állásfoglalás. Azonban munkavállalást megelőző szűrés során a közösségi oldalakon olyan képeket, posztokat találnak a potenciális vezérigazgatóról, amelyeken éves rókavadászatban vesz részt. Ha ezek az információk akkor szivárognának ki, amikor a vezérigazgató már a helyén van, az minden bizonnyal komoly botrányt okozna, esetleg a cég részvényértékének csökkenését és elbocsátásokat okozna.³⁴

Összegezve megállapítható, hogy az internet alapvető OSINT-forrásként való megjelölése nem vitatható, azonban az online térben automatikusan nem alkalmazható minden információgyűjtő eszköz. Nem tartoznak az OSINT területére azok az információgyűjtő tevékenységek, amelyeknél: hackingszközök felhasználásával, megszerzett jogosultságok felhasználásával vagy, szándékolt, az érintett megfélemlítését célzó magatartás tanúsításával történik információszerzés.³⁵

Következtetések

Az első fejezetben az OSINT fogalmát igyekeztem körbejárni, kitértem történelmi fejlődésére, továbbá taglaltam előnyeit és a hátrányait, továbbá kitértem a jogszabályi háttérrel érintő kérdésekre is. A szakirodalmak tanulmányozását követően konstatáltam, hogy manapság amikor az OSINT kifejezést használjuk, általában ma már a teljes keretrendszerre gondolunk, amely magában foglalja a nyilvánosan elérhető forrásokból származó információk összegyűjtésére használt eszközöket, eljárásokat és technikákat.³⁶

³⁴ „GDPR Essentials for OSINT Research – Blockint”, elérés 2022. március 14., <https://www.blockint.nl/methods/gdpr-essentials-for-osint-research/>.

³⁵ Solti, „Az OSINT információgyűjtő eszközeiről”.

³⁶ „The Advantages of Open Source Intelligence (OSINT)”, *Cobwebs Webint Solutions* (blog), 2021. március 15., <https://cobwebs.com/the-advantages-of-open-source-intelligence-osint/>.

2. fejezet: Az OSINT eszköztárának áttekintése

Az 1. fejezet fogalmmeghatározását követően jelen fejezetben az eszköztár ismertetésére tesztek kísérletet.

2.1. Általános bevezetés

A dolgok internetével (Internet of Things, továbbiakban IoT) és a nagy adathalmazokkal kapcsolatos közelmúltbeli fejlemények miatt az adatmennyiség határtalanul megnőtt, és ez felgyorsította az OSINT fejlődését.³⁷ Jelen fejezetben az OSINT eszköztárának bemutatására tesztek kísérletet, azonban fontosnak tartom rögzíteni, hogy a létező összes OSINT technológiát szinte lehetetlen lenne prezentálni és egybegyűjteni, hiszen akár egyik napról a másikra jelenthetnek meg új platformok, eszközök, így dolgozatomban igyekszem csak a legelterjedtebb módszereket, technológiákat kiemelni, legyen szó akár keresőmotorokról, internetes eszközökről (továbbiakban tool), vagy akár konkrét alkalmazásokról.

Az egyének korábban soha nem létező módon teszik elérhetővé az információkat az interneten, beleértve a személyes érzelmek online kifejezését, a helyi helyekről és eseményekről készült fényképeket, valamint a nyilvánosságra hozott társadalmi és közösségi szakmai hálózataikat. Heather J. Williams és Ilana Blum publikációja révén megállapíthatjuk, hogy az olyan egyéb jellegű információk elérhetősége, mint például a dokumentumokban lévő metaadatok és a közösségi hálózatok adatai, még hasznosabbá tette a nyílt forrású információgyűjtést, ugyanakkor megnehezítette annak kezelését és átláthatóságát. Ennek okán kezdődtek meg különböző fajta automatizált eszközök, programok fejlesztése, amelyek adott esetben felgyorsíthatják és helyettesíthetik a manuális keresést, azonban az automatizált eszközparkok révén az OSINT egyre inkább összetettebbé válik nem csak a források, de a módszerek tekintetében is. Ezek az új módszerek és rendszerek magas szintű technikai ismereteket is igényelnek a nyilvánosan elérhető információkat gyűjtők és a feldolgozó elemzők számára.³⁸ A számítógépes teljesítmény és az adattudományi technikák összekapcsolódásával lehetővé teszik a nyilvánosan elérhető adatok tömegeinek megőrzését és feldolgozását. A gépi tanulás, a számítógépes algoritmusok és az automatizált következtetések tovább bővítik az

³⁷ Yong-Woon Hwang és mtsai., „Current Status and Security Trend of OSINT”, *Wireless Communications and Mobile Computing* 2022 (2022. február 18.): e1290129, <https://doi.org/10.1155/2022/1290129>.

³⁸ Heather J. Williams és Ilana Blum, „Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise” (RAND Corporation, 2018. január 1.), <https://apps.dtic.mil/sti/citations/AD1053555>.

Legnagyobb vonzerője, hogy web alapú platformról van szó, így nem kell semmit sem telepíteni a számítógépre. Az OSINT Framework által felsorakoztatott toolok többsége ingyenes, de egyes esetekben előfordulhat hogy egy-egy szolgáltatásért a szoftveren belül fizetni szükséges (pl. Maltego)⁴⁰ Azonban fontos azt is látni, hogy nem minden esetben tartalmaz naprakész eszközöket, hiszen például a Facebookra vonatkozó linkek 2019 óta nem bizonyulnak aktuális és hatékony OSINT eszköznek a közösségi oldal különböző adatvédelmi szabályozása végett.

2.2. Kereső motorok és az OSINT kapcsolata

A legelső támpont, amihez az ember fordul abban az esetben, ha információt szeretne szerzeni az internetről, azok a keresőmotorok. Mindannyian ismerjük a keresőmotorokat, és használjuk őket a mindennapi böngészéseink során.

Az internet alapvetően egy globális összeköttetéssel rendelkező, információban gazdag erőforrás. Olyan sok információ áll rendelkezésre, hogy egyfajta szervezettség nélkül a szükséges weboldalak megtalálása lehetetlennek tűnhet. A keresőmotor, más néven indexelő, lehetővé teszi az azonosítását és meghatározott internetes források lekérdezését kiválasztott téma vagy kulcsszó alapján az interneten, így valójában egy adatbázisról beszélhetünk, amely hivatkozásokat tartalmaz különböző forrásokra. A felhasználók lekérdezéseket nyújthatnak be és kapcsolatba léphetnek adatbázisokkal, hogy meghatározzák, melyek tartalmazzak források megfelelnek az adott keresésnek kritériumoknak.⁴¹ A keresőmotorok tulajdonképpen azt csinálják, hogy feltérképezik a webet és számos paraméter például kulcsszavak, visszautalások alapján indexelik a weboldalakat, majd ennek az indexelésnek alapján kapjuk meg az általunk megadott kulcsszavakra vonatkozó találatokat. A legnépszerűbb keresőmotorok közé tartozik a Google, a Yahoo, Yandex és a Bing. A különböző keresőmotorok különböző módszereket használnak a linkek értékelésére és algoritmusuk alapján weboldalakat és rangsorokat rendelnek hozzá. Amikor keresünk egy kifejezésre, a keresőmotorok ezen rangsorok alapján adnak találatokat. Ezek a rangok az eltérő tényezők alapján folyamatosan változnak, és ez az oka annak, hogy esetleg más-más eredményeket kapunk ugyanarra a lekérdezésre egy eltérő időpontokban.⁴²

⁴⁰ „How to Use OSINT Framework”, Cyurex, 2019. október 13., <https://www.cyurex.com/how-to-use-osint-framework/>.

⁴¹ Sudhanshu Chauhan és Nutan Kumar Panda, „Chapter 4 - Search the Web—Beyond Convention”, in *Hacking Web Intelligence*, szerk. Sudhanshu Chauhan és Nutan Kumar Panda (Boston: Syngress, 2015), 53–75, <https://doi.org/10.1016/B978-0-12-801867-5.00004-5>.

⁴² Chauhan és Panda.

2.2.1. Meta keresőmotorok

Amikor egy kérést küldünk egy szokványos keresőmotornak, az a saját adatbázisában keresgéli a megfelelő találatokat majd ezt követően meg is megjeleníti azokat. De mi a helyzet akkor, ha több keresőmotorból szeretnénk eredményeket kapni? Itt jönnek a képbe a meta keresőmotorok. A meta kereső lehetővé teszi a felhasználó számára, hogy egyetlen lekérdezést írjon be, de több forrásból is megkapja az eredményeket, ezzel elérhetővé téve a felhasználó számára, hogy gyorsan megszerezze a legjobb válaszokat az információk széles skálájából. A meta keresőmotorok nem hoznak létre saját adatbázist, hanem különböző más adatbázisokra támaszkodnak az eredmények összegyűjtéséhez, ezáltal a keresési eredmények átfogóbbá és relevánsabbá válnak, és a kereső számára időbeli megtakarítást jelent. Ilyen keresőmotor például a Polymeta, amely a keresési lekérdezést a források széles körére küldi, majd mindegyikből a legjobb eredményt veszi ki, és tovább rangsorolja őket. Jelenleg közel 800 kereshető forrás (tudományos adatbázisok, általános keresők, video, kép, hírforrások stb.) elérhető. A Polymeta keresési eredményei nem csak az URL-eket tartalmazzák, hanem a közösségi hálózatát is.⁴³

2.2.2. Shodan

Az előrejelzések szerint 2025-re 38,6 milliárd eszköz csatlakozik majd az internethez. A támadók folyamatosan keresik a sebezhetőségeket, hogy kompromittálják a szervezeteket és kijelenthetjük, hogy minden újonnan csatlakoztatott eszköz egy lehetséges gyenge pontot, fenyegetettséget kínál. A Shodan egy olyan keresőmotor, amely az interneten létező eszközöket és eszköztípusokat megtalálja. Míg a Google és más keresőmotorok csak a weboldalt futják végig, addig a Shodan szinte mindent indexel – webkamerákat, vízkezelő létesítményeket, jachtokat, orvosi eszközöket, jelzőlámpákat, szélturbinákat, rendszámleolvasókat, intelligens tévéket, hűtőszekrényeket stb.⁴⁴ A Shodan megkeresi az eszközöket és annyi adatot kinyer ki belőlük, amennyit csak tud, mindezt adatbázisba helyezi és ezt az adatbázist elérhetővé teszi a világ számára. A Google-lal ellentétben a Shodan nem indexel fájlokat és nem keres kulcsszavakra online. Ehelyett az internetre csatlakoztatott eszközök IP-címein keres portokat és szolgáltatásokat. Számos jellemző alapján képes azonosítani az eszközöket az interneten, például földrajzi és GPS-helyzetük, firmware-verziójuk, eszköztípusuk, szoftververziójuk, protokollverziójuk és

⁴³ Chauhan és Panda.

⁴⁴ „Shodan keresőmotor használata SOC-ban”, *Black Cell* (blog), 2020. augusztus 26., <https://blackcell.hu/shodan-keresomotor-hasznalata-soc-ban/>.

még sok más alapján. Rosszindulatú hackerek előszeretettel használják a Shodan-t, mert alkalmazhatják a kihasználható célpontok felfedezésére. Ilyen célpontok lehetnek például a nagyon specifikus szoftververziókat futtató ipari vezérlőrendszerek, a dolgok internetes eszközei, például a tévék, a nem védett kamerák, amelyek élő közvetítést folytatnak, az érzékeny információkat tartalmazó FTP-szerverek. Mindez úgy működik, hogy a hét minden napján, a nap 24 órájában folyamatosan feltérképezi az internetet. A feltérképezés azonban nem söpör végig az IP-címtartományokon, mint egy hálózati szkennel, például az Nmap vagy a MassCAN. ⁴⁵A Shodan bejárók teljes protokoll-specifikus kézfogást próbálnak végrehajtani annak megállapítására, hogy egy port nyitva vagy zárva van-e. Mivel számos intézkedés létezik a portok meghamisítására, az eszköz számos intézkedést hajt végre annak biztosítására, hogy az általa jelentett port valóban nyitva legyen. Bár az ingyenes, regisztráció nélküli verzió nagyon korlátozott információkat nyújt, ez a szolgáltatáshalmaz egy regisztrált fiók használatával némileg bővül, azonban az ingyenes verzió is elégséges ahhoz, hogy megértsük ennek az egyedülálló keresőmotornak az erejét. A Shodan aktív fejlesztési múlttal rendelkezik és gyakran új funkciókkal jelentkezik, így a jövőben sokkal több újdonságra számíthatunk tőle.⁴⁶

2.2.3. Google Hacking

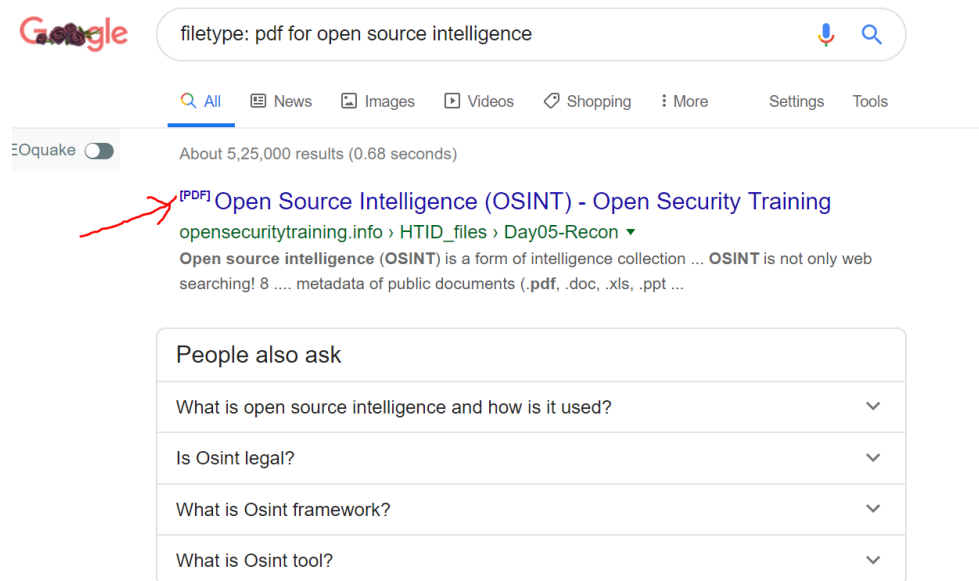
A "Google hacking" vagy „Google dorking” fogalma egészen 2002-re nyúlik vissza, amikor Johnny Long elkezdte gyűjteni azokat a Google keresési lekérdezéseket, amelyek sebezhető rendszereket és/vagy érzékeny információk felfedését mutatták ki majd Google Dorks-nek nevezve őket.⁴⁷ Azóta a Google Dorkok listája a lekérdezések nagy szótárává nőtte ki magát, amelyeket végül 2004-ben a Google Hacking Database adatbázisba szerveztek. A Google hackingben feltárt koncepciókat kiterjesztették más keresőmotorokra is, például a Bingre és a Shodanra. Mint ahogy azt a korábbiakban kifejtettem, a keresőmotorokat arra tervezték, hogy hatékonyan találjanak információt az interneten. Általában a felhasználók egyszerűen beírják a keresőszavakat (kulcsszavakat), és a keresőmotorok visszaadják a megfelelő információkat tartalmazó releváns weboldalakat. Azonban, a keresőmotorok támogatnak néhány speciális operátort is a viszonylag összetett kereséshez, mint például az inurl, intitle

⁴⁵ „A Shodan Tutorial and Primer”, Daniel Miessler, elérés 2022. március 29., <https://danielmiessler.com/study/shodan/>.

⁴⁶ „How to discover open RDP ports with Shodan”, Infosec Resources, elérés 2022. március 27., <https://resources.infosecinstitute.com/topic/how-to-discover-open-rdp-ports-with-shodan/>.

⁴⁷ Ma-No Web Design and Development, „Google Dorks: How to Find Interesting Data and Search like Hacker”, MA-NO Web Design and Development (<https://www.ma-no.org>), elérés 2022. március 28., <https://www.ma-no.org/en/security/google-dorks-find-interesting-data-search-like-hacker>.

és intext. Keresési lekérdezések ezekkel a speciális operátorokkal a Google Dorks nevet viselik.⁴⁸



2. ábra Filetype: elsősorban a fájltípusok megkeresésére vagy egy adott karakterlánc keresésére szolgál (Forrás: <https://geekflare.com/osint-tools/#anchor-google-dorks>)

A Google Dorks segítségével a felhasználók könnyen és egyszerűen gyorsabban találhatnak pontosabb keresési eredményeket, lekérdezései felhasználhatók a webalkalmazások biztonsági réseinek azonosítására, tetszőleges vagy egyedi célpontok információinak gyűjtésére, érzékeny információkat felfedő hibaüzenetek felfedezésére, hitelesítő adatokat és egyéb érzékeny adatokat tartalmazó fájlok felfedezésére.⁴⁹

2.3. Közösségi média, mint nyílt forrás

Köztudott tény, hogy a közösségi média ma már legtöbbünk életének szerves része és az emberek hajlamosak sokféle dolgot közzétenni a közösségi média fiókjaikon, például részleteket a személyes életükről, véleményüket egy adott dologról vagy eseményről, valamint képeket. Ahogy az OSINT Framework kapcsán az 1. ábrán is megfigyelhetjük, számos olyan tool létezik, amely csak is kizárólag a közösségi médiák adataiból „táplálkozik”, de általánosságban elmondható, hogy komplikáltabb automatizált alkalmazások is min-mind alapul veszik a közösségi média platformokat. A közösségi médiák esetében meglehetősen gyakori az eszközök tárházában a változás, hiszen

⁴⁸ J. Zhang, J. Notani, és G. Gu, „Characterizing Google Hacking: A First Large-Scale Quantitative Study”, *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST* 152 (2015): 602–22, https://doi.org/10.1007/978-3-319-23829-6_46.

⁴⁹ Sudhanshu Chauhan és Nutan Kumar Panda, „Chapter 5 - Advanced Web Searching”, in *Hacking Web Intelligence*, szerk. Sudhanshu Chauhan és Nutan Kumar Panda (Boston: Syngress, 2015), 77–99, <https://doi.org/10.1016/B978-0-12-801867-5.00005-7>.

különböző adatvédelmi szabályzásoknak igyekeznek a platformok szolgáltatói eleget tenni, ezzel is védve a felhasználók privát szféráját, azonban egy kevésbé körültekintő és biztonság tudatos felhasználó gyakran nem foglalkozik azzal, hogy vegye a fáradságot és ellenőrizze, hogy mely adatait osztotta meg a világ számára önkéntes módon.

A klasszikus hírszerzési ágak közt viszonylag újonnan, külön ággént jelent meg a közösségi médiában folytatott hírszerzés. A SOCMINT – habár már évek óta jelen van a szakirodalomban – terminológiai határai még mindig nem egyértelműek -. Alapesetben a tevékenység, az információgyűjtés hagyományos elemeinek a közösségi média felületeihez kapcsolódó folyamatait takarja. Természetesen módszerei a közösségi oldalak és az adatvédelmi szabályzások fejlődésével párhuzamosan változnak. Erdész Viktor értelmezése alapján a SOCMINT-ot az különbözteti meg az OSINT-tevékenységtől, hogy az érdemi információ kinyeréséhez, felhasználónévhez kötött online profil szükséges”.⁵⁰ Azonban létezik olyan értelmezés is, ami alapján úgy határozták meg, SOCMINT-tot mint az OSINT vagy a SIGINT (egyések szerint HUMINT) egyik álgazata részterülete, amely a közösségi média webhelyekről gyűjtött információkra vonatkozik. A közösségi oldalakon elérhető adatok lehetnek nyilvánosak (pl. nyilvános bejegyzések a Facebookon vagy a LinkedIn-en) vagy privátak. Azon adatok esetében, amelyhez szükséges, hogy a felhasználóval előzetesen valamilyen interakcióba lépünk (pl. egy ismerősnek jelölés, visszajelölés) már érdemes elgondolkodni a kérdésen, hogy nyílt forrásként definiálhatjuk-e őket.

A közösségi oldalakon elérhető adatok két kategóriába sorolhatók:

- A felhasználó által közzétett eredeti tartalom – például Facebook szöveges tartalom vagy feltöltött kép/videó.
- Az eredeti tartalomhoz társított metaadatok – a multimédiás fájlok metaadatai, a dátum/ide és a közzétett tartalomhoz kapcsolódó földrajzi helyadatok.⁵¹

2.4. Legnépszerűbb alkalmazások, szoftverek

2.4.1. Maltego

A Maltego az egyik legelterjedtebb OSINT platform, amely számos ingyenes és fizetős funkcióval rendelkezik. A szoftver betekintést nyújt arról, hogy hogyan kapcsolódnak egymáshoz a különböző közösségi média platformok a személyekhez, entitásokhoz,

⁵⁰ Dobák Imre és Tóth Tamás, „Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering)”, *Belügyi Szemle* 69, sz. 2 (2021. február 15.): 195–212, <https://doi.org/10.38146/BSZ.2021.2.2>.

⁵¹ „A Guide To Social Media Intelligence Gathering (SOCMINT)”, Secjuice, 2020. június 21., <https://www.secjuice.com/social-media-intelligence-socmint/>.

továbbá képes meghatározni a valós világ és az internetes infrastruktúra (legyen szó akár domain-ekről, DNS nevekről, IP címekről) közötti kapcsolatot. Alapvetően kliens-szerver architektúrán alapul, ami azt jelenti, hogy felhasználóként egy Maltego klienst kapunk, amely a használat során kölcsönhatásba lép egy szerverrel, hogy elvégezze a műveleteket.⁵² A Maltego sok időt takarít meg az elemzőnek az információk bányászása és összegyűjtése, valamint a kinyert információk könnyen érthető formában történő megjelenítése során. Számos OSINT eszköz áll rendelkezésre a piacon, de ez az eszköz kiemelkedik a többi közül egyedülálló képességei miatt, hiszen egy grafikus felhasználói felületet biztosít. Az összes információt könnyen érthető entitás-kapcsolat modellben jeleníti meg, továbbá az adatok különböző forrásokból történő kinyerése mellett más forrásokból származó adatokat is felvehetünk, és beilleszthetjük a gráfba, hogy egy nagyobb képet alkossunk. Ehhez egyszerűen csak ki kell vennünk a megfelelő entitástípust a bal oldali entitási sávból és be kell hoznunk a gráfba, majd beilleszteni a talált adatokat, és egyszerűen összekapcsolni a megfelelő entitással vagy entitásokkal. Ha nem találjuk az adattípusnak megfelelő entitást, a Maltego lehetővé teszi számunkra, hogy új entitást hozzunk létre, és azt igényeinknek megfelelően használjuk. Ezáltal nagyon könnyen kihasználhatjuk az adatbányászati funkció előnyeit, és tovább bővíthetjük azt adatelemzési célokra. Az alkalmazás adatforrásai között szerepelnek DNS rekordok, keresőmotorok, közösségi hálózati szolgáltatások, különféle API -k és különböző metaadatok.⁵³ A Maltego jelenleg két változatban érhető el: kereskedelmi és közösségi. A kereskedelmi verzió fizetős és licenckulcsra van szükségünk hozzá. A közösségi verzió viszont ingyenes, és csak regisztrálnunk kell a Pateva (a Maltego készítője) oldalán.⁵⁴

2.4.2. TheHarvester

A kézi keresések időigényességét már az első fejezetben taglaltam, többek közt a penetrációs tesztek során is előnyös, ha automatizált rendszerek végzik a pentesztetek helyett az információgyűjtést. Számos eszköz létezik, amely leegyszerűsíti és felgyorsítja a manuális keresés folyamatot, azonban fontos megemlíteni, hogy minél hatékonyabbak az ilyen eszközök, annál jobban elterjednek és egyre kevesebben fogják használni a

⁵² Samer Al-khateeb és Nitin Agarwal, „Social Cyber Forensics: Leveraging Open Source Information and Social Network Analysis to Advance Cyber Security Informatics”, *Computational and Mathematical Organization Theory* 26, sz. 4 (2020. december 1.): 412–30, <https://doi.org/10.1007/s10588-019-09296-3>.

⁵³ „How to Conduct Person of Interest Investigations Using OSINT & Maltego”, elérés 2022. március 29., <https://www.maltego.com/blog/how-to-conduct-person-of-interest-investigations-using-osint-and-maltego/>.

⁵⁴ „Discovering IoT Vulnerabilities Using Updated Shodan Transforms”, elérés 2022. március 27., <https://www.maltego.com/blog/discovering-vulnerabilities-using-shodan-transforms/>.

kereskedelmi keresőket, így a nagyágyúk, mint a Google és Bing folyamatosan küzdenek azért, hogy megnehezítsék ezt az automatizált keresési módszert.⁵⁵

A Theharvester egy hatékony Python-script, amelyet Christian Martorella írt az Edge Security-től. Alapvetően elmondható, hogy a penetrációs tesztek korai szakaszában való használatra tervezték. Használ nyílt forráskódú információgyűjtést és segíti a fenyegetések meghatározását, információkat gyűjthet, például e-maileket, aldomaineket, gazdagépeket, alkalmazottak neveit, nyitott portokat és szalaghirdetéseket különböző nyilvános forrásokból, például keresőkből.⁵⁶

2.4.3. Spiderfoot

A Spiderfoot egy python programozási nyelven írt keretrendszer, melynek használatához telepíteni kell a pythont Kali Linux operációs rendszerben. Célja, hogy automatizálja az információgyűjtés folyamatát egy adott célponttól, amely lehet IP-cím, tartománynév, gazdagépnév, hálózati alhálózat, ASN, e-mail cím vagy személy neve. A Spiderfoot használható támadó jellegű, azaz egy „fekete doboz” vizsgálat részeként, hogy információkat gyűjtsön a célponttól, továbbá védekezőképpen annak azonosítására, hogy egy adott szervezet vagy személy milyen információkat bocsát rendelkezésre szabadon a támadóknak részére.⁵⁷

2.4.4. SentiOne

SentiOne egyedülálló platformot kínál, amely lehetővé teszi az online beszélgetések nyomon követését, a közösséggel való kapcsolatfelvételt és ezek által az ügyfélszolgálat automatizálását.⁵⁸ Ez az eszköz megítélésem szerint funkcióját tekintve kilóg a sorból. A platform segítségével az előfizető olyan döntéseket hozhat valós idejű fogyasztói betekintés alapján, amely segítségével akár növelheti az ügyfélkörét, közösségi médiákon megjelenő trendek alapján fejlesztheti termékét, szolgáltatását, valamint akár egy adott márka online hírnevével kapcsolatos anomáliákat és válságokat is képes kezelni.⁵⁹ Az

⁵⁵ Z. Terneva, I. Vladimirov, és D. Nikolova, „Accessing LinkedIn and Google E-Mail Databases Using Kali Linux and TheHarvester”, 2021, 59–62, <https://doi.org/10.1109/ICEST52640.2021.9483460>.

⁵⁶ „Python TheHarvester - How to Use It?”, *GeeksforGeeks* (blog), 2020. május 26., <https://www.geeksforgeeks.org/python-theharvester-how-to-use-it/>.

⁵⁷ S. Karthika és mtsai., „NoRegINT—A Tool for Performing OSINT and Analysis from Social Media”, in *Inventive Computation and Information Technologies*, szerk. S. Smys és mtsai. (Singapore: Springer, 2021), 971–80, https://doi.org/10.1007/978-981-33-4305-4_71.

⁵⁸ A. Gillies, „Improving the Quality of Information Security Management Systems with ISO27000”, *The TQM Journal* 23, sz. 4 (2011): 367–76, <https://doi.org/10.1108/17542731111139455>.

⁵⁹ „SentiOne - Crunchbase Company Profile & Funding”, Crunchbase, elérés 2022. március 30., <https://www.crunchbase.com/organization/sentione>.

alkalmazás ön-osint szempontjából megközelítve is hasznosnak bizonyulhat a szervezetek életében, gondoljunk csak a reputáció kérdésére. Manapság már a közösségi média oldalakhoz nyúl abban az esetben is az ember, ha szimplán egy szolgáltató, vagy termék minőségéről szeretne tájékozódni, a visszajelzés pedig minden szolgáltató, cég életében megkülönböztetett szerepet tölt be.

2.4.5. Facepager

A Facepager egy Jakob Jünger és Till Keyling (2019) által webes automatikus adatlekérdezésre fejlesztett alkalmazás. A program lényegében képes letölteni a közösségi médiából származó adatokat, leginkább kommenteket YouTube-ról, Twitterről, a Facebookról és az Amazonról.

2.5. OSINT eszközök felhasználási módjai

Az előző alfejezetekben példaként bemutatott eszközök csak egy miniatűr részét képezik az eszköztár egészének, azonban jogosan merülhet fel bennünk a kérdés, hogy mindezen technológiák halmazát hogyan tudjuk akár a mindennapi munkavégzés során alkalmazni, hasznosítani. Véleményem szerint abban az esetben, ha OSINT felhasználásról beszélünk érdemes elkülöníteni az állami szférában történő alkalmazását a versenyszférában történő alkalmazástól.

A korábbiakban már szó esett arról, hogy az OSINT-ot a 9 (vagy egyes értelmezések szerint 10) hírszerzési ág egyikeként is értelmezik és hogy az összadatforrású hírszerzés organikus részeként tekintünk rá, azonban nem esett még szó a nemzetbiztonság betöltött lényeges döntéstámogatói szerepéről. Fontosságára Szabó Károly publikációja is rámutat, miszerint ma már szinte elképzelhetetlen, hogy egy döntéshozónak szóló tájékoztató a nyílt forrású információszerzés lehetőségeinek felhasználását mellőzve készüljön. A nyíltan hozzáférhető információk exponenciálisan növekvő mennyisége miatt az OSINT egyre nagyobb hangsúlyt kap a felhasználók információigényeinek kielégítésében, így a döntéshozók számára összeállított jelentések elkészítése során is. Döntéshozói tájékoztató tevékenységet pedig minden szolgálat végez. Noha a nyílt forrásokból származó információk nem helyettesíthetik a minősített információkat, de számos téren képesek kiegészíteni azokat.⁶⁰ Ahhoz, hogy az adatokat a döntéshozatal elősegítésére használhassuk fel, azokat különböző, egymást követő lépésekben kell feldolgozni. A belső adatok

⁶⁰ Szabó Károly, „Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről”, *Nemzetbiztonsági szemle* 7, sz. 2 (2019): 68–82, <https://doi.org/10.32561/nsz.2019.2.6>.

információvá, tudássá és intelligenciává alakításának folyamata sokféleképpen elvégezhető a különböző iparágakban működő különböző típusú szervezetek számára.⁶¹

Az állami szférán belül a bűnüldöző szervek is gyakran az OSINT forrásait használja fel, hogy megvédjék az állampolgárokat a visszaélésektől, a személyazonosság-lopástól és más bűncselekményektől. Ez úgy történik, hogy figyeli a közösségi média csatornáit olyan kulcsszavak és fényképek után kutatva, amelyek segítenek megelőzni a bűncselekményeket, mielőtt azok növekednének vagy bekövetkeznének. A bűnüldöző szervek az OSINT segítségével figyelik és követik nyomon a bűnözői hálózatokat számos országban. Például az OSINT-ot használva információkat gyűjtenek a bűnözőkről majd teljes profilt készítenek róluk. Ezenkívül OSINT forrásokat használnak az online hamisítások és a szerzői jogok megsértésének nyomon követésére.

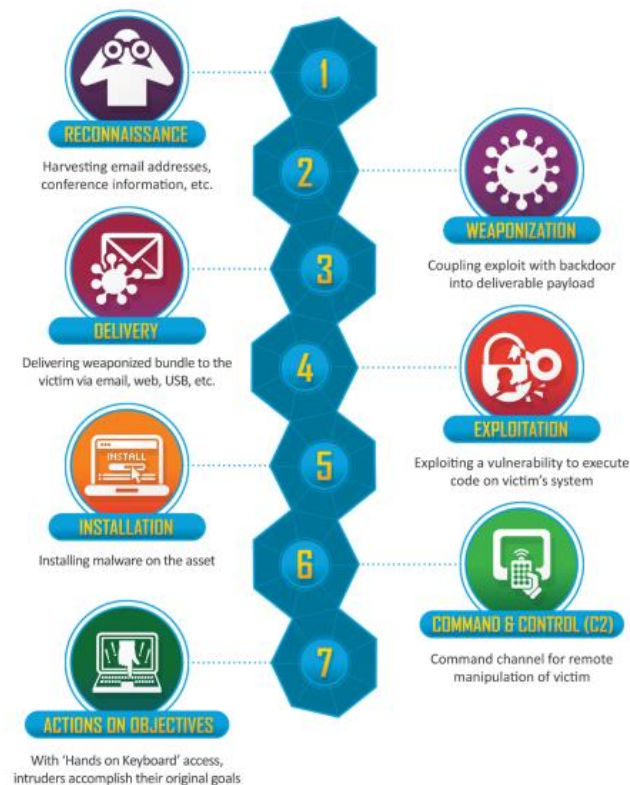
Az üzleti társaságok szempontjából már-már klisének számít azt állítani, hogy az információ hatalom, azonban ez a közhely sokszor bizonyul relevánsnak. A vállalkozások OSINT-forrásokat használnak új piacok felkutatására, a versenytársak tevékenységeinek nyomon követésére, marketingtevékenységek megtervezésére, és minden olyan előrejelzésre, ami befolyásolhatja a jelenlegi működést és a jövőbeli növekedést. Korábban az OSINT források felhasználása a kellő büdzsével rendelkező nagyvállalatokra korlátozódott, manapság azonban az internet széles körű elterjedtsége miatt a korlátozott költségvetésű kisvállalatok is használhatják az OSINT forrásait, és beépíthetik üzleti terveikbe a megszerzett információkat.⁶²

A biztonsági szakemberek OSINT segítségével is azonosíthatják a hálózatok lehetséges gyenge pontjait, hogy azokat orvosolhassák, mielőtt a támadók kihasználnák azokat, továbbá penetrációs teszteként konkrét információgyűjtési folyamatot, azaz tulajdonképp felderítést is szokás végrehajtani, melynek során a lényeg, hogy a célponttal, szervezettel kapcsolatos összes nyíltan elérhető információt összegyűjtésük. Azonban fontos látni az érem másik oldalát: ezt a fajta felderítést nem kizárólag az etikus hackerek tudják elvégezni, akiket szigorú szerződés köt arra vonatkozóan, hogy mely rendszereket vehetik górcső alá a penetrációs tesztek folyamata alatt, de értelemszerűen rosszindulatú támadók is élhetnek a nyílt források nyújtotta a lehetőségekkel. Erre kitűnően rámutat a

⁶¹ Hüseyin Akarslan, „A Model Proposal for Analyzing Open-Source Information in End-User Computers”, *International Journal of Intelligence and CounterIntelligence* 0, sz. 0 (2021. június 7.): 1–22, <https://doi.org/10.1080/08850607.2021.1899514>.

⁶² Hwang és mtsai., „Current Status and Security Trend of OSINT”.

Lockheed Martin repülőgép gyártó vállalat alkotta 7 lépcsős cyber kill chain modell, melynek első lépése „reconnaissance” azaz felderítés kifejezést viseli.



3. ábra Cyber kill chain modell (Forrás: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>)

Következtetések

Ebben a fejezetben egyfajta betekintést igyekeztem biztosítani az OSINT eszköztárára vonatkozóan. Első körben kitértem az OSINT Framework weblap alapú gyűjteményre, mely számos ingyenes eszközt gyűjt össze egy helyen, ezt követően az OSINT Framework kategóriáinak mentén bemutattam a keresőmotorok relevanciáját az OSINT tevékenységgel összefüggésben, továbbá kitértem a Shodan elnevezésű keresőmotorral, amely az egyik legelterjedtebb platform abban az esetben, ha IOT eszközök kereséséről van szó.

A továbbiakban vizsgáltam a közösségi média és az OSINT kapcsolatát, melynek alapján megállapítottam, hogy a nyílt forrásból elérhető információk nagy részét fedi le a közösségi platformokról megszerezhető információ, abban az esetben, ha konkrét személlyel kapcsolatban szeretnénk információkat gyűjteni. A fejezetben kitértem még a legnépszerűbb alkalmazásokra, melyek mind-mind különböző funkcionalitásuk miatt számítanak hatékony eszköznek. Végezetül pedig a felhasználási módszereket igyekeztem összegezni és a szakirodalmak átvizsgálását követően konstatáltam, hogy az OSINT már

nem csak az állami szférában és a nagyvállalati környezetben nyújthat hatékony megoldást számos helyzetre, költséghatékonysága végett egyre inkább elérhetővé válnak a korlátozottabb költségvetésű kisvállalatok részére.

3. fejezet: A hazai kis- és középvállalkozások információbiztonsági gyakorlata

Jelen fejezet célja, hogy megvizsgáljam a hazai kis- és középvállalkozások OSINT-hoz való hozzáállását.

3.1. Mit nevezünk kis- és középvállalkozásnak?

Mindenekelőtt fontosnak tartom a kis- és középvállalkozás fogalmát tisztázni. Magyarországon a kis- és középvállalkozások fogalmát a 2004. évi XXXIV. törvény (kkv tv.) határozza meg.⁶³ A jogszabály szerint azon szervezetek sorolhatók e kategóriába, amelyek létszáma legfeljebb 249 fő, éves nettó árbevétele nem éri el az 50 millió eurót, vagy mérlegfőösszege nem haladja meg a 43 millió eurót és az állam vagy az önkormányzati közvetlen vagy közvetett tulajdoni részesedése külön-külön vagy együttesen nem haladja meg a 25%-ot. A statisztikai lehatárolás a létszámkategória szerint történik. Ez alapján a legfeljebb 49 főt foglalkoztató szervezetek kisvállalkozásnak – ezen belül a 10 fő alattiak mikro vállalkozásnak –, az 50–249 fővel működők középvállalkozásnak minősülnek.⁶⁴

3.2. A kis- és középvállalkozások információbiztonsággal összefüggő kihívásai

A kkv-szektor szereplői számos gazdasági kihívással néznek szembe, s a szektornak információbiztonsági szempontból sincsen könnyű dolga. Miért is fontos foglalkozni ezen szervezetek információbiztonságával annak ellenére, hogy olykor a munkavállalók száma a húsz, harminc főt sem haladja meg? Ebben az alfejezetben ezt a kérdéskört igyekszem körbejárni több megközelítésben.

A kkv-k sérülékenységet 2020-ban az Európai Unió által kiadott kiberbiztonsági stratégia⁶⁵ is taglalja, továbbá különböző, vissza nem térítendő támogatásokkal ösztönzi, támogatja a szektort a kiberbiztonsággal kapcsolatos kihívások leküzdésében. 2018-ban a PWC által lebonyolított felmérésből⁶⁶ jól látszik, hogy „vállalkozások több mint kétharmada, különösen a kkv-k „újoncnak” számítanak a kiberbiztonság területén, és az európai vállalkozások felkészültsége alacsonyabbnak tekinthető, mint az ázsiai és amerikai vállalatoké.”⁶⁷

⁶³ „2004. Évi XXXIV. Törvény a Kis- És Középvállalkozásokról, Fejlődésük Támogatásáról - Hatályos Jogszabályok Gyűjteménye”, elérés 2022. április 2., <https://net.jogtar.hu/jogszabaly?docid=a0400034.tv>.

⁶⁴ „A kis- és középvállalkozások jellemzői, 2017”, 2017, 14. <https://www.ksh.hu/docs/hun/xftp/idoszaki/pdf/kkv17.pdf>

⁶⁵ „Közös közlemény az európai parlamentnek és a tanácsnak az eu kiberbiztonsági stratégiája a digitális évtizedre” (2020), <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020JC0018>.

⁶⁶ „Global State of Information Security ® Survey 2018 – Singapore highlights”, elérés 2022. április 11., <https://www.pwc.com/sg/en/publications/global-state-of-information-security-survey-2018-sg.html>.

⁶⁷ KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Az EU kiberbiztonsági stratégiája a digitális évtizedre.

Az üzleti szféra számára az egyik legfontosabb védendő adat az üzleti titok, azonban szintén egy, a PWC által publikált felmérés szerint a vállalatok, különösen a kkv-k, továbbra is kevéssé vannak tudatában, hogy az üzleti titkok technológiai módszerekkel ellophatók.⁶⁸ Magyarországon az üzleti titok védelméről szóló 2018. évi LIV. törvény szabályozza ezt a területet,⁶⁹ a törvény alapján üzleti titoknak minősül „a gazdasági tevékenységhez kapcsolódó, titkos - egészben, vagy elemeinek összességként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennél fogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja”⁷⁰. Tehát mindennapi munkavégzésünk során keletkezett, felhasznált adatainkat (az üzleti titkokat beleértve) védeni szükséges, a bizalmasság, sértetlenség, rendelkezésre állás elve mentén, hiszen ezek az adatok, információk a szervezet saját működésének felételeit is jelentik. Tovább gondolva a helyzetet pedig megállapíthatjuk, hogy abban az esetben, amikor egy kkv beszállítói funkciókkal is rendelkezik (azaz árut szállít vagy szolgáltatást nyújt egy nagyobb, akár multinacionális vállalat számára), nem csak a saját működése szempontjából nélkülözhetetlenek, hogy gondosan kialakított információbiztonsági kontrollok mentén működjön, hanem egyaránt az üzleti kapcsolatait is képes befolyásolni egy esetleges kevésbé biztonságos szervezeti környezet.

A nagy szervezetek manapság számos kisebb partner és vállalkozó által nyújtott szolgáltatásokra támaszkodnak. Ezeknek a kisebb cégeknek bizonyos szintű hozzáférést kell biztosítani a nagy szervezetek információs rendszereihez, hogy teljesíteni tudják üzleti szerződéseiket. A szervezeti információs rendszerekhez való hozzáféréssel a partnerek és vállalkozók olykor a vállalati hálózat részévé is válhatnak. Tekintettel arra, hogy a biztonsági fenyegetések és támadások bármely, a globális hálózathoz csatlakozó gépről kiindulhatnak, a kkv-k a hálózat "leggyengébb láncszemeként" működnek.⁷¹ Az ellátási lánc fenyegetésének súlyossága tavaly decemberben mutatkozott meg tömegesen, amikor kiderült, hogy hackerek feltörték a SolarWinds céget és rosszindulatú kódokat telepítettek

⁶⁸ „Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber”, é. n., 12.

⁶⁹ 2018. évi LIV. törvény az üzleti titok védelméről <https://net.jogtar.hu/jogszabaly?docid=A1800054.TV>

⁷⁰ <https://net.jogtar.hu/jogszabaly?docid=A1800054.TV>

⁷¹ Anas Tawileh, Jeremy Hilton, és Stephen McIntosh, „Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach”, in *ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference*, szerk. Norbert Pohlmann, Helmut Reimer, és Wolfgang Schneider (Wiesbaden: Vieweg, 2007), 331–39, https://doi.org/10.1007/978-3-8348-9418-2_35.

az Orion informatikai felügyeleti eszközében. Bármennyire is megdöbbentő volt ez a művelet, a SolarWinds nem egyedülálló. Súlyos ellátási lánc támadások évek óta sújtják a vállalatokat szerte a világon.⁷² Ugyan a SolarWinds sem a magyar, sem az amerikai terminológia szerint nem minősül kis- és középvállalatnak, az ügy kiválóan szemlélteti a beszállítók információbiztonságának fontosságát. Beszállító pedig nem csak nagyvállalat lehet, könnyen megeshet, hogy egy kkv-nak is egy vagy több multinacionális vállalatba történő beszállítás jelenti üzletifolyamatainak mozgatórugóját. Azonban fordítva is előfordult már ez a támadási forma. Az egyik legnagyobb hazai autóalkatrész-kereskedőnek számító UNIX Autó Facebook-oldalán közölte 2021-ben, hogy zsarolóvírus-támadás érte informatikai rendszereit, melynek alkalmával az ügyfelek nem érték el a kereskedő webáruházát, így közvetlen hatást gyakorolt volt a kisebb méretű saját üzleti partnereire, beszállítóira.⁷³

Az ellátási lánc információbiztonsági kihívásai végett alkotta meg a Német Autóipari Szövetség német autóipari szövetség (Verband der Automobilindustrie) az úgynevezett Trusted Information Security Assessment Exchange modellt, amelynek lényege, hogy az autó ipari beszállítók szereplők számára is egységesítse a kiberbiztonsági elvárásokat. Lényegében az ISO/IEC 27001-es szabványra építve biztosítja az adatok, információk, személyes adatok és prototípusok védelmét.⁷⁴ Azonban mit sem érnek ezek az útmutatóként szolgáltató szabványok, ajánlások abban az esetben, ha értelmezésük és a jó gyakorlatok implementálása nehézkesen megy egy alacsonyabb munkavállalói létszám és egy szűkösebb éves költségvetés esetén. Az Információbiztonsági Irányítási Rendszer (továbbiakban IBIR) jelentős elemei a tervezéssel, fejlesztéssel, megvalósítással és leszereléssel kapcsolatos költségek. Jelentős beruházásokat kell eszközölni a rendszer kiépítéséhez és megbízható, érzékeny és megbízható információbiztonsági rendszerek kiépítése és fenntartása érdekében.⁷⁵ A vagyoneleltárral egybekötött kockázatelemzés, üzletmenet folytonossági terv készítése és a jogosultságkezelés csak három példája annak a témérdek mennyiségű tevékenységnek, amely plusz feladatként felmerülhet például egy IBIR kialakítása során, így ezen feladatkörök szétosztása is nehézkesen történhet meg egy

⁷² Andy Greenberg, „What Is a Supply Chain Attack?“, *Wired*, elérés 2022. április 2., <https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/>.

⁷³ „Zsarolóvírussal támadták meg az egyik legnagyobb hazai autóalkatrész-kereskedőt”, *24.hu* (blog), 2021. április 1., <https://24.hu/tech/2021/04/01/zsarolovirus-ransomware-unix/>.

⁷⁴ „TISAX - A megfélelésen túl | Deloitte Magyarország”, *Deloitte Croatia*, elérés 2022. április 2., <https://www2.deloitte.com/hu/hu/pages/fogyasztoi-agazat/articles/tisax----a-megfélelesen-tul---deloitte-magyarorszag.html>.

⁷⁵ Tawileh, Hilton, és McIntosh, „Managing Information Security in Small and Medium Sized Enterprises”.

erőforrásokban szűkölködő szervezet életében. Meglátásom szerint a szerepkörökre is érdemes kitérni, főképp az információbiztonsági vezető személye végett. Kisebb vállalatoknál gyakran előforduló jelenség, hogy a cég informatikai vezetője viseli az információbiztonsággal kapcsolatos tisztséget egyaránt, mely jócskán hagy kivetni valót maga után.

A kisebb szervezeteket érintő nehézségekre reflektált a 2008-ban Közigazgatási Informatikai Bizottság által kiadott 25. számú ajánlása (Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/3.) amely Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX) nevet viseli.⁷⁶ 14 év távlatában mondhatjuk, hogy az ott leírt informatika tanácsok, jó gyakorlatok már nem minden esetben bizonyulnak relevánsnak a technológiai fejlődés végett és a dokumentum célközönsége egyébként is főképp az állami szektor kis szervezetei (pl. önkormányzatok), azonban ez a dokumentum is bizonyítja, hogy a kis szervezeteket érintő információbiztonsági és informatikai nehézségek által generált problémakör legkevésbé sem az elhanyagolható kérdések közé tartozik.

A nagy szervezetek manapság számos kisebb partner és vállalkozó által nyújtott szolgáltatásokra támaszkodnak. Ezeknek a kisebb cégeknek bizonyos szintű hozzáférést kell biztosítani a nagy szervezetek információs rendszereihez, hogy teljesíteni tudják üzleti szerződéseiket. A szervezeti információs rendszerekhez való hozzáféréssel a partnerek és vállalkozók olykor a vállalati hálózat részévé is válhatnak. Tekintettel arra, hogy a biztonsági fenyegetések és támadások bármely, a globális hálózathoz csatlakozó gépről kiindulhatnak, a kkv-k a hálózat "leggyengébb láncszemeként" működnek.

3.2.1 OSINT lehetőségek a kis- és középvállalati szektorban

Az alkalmazási módokra már korábban kitértem a 2.5. számú alfejezetben, ezúttal konkrétan azokat a megoldásokat igyekszem taglalni, melyet könnyen implementálhat bármelyik kkv. Véleményem szerint az első és legfontosabb dolog, amit különösebb erőfeszítések nélkül véghez vihetnek az az „ön-OSINT” végrehajtása és tájékozódás azzal kapcsolatban, milyen információk érhetőek el például a hivatalos weboldalon, illetve Facebook profilon kívül. Ezt könnyen véghez lehet vinni az OSINT Framework kapcsán prezentált ingyenes tool-ok segítségével. Amire még mindenképp felhívnam a figyelmet, azok a különböző oktató jellegű csatornák jelentősége a Youtube-on, melyek lépésről

⁷⁶ „KÖZIGAZGATÁSI INFORMATIKAI BIZOTTSÁG. 25. számú Ajánlása. Magyar Informatikai Biztonsági Ajánlások (MIBA) - PDF Ingyenes letöltés”, elérés 2022. április 4., <https://docplayer.hu/1361183-Kozigazgatasi-informatikai-bizottsag-25-szamu-ajanlasi-magyar-informatikai-biztonsagi-ajanlasok-miba.html>.

lépésre mutatnak be egyes OSINT tool-okat a legegyszerűbb web alapú platformoktól egészen a komplex szoftverekig.

3.3. Kis- és középvállalkozások nyílt forrású információszerzéssel kapcsolatos tudatossága és képessége

3.3.1. Kérdőív bemutatása

Kutatásom központi elemét az általam készített kérdőív jelentette, melyet csak is kizárólag olyan munkavállalók tölthettek ki, akik egy hazai kis- és középvállalkozásnál dolgoznak, netalántán vezetői pozíciót töltenek be. A kérdőívemre összesen 36 válasz érkezett. Ez a szám kitűnően rámutat arra a nehézségre, amivel szembesültem kutatásom során: a közösségi médiában történő többszörös megosztás ellenére is nehéz volt eljuttatni a kérdőívemet a releváns munkavállalók részére.

A kérdőív 2 fő részből állt össze. Az első öt kérdésben a szervezet jellegére, felépítésére voltam kíváncsi így létszámra, működési területre, székhelyre, valamint telephelyre vonatkozó kérdéseket fogalmaztam meg. Az első rész további pontjainál a szervezet információbiztonsági gyakorlatával kapcsolatban találtak kérdéseket a kitöltők, melynek során Tarján Gábor doktori értekezésében⁷⁷ szereplő felmérést ismételtam meg részben. 5 fokozatú Likert-skálákkal dolgoztam, a következő válaszlehetőségekkel:

- Egyáltalán nem értek egyet
- Nagyrészt nem értek egyet
- Közömbös számomra
- Nagyrészt egyetértek
- Teljes mértékben egyetértek

A kérdőív második részben pedig OSINT-tal kapcsolatban tettem fel kérdéseket. Összesen 10 olyan kitöltés érkezett, amikor egy 1-10 fős szervezetre vonatkozóan vette figyelembe a válaszadó a kérdéseket, 14 olyan, melynek során egy 11-50 fős vállalkozás volt az alap, továbbá 12 olyan válasz, amikor 51-250 fős vállalat volt a kiindulási alap.

3.3.2. Kérdőív kiértékelése

Kutatási eredményeim szöveges, statisztikai kiértékeléshez Dr. Németh Anikó: Adatelemzés statisztikai módszerekkel című publikációt hívtam segítségül. A H1 és a H2 hipotézisemet az SPSS program keretein belül Mann Whitney U próba segítségével

⁷⁷ Tarján Gábor, „Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben” (phd, Budapesti Corvinus Egyetem, 2020), <https://doi.org/10.14267/phd.2020015>.

elemeztem ki. A Mann Whitney U próba ordinális (rangsorolt) adatok esetén a mediánokat hasonlítja össze. Kontrollcsoportos vizsgálatnál alkalmazzuk, amikor két részmintát vagy mintát hasonlítunk össze nagyság szintjük alapján.⁷⁸ Arra voltam kíváncsi, hogy a két minta rangsora jelentős mértékben eltér-e egymástól. Ennél a vizsgálatnál a rangpontoszámok átlagának (Mean Ranks) is jelentősége van, sok információt hordoz: a kisebb átlagérték az adott részminta/minta rangsorban elfoglalt jobb helyzetére utal.

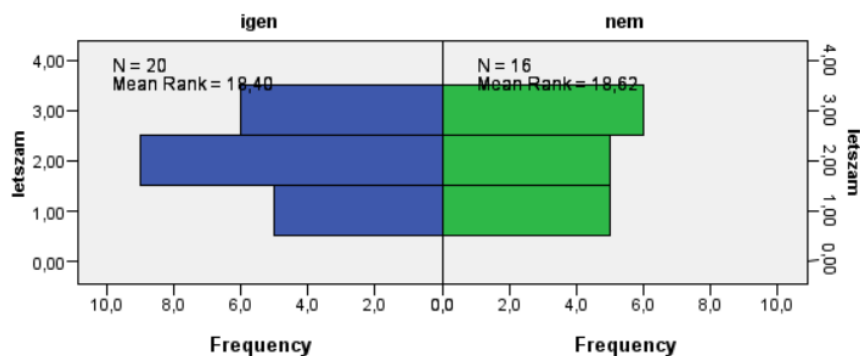
A H1 hipotézisem így szól: A nagyobb (munkavállalók számában mérve) kis- és középvállalkozások munkavállalói többször hallottak az OSINT-ről, mint azok, akik egy kisebb szervezetnél dolgoznak. A vizsgálat során kérdőívem első és tizenkettedik kérdését értékeltem ki, ezek a következők:

1. A szervezet mérete (munkatársi létszám) - alkalmazottak és a rendszerekhez hozzáférésekkel bíró külsős munkatársak összesen:

12. Hallott-e korábban az OSINT fogalmáról?

Az első kérdés esetében a munkavállalói létszámra vonatkozó 3 opció közül választhattak a kitöltők (1-10, 11-50, 51-250), míg a tizenkettedik kérdésnél „igen”, „nem” válaszokat tudtak adni. Az 4. ábrán található diagramon láthatjuk az elemszámokat az elemszámokat (N) és a rangpontoszámok átlagát (Mean Rank továbbiakban MR), melyek a következőképp alakultak:

⁷⁸Dr. Németh Anikó: Adatelemzés statisztikai módszerekkel http://eta.bibl.u-szeged.hu/458/1/EFOP343_AP2ETSK_jegyzet_N%C3%A9meth_Anik%C3%B3_Adatelemz%C3%A9s_s_tatisztikai_m%C3%B3dszerekkel_20180620.pdf



Total N	36
Mann-Whitney U	162,000
Wilcoxon W	298,000
Test Statistic	162,000
Standard Error	29,523
Standardized Test Statistic	,068
Asymptotic Sig. (2-sided test)	,946
Exact Sig. (2-sided test)	,962

4. ábra Képernyőfelvétel az SPSS program lefuttatott Mann Whitney U teszt eredményéről a H1 vonatkozásában

Az ábráról leolvashatjuk, hogy azok esetében, akik hallottak korábban az OSINT fogalmáról az MR=18,40, azok esetében, akik nem hallottak róla pedig MR=18,62.

Az eredményeket jól ábrázolja, ha összehasonlítjuk a csoportokra vonatkozó átlagos értékelési eredményeket, ezt a következő táblázat tartalmazza:

2. táblázat Átlagok a H1 hipotézisre vonatkozóan. (saját szerkesztés)

Hallott-e korábban az OSINT fogalmáról?	Átlag	Elemszám
1-10	1,5000	10
11-50	1,3571	14
51-250	1,5000	12
Összesen	1,4444	36

Jól láthatjuk, hogy mind az MR értékek, mind az átlagok rendkívül közel esnek egymáshoz. Az átlagos értékek azt mutatják meg, hogy azok a kitöltők, akik azt jelölték, hogy hallottak már az OSINT fogalmáról, nem feltétlenül tartoznak nagyobb létszámú szervezetekhez.

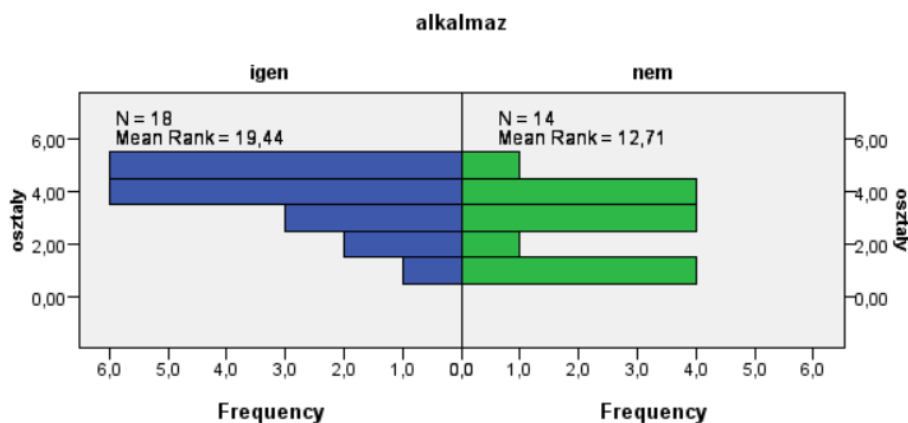
A szignifikanciát, tehát azt, hogy van-e jelentős különbség a két csoport között pedig a 4. ábráról olvashatjuk le. Szignifikanciáról akkor beszélhetünk, ha a p érték kisebb mint 0,05. Estünkben a $p=0,946$; $U=162,00$, így szignifikanciáról nem beszélhetünk, tehát nincs jelentős különbség a két csoport között. Ezzel a H1 hipotézisem megdőlt. Érdekességképp megjegyezném, hogy az összes kitöltő 55,6%-a, azaz 20 ember jelölte azt, hogy hallott korábban az OSINT fogalmáról, míg 44,4% százalék, azaz 16 embere jelezte azt, hogy soha nem hallotta még a fogalmat.

A H1 hipotézisem vizsgálatát követően áttértem a H2 hipotézisemre. A H2 hipotézisem a következő: Azok a kis- és középvállalkozások, akik alkalmaznak OSINT technológiát, átlagosan nagyobb biztonsági szintre értékelik saját magukat, mint akik nem alkalmaznak. Az elemzés során kérdőívem 11. és 13. kérdését elemeztem ki. A kérdések így szólnak:

11. Kérem, az előző kérdések fényében értékelje saját szervezetének információbiztonsági érettségét

13. Tudomása szerint alkalmaznak a szervezetében OSINT tevékenységet?

A 11. kérdés esetében 5 szint közül választhatták ki a kitöltők az ideálisat: (1=nem létező biztonsági érettség, 2=tervezés alatt, 3=alacsony, 4=elfogadható, 5=kifinomult) A 13. kérdés esetében három válaszlehetőség közül tudtak választani a kutatásban részt vevők, (1=Igen, 2=nem, nem tudom) azonban, az adatok helyes kiértékelésének végett adattisztítást végeztem, melynek során kitöröltem azokat a válaszokat, akik a „nem tudom” opciót adták meg, így az összes 36 kitöltés helyett csak 32 válaszadást értékeltem.



Total N	32
Mann-Whitney U	73,000
Wilcoxon W	178,000
Test Statistic	73,000
Standard Error	25,588
Standardized Test Statistic	-2,071
Asymptotic Sig. (2-sided test)	,038
Exact Sig. (2-sided test)	,045

5. ábra Képernyőfelvétel az SPSS program lefuttatott Mann Whitney U teszt eredményéről a H2 vonatkozásában

Hasonlóan a 4. ábrához, az 5. ábrán láthatjuk a H2-re vonatkozó elemszámokat (N) és a rangpontszámok átlagát (MR). Leolvashatjuk, hogy az OSINT tevékenységet alkalmazók esetében az MR= 19,44, a nem alkalmazók esetében pedig MR= 12,71. Az átlagokat itt is egy táblázat segítségével szemléltetem:

3. táblázat Átlagok a H2 hipotézisre vonatkozóan. (saját szerkesztés)

Alkalmaz-e OSINT tevékenységet	Átlag	Elem szám
igen	3,7778	18
nem	2,7857	14
Összesen	3,3438	32

Az átlagos értékek azt mutatják meg, hogy az OSINT-ot alkalmazók (tehát aki, az igen választ jelölte) között magasabb a kkv-k érettségi szintje (kihangsúlyoznám, hogy önértékelésről van szó), hiszen az igen esetében 3,7778 az átlag, a nem esetében pedig 2,7857. Ezekből az átlagokból láthatjuk, hogy azok közül, akik alkalmaznak OSINT tevékenységet magasabb érettségi szintet választottak maguknak, de nem tudjuk még, hogy a két csoport között jelentős-e (szignifikáns-e) a különbség. Ezt a 5. ábrán található táblázatból olvashatjuk le. Ebben az esetben a $p=0,038$; $U=73,000$ így ezek alapján mondhatjuk, hogy szignifikáns különbség van aközött, hogy milyen érettségi szintre osztották be saját magukat azok, akik alkalmaznak OSINT tevékenységet és azok, akik azt jelölték, hogy nem alkalmaznak OSINT tevékenységet. Megállapíthatjuk, hogy átlagosan a magasabb biztonsági érettségű kkv-k esetébe jelenik meg az OSINT tevékenység. Ezzel a H2 hipotézisemet alátámasztottam.

3.3.3. OSINT teszt végrehajtása egy hazai kis- és középvállalkozásra vonatkozóan

A H3 hipotézis esetében a korábbi kettő hipotézis vizsgálattól eltérő módszert alkalmaztam. Arra voltam kíváncsi, hogy egyszerű, internetes alapú OSINT tool-ok mennyire visznek közel egy adott hazai kkv-hoz. Abból kiindulva, hogy az OSINT tevékenységek során gyakran futhatunk úgynevezett „fals pozitív” találatokba egyfajta dilemmával indultam neki a kutakodásnak, arra vonatkozóan, hogy mit tekintsek a vizsgálat tárgyának. Mivel a 2. fejezetben bemutatott Cyber Kill Chain modell felderítés pontjánál az e-mail címek voltak megnevezve, így ebből kiindulva a H3 hipotézisem során ezt igyekeztem reprodukálni. A H3 hipotézisem a következő: OSINT toolok segítségével olyan információk is megszerezhetők, amelyek nincsenek feltüntetve a vizsgált szervezet hivatalos honlapján. Véleményem szerint fontos, hogy kellő körültekintéssel bánjunk vállalati e-mail címünkkel, hiszen ezen e-mail címek személyes használatra történő alkalmazása veszélybe sodorhatja a szervezeteket. Ha az e-mail hitelesítő adatok veszélybe kerülnek, a vállalati fiókok könnyen válhatnak eltérítés áldozatává, melynek során a támadó birtokában kerülhet a jelszó is.

A vizsgálatot három internetes OSINT tool-al kezdtem, ezek a következők: <https://hunter.io/>, <https://phonebook.cz/> és a <https://clearbit.com/> Gmail levelező felületére beépülő kiegészítője. A hunter.io elnevezésű platform az OSINT framework weboldalon szereplő gyűjteményben is megjelenik, azonban fontos azt is látni, hogy a felsorolt az eszközök főképp marketing célokra készültek, annak érdekében, hogy minél több potenciális üzleti partner képes legyen egymást a partner levelezőlistákra felvenni.

A vizsgálatom alap kiinduló pontjának tekintem azt a tényt, hogy a górcső alá vett hazai kkv hivatalos honlapján csupán csak egy e-mail elérhetőség található meg, melyet nem lehet kötni egy munkavállaló személyéhez sem, hiszen az alábbi módon képződik: cégnév@cégnév.com. A korábban felsorolt három platformon lefuttattam egy-egy keresést, mely jócskán dobott ki találatokat. Az eredményeket, találatokat a következő táblázatban foglaltam össze:

4. táblázat H3 hipotézisemre vonatkozó eredmény szemléltetése. (saját szerkesztés)

Pozíció	hunter.io	phonebook.cz	clearbit
Alapító tulajdonos	X	X	
Ügyvezető		X	
Üzletfejlesztési menedzser	X	X	X
HR igazgató		X	
Senior toborzási szakértő		X	
Senior szoftvermérnök		X	
Marketing és márka menedzser	X		
Adatvédelmi tisztviselő	X	X	

A „X” jelen esetben a találatot jelenti, tehát azt, hogy az adott platformon történő keresés eredményesen megjelenítette az adott pozíciót betöltő személy e-mail címét. A legtöbb e-mail címet a phonebook.cz elnevezésű platform találta, azonban fontos megemlíteni, hogy számos olyan eredményt is megjelenített, amelyek régi kollégákhoz tartozó e-mail címek, míg a hunter.io ilyen tekintetben naprekészebbnek bizonyult. Egyedül az üzletfejlesztési menedzser elérhetősége található mindhárom platformon, ez valószínűleg a már korábbiakban emlegetett marketinges okok miatt fordulhat elő. Fontosnak tartom megjegyezni, hogy a LinkedIn, mint a világ legnagyobb üzleti közösségi hálózata egyaránt

tartalmazhat számos e-mail címet, ezt az eshetőséget jelen esetben nem vizsgáltam, hiszen épp az automatizált OSINT keresések eredményére és pontosságára voltam kíváncsi, továbbá azt is lényegesen tartom kiemelni, hogy azért esett a választásom ezekre az OSINT eszközökre, mert bárki által ingyen elérhető eszközökről van szó, nincs szükség előfizetésre, így akár egy pénzügyileg szűkös helyzetben lévő szervezet is könnyen tudja alkalmazni.

Következtetések

Ebben a fejezetben az OSINT és hazai kis- és középvállalkozások kapcsolatát taglaltam. Összességében a szakirodalmak átvizsgálását követően megállapítottam, hogy a nagy vállalatok és kis- és középvállalkozások közötti szakadék az információbiztonság terén a technológiai fejlődések mentén jelentősen nőtt, ami főképp a kkv-k számára rendelkezésre álló források szűkösségének következménye. A fejezetben bemutattam, hogy szűkös erőforrások ellenére számos olyan megoldás érhető el az interneten, melyek képesek hatékonyan hozzájárulni az úgynevezett „ön-osint” folyamathoz (pl. google dorks, az említett e-mail keresésre szakosodott weboldalak), azonban a probléma gyökerét nem kizárólag az anyagi tényezők jelentik, sokkal inkább gondot jelent az a tény, hogy véleményem szerint nem látják még a potenciált és a teljesítőképességet az OSINT megoldásokban.

Összegzett következtetések

Kutatásom arra világított rá, hogy számos OSINT technológia áll rendelkezésre mind a magánszemélyek, mind a gazdálkodó társaságok számára. Ezek implementálása nem történt meg a szervezetek életében, vagy pedig számos helyen kimerül a potenciális új munkavállaló közösségi médiában történő ellenőrzésével.

Felmerült bennem a gondolat, miszerint a hazai kkv-k esetében befolyásoló tényezőként játszik szerepet a szervezet mérete, azaz a foglalkoztatottak száma annak vonatkozásában, hogy hallottak-e az OSINT fogalmáról vagy sem, azonban ezt T1 tézisem cáfolja.

T2 tézisem azonban igazolta, hogy átlagosan nagyobb biztonsági érettségi szintre osztotta be magát az a munkavállaló, aki úgy nyilatkozott, hogy alkalmaz a munkahelye OSINT tevékenységet.

T3 tézisem pedig alátámasztotta, hogy meglehetősen egyszerű és gyors módszerrel lehet számos e-mail címhez hozzájutni, annak ellenére, hogy a vizsgát szervezet hivatalos honlapján tudatosan nincsen publikálva egy személyhez köthető e-mail cím se.

Kutatási eredmények

A kutatási téma feldolgozása során az alábbi eredményeket értem el:

T1: A nagyobb (munkavállalók számában mérve) kis- és középvállalkozások munkavállalói többször hallottak az OSINT-ről, mint azok, akik egy kisebb szervezetnél dolgoznak.

T2: Azok a kis- és középvállalkozások, akik alkalmaznak OSINT technológiát, átlagosan nagyobb biztonsági szintre értékelik saját magukat, mint akik nem alkalmaznak.

T3: OSINT toolok segítségével olyan információk is megszerezhetők, amelyek nincsenek feltüntetve a vizsgált szervezet hivatalos honlapján.

Felhasznált irodalom

- Secjuice. „A Guide To Social Media Intelligence Gathering (SOCMINT)”, 2020. június 21.
<https://www.secjuice.com/social-media-intelligence-socmint/>.
- „A kis- és középvállalkozások jellemzői, 2017”, 2017, 14.
- Daniel Miessler. „A Shodan Tutorial and Primer”. Elérés 2022. március 29.
<https://danielmiessler.com/study/shodan/>.
- Abdullah, A., S.A. Laghari, A. Jaisan, és S. Karuppayah. „OSINT Explorer: A Tool Recommender Framework for OSINT Sources”. *Communications in Computer and Information Science* 1487 CCIS (2021): 389–400. https://doi.org/10.1007/978-981-16-8059-5_24.
- Expert.ai. „Advantages and Disadvantages of Open Source Intelligence”, 2017. február 23.
<https://www.expert.ai/blog/advantages-disadvantages-open-source-intelligence/>.
- Akarslan, Hüseyin. „A Model Proposal for Analyzing Open-Source Information in End-User Computers”. *International Journal of Intelligence and CounterIntelligence* 0, sz. 0 (2021. június 7.): 1–22. <https://doi.org/10.1080/08850607.2021.1899514>.
- Al-khateeb, Samer, és Nitin Agarwal. „Social Cyber Forensics: Leveraging Open Source Information and Social Network Analysis to Advance Cyber Security Informatics”. *Computational and Mathematical Organization Theory* 26, sz. 4 (2020. december 1.): 412–30. <https://doi.org/10.1007/s10588-019-09296-3>.
- MUO. „All You Need to Know About Open Source Intelligence (OSINT)”, 2020. november 20. <https://www.makeuseof.com/all-you-need-to-know-about-open-source-intelligence-osint/>.
- Chauhan, Sudhanshu, és Nutan Kumar Panda. „Chapter 4 - Search the Web—Beyond Convention”. In *Hacking Web Intelligence*, szerkesztette Sudhanshu Chauhan és Nutan Kumar Panda, 53–75. Boston: Syngress, 2015. <https://doi.org/10.1016/B978-0-12-801867-5.00004-5>.
- . „Chapter 5 - Advanced Web Searching”. In *Hacking Web Intelligence*, szerkesztette Sudhanshu Chauhan és Nutan Kumar Panda, 77–99. Boston: Syngress, 2015. <https://doi.org/10.1016/B978-0-12-801867-5.00005-7>.
- Day, Tony, Helen Gibson, és Steve Ramwell. „Fusion of OSINT and Non-OSINT Data”, 133–52, 2016. https://doi.org/10.1007/978-3-319-47671-1_9.
- Development, Ma-No Web Design and. „Google Dorks: How to Find Interesting Data and Search like Hacker”. MA-NO Web Design and Development. <https://www.ma-no.org>. Elérés 2022. március 28. <https://www.ma-no.org/en/security/google-dorks-find-interesting-data-search-like-hacker>.
- „Discovering IoT Vulnerabilities Using Updated Shodan Transforms”. Elérés 2022. március 27. <https://www.maltego.com/blog/discovering-vulnerabilities-using-shodan-transforms/>.
- Dobák Imre. „OSINT – Gondolatok a kérdéskörhöz”. *Nemzetbiztonsági szemle* 7, sz. 2 (2019): 83–93. <https://doi.org/10.32561/nsz.2019.2.7>.
- Dobák Imre, és Tóth Tamás. „Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering)”. *Belügyi Szemle* 69, sz. 2 (2021. február 15.): 195–212. <https://doi.org/10.38146/BSZ.2021.2.2>.
- Dokman, Tomislav, és Tomislav Ivanjko. „Open Source Intelligence (OSINT): issues and trends”, 2020. <https://doi.org/10.17234/INFUTURE.2019.23>.
- Evangelista, João Rafael Gonçalves, Renato José Sassi, Márcio Romero, és Domingos Napolitano. „Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence”. *Journal of Applied Security*

- Research* 0, sz. 0 (2020. május 7.): 1–25.
<https://doi.org/10.1080/19361610.2020.1761737>.
- „GDPR Essentials for OSINT Research – Blockint”. Elérés 2022. március 14.
<https://www.blockint.nl/methods/gdpr-essentials-for-osint-research/>.
- Gillies, A. „Improving the Quality of Information Security Management Systems with ISO27000”. *The TQM Journal* 23, sz. 4 (2011): 367–76.
<https://doi.org/10.1108/17542731111139455>.
- „Global State of Information Security ® Survey 2018 – Singapore highlights”. Elérés 2022. április 11. <https://www.pwc.com/sg/en/publications/global-state-of-information-security-survey-2018-sg.html>.
- Greenberg, Andy. „What Is a Supply Chain Attack?” *Wired*. Elérés 2022. április 2.
<https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/>.
- „How to Conduct Person of Interest Investigations Using OSINT & Maltego”. Elérés 2022. március 29. <https://www.maltego.com/blog/how-to-conduct-person-of-interest-investigations-using-osint-and-maltego/>.
- Infosec Resources. „How to discover open RDP ports with Shodan”. Elérés 2022. március 27.
<https://resources.infosecinstitute.com/topic/how-to-discover-open-rdp-ports-with-shodan/>.
- Cyurex. „How to Use OSINT Framework”, 2019. október 13. <https://www.cyurex.com/how-to-use-osint-framework/>.
- Hwang, Yong-Woon, Im-Yeong Lee, Hwankuk Kim, Hyejung Lee, és Donghyun Kim. „Current Status and Security Trend of OSINT”. *Wireless Communications and Mobile Computing* 2022 (2022. február 18.): e1290129.
<https://doi.org/10.1155/2022/1290129>.
- Karthika, S., N. Bhalaji, S. Chithra, N. Sri Harikarthick, és Debadyuti Bhattacharya. „NoRegINT—A Tool for Performing OSINT and Analysis from Social Media”. In *Inventive Computation and Information Technologies*, szerkesztette S. Smys, Valentina Emilia Balas, Khaled A. Kamel, és Pavel Lafata, 971–80. Singapore: Springer, 2021. https://doi.org/10.1007/978-981-33-4305-4_71.
- Kft, Wolters Kluwer Hungary. „2004. Évi XXXIV. Törvény a Kis- És Középvállalkozásokról, Fejlődésük Támogatásáról - Hatályos Jogszabályok Gyűjteménye”. Elérés 2022. április 2.
<https://net.jogtar.hu/jogszabaly?docid=a0400034.tv>.
- „KÖZIGAZGATÁSI INFORMATIKAI BIZOTTSÁG. 25. számú Ajánlása. Magyar Informatikai Biztonsági Ajánlások (MIBA) - PDF Ingyenes letöltés”. Elérés 2022. április 4. <https://docplayer.hu/1361183-Kozigazgatasi-informatikai-bizottsag-25-szamu-ajanlasi-magyar-informatikai-biztonsagi-ajanlasok-miba.html>.
- KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Az EU kiberbiztonsági stratégiája a digitális évtizedre (2020). <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020JC0018>.
- Európai Bizottság - European Commission. „Mi számít »jogos érdeknek«?” Text. Elérés 2022. március 14. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_hu.
- „Munk Sándor: INFORMÁCIÓBIZTONSÁG VS. INFORMATIKAI BIZTONSÁG”. Elérés 2022. február 15.
http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html.
- Military Wiki. „NATO Open Source Intelligence Reader”. Elérés 2022. február 19.
https://military-history.fandom.com/wiki/NATO_Open_Source_Intelligence_Reader.

- InfoSec Insights. „Open Source Intelligence: What Is OSINT & How Does It Work?”, 2020. július 17. <https://sectigostore.com/blog/open-source-intelligence-what-is-osint-how-does-it-work/>.
- GeeksforGeeks. „Python TheHarvester - How to Use It?”, 2020. május 26. <https://www.geeksforgeeks.org/python-theharvester-how-to-use-it/>.
- Roop, Joseph E. „Foreign Broadcast Information Service. History. Part 1: 1941-1947”. CENTRAL INTELLIGENCE AGENCY WASHINGTON DC, 1969. április 1. <https://apps.dtic.mil/sti/citations/ADA510770>.
- Crunchbase. „SentiOne - Crunchbase Company Profile & Funding”. Elérés 2022. március 30. <https://www.crunchbase.com/organization/sentione>.
- Black Cell. „Shodan keresőmotor használata SOC-ban”, 2020. augusztus 26. <https://blackcell.hu/shodan-keresomotor-hasznalata-soc-ban/>.
- Solti István. „Az OSINT információgyűjtő eszközeiről”. *Nemzetbiztonsági szemle* 7, sz. 2 (2019): 3–18. <https://doi.org/10.32561/nsz.2019.2.1>.
- „Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber”, é. n., 12.
- Szabó Károly. „Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről”. *Nemzetbiztonsági szemle* 7, sz. 2 (2019): 68–82. <https://doi.org/10.32561/nsz.2019.2.6>.
- Tarján Gábor. „Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben”. Phd, Budapesti Corvinus Egyetem, 2020. <https://doi.org/10.14267/phd.2020015>.
- Tawileh, Anas, Jeremy Hilton, és Stephen McIntosh. „Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach”. In *ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference*, szerkesztette Norbert Pohlmann, Helmut Reimer, és Wolfgang Schneider, 331–39. Wiesbaden: Vieweg, 2007. https://doi.org/10.1007/978-3-8348-9418-2_35.
- Terneva, Z., I. Vladimirov, és D. Nikolova. „Accessing LinkedIn and Google E-Mail Databases Using Kali Linux and TheHarvester”, 59–62, 2021. <https://doi.org/10.1109/ICEST52640.2021.9483460>.
- Cobwebs Webint Solutions. „The Advantages of Open Source Intelligence (OSINT)”, 2021. március 15. <https://cobwebs.com/the-advantages-of-open-source-intelligence-osint/>.
- Deloitte Croatia. „TISAX - A megfelelésen túl | Deloitte Magyarország”. Elérés 2022. április 2. <https://www2.deloitte.com/hu/hu/pages/fogyasztoi-agazat/articles/tisax---a-megfelelesen-tul---deloitte-magyarorszag.html>.
- Veronika Deák. „A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során”. *Hadmérnök* 13, sz. 3 (2018. szeptember 30.): 391-402-391–402.
- Williams, Heather J., és Ilana Blum. „Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise”. RAND Corporation, 2018. január 1. <https://apps.dtic.mil/sti/citations/AD1053555>.
- Wong, B.L. „Fluidity and Rigour: Addressing the Design Considerations for OSINT Tools and Processes”, 167–85, 2016. https://doi.org/10.1007/978-3-319-47671-1_11.
- Zhang, J., J. Notani, és G. Gu. „Characterizing Google Hacking: A First Large-Scale Quantitative Study”. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST* 152 (2015): 602–22. https://doi.org/10.1007/978-3-319-23829-6_46.
- 24.hu. „Zsarolóvírussal támadták meg az egyik legnagyobb hazai autóalkatrész-kereskedőt”, 2021. április 1. <https://24.hu/tech/2021/04/01/zsarolovirus-ransomware-unix/>.

Táblázatok jegyzéke

1. táblázat Saját szerkesztés. (Forrás: https://www.hindawi.com/journals/wcmc/2022/1290129/)	10
2. táblázat Átlagok a H1 hipotézisre vonatkozóan. (saját szerkesztés)	33
3. táblázat Átlagok a H2 hipotézisre vonatkozóan. (saját szerkesztés)	35
4. táblázat H3 hipotézisemre vonatkozó eredmény szemléltetése. (saját szerkesztés)	37

Kérdőív kérdései

1. A szervezet mérete (munkatársi létszám) - alkalmazottak és hozzáférésekkel bíró külsős munkatársak összege:

- ☐ 1-10
- ☐ 11-50
- ☐ 51-250

2. A szervezet működési területe / iparága

- ☐ autó ipar
- ☐ elektronika
- ☐ energia
- ☐ építőipar
- ☐ gyógyszeripar
- ☐ informatika
- ☐ kereskedelem
- ☐ közlekedés
- ☐ kultúra
- ☐ kutatás fejlesztés
- ☐ mezőgazdaság
- ☐ oktatás
- ☐ önkormányzat
- ☐ pénzügy
- ☐ szállítmányozás, logisztika
- ☐ szolgáltatás, egyéb szolgáltatás
- ☐ telekommunikáció
- ☐ termelés
- ☐ vendéglátás

- egyéb

3. Melyik megyében működik a vállalkozás székhelye?

- Bács-Kiskun megye
- Baranya megye
- Békés megye
- Borsod-Abaúj-Zemplén megye
- Csongrád-Csanád megye
- Fejér megye
- Győr-Moson-Sopron megye
- Hajdú-Bihar megye
- Jász-Nagykun-Szolnok megye
- Komárom-Esztergom megye
- Nógrád megye
- Pest megye
- Somogy megye
- Tolna megye
- Vas megye
- Veszprém megye
- Zala megye
- Szabolcs-Szatmár-Bereg megye

4. Van és megyében székhelye?

- - igen
- - nem

5. Amennyiben van más megyében telephelye, van digitális adatkapcsolat a telephelyek között?

- - igen
- - nem

6. A szervezetben az információbiztonsági kockázatokat minden működési folyamat kapcsán azonosítják és figyelembe veszik.

- Egyáltalán nem értek egyet
- Nagyrészt nem értek egyet
- Közömbös számomra
- Nagyrészt egyetértek
- Teljes mértékben egyetértek

7. A szervezet számára kritikus információkat és informatikai infrastruktúra elemeket (pl. hálózati elemek, alkalmazások stb.) azonosították.

- ☐ Egyáltalán nem értek egyet
- ☐ Nagyrészt nem értek egyet
- ☐ Közömbös számomra
- ☐ Nagyrészt egyetértek
- ☐ Teljes mértékben egyetértek

8. A információbiztonsági eseményekre a felsővezetés azonnal reagál.

- ☐ Egyáltalán nem értek egyet
- ☐ Nagyrészt nem értek egyet
- ☐ Közömbös számomra
- ☐ Nagyrészt egyetértek
- ☐ Teljes mértékben egyetértek

9. Az informatikai rendszerek felhasználóit oktatják arra, hogy a gyanús tevékenységeket azonosítsák és jelentsék.

- ☐ Egyáltalán nem értek egyet
- ☐ Nagyrészt nem értek egyet
- ☐ Közömbös számomra
- ☐ Nagyrészt egyetértek
- ☐ Teljes mértékben egyetértek

10. A munkatársak rendszeresen vesznek részt információbiztonsági tréningeken.

- ☐ Egyáltalán nem értek egyet
- ☐ Nagyrészt nem értek egyet
- ☐ Közömbös számomra
- ☐ Nagyrészt egyetértek
- ☐ Teljes mértékben egyetértek

11. Kérem az előző kérdések fényében értékelje saját szervezetének információbiztonsági érettségét!

- ☐ 1. szint Nem létező
- ☐ 2. szint Tervezés alatt
- ☐ 3. szint Alacsony
- ☐ 4. szint Elfogadható

- 5. szint Kifinomult

12. Hallott-e korábban az OSINT fogalmáról?

- - igen
- - nem

13. Tudomása szerint alkalmaznak-e a szervezetében OSINT tevékenységet?

- - igen
- – nem
- – nem tudom

14. Amennyiben alkalmaznak, hogyan értékeli szervezete OSINT képességét?

(1-5-ös likert skála, nem kötelező a válaszadás)

15. Mit gondol, ezen képesség kialakításában melyik tényezők jelentik a legfőbb kihívásokat az alábbiak közül:

- szükséges technológiai erőforrások beszerzése;
- szükséges humán erőforrás biztosítása;
- szükséges szaktudás biztosítása;
- vezetői támogatás hiánya;
- nem tudom

16. Véleménye szerint az OSINT a szervezetre nézve inkább lehetőség vagy kockázat?

- lehetőség
- kockázat
- nem tudom megítélni

17. Történt-e a szervezetükben olyan információbiztonsági incidens, amely háttérben OSINT tevékenység állhatott?

- igen
- nem
- nem tudom

18. Végeznek-e szervezetében rendszeres sérülékenységvizsgálatot?

- ☐ -igen
- ☐ -nem
- ☐ - nem tudom

19. Amennyiben igen, a sérülékenységvizsgálatoknak része-e fingerprinting / reconnaissance, vagyis a konkrét teszteket megelőző információgyűjtési fázisának része-e a vállalatukról online hozzáférhető információk vizsgálata?

- ☐ igen
- ☐ nem
- ☐ nem tudom

-

20. Új munkavállaló felvételi folyamata során ellenőrzik-e a jelölékkel kapcsolatos, nyílt forrásból elérhető információkat?

- ☐ igen
- ☐ nem
- ☐ nem tudom

Kérdőív kiértékelése

Ranks				
	hallote	N	Mean Rank	Sum of Ranks
letszam	igen	20	18,40	368,00
	nem	16	18,63	298,00
	Total	36		

Test Statistics^a

	letszam
Mann-Whitney U	158,000
Wilcoxon W	368,000
Z	-,068

Asymp. Sig. (2-tailed)	,946
Exact Sig. [2*(1-tailed Sig.)]	,962 ^b

a. Grouping Variable: hallote

b. Not corrected for ties.

Report

hallote

letszam	Mean	N	Std. Deviation
1-10	1,5000	10	,52705
11-50	1,3571	14	,49725
51-250	1,5000	12	,52223
Total	1,4444	36	,50395

Ranks

	alkalmaz	N	Mean Rank	Sum of Ranks
osztaly	igen	18	19,44	350,00
	nem	14	12,71	178,00
	Total	32		

Test Statistics^a

	osztaly
Mann-Whitney U	73,000
Wilcoxon W	178,000
Z	-2,071
Asymp. Sig. (2-tailed)	,038
Exact Sig. [2*(1-tailed Sig.)]	,045 ^b

a. Grouping Variable: alkalmaz

b. Not corrected for ties.

Report

osztály

alkalmaz	Mean	N	Std. Deviation
igen	3,7778	18	1,21537
nem	2,7857	14	1,36880
Total	3,3438	32	1,35859

Rövidítések jegyzéke

Rövidítés	Magyar nyelvű kifejezés	Idegen nyelvű kifejezés
OSINT	nyílt forrású információgyűjtés	open source intelligence
KKV	kis- és középvállalkozás	small and medium-sized enterprises
GDPR	általános adatvédelmi rendelet	general data protection regulation
IBIR	Információbiztonsági Irányítási Rendszer	Informationsecurity management system
CYBINT	kiber hírszerzés	Cyber Intelligence
DNINT	digitális hálózati hírszerzés	Digital Network Intelligence
IMINT	képfelderítés	Image Intelligence
MASINT	mérés- és jelmeghatározó hírszerzés	Measure,ent and Sinature Intelligence
TECHINT	technikai hírszerzés	Technical Intelligence
FININT	pénzügyi hírszerzés	Financial Intelligence
MEDINT	orvosi hírszerzés	Medical Intelligence
IoT	dolgok internete	Internet of Things

MR	rangátlag	Mean Rank
MIBA	Magyar Informatikai Biztonsági Ajánlások	Hungarian IT Security Recommendations