DOI: 10.31915/NWS.2021.21

OSINT technológiák és alkalmazási lehetőségeik a felsőoktatási rendszerek ellen

Koczka Ferenc
Eszterházy Károly Egyetem
ORCID: 0000-0002-7541-6495

Absztrakt
A tudomány és eredményeinek szabadsága, az egyetemek szabad szellemisége, a nyílt működés és az alkotói szabadság évszázadok óta fontos jellemzője az akadémiai szférának. A tudományos eredmények publikálása számos, akár nemzetközi szintű szakmai csoportok kialakulását segítette, s hozzájárult a tudományos élet színvonalának emelkedéséhez. Az Internet szolgáltatásaiban rejlő lehetőségeket a tudományos világ az elsők közt használta fel, új csatornákon tette közzé kutatásainak folyamatát és eredményeit, ami korábban nem látott mértékben segítette az azonos érdeklődésű kutatók kapcsolatépítési lehetőségeit. A közzétett információk nem korlátozódnak a tudományos környezetre, a tudományos eredmények gyakorlati felhasználása értéket jelent a gazdasági és a bűnözői körök számára is. E szereplők elsődleges célja azonban más, szinte kizárólag a gazdasági előny megszerzésére korlátozódik. Cikkemben rámutatok, hogy mások mellett az akadémiai szféra intézményei is túlzott mennyiségű információt tesznek közzé magukról, azok védelmét magasabb szinten kellene ellátniuk, és javaslatot teszek arra, hogy nagyobb hangsúlyt fektessenek a nyílt forrású felderítés elleni védekezésre.

Abstract
The freedom of science and its results, the free spirit of universities, openness and creative freedom have been an important feature of the academic world for centuries. The free access to university courses and the publication of scientific results have helped the development of many professional groups, even at the international level, and have contributed to raising the quality of academic life. The scientific world was among the first to take advantage of the Internet's services, using new channels to publish their research and results, which greatly facilitated networking opportunities for researchers with similar interests. The information published is not limited to the scientific environment, the practical use of scientific results is of value to economic and criminal circles. Although the primary objective of these roles is different, in most cases, they seek to gain an economic advantage. In my article, I point out that academic institutions also publish too much information about themselves, that they should have a higher level of protection, and I suggest that they should put more emphasis on protecting themselves against open-source intelligence.

Bevezetés

A nyílt forrású felderítést (OSINT – Open Source Intelligence) az amerikai kormányok már a múlt században is alkalmazták, elsősorban a külföldi média által közölt információk begyűjtésére és rendszerezésére. Pearl Harbor megtámadása után a módszert rendszerszintűvé tették, 1941-ben felállt az FBIS (Foreign Broadcast Information Service) mely néhány év múlva már a CIA részeként működött az USA hírszerzési rendszerében [1]. Az OSINT azóta is fontos eleme a hírszerzésnek, definíciója olyan publikus, vagy korlátozott körben elérhető adatok legális eszközökkel történő megkeresését, összegyűjtését, szintetizálását és felhasználását határozza meg, melynek eredményeképp új információ hozható létre. A legalitás lényeges elem a meghatározásban, ez kizárja a minősített információk megszerzésére irányuló célzott támadásokat, és más olyan eseteket, melyek során az információ megszerzése valamilyen forrás legális felhasználásán túl jött létre. Bár eredetileg kormányzati, hírszerzési, katonai, bűnüldözési és belbiztonsági szervezetek alkalmazták, de az OSINT már jelen van az üzleti szférában is[1].

Mivel célzott támadások előkészítésére az egyik legegyszerűbb módszer az OSINT, a metodikát kiberbűnözők is alkalmazni kezdték. Alkalmazásával elkerülhetők az olyan kockázatos műveletek, mint pl. az illegális belépési kísérletek, és nem szükséges social engineering módszerekkel személyes kapcsolatokat építeni, megtéveszteni vagy megvesztegetni kulcspozícióban levő alkalmazottakat sem. Annak ellenére, hogy az OSINT metodikák egy része kifejezetten a manuális adatgyűjtésre épül, egy részük technikai szempontból könnyen automatizálható és naprakészen tartható. A mesterséges intelligencia fejlődésével pedig úgy tűnik, az automatizálási lehetőségek tovább erősödnek majd. Nem tétlenek a bűnözői körök sem, a technikai újításokat és tudományos eredményeket felhasználva olyan új típusú bűncselekményeket valósíthatnak meg, melyek ma még szinte kivédhetetlennek bizonyulnak. Miközben vállalatok a humán telefonos ügyfélszolgálataik mesterséges intelligencián alapuló kiváltásával kísérleteznek, utóbbiak ugyanezzel a technológiával már sikeresen tévesztettek meg munkatársakat és vették rá őket fiktív kifizetések indítására [2].

Az adatszerzés forrásai

Az OSINT technológia alkalmazásának kiszélesedését az adatforrások körének kiszélesedése, jogszabályi követelmények és társadalmi elvárások változásai is segítik.

Az üzleti szférában a szolgáltatók a meglevő és a potenciális klienseik tájékoztatására minél több információt igyekeznek közzétenni, melyek begyűjtését az ellenérdekelt oldal a megfigyeléstől az internetes kereséseken át, a különféle adatbázisokra történő előfizetéssel, szabadon elérhető információhordozókkal, publikációk begyűjtésével, könyvek, tanulmányok, napilapok, televízió- és rádióadások, podcastok, blogok, vblogok, konferenciák, beszámolók elemzésével végzi [3].

1 Egy norvég OSINT adatokat szolgáltató cég pl. nyílt forrású adatgyűjtéssel teszi lehetővé biztosítók számára, hogy olyan kelet-európai országok mezőgazdasági termelők számára is biztosítást nyújthassanak, amelyekben nem áll rendelkezésre hivatalos adat a kockázatok kiszámításához. Forrás: https://www.osintanalytics.com.

A közösségi média és alkalmazások népszerűségének felértékelődése különösen értékes információforrást biztosít a nyilvános forrású adatgyűjtéshez, mivel az eredeti adatközlésen túlmutató, másodlagos adatforrást is jelentenek. Előfordul, hogy munkahelyi adatok publikálását végző munkatársak nincsenek tisztában azzal, hogy olyan információkat is közzétesznek, amely eredetileg nem állt szándékukban[2]. A Facebook megosztások kockázatának ismerete általánosnak mondható, de gyakorlatozó amerikai katonák számára már nem volt nyilvánvaló, hogy a sporttevékenységeik megosztásával a katonai egységeik helyzetére és mozgására engednek következtetni[3].

Nagy tömegű anonim GPS adat összegyűjtésével kapcsolatos nemzetbiztonsági kockázatra a New York Times vizsgálatai hívták fel a figyelmet. Az újságíró számára egy adatbázist juttattak el, mely mobiltelefonok egyedi azonosítóit és azok mozgását leíró GPS adatokat tartalmazott. Bár abban személyes adat nem állt rendelkezésre, a koordináták helyét és idejét más, publikus forrásokkal összevetve az eszközök tulajdonosai könnyűszerrel azonosíthatóvá váltak. A vizsgálatban védett személyek mellett sikeresen azonosították az amerikai elnök telefonját is és bizonyították mozgásának további követhetőségét [4] [5].

Bár az egyes rendszerek és komponenseik sérülékenységeit közlő források[4] többsége alkalmazható a nyílt forrású felderítésben, a sérülékenység kiaknázásához szükséges eszköz kifejlesztéséhez etikai okokból nem nyújtanak elégséges információt. Ezt a hiányt a Darkneten elérhető források fedik le.

Jogszabályok és eszközök

Az Európai Parlament és a Tanács 2016/679 rendelete (közismert nevén GDPR) az EU állampolgárai számára nyújt védelmet a személyes adataik kezelése terén. A jogszabály számos ponton részesíti előnyben a magánszemélyek személyes adatainak védelmét az üzleti szférával szemben, ugyanakkor a jogszabályban meghatározott adatkezelési folyamatokat természetesen nem akadályozza. Bár a jogszabály bonyolult és a gyakorlati alkalmazása is nehézkes, súlyos szankciókat határoz meg az adatkezelés tömeges megsértése esetén. A GDPR kizárólag magánszemélyek adatainak kezelését szabályozza, hatálya nem terjed ki cégek, szervezetek védelmére [6].

Az OSINT alkalmazási lehetőségeinek korlátozásában a GDPR-nak fontos szerepe volt az EU-ban. Az EU-n kívüli államokban a magánszemélyek adatainak védelme korántsem olyan egységesen szigorú, a személyes adatok sok esetben árucikkek, melyekkel a hatályos jogszabályok betartásával kereskedni is lehet.

2 A weblapokon, közösségi hálózatokon és más forrásokban közzétett képek metaadatainak elemzése bizonyos esetekben lehetővé teheti azok készítési helyének és idejének megállapítását.

3 https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

4 A Common Vulnerabilities and Exposures adatbázisa a https://cve.mitre.org címen érhető el, és nyújt információt az ismertté vált sérülékenységekről, de nem nyújt részletes információkat ahhoz, hogy a sérülékenységek kihasználására alkalmas eszköz kifejleszthető legyen.

Az Egyesült Államokban számos szolgáltatás kínál nyílt forrású adatok alapján készült jelentéseket magánszemélyekről is, melyek összehasonlítása során kimutatható, hogy az alapszolgáltatásaik jórészt azonos forráson alapulnak. Egy ilyen jelentés részleteinek megismerésére, és a közölt adatok érvényességének ellenőrzésére egy interjút készítettem egy amerikai állampolgárral.

Az ő előzetes engedélyével kb. 20 dolláros áron vásároltam meg egy jelentést róla, melyhez kiinduló információként pusztán a nevét és egy lehetséges lakhelyét kellett megadnom. A szolgáltatás számára ennyi már elég volt ahhoz, hogy azonosítsa és egy 24 oldalas jelentést generáljon róla. A dokumentum a leíró adatok mellett részletezte a munkahelyeit, felsorolta rokoni és egyéb lehetséges kapcsolatait, megnevezte a vele korábban közös lakcímen lakó személyeket és annak időtartamát, a SSN (Social Security Number) forrását, korábbi telefonszámait, e-mail címeit, lakcímeit és szomszédjait, korábban birtokolt gépjárműveit. A hatósági ügyekkel kapcsolatos információk közt bírósági meghallgatások, szabálysértések szerepeltek. Önálló részt kapott a környezetében nyilvántartott szexuális bűncselekmény elkövetésével kapcsolatba hozott személyek fényképes listája. Az érdeklődési köréről és attitűdjeiről nem csak a legismertebb közösségi hálózatok konkrét azonosítói adtak tájékoztatást, ebből vallási hovatartozása is egyértelművé vált.

Az interjú alanya ellenőrizte a dokumentum tartalmát, egy kontakt személy és néhány, a hatósági nyilvántartásban szereplő adat kivételével megerősítette azok helyességét.

A nyílt forrású felderítés támogatására első látásra bőséges eszköztár érhető el az Interneten[5]. Ezek a szoftverek jól dokumentáltak, bár megítélésem szerint számos olyan van köztük, melyek elsődleges célja nem az OSINT támogatása, legfeljebb bizonyos körülmények közt adhatnak használható információt. A valóban jól használható, hatékony és mély műszaki ismereteket nem igénylő megoldások ingyenesen használható verziói rendszerint csak erősen korlátozott funkcionalitással érhetők el, és jellemzően adott időszakra szóló előfizetéssel használhatók.

Az OSINT és az akadémiai szféra

Az OSINT a mindennapi életben hatékonyan segítheti a különféle szervezetek munkáját, pl. a munkáltatók korlátozásokkal ugyan, de megtekinthetik és döntésükhöz felhasználhatják az adott munkakör betöltésére jelentkezők nyilvános profilját [7]. Ugyanakkor nem csak az intézményt érő célzott támadások elkerülésének érdekében kellene minimalizálniuk a publikusan elérhető adatok körét.

2021-ben több magyar egyetem esett áldozatul a bankszámlaszám változását elérő csalásnak, mely során a csalók egyetemi ügyintézők számára telefonon is megerősítették a változás tényét. Az eset bizonyítja, hogy az akadémiai szféra Magyarországon is lehet célpontja olyan jellegű támadásoknak, melynek megtervezésében az OSINT is szerepet kaphatott, és bár az nem kapott széles körű publicitást, az érintett intézmények megítélését is negatívan befolyásolhatja.

5 Az OSINT eszközök egyfajta rendszertana a https://osintframework.com oldalon érhető el.

A nyilvános telefonkönyvek, dolgozói katalógusok, e-mail címjegyzékek és organogramok segítenek feltérképezni a kulcspozícióban levő döntéshozókat. Az egyetemek működésére vonatkozó adatok közérdekből nyilvánosak, könnyen megtalálhatók a szerződött partnerek és szerződés részletei[6]. Ezek birtokában sokkal könnyebb rést találni a szervezet működésében, főleg, ha a dolgozók nem feltétlenül ismerik egymást. A vezetők által aláírt és közzétett dokumentumok nagyban leegyszerűsítik olyan hamisított iratok előállítását, amelyek a belső munkatársak számára is hitelesnek tűnhetnek[7].

A nyilvánosság ilyen formája kifejezetten negatív hatású a munkaerő megőrzésének területén. Önéletrajzok, tudományos eredmények közzététele OSINT forrást jelent a fejvadász cégek számára, de az adathalász és megtévesztő támadások kiindulópontja lehet.

A munkatársainak kapcsolati adatainak egy részét a legtöbb felsőoktatási intézmény valamilyen formában elérhetővé teszi. Csak néhány esetben találkozhatunk olyan stratégiával, melyben nem személyek, hanem szerepkörök ismerhetők meg az e-mail címek alapján. Bár általában a telefonkönyvek fejlesztői igyekeznek megakadályozni a kapcsolati adatok tömeges leszüretelését, tapasztalataim szerint ez könnyen kijátszható. Erre vonatkozó országos mérés nehezen végezhető, mivel a munkahelyi e-mail cím is személyes adat, és tulajdonosának hozzájárulása nélkül nem kezelhető. Sajnos a felkeresett egyetemi informatikai vezetők nem támogatták egy ilyen vizsgálat elvégzését, így csak kerülő megoldással lehet megállapítani, hogy pl. dolgozói személyes adatok leszüreltelhetők-e az adott intézmény esetében. Az alábbi anonimizált példa demonstrálja, hogy egy ilyen feladat néhány soros scripttel is megoldható úgy, hogy a forrás kilétének rejtését a Darknet infrastruktúrája adja.

```
#!/bin/bash
URL="https://www.uni-ANON.hu/telefon/index.php?menu_id=2&myaction=details&
key_field_value=XXX"
for I in $(seq 250 1 10000) ; do
  echo $URL | sed „s/XXX/$I/g"
  torify wget $(echo $URL | sed „s/XXX/$I/g" ) -q -O - | grep -EiEio
',\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b'
done
```

6 Az EKE jelentősebb szerződéseit és beszerzéseit a https://uni-eszterhazy.hu/public/uploads/5-millio-ft-feletti-erteku-szerzodesek-2019-5e382fcbd6e7e_5e4ec05f04e0b.pdf oldalon tette közzé. Az Államkincstár az egyetem élő szerződéseinek listáját a http://www.allamkincstar.gov.hu/files/A%20Kincstárról/Üvegzseb/2021/ÜVEGZSEB_20210312.pdf oldalon publikálta.

7 Érdemes egy Google keresést indítani a "Szervezeti és Működési Szabályzat" filetype:pdf kifejezéssel, a találatok közt alig van olyan dokumentum, amelyben ne szerepelnének eredeti aláírások.

Összegzés

A magyar felsőoktatás informatikai rendszereinek működését csak általános jogszabályok szabályozzák, bár az elmúlt időszakban néhány egyetem kutatási egysége nemzetbiztonsági védelem alá került [8]. A teljes felsőoktatás stratégiai besorolásának megváltoztatására már van nemzetközi példa [9], így várható, hogy idővel azt más országok is követik. Ezen a téren a magyar jogi helyzet nem koherens: miközben az esetenként több tízezres létszámú egyetemek szabadon határozzák meg az informatikai rendszereik működtetésének szabályait, egy kis vidéki önkormányzatnak sokkal szorosabb jogszabályi keretek közt kell működnie.

Műszaki szempontból tekintve a felsőoktatási informatikai rendszerek nem speciálisak, a fő eltérések a finanszírozásban, a nyílt működés támogatásában és a szektor speciális szoftvereiben jelennek meg. Több eset igazolja, hogy az OSINT eszközök a felsőoktatási informatikai rendszerekkel szemben is alkalmazhatók, és a publikus információs felületeken megjelenő tartalmak mennyiségét jelentős mértékben szűkíteni kellene. Különösen kerülendő a munkatársak személyes és kapcsolati adatainak teljes körű begyűjthetősége, a belső szabályzatok, és egyéb dokumentumok korlátozás nélküli hozzáférésének biztosítása. Ezek publikálására célszerű védett területet kialakítani, az intézményi publikus felületek szerkesztését pedig olyan centralizált szervezeti egységre bízni, melynek tagjai ismerik az OSINT célokat módszereket, így azok képesek a publikált tartalmakat a nyílt forrású felderítés számára a lehető legkevésbé ellene fordítható mértékben és formában megjeleníteni.

A jogalkotás szintjén célszerű lenne újragondolni azokat az előírásokat, melyek a kiberbűnözők információhoz jutását segítik elő. Bár az üvegzseb programmal járó részletes adatszolgáltatási kötelezettségek és a pályázati források felhasználását bemutató weboldalak a közpénzek felhasználását, így a közintézmények átláthatóságát teremtik meg, egyúttal gazdag információforrást nyújthatnak előre megtervezett, célzott támadások kivitelezéséhez.

Jogi támogatás hiányában az felsőoktatás döntéshozói nem tudnak ezen a területen hatékony védelmi lépéseket tenni, mivel saját belső szabályzataik nem kerülhetnek ellentmondásba az érvényes jogszabályokkal. Az adatszolgáltatási kötelezettség gyakorlata felülírja az OSINT védelmi szabályokat, elsődleges szempontként a jogszabályok betartása és az esetleges szankciók elkerülése érvényesül. Általános intézményi jó gyakorlatok megítélésem szerint legfeljebb szigetszerűen léteznek, az egyetemek informatikai vezetésének jelenleg nincs olyan működő platformja, melyben tapasztalataikat megoszthatnák, illetve egy esetleges informatikai incidens esetén a társintézmények számára információt nyújthatnának.

Az intézményi informatikai biztonsági szabályzatok és az azokhoz kapcsolódó oktatások megtervezése során célszerű az nyílt forrású felderítés kérdéskörére is kitérni. Ennek eredményeként az OSINT által alkalmazott technikák ismeretében egy olyan területen javítható az intézmény információbiztonsága, melyet manapság az informatikai szakemberek szinte alig felügyelnek.

Irodalomjegyzék

[1] F. Schaurer és J. Störger, „The Evolution of Open Source Intelligence (OSINT),” *Journal of U.S. Intelligence Studies*, 2013, 19. kötet, 3. szám, 53. o.

[2] C. Supp, „Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case,” 30 08 2019. [Online]. Elérhető: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402. Hozzáférés dátuma: 2021.01.01.

[3] V. Deák, „A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során,” *Hadmérnök*, 2018. XIII. évf. 3. szám, 393. o.

[4] S. A. Thompson és S. Warzel, „welve Million Phones, One Dataset, Zero Privacy,” The New York Times, 19 12 2019. [Online]. Elérhető: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. Hozzáférés dátuma: 2021.01.12.

[5] S. A. Thompson és C. Warzel, „How to Track President Trump,” New York Times, 20 12 2019. [Online]. Elérhető: https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html. Hozzáférés dátuma: 2021.01.15.

[6] Európai Parlament és a Tanács, *Az Európai Parlament és a Tanács 2016/679 Rendelete a a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról*, 04: 27, 2016.

[7] Nemzeti Adatvédelmi és Információszabadság Hatóság, „A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről,” [Online]. Elérhető: https://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf.

[8] *187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásá*, Budapest: Magyarország Kormánya, 2015.

[9] „Australian Government Department of Home Affairs,” 11 2020. [Online]. Elérhető: https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf. Hozzáférés dátuma: 2021.03.11.