NAGY ZOLTÁN ANDRÁS

A személyiséglopás és a kapcsolódó bűncselekményekről készült EU Szakbizottság Tanulmányáról

Az Európai Unió Európai Bizottságának Migrációügyi és Uniós Belügyi Főigazgatósága (DG HOME) több európai szervezet, egyetem és vállalkozás támogatásával 2000 elején Szakbizottságot hívott életre az online személyiséglopás, valamint az ezzel összefüggő bűncselekmények, visszaélések európai helyzetéről készítendő átfogó vizsgálat elvégzésére.

Ebben az Európai Unió 27 tagállamának képviselője vett részt, akiknek a feladatuk a Főigazgatóság által összeállított szempontok, kérdések alapján Nemzeti Jelentések elkészítése volt, amelyekből megszületett a Szakbizottság közös állásfoglalása.[1] A kérdések a kutatómunka előrehaladtával változtak, vagy még inkább bővültek. A munkám elvégzéséhez segítséget kaptam a Legfőbb Ügyészségtől, a Kúriától, rendőrségi szakemberektől, a Nemzeti Adatvédelmi és Információszabadság Hatóságtól (NAIH), a Nemzeti Kibervédelmi Intézettől, kollégáimtól a Közszolgálati Egyetemen és a Pécsi Tudományegyetemen. Utólag ismételten köszönetet mondok valamennyiüknek a támogatásukért. Ki kell emelnem a Nemzeti Kibervédelmi Intézet munkáját, amelyet a Szakbizottság is nagyra értékel.[2]

Sajnos az egész Európát sújtó karantén a közvetlen kapcsolattartást megnehezítette, de a modern kommunikációs eszközök segítettek ezt a problémát áthidalni.

A magyarországi Nemzeti Jelentést a Főigazgatóság felkérésére jómagam készítettem.

---

[1] Forrás: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1 (a továbbiakban: Tanulmány)
Letöltés ideje: 2022.10.21.

[2] Forrás: https://nki.gov.hu/
Letöltés ideje: 2022.10.21.

A kutatómunka célja

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) a *„személyazonosság-lopást”* olyan bűncselekményként írja le, amely akkor történik, *„amikor egy fél megszerzi, átadja, birtokolja vagy felhasználja természetes vagy jogi személy személyes adatait jogosulatlan módon, azzal a szándékkal csalást vagy más bűncselekményt követ el”*.[3]

Ugyanakkor a technikai-technológiai fejlődés a személyi adatok körét kibővítette,[4] amire az Európai Parlament és a Tanács 2016/679. rendelete (GDPR – General Data Protection Regulation, azaz az Általános Adatvédelmi Rendelet) reagált.

A kutatómunka célja a személyazonosság-lopás jelenségének megértése és annak bűnügyi és szabályozási kihatásainak vizsgálata az Európai Unióban.

A kutatás a következő konkrét célokat tűzte ki:

- Felmérni az online személyazonosság-lopás és az identitáshoz kapcsolódó probléma természetét és mértékét az Európai Unióban.
- Feltérképezni és elemezni az online személyazonosság-lopás és személyazonossághoz kapcsolódó bűncselekmények jelenlegi törvényi szabályozását, továbbá a hiányzó intézkedéseket feltárni tagállami szinten.
- A bevált gyakorlatok (best practice) és intézkedések, illetve ezek lehetséges hiányosságainak felmérése.

---

[3] OECD, 2008, ‘OECD Policy Guidance on Online Identity Theft.
Forrás: https://www.oecd.org/sti/ieconomy/onlineidentitytheft.htm
Letöltés ideje: 2022.10.21.

[4] „Személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági azonosságára vonatkozó egy vagy több tényező alapján azonosítható (4. cikk. 1.pont)
Forrás: https://www.naih.hu/altalanos-adatvedelmi-rendelet-gdpr

– Javaslatok megfogalmazása a jövőbeli uniós szintű intézkedésekre és fellépésekre vonatkozóan.[5]

A kutatómunka hatóköre

A kutatás elsősorban az online személyazonosság-lopásra összpontosított, melynek megszerzésével lehetővé válnak különböző bűncselekmények vagy a polgári és közigazgatási jogi visszaélések.

Bár a kutatás az online személyazonosság-lopásra fókuszált, ám kitekintett a valós térbeli (offline) személyiséglopásra is, gondoljunk a különböző plasztikkártya igazolványainkra, bírósági ítéletekre, vádiratokra, végzésekre, amelyek jogellenes megszerzésével a virtuális térben is végrehajtható bűncselekmény (többek között például a vásárlások, banki tranzakciók, valódi, más nevére szóló közokirat felhasználásával történő intellektuális közokirathamisítás [6]). Valós térbeli személyes adataink minden esetben digitalizálva is vannak.

Bevezetésképpen, mintegy alátámasztva a kutatómunka fontosságát, tegyünk néhány megjegyzést. A személyes adatok megszerzésére és a velük való visszaélésre használt legkiterjedtebb technika, az adathalászat az elmúlt években egyre szofisztikáltabbá és célzottabbá vált.[7]

Az Európai Unióban az internethasználók 31%-a (148 millió állampolgár) számolt be arról, hogy 2017 és 2019 között az adathalászat különböző formáinak célpontjai vagy áldozatai voltak. Az adathalászat következtében az uniós polgárokat érő teljes közvetlen veszteség a becslések szerint 27,0 milliárd euróra tehető.[8]

Ezt a negatív tendenciát a COVID-járvány miatti bezárások tovább erősítették.

---

[5] Tanulmány 12. o.
[6] Btk. 342. § (1) bekezdés esetei
[7] Business Email Compromise, Spear Phishing, Whalilng – csalárd e-mail fajták és a legkülönfélébb malware-ek.
[8] Tanulmány 5. o.

Az online munka és tanulás miatt egyre többen végezték napi munkáikat az Interneten, ám az itthoni védelem általában nem azonos a munkahelyi hálózatok védelmével, ami miatt megsokszorozódott a potenciális sértettek száma. Sajnos, a felhasználók ismeretei, felkészültsége, gondatlansága, az elkövetők magasabb tudásszintje sértetté válásuk legfőbb oka.

A személyazonosság-lopást és a személyazonossághoz kapcsolódó bűncselekményeket túlnyomórészt anyagi haszonszerzés céljából követik el, a leggyakrabban a bankkártya adatait célozzák meg (card-not-present csalás).[9]

A kutatómunkánk alapján készült Tanulmány összegezte a személyiséglopás elkövetésének átalános metódusait, szakaszait, céljait.

A személyiséglopás első szakasza a személyes adatok megszerzése a potenciális sértettektől.

Az elkövetők erre a célra a technikák széles skáláját alkalmazhatják, ezek a megoldások online és offline környezetben egyaránt alkalmazhatók.

A célba vett adatok a személyazonosság adatain túl az IT-rendszerekbe való belépéshez szükséges hitelesítők, a pénzügyi tranzakciók és más adatok.

Az adatok megszerzésének első szakasza különösen rejtett. Az új fenyegetésekre, veszélyekre a felhasználók nem készültek fel, emiatt többen és hamarabb válnak sértetté.

Feltételezhetően a nagy és tőkeerős vállalkozások, a kibervédelemmel foglalkozó állami és privát szervezetek, továbbá a rendészeti szervek reagálnak a leghamarabb.

A személyazonosság-lopással összefüggésben az adathalászat jön szóba, amely egy széles támadási kategória, számos megvalósítási technikával.

[9] A bankkártyacsalások két fő fajtája ismert: a card present csalás – amikor jelen van a bankkártya a bűncselekmény elkövetésekor (többek között offline vásárlás, ATM-ből pénzkivétel).
Card-not-present csalás – az Internetes vásárlásoknál a bankkártyák adataira van szükség.

A valós térben végrehajtott social engineering különböző szociotechnikai, technikai, társadalmi támadások gyűjtőfogalma. Idetartoznak az emberek által végrehajtott manipulációk, továbbá a személyes adatok különböző csatornákon (például e-mailen, üzenetküldő rendszereken, telefonon, VoIP-n keresztül, közösségi médiában) történő megszerzése.

A virtuális térbeli adathalászat az informatikai rendszereken zajló kommunikáció elleni támadásokkal is megvalósítható.

A Szakbizottság a bűnüldöző szervek válaszából a következő támadásfajtákra utalt:

- a hacking („elektronikus betörés”),
- a közbeékelődő támadás (Man-in-the-middle), amikor a támadás a két weboldal közötti kommunikáció közé ékelődve hamis weboldalról kér és fogad el adatokat,
- a billentyűleütés-naplózó kémprogram (Keystroke loggers),
- a trójai falók vagy más típusú rosszindulatú malware (malicious software-ek – rosszindulatú programok).

Ezeket a támadási vektorokat gyakran használják a social engineering technikákkal együtt.[10]

A személyes adatok beszerzése (általában) nem a végső cél az elkövetők számára, hanem azokat további bűncselekmények elkövetéséhez használják fel. A személyi adatok elleni támadás tipikusan elő- vagy eszközcselekmény.

Sajnos a sértettek az esetek nagy részében nincsenek tudatában annak, hogy személyes adataikat ellopták. Csak akkor szembesülnek ezzel, ha az ellopott személyazonosságukat a bűnelkövetők bűncselekményekhez, viszszaélésekhez használták fel.

A személyiséglopás második szakasza a személyes adatok értékesítése, az azokkal való kereskedés különböző platformokon, kapcsolaton keresz-

[10] Tanulmány 18. o.

tül. Az Internet Relay Chat alkalmazástól a Telegrammon át a tor-hálózatokig megtalálják egymást a bűnözők. A kapcsolatok kialakultak, a kínált termékek értékesítésére, felhasználására az elkövetők, szervezett bűnözői csoportok szakosodtak, adatpiacok alakultak ki az Internet sötét bugyraiban.

Az eltulajdonított személyi adatokat, legfőképpen a bankkártya adatokat vagy maguk használják fel bűncselekményekhez, visszaélésekhez, vagy maguk vagy mások közreműködésével értékesítik.

A személyiséglopással összefüggő cselekménysorozat harmadik szakasza azok felhasználása.

A Tanulmány szerint a legtöbb megkérdezett rendészeti szakember szerint a személyiséglopást vagyonszerzési célú bűncselekményhez használják. A cselekményeket a magánszemélyek 92%-a és a vállalatok 77%-a szenvedi el.[11] Nem volt teljes körű a felmérés, így a valódi (már ha egyáltalán felmérhető) százalékszámok eltérhetnek, de a tendenciát – vitán felül – jellemzi.

A megkérdezettek véleményét erősítik az Europol IOCTA-jelentései is, amelyek a leggyakoribb támadások céljaként a pénzügyi vonatkozású bűncselekményeket említik.[12]

A személyiséglopás cselekményeivel okozott károk azonban sokféle formában jelentkezhetnek:

- Gazdasági károk, amelyek közvetlenek vagy közvetettek egyaránt lehetnek.
- Nem gazdasági károk.

Két megjegyzést kell tennünk az elején.

A magánszemélyeket/háztartásokat és a vállalkozásokat ért károkat külön érdemes számba venni.

[11] Tanulmány 23. o.

[12] Forrás: https://www.europol.europa.eu/publications-events/main-reports/iocta-report Letöltés ideje: 2022.10.22.

Második megjegyzésünk az, hogy a valós károk számításakor nem kevés problémával nézünk szembe. A személyiséglopást, mint előcselekményt a bűnügyi statisztikákban kellene szerepeltetni, összefüggésbe hozni a magánszemélyeknél, illetve a vállalkozásoknál keletkezett közvetlen károkkal. Ne feledkezzünk el a személyiséglopás magas látenciájáról, ami szintén ellene hat a valós adatok meghatározásának. Talán a magyarországi Robotzsaruba feltöltött esetek részletesebb leírása lehetne megoldás.

A francia Nemzeti Jelentésben a magánszemélyeket ért bankkártyával visszaélés bűncselekményeknél a háztartások/áldozatok 34%-a 100 euró alatti összegű, 37%-a 100 euró és 500 euró, 13%-a 500 euró és 1000 euró közötti és 16%-a 1000 euró feletti kárt szenvedett.[13]

Az Eurobarometer, együttesen kezelve a személyiséglopást és annak folyományait, megállapítja, hogy felmérése alapján azok 87%-ában nem keletkezett veszteség. A fennmaradó részben mérhetünk kárértékeket. A sértettek 5%-ának 50 euró alatti, 6%-ának 50 és 500 euró közötti, 1%-ának 500 és 2 000 euro közötti, és újabb 1%-ának 2000 euró feletti volt a kára.[14]

A vállalkozások esetében ugyanazok a metodológiai problémák vannak, mint a magánszemélyeknél, azaz a károk nem különböztethetők meg a bűncselekmény típusa szerint. Így valós számokhoz nem jutunk. [15]

A gazdasági károk másik nagy csoportjába tartoznak a közvetett károk, amelyek szintén kétfélék lehetnek.

- Egy részük pénzben nem mérhető. Ilyen a rossz érzés, a fájdalom, a szenvedés, az érzelmi szorongás, a kényelmetlenség, a vállalkozásoknál jellemző hírnévkárosodás.
- Más részük viszont költségekkel, kiadásokkal jár a sértett számára: a kieső munkabér, más kereset, továbbá ha szükséges, új számítás-

[13] Tanulmány 113. o.
[14] Tanulmány 113. o.
[15] Tanulmány 43. o.

technikai eszközök beszerzése, a számítógép, mobileszköz védelmének újraépítése (új programok beszerzése), banki, jogi költségek (új igazolványok, útlevelek igénylési díjai), netán orvosi költségek.

A közvetlen és közvetett károk számbavételekor nem volna szabad elfeledkezni az igazságszolgáltatás költségeiről sem, különös tekintettel a magas szakértői díjakra.

A személyiséglopás megelőzésének követelményrendszerét a Szakbizottság az alábbiak figyelembevételével javasolja:

– Minimális költségekkel kell járnia a felhasználók számára.
– Biztosítani kell, hogy a technológiai folyamatfejlesztések mindenki érdekeit tartsák szem előtt.
– Megfelelő képzésben kell részesíteni minden érintett felet.
– Hatékony észlelés, kezelés és/vagy megelőzés szükséges a személyazonosság-lopással
– kapcsolatos bűncselekmények esetében.
– Átfogó tájékoztatás és források biztosítása a bűncselekmények sértettjei számára.[16]

A Szakbizottság kiemelte a magyarországi áldozatsegítés példáit, így a Kék Vonal, a Safer Internet, a Gyermekkrízis Alapítvány tevékenységét,[17] továbbá egyedülállóként a Digitális Gyermekvédelmi Stratégiát és a Digitális Oktatási Stratégiát.[18] Ez utóbbiak azért kiemelésre méltóak, mert más országokban jellemzően általános kiberstratégiák léteznek.

A Szakbizottság Tanulmánya bőséges teret szentel az egyes országok bűnmegelőzési gyakorlatának bemutatására és a tapasztalatok összegzésére a felvilágosító kampányok. A summázott tapasztalatokból leszűrtük, hogy a bűnmegelőzési stratégiák általános figyelemfelhívása helyett inkább a ve-

[16] Tanulmány 173. o.
[17] Tanulmány 87. o.
[18] Tanulmány 195. o.

szélyeztetett területek jellemző veszélyeire, kockázataira kellene koncentrálni. Így például a médiahasználat, az online vásárlások, az online tanulás, távmunka, a közösségi oldalakon az aktivitások során, továbbá az automatizált háztartási (Internet of Thing) rendszerek használata idején jelentkező realitásokra, a potenciális visszaélések megelőzésére, az elszenvedett sérelmek orvoslásának lehetőségére, az eljáró hatóságok, civilszervezetek (0–24-ben) való postai, telefonos vagy elektronikus elérhetőségére felhívják a figyelmet, továbbá bemutatják a támadó cselekmények büntetőjogi vagy más jogági értékelését. A felvilágosító internetes oldalak és kampányok legyenek figyelemfelhívóak, érdekesek. A weboldalakat a fenti tartalmakon túl színesítsék video-, podcast-anyagok, kvíz- és nyereményjátékok, valamint adjanak helyet híreknek a legfrissebb veszélyekről. A kampányok jelenjenek meg a városokban, iskolákban, fiatalok rendezvényein, az ő nyelvükön szólva.

A magánszemélyek irányában mindenképpen hangsúlyozni kell, hogy számítógépeik, mobiltelefonjaik védelméről gondoskodjanak, hiszen naponta malware-ek tucatjai jelennek meg, amelyek veszélyeztetik az eszközök működéséét, adatokat lophatnak, terheléses támadás végrehajtására, bitcoin-bányászatra kényszeríthetik eszközeinket. Ugyanígy fontos, hogy a kellő óvatossággal, bizalmatlansággal viseltessünk azon személyekkel szemben, akik számítógéppel végzett tevékenységünk, jelszavaink iránt érdeklődnek.

Ne feledjük, hogy amit egyszer feltöltünk az Internetre, az már ott marad. Még a legrövidebb időtartamra történő megjelenítés és törlés közben is, azt ellophatják, majd manipulálhatják és felhasználhatják az eszköz tulajdonosa, használója ellen.

Sajnos a felhasználók azt hiszik, hogy ugyanúgy ki kell tölteni minden rubrikát a közösségi oldalakon, mint mondjuk a kormányhivatalban elénk tett űrlapon.

Összegzés

A személyiséglopás nem újkeletű jelenség. Az emberi jellemproblémákat megtapasztalva vélelmezhetjük, hogy egy személy egy másik személynek adja ki magát, használja iratát vagy annak nevében anyagiakról rendelkezik.

Az online személyiséglopás jelenségével összefüggő szakbizottsági munkánk során kiderült, hogy az Európai Unió tagországai a jelenséget bár jellemzően azonos keretek között értelmezik, de egységes fogalom és egységes joggyakorlat nem létezik. A fogalom széles körű és általános jellege miatt a Tanulmány is az OECD-jelentés definícióját fogadta el. Ebből adódóan vélhetőleg a Szakbizottság Tanulmánya további európai uniós állásfoglalást alapoz meg.

A büntetőjogi minősítésről szólva nem tartom támogatandónak azt a minősítést, ahol a személyi adat ellopását, mint eszközcselekményt quasi elnyeli a célcselekmény, például a card-not-present csalásoknál, amikor egy internetes vásárlást lopott bankkártyával hajtanak végre. Láthatóan két különböző jogi tárgy sérül.

A Tanulmány kriminalisztikai részében feltárta azt, hogy az online személyiséglopás módszerei jelentősen bővültek és egyre szofisztikáltabbak is lettek. Az adathalászat eszköztárában megtévesztő e-mailekkel, kémprogramokkal vagy a sértett bizalmába férkőzve szerzik meg a személyes adatokat, hol célzottan, hol random módon.

E gondolatok megírásában a büntetőjogi tapasztalatom segített. Örömmel tölt el, hogy hozzájárulhattam egy további kutatásra érdemes, számos jogi, kriminalisztikai kérdést felvető problémakör európai uniós vizsgálatához.