

Európai Bűnmegelőzési Hálózat

EUCPN Eszköztár Sorozat

13. szám

Az egyedi csalás megelőzése

Összefoglaló

Az EUCPN Titkárság által kiadott Eszköztár Sorozat 13. száma az *egyedi csalás* megelőzésével foglalkozik. A bolgár elnökség (2018 első féléve) a döntése alapján az alábbiakban megfogalmazottakkal kívánt foglalkozni:

"[...] csalásokhoz köthető ügyek, különösen a telefonos átverések. Az ilyen típusú bűnözés az elmúlt években vált nyereséges bűnözői tevékenységgé, és mind nemzeti, mind határokon átnyúló szinteken fejlődést mutat. Az ilyen tevékenységekre specializálódott bűnszervezetek dinamikusán fejlődnek és áldozatok egyre szélesebb körét károsítják meg. Tekintettel az áldozatok aktív közreműködésére és a bűnesetekbe való bevonásukra, valamint az áldozatok lelkére ható traumatizáló hatásokra, szigorú megelőző intézkedéseket kell tenni, figyelembe véve a helyi, nemzeti és határokon átnyúló szintek sajátosságait."

Az egyedi csalás olyan csalás, amelynek célpontjai átlagos, önálló állampolgárok. Az áldozatot először együttműködő magatartásra veszik rá, majd becsapják. Az e típusba tartozó csalásokkal kapcsolatos mai felfogásunk főként a jelenkori formákhoz kapcsolódik, és legvalószínűbben előforduló példája az adathalászat. Azonban fontos felismerni, hogy az egyedi csalás már sokkal régebb óta jelen van az emberek életében és az utóbbi évtizedek technikai fejlődése csak hozzájárult ahhoz, hogy ezek az átverések szélesebb körben elterjedhessenek és nagyobb méreteket ölthessenek annál, mint amit valaha is el tudtunk képzelni. Ki az, aki még soha életében nem kapott adathalász e-mailt?

Ahogy az a bolgár elnökség *magyarázatából* kiderül, az áldozatok aktívan részt vesznek az áldozattá válásuk folyamatában. A tettes szemet vet az áldozat pénzére, amit csak úgy

szerezhet meg, ha meggyőzi az áldozatot, hogy adja át neki. Ennek alapvető taktikája az, hogy az áldozatot szolgálatkész magatartásra veszi rá; ezt nevezik **bizalomra épülő manipulációnak** („social engineering”). A tettes így férkőzik az áldozat bizalmába, ami alapvetően fontos az átverése sikeréhez. A szociálpszichológia a jelenség még jobb megértését kínálja. A mindennapi társadalmi alapelvekhez való alkalmazkodással és az „emberi gyengeség” kihasználásával az elkövetők képesek beindítani a „meggyőzés második útjának” nevezett viselkedést. Az „első út” sok gondolkodást és kognitív erőfeszítést kíván, a másodikhoz viszont nem kell sok kidolgozás, és a reakció szinte öntudatlanul történik. Például egy hivatalos személy (rendőr) szerepének eljátszásával az elkövetők bizonyos fokú engedelmességet érnek el az áldozatok részéről. Ezeknek a társadalmi és kognitív tapasztalati szabályoknak megvan a maguk hétköznapi haszna, ugyanakkor megengedik az elkövetőknek, hogy saját javukra használják fel őket.

Ezeket a megtévesztési taktikákat **számos átverésnél** alkalmazzák. *Afrikai internetes pénzvadászok („419 scam”), „unokázós” vagy romantikus csalások, vezetői átverések („CEO fraud”)*... a lehetőségek tárháza kimeríthetetlen, ahogy a csalók kreativitása is. A megtévesztő csalások elkövetőinek skálája az egyszerre nagy nyilvánosságot elérő csalóktól az egyedi megközelítéseket alkalmazó átverőkig terjed. Az utóbbi eset tűnik egyre gyakoribbnak. A csalók ráeszméltek, hogy az áldozatok okos megválasztásával a „befektetésük hozama” nagyobb lesz. Az adathalász e-mailek egyre kifinomultabbak, és jól megválogatott egyénekhez (csoporthoz) szólnak. Ennek a fejlődésnek a meglepő utolsó lépéséhez hozzátartozik az új és a régi technológia egyesítése: a telefon. A „vishing”, vagyis telefonos adathalászat lehetőséget ad az internet és a telefon előnyeinek egyesítésére. Egy online telefonhívás gyakorlatilag semmibe sem kerül, nehezen lehet nyomon követni, és automatizálható. A telefon használata további előnyökkel is jár: az emberek jobban bíznak benne, és a meghittebb környezet hatására az áldozatokat könnyebben meg lehet győzni. Egy példája az egyre nagyobb szintű kifinomultságnak, amikor az elkövetők anyanyelvi beszélőket bérelnek fel, hogy a telefonhívás a lehető legtermészetesebben hasson.

Az egyedi csalások megértése egyelőre gyerekcipőben jár. Ezt a fajta büntényt nagy **sötétség** veszi körül, hiszen nagy részüket be sem jelentik. Az áldozatok nem tudják, hogy áldozattá váltak, az átverést nem élik meg elég súlyos incidensként, és nem gondolják, hogy a bejelentésnek van értelme, vagy egyszerűen azt sem tudják, hova forduljanak. Ezen kívül – mivel az áldozat szerepet játszik a saját viktimizációjában – a büntudat és a szégyen is visszatarthatja az áldozatot attól, hogy elmondja a történeteket. Egyes átverések beépített

„bejelentésgátló” mechanizmussal bírnak azért, hogy az áldozatoknak illegális tevékenységet kell végrehajtaniuk, így a bejelentéssel saját magukat is gyanúba kevernék. Ez olyan, mintha feladnák magukat.

Ez a nagy sötétség azt a **legendát** is elterjesztette, hogy az átverések áldozatai – könnyű prédaként – főként idős emberek. Néhány tanulmány cáfolta ezt a legendát, de azért elővigyázatosnak kell maradnunk, mivel a témában kevés kutatási eredmény áll rendelkezésre. Mindenesetre a fiatalabb vagy középkorú korosztály állítólag kevésbé fogékony a csalásokra. Egy másik létező legenda szerint az áldozatokat jellemzően tanulatlanok vagy a pénzügyekhez nem sokat értőnek állítják be, de ennek éppen az ellenkezője tűnik igaznak. Egy lehetséges magyarázat az ún. „knowing-doing gap”, ami azt jelenti, hogy az emberek sikeresen felismerik az átverés jeleit, de képtelenek ezt a tudást a saját helyzetükre alkalmazni.

Sajnos az ún. **balekok listája** létezése nem legenda. A telefonos csalók áldozataikat véletlenszerűen vagy nyilvánosan hozzáférhető jegyzékeket böngészve is kiválaszthatják, de keringenek közöttük olyan listák, amelyek a már megkárosított célpontokat tartalmazzák. Az ilyen listák létezése az ismételt viktimizáció magas szintjét mutatja. Például, egyes csalók rögtön jelentkeznek, hogy „segítenek” visszaszerezni az áldozat elveszett értékeit...

Mivel az ilyen típusú bűncselekmények rendőrség felé terelése különösen nehéz, a megelőzés szükségessége magas. Azonban az egyedi csalásokkal kapcsolatban eddig kevés tudományos és értékelő kutatást végeztek, mindenesetre néhány általános megállapítást azért megfogalmazhatunk. A leggyakoribb megelőzési taktika a nyilvánosság tájékoztatása. Ez megvalósítható akár általános figyelemfelkeltő kampányok révén, de amikor valamilyen képzés formájában történik, a pozitív hatások nagyobbak. Lényegében a képzések a korábban említett „knowing-doing gap”-et próbálják megszüntetni. Egy másik kulcsfontosságú taktika az áldozatokkal való munka. Az aktív szerepük, és az ismételt áldozattá válás létező veszélye miatt az áldozatok támogatásra szorulnak, és fel kell hívni a figyelmüket a különleges helyzetükre.

A bolgár elnökség alatt a Titkárság összegyűjtött néhány, a témához illő **bevált gyakorlatot**, amelyek a célcsoportjaik szerint kategorizálhatók. Az első kategória a teljes népességre összpontosít. Ezek figyelemfelkeltő kampányok, amelyeket például Bulgária, Svédország, Belgium vagy az Europol is megvalósított. A kampányokban igénybe vettek rádiós spotokat,

plakátokat, szórólapokat, apró reklámtárgyakat stb., amelyek hasznos információkat adtak át a nyilvánosságnak, és bemutatták, az emberek hogyan védhetik meg magukat az áldozattá válástól. A tevékenységek második köre az időseket célozza. Ebben a kategóriában már jóval interaktívabb módszereket alkalmaznak, ahogy a cseh példa is mutatja. Az idősek interaktív, oktatási célú szerepjátékokon vesznek részt, ahol megismerhetik a leggyakoribb megtévesztő csalásokkal, és megtudhatják, hogyan védekezzenek ezek ellen. Ez a „megélt tapasztalat” segíti őket abban, hogy megfelelően reagáljanak, ha a való életben találják szembe magukat ilyen helyzetekkel. A projekt értékelésekor bebizonyosodott, hogy ez a feltételezés megállja a helyét, hiszen a csoport tagjai közül két és félszer annyian utasítottak vissza hamis tranzakciókat, mint a kontrollcsoport tagjai, akik nem vettek részt az előadáson. A megelőzési tevékenységek utolsó kategóriája az áldozatokra összpontosít. Az ilyen típusú megelőzés szükségességét Ausztráliából, az Egyesült Királyságból és Kanadából származó példák támasztják alá. Azonban – még globális szinten is – kevés támogató szolgálat áll az egyedi családok áldozatainak rendelkezésére.

Végül, az EUCPN Titkársága különböző szakértők részvételével szervezett egy workshopot, hogy **ajánlásokat** fogalmazzanak meg a telefonos átverések megelőzése érdekében. Ezek az ajánlások a helyzeti bűnmegelőzés öt stratégiája köré szerveződnek. Az első lehetséges stratégia azon erőfeszítések növelése, amelyeket egy elkövetőnek meg kell tennie az átverés sikere érdekében. Ez akár elérhető a telefonszámok nyilvánossá tételének és elérésének korlátozásával is. Egy másik módszer lehet az egy személyhez tartozó telefonszámok korlátozása, vagy legalább ezek összekapcsolása egy bankszámlaszámmal vagy személyi igazolvány-számmal.

A második stratégia a kockázat növelése. Ebben az esetben kulcsfontosságú az információk megosztása. Az információk megosztása nem állhat meg a köz- vagy magánszféra határainál, vagy akár a nemzeti szintnél. Az összes partner rendelkezik olyan fontos információdarabokkal, amelyek beleillenek a „kirakóba”. Aki tudja, mivel áll szemben, az nagyobb eséllyel előzi meg az átverést. Azt mondanunk sem kell, hogy a bejelentést még egyszerűbbé és jobban hozzáférhetővé kell tenni. Az információt azonban a megosztás előtt még meg is kell szerezni. További javaslatokat tettek a hívó fél névtelenségének csökkentésére azért, hogy szinte lehetetlen legyen csalni a hívás helyszínével. A hangfelismerő szoftverek szintén érdekesek lehetnek.

Az ilyen típusú bűncselekményből származó jutalom csökkentése a telefonos átverések megelőzésének harmadik stratégiája. Ebben a vonatkozásban az illegálisan szerzett értékek lefoglalása a fő ajánlás. Ezért a pénz útjának nyomon követése kritikus fontosságú a gyanús tranzakciók felderítéséhez. Szakértőink egy EU-szintű kezdeményezést javasoltak, amit a bankszektor valósíthat meg.

Egy másik stratégia a provokáció csökkentése. Ebből a szempontból nagyon fontos, hogy nem szabad túl sok információt megosztani az átverés pontos elkövetési módjáról, mivel ezzel elkerülhető, hogy mások lemásolják a bűncselekményt. Emellett az ismételt áldozattá válás egyes formái is elkerülhetők. Az utolsó stratégia a kifogások megszüntetése. Ez a stratégia főleg a telefonos átverésekre vonatkozó figyelemfelkeltésről és az ellenük való védekezésről szól. Erre a korábban bemutatott bevált gyakorlatok szolgálnak példaként. A figyelemfelkeltő kampányoknak ugyanazt az üzenetet kell terjeszteniük. Ezért a köz- és magánszféra szereplői közötti, valamint nemzetközi együttműködéseket kell létrehozni a lehető legnagyobb konzisztencia érdekében, aminek a lényege, hogy *igenis nemet kell mondani*.