Illés Roland:

AZ ÁLLAMI SZEKTORBAN DOLGOZÓ SZEMÉLYEK KIBERTÁMADÁSOKKAL SZEMBENI VESZÉLYEZTETETTSÉGE

DOI: 10.35926/HSZ.2025.4.6

ÖSSZEFOGLALÓ: *A digitális kornak megfelelően a mindennapi ügyintézés mind állami, mind pedig vállalati szinten döntően a kibertérben történik. A kibertér azonban számos rosszindulatú felhasználó otthona is, akiknek adott esetben céljuk lehet akár egy állam megbénítása különböző kibertámadásokkal. A felhasználók közül az állami szféra munkatársai sem kivételek, jóllehet tevékenységük miatt érdemes fokozott óvatossággal használniuk a kibertér adta lehetőségeket.*

KULCSSZAVAK: *kibertámadás, social engineering, adathalászat, hírszerzés*

A SZERZŐRŐL:
Illés Roland szakreferens (Honvédelmi Minisztérium Katonai Örökség Főosztály – az MH vitéz Szurmay Sándor Budapest Helyőrség Dandártól vezényelve). (ORCID: 0000-0002-5584-5508; MTMT: 10096507)[1]

A KIBERFENYEGETETTSÉGEK AKTUALITÁSA

Magyarország egyik, ha nem a legnagyobb, kibertámadás kapcsán történő érintettségének tekinthető a 2024-ben a Védelmi Beszerzési Ügynökséget (VBÜ) ért zsarolóvírus-támadás *(ransomware attack)*. Maguk a támadás körülményei, a támadási vektor, illetve az, hogy a támadók hogyan fértek hozzá a szerver tartalmához, ismeretlenek, illetve nem nyilvános adatok. A támadás ugyanakkor megmutatta, hogy a különböző, a kibertérből származó fenyegetettségek igenis valósak, illetve hogy szervesen érintik az állami szférát, beleértendő annak dolgozóit is.

A kibertámadásoknak azonban van egy fontos „mellékszereplője", ez pedig a felhasználó. Megfelelő kompetenciák, tudatosság és kibertérre vonatkozó ismeretek nélkül még inkább kidomborodik az az axióma, amely szerint minden rendszer leggyengébb eleme a felhasználó. A felhasználókat ténylegesen megcélzó támadások pszichológiai alapúak, lényegük, hogy a támadott személyt különböző cselekedetek elvégzésére vegyék rá, és/vagy bizalmas információt nyerjenek ki tőle. Ezeket a támadásokat nevezi a szakterület összefoglalóan *social engineering*nek.[2]

A támadások gyakoriságáról, illetve arról, hogy mekkora súllyal bír a rendszerfelhasználók tudatosságának növelése a megelőzés érdekében, mindent elárul az a statisztika, amely sze-

[1] A szerző 2019-től a Honvédelmi Minisztérium munkatársa, a cikkben megfogalmazott észrevételei és megállapításai teljes mértékben önállóak, a cikkben szereplő vélemények és következtetések nem a Honvédelmi Minisztérium, a Katonai Nemzetbiztonsági Szolgálat és/vagy a Magyar Honvédség hivatalos álláspontjai.

[2] What is Social Engineering?

rint a 2023-ban elkövetett összes kibertámadás 91%-ban tartalmazott *social engineering*et, illetve használta fel az ily módon megszerzett információt.[3]

Mindezekkel összefüggésben azonban kijelenthető, a *social engineering* támadás „kilép" a kibertérből, és a fizikai felhasználót, annak viselkedését, személyiségét és gyengeségeit célozza meg, így okozva súlyos biztonsági kockázatot.

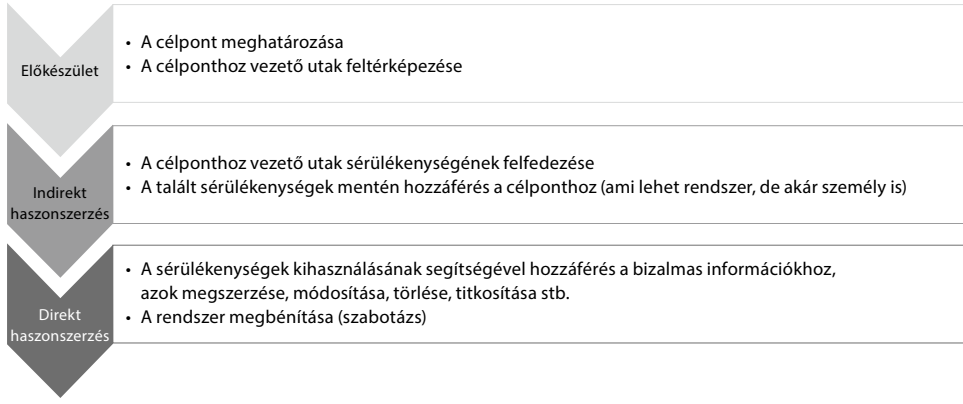
KI A TÁMADÓ, ÉS MIÉRT AZ ÁLLAMI SZFÉRA ELLEN?

A válasz az első kérdésre közhelyes, de nagyon egyszerű: bárki lehet a támadó. A *social engineering* támadás (ahogyan minden kibertámadás) célpontját kiválaszthatta egy egyszerű hacker, egy hackercsoport valamely tagja, vagy – legsúlyosabb esetben – egy ellenérdekelt állam hírszerző szolgálata. Az elkövető kilétét átmenetileg háttérbe szorítva koncentráljunk a támadás céljára, ami minden esetben haszonszerzésre irányul, legyen az direkt vagy indirekt.

Direkt haszonszerzésnek minősül, ha közvetlenül vagy rövid távon kézzelfogható eredményt produkál a támadás, például a támadó adatokhoz jut hozzá, anyagi hasznot szerez, megbénít/működésképtelenné tesz egy informatikai rendszert. Előbbi kategorizálás alapján joggal tekinthetjük a VBÜ-t ért kibertámadást is direkt haszonszerzést eredményező, ámbár illegális tevékenységnek.

Indirekt haszonszerzésnek tekinthető az, ha a támadó nem fedi fel kilétét, nem teszi egyértelművé jelenlétét a rendszerben, hozzáférését a rendszer bizonyos elemeihez, fájljaihoz, hanem azokat – katonásan szólva – tartalékban tartja, annak érdekében, hogy egy későbbi támadást készítsen vele elő. Például a támadó ugyan hozzáfér egy felhasználó bejelentkezési azonosítójához, vagy felfedezett egy sérülékeny pontot a rendszerbiztonságban, ugyanakkor ezzel még nem élt vissza. Összegezve a bekezdést, megállapíthatjuk, hogy az indirekt haszonszerzés a direkt haszonszerzés előkészülete.

Az előbbiekben ismertetett kategorikus megkülönböztetés azonban további kifejtést igényel, lévén minden kibertámadás folyamatának szerves része az indirektből direkt haszonszerzésbe történő átmenet. Egy kibertámadás menetét az alábbi ábra szemlélteti:



1. ábra *Egy kibertámadás kronológiája (Szerkesztette a szerző)*

[3] Social engineering emerges... 2024.

Teljesen jogosan merül fel a kérdés, hogy hogyan is jön ehhez az egészhez a *social engineering*, hogyan kapcsolódik a felhasználó és személyes biztonsága, védettsége a rendszerszinten megvalósuló támadásokhoz. A válasz abban rejlik, hogy a felhasználó ugyanúgy részese egy informatikai rendszernek, mint az azt üzemeltető informatikus, a fájlszerverek, a szoftverek és egyebek. A felhasználó így válik egy élő, lélegző és beszélő, potenciális támadási felületté. A felhasználó sérülékenysége sokrétű, de minden esetben valamilyen hiba/mulasztás kihasználása teszi lehetővé azt a támadónak, hogy *social engineering* támadása sikerrel járjon. Az ilyen jellegű támadások sokrétűek, a teljesség igénye nélkül következzen hat a leggyakrabban előforduló metódusok közül:

– *Phishing* és *spear phishing*: ebben az esetben a támadó önmagát egy valós, hivatalos személynek/szervezet képviselőjének adja ki, annak érdekében, hogy adatokat szerezzen. Példának okáért egy, a hivatalos bejelentkezési űrlapra hasonlító weboldal linkjét küldi, és megkéri a felhasználót, hogy karbantartás miatt ismét jelentkezzen be. A *spear phishing* a *phising* „fejlesztett" változata, ebben az esetben a támadó tudatosan keresi meg a potenciális áldozatot, annak nyilvánosan elérhető adatai, illetve közösségi médiában fellelhető profilja, profiljai nyomán, lényegében nyílt forrású hírszerzést (OSINT) alkalmazva. Szorosan kapcsolódik e két támadási formához a *whaling*, ami tudatosan a vállalatban/cégben/szervezetben magas beosztást betöltő személyt célozza meg.[4]
– *Smishing* és *vishing*: e támadási technikák alkalmazásakor a támadó a *phishing*hez hasonló céllal keresi fel a potenciális áldozatot, azonban nem e-mailt, hanem telefonhívást/SMS-üzenetet/egyéb üzenetküldési módot használ.[5] A *vishing* kapcsán érdemes megemlíteni, hogy a mesterséges intelligencia hangklónozási képességei komoly veszélyt hordoznak magukban, és jelentősen növelhetik az ilyen jellegű támadások sikerességét, ha a potenciális áldozatot a főnöke/felettese hangjával visszaélve tévesztik meg.
– *Pretexting*: ebben az esetben a támadó olyan környezetet teremt, ahol az áldozat kötelességének érzi az együttműködést. Leggyakoribb metódus az, amikor a támadó ügyfélnek vagy a cég egy magas rangú tisztségviselőjének adja ki magát. A technika inkább a nagy mennyiségben ügyfelek adatait kezelő és tároló cégekkel szemben számít gyakorinak, ugyanakkor az állami szektorban a személyügyi nyilvántartás is olyan területet jelent, amely fokozottan veszélyes a támadások szempontjából.[6]
– *Baiting*: nem véletlen veszi át a csali kifejezést az angol terminológia, a támadási technika abból áll, hogy az áldozat bekapja-e a horgot, megteremtve a támadás sikerét. A hivatkozott forrás által hozott példával élve egy konferencia szervezője ingyen pendriveokat osztogathat – reprezentációs célból. A probléma abban rejlik, amikor a pendrive kártékony kódot tartalmaz, ami már az első használatkor települ az immár fertőzött gépre, ahonnan – amennyiben nincs megfelelő biztonsági rendszerrel ellátva a teljes számítógépes hálózat –, rendszerszintű problémákat okozhat.[7]
– Felsorolásom végén kap helyet a „valamit valamiért" típusú támadás. Ennek motivációja rengeteg lehet, az áldozat belekényszerülhet zsarolásból, anyagi/erkölcsi haszonszerzés céljából, illetve bármilyen egyéb motivációnak betudhatóan is.[8] Nagyon banális példán

[4] 6 types of social engineering attacks... 2024.
[5] Uo.
[6] Uo.
[7] Uo.
[8] Uo.

keresztül bemutatva: a támadó anyagi haszonszerzés lehetőségét kínálja fel áldozatának, aki anyagi ellenszolgáltatásért cserébe bizalmas adatokat juttat el a támadónak.

Nem indokolatlan, hogy a felsorolásban külön pontot kapott a valamit valamiért típusú támadás, hiszen ez szoros összefüggésben áll a bizalmas adatokat kezelők/bizalmas pozíciót betöltők leggyakoribb ellenségével, a kompromittációból fakadó zsarolással.

A bizalmas adatok az állami szféra szervezetének és rendszerének külön szegmensét képezik, így az azokat kezelő személyek fokozottan kockázatosak a *social engineering* alapú támadások tekintetében. Az állami szférában dolgozók veszélyeztetettsége érdekében elengedhetetlen írnunk a kibertámadások elkövetőiről és az elkövetési motivációról.

A kibertérben a határok összemosódnak, egy-egy állami cég/szervezet/hivatal elleni támadás mögött ugyanúgy meghúzódhat egy hackercsoport, mint egy ellenérdekelt állam. Noha az elkövető egy hackercsoport, büntetőjogi fogalommal élve a felbujtó szerepét betöltheti egy másik állam is, mint ahogyan arra a közelmúlt eseményei példával is szolgáltak.

2017-ben a WannaCry nevű zsarolóvírus-támadás több mint 150 országot érintett. A támadások mögött az Amerikai Egyesült Államok egyértelműen Észak-Koreát nevezte meg mint felbujtót. Ukrajnát szintén 2017-ben érte hasonló támadás a NotPetya nevű vírus által, viszont itt a vírus kifejezett célja pusztítás okozása volt a kormányzati és a pénzügyi szektor tudatos célbavételével. Elkövetőként Oroszország volt sejthető, a Kreml azonban tagadta, hogy bárminemű köze volna a támadáshoz.[9]

Az állam mint célpont több szempontból vet fel aggályokat, amelyek a támadó céljától, szándékától függenek. Amennyiben egy állam működését egy másik entitás képes megbénítani, úgy az érintett állam akár egy óriási (anyagi) követelés teljesítésére is kényszeríthető, ha a támadás olyan létfontosságú rendszerelemet is legyőzött, mint például az egészségügyi szektort, a bankszektort, az államigazgatást, vagy legvégső esetben a nemzetvédelmi képességeket.

Emellett egy megbénított állam magán hordozza azt a negatív politikai üzenetet, hogy a vezetés képtelen garantálni állampolgárainak (és adataiknak) védelmét és biztonságát. Példának okáért egy, az egészségügyi rendszerben tárolt adatokat ért támadás során a CIA-triád (Confidentiality – bizalmasság, Integrity – sértetlenség, Availability – elérhetőség) mindhárom adatkezelésre vonatkozó alappillére sérül.

Összefonódó területek – nyílt forrású hírszerzés, social engineering

Különösen érdekes terület a már korábban említett *spear phising*, ahol a támadó tudatosan választja ki és célozza meg áldozatát annak érdekében, hogy kárt okozzon és/vagy bizalmas adatokhoz férjen hozzá. Az olyan sokszor és sokat ismételgetett „közmondás", mely szerint az internet nem felejt, az ilyen támadás előkészítésekor fokozottan aktuális.

Tekintsünk vissza az írásom korábbi részében bemutatott ábrára, annak is első részére, amely a célponthoz vezető utak és sérülékenységek megtalálásáról és feltérképezéséről szól. Az áldozat megkereséséhez és feltérképezéséhez, azaz a profilozáshoz a támadónak a legnagyobb segítséget a közösségi médiafelületek adhatják, különösen akkor, ha az áldozat nincs tisztában az ilyen jellegű platformokon rá leselkedő fenyegetésekkel, illetve potenciális adatvédelmi kockázatokkal. A jelenség olyannyira elterjedt, hogy a hír- és információszer-

[9] Medhurst 2024.

zésnek egy külön ága, a Social Media Intelligence (SOCMINT) mára egy létező fogalommá vált, hiába tűnhetett ez korábban csak egy utópisztikus/disztópikus fantáziaterméknek.[10] Amennyiben rendszertani kategóriákat kívánunk felállítani, a nagyobb halmaz továbbra is a nyílt forrású hírszerzés, tekintettel arra, hogy ide tartozik az illetőről nyilvánosan elérhető összes információ, amelynek egy alrendszere a közösségi média és a közösségi média alapján történő hírszerzés (SOCMINT).

Maga a – nevezzük nevén – hírszerzési és profilozási tevékenység elengedhetetlen a hatékony támadás kivitelezéséhez. A digitális és tömegkommunikáción alapuló világban azonban már nem feltétlenül indokolt, hogy a támadó áldozatát személyesen is megfigyelje, az áldozat profilja annak internetes/nyilvánosan elérhető tevékenységével javarészt összeállítható.

A legnagyobb veszélyt a felhasználóra az internet és a közösségi média területén nem feltétlenül az ellenérdekelt fél jelenti, hanem saját felhasználási szokásai. A legnagyobb súllyal bíró hiba az, ha a felhasználó nincsen tudatában az internetes tevékenység által hordozott veszélyeknek, illetve nem tesz meg minden tőle telhetőt azért, hogy adatai ne kerüljenek illetéktelen kézbe.

A már említett közösségi oldalak száma végtelen, így a teljesség igényével nem is lehet bemutatni, mekkora kockázatot rejt magában azok kellő körültekintés és odafigyelés nélküli használata. A teljesség igénye nélkül azonban négy közösségimédia-platform felhasználásával bemutatom, hogy hogyan is képes egy támadó „lenyomozni" bárkit, aki nem kellően körültekintő.

Első ránézésre egy profilkép is kellő kiindulási alapot nyújthat a támadónak ahhoz, hogy az áldozat „feltérképezését" megkezdje. A profilkép árulkodhat lakóhelyről, hobbiról, családi állapotról, tanulmányokról és – bizonyos esetekben – anyagi, társadalmi helyzetről is. A profilképet követően kerülhet sor a nyilvános adatok begyűjtésére és feldolgozására, amelyek a korábbi mondatban ismertetett körülmények mellett immáron tartalmazhatnak egyéb közösségi médiafelületeken használt felhasználóneveket, email-, de akár telefonos elérhetőséget is.

Esetünkben az email-cím, illetve a telefonszám nem megfelelő kezekbe kerülése jelenti a legnagyobb biztonsági kockázatot. Egy email-címhez történő jogosulatlan hozzáféréssel a támadó kis túlzással megbéníthatja áldozatát, illetve annak digitális tevékenységét is, beleértve például az eltulajdonított fiók(ok) visszaszerzésének lehetőségét.

Megmaradva a közösségi médiaplatformok területén, a következő, önmagában jelentős veszélyt hordozó kockázati tényező az, ha a támadó az ismerősök listájához is sikeresen hozzáfér. A kapcsolati térkép meglétének további mélységekig történő kibővítésével a támadó sikeresen hozzáférhet olyan adatokhoz is akár, mint az áldozat kollégáinak, adott esetben felettesének, feletteseinek kiléte. Fontos kiemelni, hogy a közösségi média kellő óvatossággal történő használatára vonatkozó okfejtésemben továbbra is „csupán" annál a lépcsőnél tartunk, ahol a támadó nyílt forrású adatokhoz fér hozzá, a fiók feltörése még nem került szóba.

Az általános, profilozási munkának tekinthető információszerzésben, mint említettem a korábbiakban, négy közösségimédia-platformnak tulajdonítok kiemelt jelentőséget. A megszerzendő, illetve megszerezhető adatok platformonként szoros átfedésben állnak, a kategorizálás hangsúlya a médiaplatform, illetve a bizonyos információ megszerezhetőségének valószínűsége közötti összefüggésen nyugszik. Maga a cél továbbra is az, hogy a támadó a potenciális áldozatról a lehető legtöbb terület vonatkozásában a lehető legtöbb információt szerezze meg, a teljesség igénye nélkül olyanokat, mint profilkép és egyéb fotók, amelyek

[10] Social Media Intellgience... 2024.

azonosításra alkalmasak, iskolai végzettség(ek), családi állapot, lakó- és tartózkodási hely, érdeklődési kör(ök), anyagi és társadalmi helyzet stb.

1. táblázat *Az egyes médiaplatformokról beszerezhető információk (Szerkesztette a szerző)*

A médiaplatform neve	Adatok, amelyekhez a támadó a legnagyobb valószínűséggel hozzáférhet
Facebook	képanyag, végzettségek, munkahely, családi állapot, lakó- és tartózkodási hely
Instagram	képanyag (alapvetően több, mint ami a Facebookon fellelhető), végzettségek, munkahely, családi állapot, lakó- és tartózkodási hely
LinkedIn	képzettségek, végzettségek, szakmai tapasztalat, munkahely és beosztások
TikTok	hobbik, szabadidős tevékenyég, képanyag, hanganyag

Az e platformokon elvégzett SOCMINT, valamint az áldozatról nyílt forrásból elérhető egyéb anyagok és információk, mint látjuk, kellő adatot szolgáltatnak ahhoz, hogy egy profil készülhessen a delikvensről.

HOGYAN LESZ AZ ADATOKBÓL, INFORMÁCIÓKBÓL ÉS PROFILBÓL TÁMADÁS?

Elsőként érdemes tisztázni azt, hogy az áldozat valóban a támadás elsődleges célpontja-e, avagy csupán járulékos veszteség az eredményes támadás előkészítéséhez, lebonyolításához és megvalósításához. Példának okáért, egy állami szervezet esetében a kifejezett célpont lehet a szervezet vezetője vagy a szervezetben egyéb tisztséget betöltő személy, de a hozzá vezető út munkatársakkal, akár családtagokkal is lehet „kikövezve".

2. ábra *Állomások a támadási folyamatban (Szerkesztette a szerző)*

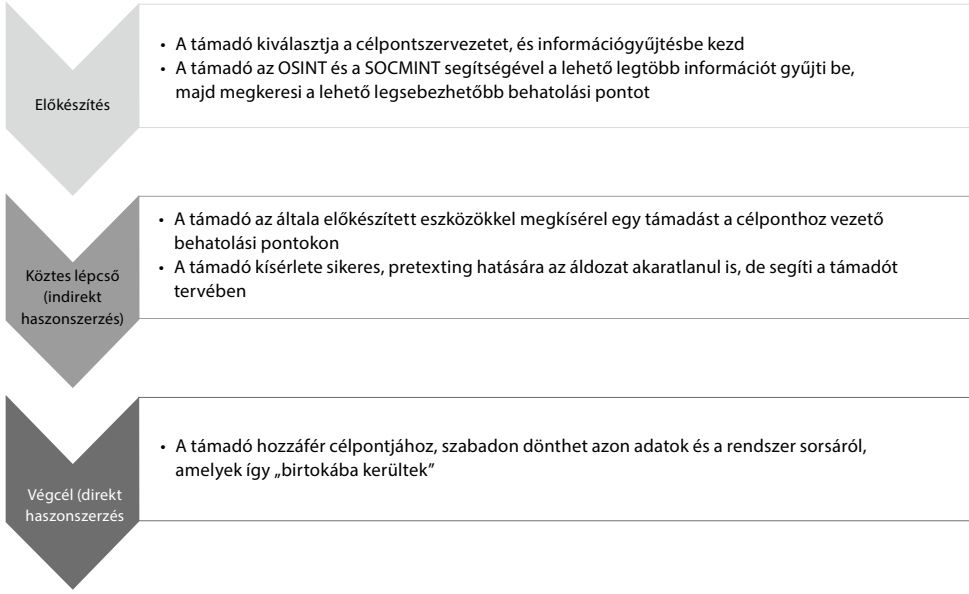
Érdemes visszatekinteni arra a fejezetre, amelyben a leggyakoribb *social engineering* támadástípusokat mutattam be, hiszen ezeket a metódusokat alkalmazzák a „szimulált esetünkben" is. Tételezzük fel, hogy a támadónak olyan egyszerű dolga volt, hogy csupán nyílt forrású adatokból és a közösségi médiából összeállította a szervezet hierarchiáját, felépítette annak „állománytábláját" is (amit nem nehéz úgy megvalósítani, hogy az áldozat profiljain a munkahely, adott esetben még akár a beosztás is nyilvános adat). A 2. ábrára tekintve, balról jobbra haladva a hozzáférési jogosultság is növekszik, így amennyiben a támadó célja adatszerzés, nyilvánvaló érdeke, hogy a szervezeti vezetőtől tulajdonítson el annyi információt, amennyit csak lehetséges, felhasználva a beosztott(ak)at és a vezetőhelyettes(eke)t. A korábbiakban már kifejtett *pretexting* ilyenkor juthat kiemelkedő szerephez. Maga a *pretexting* veszélyessége a nagyvállalatok körében is fokozott aggodalomra ad okot, lé-

vén a tiltott információszerzésből fakadó következmények az üzleti szférában is súlyosak, adott esetben maradandóak is.[11]

Visszatérve az állami szektorban felhasználható *pretexting*re, ahogyan a piaci szereplőknél is, leggyakrabban a munkahelyi vezető és/vagy az informatikai üzemeltetés nevével, látszatával élnek vissza. A gyakoriság mértékéről egy 2021-es tanulmány tanúskodik: a szerzők által meginterjúvolt vállalatok 69%-a tapasztalt olyan *social engineering* támadási kísérletet, amikor a támadó az informatikai/biztonsági üzemeltetés „álarcát" öltötte magára.[12]

Amennyiben annyira előnyben van a támadó, hogy a profil mellett (természetesen az ahhoz szükséges adatokkal és információkkal) még viselkedési mintázatot is sikerül reprodukálnia (például rövidítések, szleng, egyedi beszédelemek, emoji használata stb.), úgy az növeli a sikeres támadás valószínűségét. Amiatt, hogy a *pretexting* sikeresen működhessen, ahogy már említettem, a támadó szempontjából érdemes lehetőség szerint a legnagyobb befolyással rendelkező személynek kiadnia magát (ideértendő az IT- és/vagy a biztonsági üzemeltetés is), hiszen így tudja áldozatát a lehető legkönnyebben presszionálni. A sikeres *pretexting* elengedhetetlen elemét képezi a figyelmet felkeltő nyelvezet[13] és az érzelmekre, naivitásra, járatlanságra, illetve egyéb, egyéni érdekekre való ráhatás.[14]

Fontos kiemelni, hogy a *pretexting* nem feltétlenül csak önmagában jelentkező támadási forma, gyakran összefügg más, *social engineering* alapú eljárási metódusokkal, például a *spear phishing*gel, hiszen a támadó elsőnek elhiteti áldozatával a szükséghelyzetet, illetve azt, hogy a helyzet megoldásához az áldozat közvetlen segítségére van szükség, majd ezt követően alkalmaz olyan *(spear) phishing* eljárásokat, amelyek a támadás sikerét és hatásait



3. ábra *Spear phishing és pretexting alapú támadási folyamat (Szerkesztette a szerző)*

[11] Sandberg 2015.
[12] Ngugi et al. 2021.
[13] Ganchenko 2022.
[14] Longtchi et al. 2024.

fokozzák. Példának okáért, a *pretexting* keretein belül küldhető az áldozat számára olyan hamis űrlap, amelynek segítségével a támadó megszerezheti bejelentkezési adatait, telepíthető számítógépére olyan kártékony szoftver, amely naplózza a billentyűleütéseket *(keylogging)*, létesíthető a géppel távoli asztali kapcsolat stb. Mindebből kitűnik, hogy a *social engineering* támadás során használható eszközök nem egymást kizáró viszonyban, hanem mellérendelt szerepekben helyezkednek el.

Az csupán a támadó szándékán múlik, hogy sikeres adatszerzés után mihez kezd, szabotálja-e a rendszert, vagy csak adatokat tulajdonít el, módosítja őket stb. Amennyiben a biztonsági fenyegetést nem térképezték fel időben, ezért természetesen a megelőzésnek mindig előnyt kell élveznie.

Vizualizálás, illetve a fenyegetés súlyosságának hangsúlyozása érdekében a 3. ábra egy olyan kibertámadás menetét mutatja be, amely során a támadó sikeresen alkalmaz *spear phishing* és *pretexting* technikákat, hogy egy rendszerhez hozzáférjen.

Mik is lehetnek ezek a *pretexting* technikák, amelyekkel ennyire könnyen meg lehet téveszteni valakit, hogy gyakorlatilag gyanútlanul kiadja adatait illetéktelen személynek?

VIRTUÁLIS ESETTANULMÁNY

Ahogyan azt korábban kifejtettem, a sikeres *pretexting* (ahogy minden *social engineering*) támadás alapja a pszichológiai nyomásgyakorlás és manipuláció, amelyek nem ritkán hangsúlyozzák, hogy a probléma megoldásában a potenciális áldozatnak mekkora szerepe van, vagy mekkora károkat okozhat az, ha az áldozat nem működik együtt.

Olyan, látszólag bagatellnek tűnő támadási kísérletekről beszélünk, mint amikor a támadó az informatikai üzemeltetés egyik vezetőjének adja ki magát, levelében pedig arra kéri a felhasználót, hogy jelentkezzen be újra adataival a megadott űrlapon, mivel szerverkarbantartás miatt minden korábbi bejelentkezett felhasználónak újra be kell jelentkeznie.

A megadott űrlap természetesen csak egy klónja a valós belépési felületnek. Egyes esetekben ez első pillantásra is eldönthető (például helyesírási hibából, „fordítószagú" magyar mondatokból, helytelen ragozási forma használatából, illetve magára a linkre tekintve is könnyedén kiderül), hogy hamisított weblapról beszélünk, de vannak esetek, amikor csak nagyon „szakavatott" szemeknek tűnik fel, hogy hamisság van a kérés mögött. Egyik legnehezebben kiszűrhető csalási trükk például az URL-ben a latin ábécé „a" karaktere helyett a cirill ábécé „α" betűjének használata (főleg dőlt betű esetén még nehezebb a különbségtétel). Megfelelő felkészítés, illetve tudatosságnövelési tréningek nélkül – saját meglátásom szerint – marginális annak az esélye, hogy az átlagos rendszerhasználó képes egy pillantásra kiszűrni a különbséget a két karakter között, ezzel is elkerülve azt, hogy kibertámadás áldozatává váljon.

Ugyancsak nem mindennapos az, hogy egy látszólag valódi weboldalt megnyitva a felhasználó megvizsgálja a hamis weboldal forráskódját, és összevesse azt az eredetivel. Ugyanakkor alapesetben nem is bátorítandó erre a felhasználó, hiszen kellő óvintézkedések hiányában már a hamisított weboldal linkjére kattintva települhet számítógépén/böngészőjében olyan kártékony bővítmény, amely, ha észrevétlen marad, jelentős károkat képes okozni (billentyűzetnaplózás, távoli asztali elérés, internetforgalom keresztülvitele harmadik állomáson, azaz *packet sniffing* stb.).

Esettanulmányunk onnan folytatódik, hogy a gyanútlan áldozat megadta belépési adatait a támadónak, hiszen azt gondolta róla, hogy az valóban az informatikai üzemeltetésnél dolgozik. A támadó innentől hozzáférhet áldozatának levelezőrendszeréhez (ha a vállalat ext-

ranet-kereteken belül lehetőséget biztosít arra, hogy a felhasználó a munkaállomásától távol is megtekintse levelezését), ideértve a naptárbejegyzéseket, kontaktszemélyeket, valamint minden korábbi, ki nem törölt beérkezett, továbbá elküldött levelet is, azok címzettjeivel együttesen. A levelezőrendszerhez hozzáférve lehetősége nyílik továbbá a teljes szervezeti névjegyzékhez való hozzáféréshez, amely nem csak e-mail-címeket, hanem vezetékes és/vagy mobiltelefonszámokat, fizikai címeket (pl. az iroda székhelye, az érintett személy irodája) tartalmazhat.

Nem érdemes eltekinteni attól sem, hogy az így a támadó birtokába jutó üzleti titkok, illetve egyéb minősített információk mellett a „fertőzött" felhasználó kiváló lehetőség a támadó számára ahhoz, hogy a fertőzött gépek számát tovább növelje különböző technikák bevetésének segítségével (például a fertőzött e-mail-címről kártékony kódot tartalmazó fájlt küld el a szervezet minden egyes alkalmazottjának). Ismételten fontosnak találom kihangsúlyozni azt, hogy a szervezeten belüli valódi e-mail-címről érkező levelekkel szemben az ember alapvetően nem viselkedik defenzív előítélettel, hacsak nem tűnik ki egyértelműen a levél tárgyából, szövegéből vagy a mellékletből, hogy valójában nem az küldte a levelet, mint akinek a neve a feladó mezőben szerepel.

Megmaradva példánknál, áldozatunk olyan munkakörben dolgozik, amelyben a felső vezetők számára készít kivonatos elemzéseket (támadónk ezt pedig a nyilvánosan hagyott közösségimédia-adatokból tudta meg…), átvizsgálva levelezését a támadó megtalálja, hogy rövid határidős elemzést kell készítenie áldozatunknak a vezetőség számára. Támadónk ebből kiindulva elkészít egy olyan .pdf kiterjesztésű fájlt, amely kártékony kódot tartalmaz – lévén a .pdf fájlkiterjesztés támogatja a JavaScript programozási nyelvet[15] –, amely lehet zsarolóvírus, botnet stb., és a felhasználó számára megnyitáskor csak egy hibaüzenetet jelenít meg. Ezt a fertőzött fájlt szétküldve a felhasználó nevében a támadónak nincsen más dolga, csak várnia kell, hogy a címzettek (akár csak egy is) megnyitják a fájlt, pontosabban megpróbálják megnyitni. Amennyiben ez megtörténik, és a kódnak van hozzáférése a rendszert működtető szerverhez, úgy a következmények bénító hatással jelentkeznek.

Zsarolóvírus-támadás esetén egy ilyen akció – amennyiben olyan létfontosságú rendszerelemet bénít meg, amely az életfenntartással, illetve az életminőség fenntartásával szoros összefüggésben áll –, félelmetes, akár azonnali károkat képes okozni. Elég ehhez csak a 2020-as düsseldorfi kórház elleni zsarolóvírus-támadásra gondolni, amelynek bár halálos áldozata nem volt, mégis rávilágított arra, az egészségügyi intézmények mennyire sebezhetők, illetve mekkora károkozás lehetséges azok elleni sikeres kibertámadásokkal.[16]

Esettanulmányunk tanulságát leegyszerűsítve megállapítható, hogy az egész támadás origója az óvatlan közösségimédia-használatra, illetve a virtuális térben való navigálás közbeni figyelmetlenségre vezethető vissza. Visszautalva írásom korábbi fejezeteire, amennyiben itt a kiberbűncselekmény célja kifejezetten zavar- és pánikkeltés, adatszerzés, valamint e tevékenységek elvégzése úgy, hogy a támadó ezzel kifejezetten egy államot és/vagy annak lakosságát kívánja „büntetni", vagy az államot feladatainak ellátásában korlátozni, joggal beszélhetünk kiberterrorizmusról is.

[15] Fishbein 2023.
[16] Krempl 2024.

ÖSSZEGZÉS

Összegezve az írásomban foglaltakat, meg kell állapítani: kiberbűncselekmény áldozatává bárki válhat, amennyiben nem kellően körültekintő és óvatos a digitális térben való navigálás során. A megelőzés kapcsán elengedhetetlen kiemelni: az érintett szakemberek hívják fel az adott szervezetnél dolgozók figyelmét arra, hogy „közkinccsé" tett adataikat bárki bármire, bármikor felhasználhatja, így indokolt fokozott óvatossággal elvégezni közösségimédia-profiljaikon az adatvédelmi beállításokat, beleértve azt is, hogy mely adataik kik számára láthatóak, ismerőseik listájához ki férhet hozzá, ki láthatja érdeklődési köreiket, munkahelyüket, beosztásukat.

Érdemes emellett a felhasználók figyelmét arra is ráirányítani, hogy tájékozódjanak a leggyakoribb *social engineering* támadási formákról, eljárásokról, az azokkal kapcsolatos megelőzési lehetőségekről. Legyenek továbbá tudatában annak, hogy eszközeiken a szoftvereket lehető leghamarabb frissítsék, valamint tegyenek meg mindent saját informatikai biztonságukért (beleértendő az is, hogy ne használjanak nyilvános internethálózatot, a már említett *packet sniffing* nevű jelenség okán se).

A probléma szervezetszintű megközelítésében a szervezetek által kidolgozott veszélyhelyzeti és helyreállítási terveknek tartalmaznia kell külön kibertámadásokkal foglalkozó fejezeteket, ideértve a kibertámadásokra vonatkozó kockázatelemzést is. Továbbá a digitális kor követelményeinek megfelelve kiemelt fontosságú, hogy az adott szervezetnek megfelelő minőségű, képzett és elegendő létszámú informatikai üzemeltetési állománnyal kell rendelkeznie.

FELHASZNÁLT IRODALOM ÉS FORRÁSOK

- *6 types of social engineering attacks and how to prevent them.* Mitnick Security, 2024. 11. 07. https://www.mitnicksecurity.com/blog/types-of-social-engineering-attacks (Letöltés időpontja: 2025. 01. 20.)
- Fishbein, Nicole: *How to analyze malicious PDF files.* Intezer, 2023. 11. 01. https://intezer.com/blog/incident-response/analyze-malicious-pdf-files/ (Letöltés időpontja: 2025. 01. 27.)
- Ganchenko, M. I.: *Human psychological and biometric factor in the development and use of social engineering methods in peacetime and wartime.* Semantic Scholar, 2022. https://doi.org/10.31673/2409-7292.2022.011626 (Letöltés időpontja: 2025. 01. 27.)
- Krempl, Stefan: *Ransomware: cyberattacks on large German hospitals on the decline.* Heise.de, 2024. 04. 10. https://www.heise.de/en/news/Ransomware-cyberattacks-on-large-German-hospitals-on-the-decline-9679711.html (Letöltés időpontja: 2025. 01. 27.)
- Longtchi, Theodore et al.: *Quantifying Psychological Sophistication of Malicious Emails.* Arxiv, 2024. 08. 22. https://doi.org/10.48550/arXiv.2408.12217 (Letöltés időpontja: 2025. 01. 27.)
- Medhurst, Rachael: *Five notorious cyberattacks that targeted governments.* The Conversation, 2024. 08. 30. https://theconversation.com/five-notorious-cyberattacks-that-targeted-governments-230690 (Letöltés időpontja: 2025. 01. 20.)
- Ngugi, Benjamin K. et al.: *Reducing tax identity theft by identifying vulnerability points in the electronic tax filing process.* Semantic Scholar, 2021. 08. 30. https://doi.org/10.1108/ics-05-2021-0056 (Letöltés időpontja: 2025. 01. 27.)
- Sandberg, J.: *Human element of corporate espionage risk management: literature review on assessment and control of outsider and insider threats.* Semantic Scholar, 2015. https://www.

semanticscholar.org/paper/Human-element-of-corporate-espionage-risk-%3A-review-Sandberg/040077453925de9326ae70be879c7227989f8475 (Letöltés időpontja: 2025. 01. 27.)

- *Social Media Intellgience (SOCMINT) in Modern Investigations.* Osint Industries, 2024. 10. 31. https://www.osint.industries/post/social-media-intelligence-socmint-in-modern-investigations (Letöltés időpontja: 2025. 01. 21.)
- *Social engineering emerges as top threat in the cyber security landscape.* Fintech Global, 2024. 10. 17. https://fintech.global/2024/10/17/social-engineering-emerges-as-top-threat-in-cyber-security-landscape/ (Letöltés időpontja: 2025. 01. 20.)
- *What is Social Engineering?* Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering (Letöltés időpontja: 2025. 01. 20.)