DOI: https://doi.org/10.12700/btsz.2025.7.2.49

DIGITAL DATA PROTECTION AND INFORMATION SECURITY: SOURCES OF DANGER IN THE ONLINE SPACE, METHODS OF PHISHING (SOCIAL ENGINEERING)

ADATVÉDELEM ÉS INFORMÁCIÓBIZTONSÁG: AZ ONLINE TÉRBEN FELLELHETŐ VESZÉLYFORRÁSOK, ADATHALÁSZATI-MÓDSZEREK (SOCIAL ENGINEERING)

CSERCSA Klaudia[1] – RAJNAI Zoltán[2]

Abstract

Enhanced protection of data and information security are areas of high importance these days. The misuse of data that has fallen into the hands of unauthorized persons has reached unprecedented proportions. In the online space, we can face many phishing techniques, so conscious use and up-to-date information and device protection are essential in our daily lives. Social engineering techniques are diverse and creative, so constant vigilance is essential when logging into each application. Cyber attacks are a threat to an individual's life in the same way as they are to a small or medium-sized company, a multinational company or a country or nation.

Keywords

data protection, information security, social engineering, phishing

Absztrakt

Az adatok fokozott védelme és az információbiztonság kiemelt fontosságú terület napjainkban. Korábban sosem látott méreteket ölt az illetéktelen személyek kezébe került adatokkal való visszaélés. Az online térben számos adathalászati technikával szembesülhetünk így a tudatos felhasználás és a naprakész információ és eszköz védelem elengedhetetlenül fontos a mindennapi életünk során. A social engineering technikák sokrétűek és kreatívak, így elengedhetetlen a lankadatlan éberség minden alkalmazásba történő bejelentkezés során. A kibertámadások veszélyt jelentenek egy magánszemély életében ugyanúgy, ahogyan egy kis vagy középvállalat esetében, egy multinacionális cégnél vagy egy országnál, nemzetnél.

Kulcsszavak

adatvédelem, információbiztonság, social engineering, adathalászat

[1] claudiacsercsa@gmail.com | ORCID: 0000-0003-2800-9106 | PhD student, Obuda University | doktorandusz hallgató, Óbudai Egyetem

[2] rajnai.zoltan@bgk.uni-obuda.hu | ORCID: 0000-0002-9139-736X | dean/dékán | Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering / Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A bűnözés ezerarcú szörnyeteg, kiismerhetetlen, megfoghatatlan, napról napra megújul, alakot vált. Ebből a jellegéből fakadóan válik annyira nehézkessé a prevenció. Mikor megtanulunk védekezni valamely formája ellen, rögtön megjelenik új alakban. Ez hatványozottan igaz az online térben történő visszaélésekkel kapcsolatban. Az elkövető arcát, legtöbb esetben még a hangját sem tudjuk azonosítani, sőt olyan is megtörténhet, hogy tudatában sem vagyunk annak, hogy kiberbűnözők áldozataivá váltunk. Az elkövetések módja olyannyira változik, mondhatjuk olyannyira naprakészek a tettesek, hogy komoly kihívást jelent a hétköznapi állampolgárok védelme. Minden online platformon, minden egyes linken, melyre kattintani lehet, ott leselkedik a veszély a gyanútlan felhasználókra, melyek gyakran nagy áldozatot követelnek. Az oktatás és a tudatos jelenlét az online térben korábban sosem tapasztalt fontosságú területté vált napjainkra. Minden felületen komoly károkat tudnak okozni az illetéktelen behatolók. A védelem minden platformon indokolt, de vannak kiemelt súllyal bíró területek. Az is veszteséggel jár, ha jogosulatlanul használják fel vagy tárolják a személyes adatainkat, fényképeinket, social media felületeken fellelhető adatainkat, de az online térben történő károkozás banki tevékenységünket még hatványozottabban fenyegeti, gazdasági helyzetünket, egzisztenciális állapotunkat szüntelenül veszélynek kitéve. A bankokra és pénzintézetekre nagy nyomás nehezedik, hogy védje a partnereik adatait és biztonságát.

Napjainkban igen használatos kifejezéssé vált a social engineering. Széles körben elfogadott, egzakt definiálása még várat magára, több kutató is vizsgálat tárgyává tette már a jelenséget. A közös metszet, hogy kibertámadási technikák gyűjtőfogalma, azonban a social engineering fogalmán belül többféle elnevezéssel is találkozhatunk egy-egy technika bemutatása során és a technikákat különböző szempontok alapján csoportosították az egyes kutatók. Ezeket kerülnek ismertetésre a továbbiakban.

SOCIAL ENGINEERING

A social engineer tükörfordításban társadalmi mérnökök, egy kifejezés, mely arra utal, hogy néhány ember a társadalmi manipulációikat mérnök szintre fejlesztette fel. Ugyanakkor a magyarosított kifejezést nem használjuk, így az angol megfelelőjét alkalmazzuk a továbbiakban. A social engineer-ek ugyanazokat a meggyőzési technikákat alkalmazzák, mint mi hétköznapi emberek a mindennapjaink során. Szerepeket játszunk, igyekszünk hitelességet teremteni, viszonozzuk a szívességeket. A social engineer-ek azonban manipulatív, megtévesztő, erősen etikátlan módon használják ezeket a technikákat, gyakran elsöprő sikerrel. [1]

Bár a pénzügyi bűnözés motivációja magától értetődőnek tűnhet, nem ez az egyetlen motiváció. Sok esetben kiderül, hogy egyes elkövetőket nem a haszonszerzés, az anyagi javak növelése, hanem a szakmai kíváncsiság és a kalandvágy, vagy valamilyen (vélt vagy valós) sérelem vagy személyes bosszúvágy motivál. Emellett egyes országok nemzeti érdekből, más esetben terrorista szervezetek vagy bűnszövetkezetek politikai célok elérésére irányulva hajtanak végre kibertámadást a védett infrastruktúrák –például a pénzügyi szektor – ellen.” [2]

A legjobb példa erre a social engineering egyik legkiemelkedőbb egyénisége Kevin Mitnick, aki az amerikai FBI egyik legkeresettebb ifjú bűnelkövetője volt az 1980-as években. Több nagyvállalat informatikai rendszerébe hatolt be illetéktelenül, anyagi, illetve bármilyen egyéb haszonszerzési cél nélkül. Kizárólag az izgalom, a hecc kedvéért. Az ifjú kiberbűnöző, büntetőjogi felelősségre vonása után, 2023. júliusban bekövetkezett haláláig harcolt a kiberbiztonság megerősítése érdekében. [3] [4] [5]

Munkássága sokat hozzátett az online tér biztonságosabbá tételéhez. Sok hiányosságra és veszélyre hívta fel a közvélemény figyelmét a rablóból lett pandúr. Könyvében úgy határozza meg a social engineering fogalmát, hogy az adathalász meggyőzi az áldozatát arról, hogy ő valaki más, akinek éppen eljátssza a szerepét attól függően, hogy milyen szerepre van szüksége ahhoz, hogy a hőn áhított információt megszerezze. Nagyon jól ért a manipuláláshoz és az emberek megtévesztéséhez. Az adathalász kialakít egy bizalmas légkört az áldozatával és a bizalmába férkőzik. [6]

A social engineering fogalmát megfeleltethetjük magyarul pszichológiai manipuláció vagy pszichológiai befolyásolás gyanánt is. Ezen támadások ellen elsősorban nem technikai eszközök alkalmazásával kell védekezni, hanem a felhasználói ismeretek széles körben kiterjesztett oktatása és ismeretnövelése által. Ezekben az incidensekben nagy hangsúly van az emberi természet megismerésén, az emberek megtévesztésén és nem a technológiai eszközök sebezhetőségével él vissza a támadó. A módszer lényege, hogy több esetben egy bizalmi viszony alakul ki az elkövető és az áldozat között, mely során értékes információkat nyer meg a támadó és ezt saját érdekére fordítja és kihasználja az áldozat óvatlanságát, jóhiszeműségét. Más helyzetben pedig a célszemély vagy inkább kiszemelt áldozat figyelmetlenségéből fakadhat a károkozás.

FOGALMAK AZ IT ALAPÚ TUDÁST NEM IGÉNYLŐ ADATHALÁSZATI TECHNIKÁKKAL KAPCSOLATBAN

Ezek az adathalászati módszerek igen hétköznapiak és ezek a legveszélyesebbek az elkövetők szempontjából, hiszen ezekkel a módszerekkel a legnagyobb a lebukás veszélye. Jellegükből fakadóan többnyire fizikai jelenlétet is igénylő információ szerzésre irányuló technikák, de némelyik adathalász módszer elkövetése során csak a hangját használja a támadó. De ez is egy közvetlen kapcsolatot alakít ki a támadó és az áldozat között. Ezek a módszerek komoly felkészülést és lélekjelenlétet követelnek az alkalmazásuk során.

Az első taktikai lépés a környezet felderítése a lehető legrészletesebb módon. Minden jelentéktelennek tűnő információt meg kell jegyezni. Meg kell ismerni, hogyan veszik fel a telefont, hogyan köszönnek egymásnak, vannak-e sajátos nyelvi fordulatok, frázisok, milyen szakmai nyelvezetet használnak a kiszemelt egységnél, hogyan működnek a napi rutinok és hol lehet elérni a különböző osztályokat. Van-e beléptető rendszer, hogyan működik, mikor vannak a szünetek, kik és mikor mennek el dohányozni és hová. Ezeknek az információknak a birtokában már sokkal könnyebb észrevétlenül elvegyülni és beépülni egy cég életébe. [7]

Vishing: A támadó telefonhíváson keresztül igyekszik az áldozat bizalmába férkőzni és megszerezni a számára értékes információt. Ehhez a módszerhez gyakran üzletkötőnek adják ki magukat az adathalászok és így próbálják meg elérni céljukat. Ehhez a módszerhez is tanácsos már előre informálódni az áldozatról. Gyakori eset, hogy banki vagy valamilyen egyéb pénzintézet alkalmazottjának adják ki magukat a csalók és a gyanútlan

áldozatok megadják a bankkártya adataikat. Emellett személyes adatokat is könnyedén meg tudnak szerezni a támadók, ha sikerül egy bizalmas légkört kialakítaniuk. Mitnick például egy magasan védett intézmény rendszerébe tudott betörni annak a módszerének köszönhetően, hogy telefonos adategyeztetés keretében felhívta a kiszemelt áldozatot és helytelenül adta meg a kódot, amit az ügyintéző rögtön kijavított a helyesre. Így sikerült is hozzáfernie a bizalmas információhoz, hiszen az emberek ilyen esetben nem gyanakodnak. [7]

Dumpster diving (Kuka búvárkodás): Többször előfordul, hogy nem kellő körültekintéssel semmisítik meg az emberek a dokumentumokat mielőtt kidobnák a szemetesbe. A támadó kereskedelmi vagy lakossági szemét tárolókban keresgél. Először információt gyűjt a kukák tárolásáról, elszállításáról majd a kuka tartalmát átvizsgálva kerül értékes információk birtokába, amelyek alapján a későbbiekben csalást vagy lopást tud elkövetni. A módszer egyszerű és hatásos, a támadó időről időre átnézi a kiszemelt áldozata kidobott hulladékait. Ajánlatos minden dokumentumot megfelelő körültekintéssel megsemmisíteni.

Pretexting: A támadás olyan formája, amelyben a támadó előzetesen információkat készít az áldozatról akár nyílt forrásból, akár adathalászatból, és többnyire legtöbbször telefonon próbál meg minél több információt megszerezni.

Eavesdropping – vagyis a hallgatódzás: Egy régi, jól bevált módszer amikor mások beszélgetésére figyel valaki jogosulatlanul. Ha egy illetéktelen harmadik fél lehallgatja két fél beszélgetését, akár személyesen, akár telefonon, akkor gyakran fontos adatok gyűjthetők össze. Ha a lehallgatást számítógéppel végzik, a támadó kihasználhatja a hálózati kommunikáció bizonytalanságát, hogy hozzáférjen a küldött és fogadott adatokhoz. Az ilyen támadásokat nehéz észlelni, mert nem okoznak hálózati átviteli rendellenességeket. Kiemelendő, hogy milyen környezetben kivel, mit beszélünk meg. Az igazán bizalmas információk közlése során még hangsúlyosabb tényező a körültekintés.

A shoulder surfing – vagyis a váll feletti leskelődés: Egy igen egyszerű módja valamilyen PIN-kód vagy jelszó megszerzésének. Az adathalász személynek nincs közvetlen kapcsolata az áldozattal, de közel van az áldozatához. Mögé áll, és közvetlenül az áldozat válla fölött néz, hogy megfigyelje, amint az áldozat melyik billentyűket gépeli be az adott felületen. Közben természetesen viselkedik, úgy tesz, mintha valami fontos dolga volna és észre sem venné az áldozat gépelését. A legelterjedtebb esetek a PIN kódok lelesése például a pénzkiadó automatáknál, de gyakori incidensek a beléptető rendszerek, kaputelefonok kódjai. Az is előfordulhat, hogy valamilyen szerkezet segítségével (például távcső vagy kamera esetleg jól beállított tükör) messziről próbálják megszerezni a PIN kódot. A legegyszerűbb módja annak, hogy megvédjük magunkat ettől a fajta támadástól, ha figyeljük a mögöttünk álló személyt, és a kód beírása közben letakarjuk a kijelzőt. [8]

Segítségkérés-segítségnyújtás: A támadó az emberek segítőkészségére támaszkodva csal ki információkat. A hibát maga a támadó is okozhatja, így ő teremti meg a helyzetet, ahol segítségét felajánlva szerez meg bizalmas információkat.

Tailgating-besurranási módszer: Ezen technika alkalmazása során a támadó besurran egy épületbe. Ehhez használhat hamis beléptetőkártyát, megtévesztheti a beléptetésért felelős személyeket vagy besurranhat egy belépésre jogosult személy mögött az automata ajtózáródásig. Értékes információkhoz juthat az irodákba való bejutás során, ahol számítógépekhez és nyomtatott dokumentumokhoz is hozzáférhet. [7]

Jelszavak kitalálása: Itt kifejezetten a nem megfelelő erősségű jelszavak kitalálásáról van szó, ahol a támadó egyszerűen próbálkozik különböző jelszavak használatával.

Gyakran a felhasználók megadják egymásnak a jelszavaikat, illetve mások által hozzáférhető helyen tárolják.

ÖSSZEGZÉS

Ezeknek az adathalászati technikáknak az eredménye általában olyan információ, melyet a későbbiekben fel lehet használni más jellegű, technikai támadások kivitelezéséhez. Ezek az egyszerűnek tűnő technikák nem kívánnak IT alapú tudást, csupán rátermettséget és bátorságot. A későbbiek folyamán azonban az ilyen jellegű támadások tekintélyes anyagi károkat tudnak okozni mindenféle a felhasználónak és szervezetnek. Ezért nagyon fontos a tudatos felhasználás és az odafigyelés a leghétköznapibbnak tűnő szituációkban is.

Az összes eddig bemutatásra került adathalászati technika szerves része volt az emberi manipuláció alkalmazása, ennek okán technikai intézkedésekkel szinte lehetetlen ezeket kivédeni. A leghatékonyabb védelem ezekkel a támadásokkal szemben tudatos felhasználás kialakítása és a hatékony adatvédelmi tudatosság felépítése lehet.

IT ALAPÚ TUDÁST IS IGÉNYLŐ ADATHALÁSZATI TECHNIKÁK

Ezek közé tartoznak a valamilyen IT eszköz segítségével végrehajtott támadások, ahol rendszerint az elkövető nem is lép közvetlenül kapcsolatba az áldozatával és ebből fakadóan kisebb a lebukás veszélye. A támadók felkészültek és járatosak a szoftverek és az IT eszközök használatában. Ezeknek a támadásoknak a kivédése már bizonyos fokú felhasználói tudást igényel, hiszen itt már az online lét világában történnek a különböző incidensek.

Phishing – Adathalászat: Ezt az elnevezést gyűjtőfogalomként használjuk. A személyes adatok visszaélés céljából történő gyűjtésének egyik leggyakoribb módja.

Az ilyen támadásokat tapasztalt bűnözők vezetik, gyakran egész bűnözői csoportokkal vagy akár egész államokkal szövetkezve. A legegyszerűbb támadási módszer az e-mail, melynek során a támadók különféle ürügyeket alkalmaznak a szenzitív adatok megszerzése érdekében. Például: Egy értesítés a banktól, hogy a Tisztelt Ügyfél számlája hamarosan lejár, és elkéri a bank a személyazonosításra alkalmas adatokat (hitelkártyaszám vagy online banki hozzáférési kód) a szerződés meghosszabbításához. Ezek az adathalász jellegű e-mailek gyakran olyan emberektől származnak, akiket a kiszemelt célpont ismer és akikben megbízik, és/vagy a munkahelyi felettesük e-mail-céméről érkeznek. Az ilyen jellegű leveleket egyszerre több e-mail címre is elküldik, abban a reményben, hogy csak lesz majd valaki, aki gondolkodás nélkül válaszol ezekre a sürgető jellegű kérésekre és felfedi személyes adatait, úgymint például a hitelkártya adatokat, a személyi igazolvány adatait, lakcímet vagy egyéb személyazonosításra alkalmas adatát. Az adathalászat célja érzékeny személyes adatok megszerzése, bejelentkezési adatok beszerzése az áldozat információs rendszeréhez, valamint rosszindulatú alkalmazások telepítése a személyi számítógépre, laptopra, tabletre vagy mobiltelefonra. Ha ez sikeresen megtörténik, akkor ezek után már szinte bármit meg tud tenni a támadó a felhasználó eszközein és különböző platformjain akár az áldozat tudta nélkül is. Például törölheti vagy titkosíthatja az áldozata fájljait, hozzáférhet banki tevékenységéhez, vírusokat terjeszthet a nevében vagy minden adatát zárolhatja. Tipikus jellemzője az ilyen email-eknek, hogy helyesírási és ragozási hibákkal vannak tele,

sürgető jellegű adatok vagy linkre való kattintásra szólít fel és általános, nem személyre szóló a megszólítása.

Whaling – bálnavadászat: Kifejezetten egy konkrét célszemély elleni támadás, mely leggyakrabban a cégvezetők („bálnák") ellen irányul. A célzott támadások az internetről származó fenyegetések, amelyek során a támadók az elektronikus információs rendszerek infrastruktúrájának egyes részeit veszik célba, hogy azon a részen felügyelet nélkül "garázdálkodhassanak". Ennek a viselkedésnek az a célja, hogy a támadó hozzáférjen a céleszköz feletti rendelkezés jogával. Ez a támadások egyik rendkívül kifinomult módszereket és magas szintű szakértelmet igénylő formája, amely ellen kifejezetten nehéz védekezni, ezért gyakran sikeres eredménnyel zárul. A whaling avagy úgymond bálnavadászat során az adathalász megkeresi a vállalat legfontosabb vezetőjének vagy valamely kiemelten fontos cégvezetőnek a nevét és e-mail címét (amely a legtöbb esetben egy-két kattintással könnyedén megtalálható az adott vállalat honlapján), és személyre szabott e-mailt küld a kiszemelt áldozat vezetői szerepéhez szorosan kapcsolódó tárgyban. Az e-mail tartalmaz egy linket, amelyre, ha a kiszemelt cégvezető rákattint, akkor kártékony programok töltődnek le az illető eszközére és a hackertámadás sikeressé válik. [9]

Spear phishing – szigonyozás: Van, ahol lándzsás adathalászatként hivatkoznak erre a módszerre. Ennél a taktikánál pont az ellenkezője történik, mint az a phising technikánál ismeretes, vagyis kevés címzetthez érkezik meg az adathalász jellegű email, ami jól megfogalmazott, szépen strukturált levél, amely úgy tűnik, hogy egy banktól, vagy jól ismert vállalattól érkezik és megbízható forrásból származik. Válaszban kérheti a gyanútlan felhasználótól a jelszavát, hozzáférési adatait, személyes adatait. Előfordulhat emellett az is, hogy linket tartalmaz, amely egy kártékony álweboldalra irányítja a célszemélyt, vagy egy káros mellékletet tartalmaz.

Baiting: Az adathalász egy hordozható adathordozót (például pendrive vagy külső winchester) ott „felejt" egy jól látható helyen, többnyire egy számítógép közelében és az emberi természet kíváncsiságát használja ki. Gyakran jól olvashatón ráírnak valamilyen extra figyelemfelkeltő szöveget is, hogy még nagyobb legyen a csábítás, úgymint például titkos, szexi, bizalmas satöbbi. Amikor a kíváncsi megtaláló csatlakoztatja a talált tárgyat a számítógéphez, akkor történik meg a fertőzés. Ez a módszer online módon is működik például egy ingyen letölthető játék vagy valamilyen egyéb szoftver alkalmazása során. Ezért is fontos hangsúlyozni, hogy csak biztonságos oldalakról szabad letölteni programokat.

Typosquatting más néven URL-eltérítés: Az eredeti weblappal első ránézésre teljesen megegyező, alternatív weboldalra irányítja a felhasználót. Az alternatív oldal grafikai dizájnja, nagyon hasonlít az eredeti weboldaléra és első ránézésre nem is lehet megkülönböztetni. Az álweboldal webcíme többnyire egyetlen karakterrel különbözik az eredetileg felkeresni kívánt weboldal címétől és a legtöbb esetben a felhasználó észre sem veszi, hogy nem megfelelő helyen jár. Gyanútlanul megadja a hitelesítő adatait, amit a támadó ezután könnyedén felhasználhat.

Kiváló magyar példa erre: legjobbank.hu vagy Iegjobbank.hu A különbség nehezen észrevehető. Az első karakter az egyiknél a kis „L" betű a másiknál a nagy „i".

A farmolás vagy angolul pharming: (átirányítás hamisított weblapra) A támadó a felhasználót egy hamis, de a megbízhatóhoz nagyon hasonlító weboldalra irányítja. Az át-

irányítás általában valamilyen szoftver segítségével történik, többnyire nem is látszik különbség az eredeti és az álweboldal URL címében. A hacker az általa létrehozott hamis weboldal segítségével szerzi meg a felhasználótól a bizalmas információkat.

SMiShing – adathalászat SMS segítségével: Az adathalász hacker egy rövid szöveges üzenetet küld az áldozatának (SMS: Short Message Service) aminek segítségével megpróbálja rábírni az áldozatát arra, hogy az valamilyen személyes adatát vagy a támadó szempontjából fontos információt osszon meg vele, esetleg az sms egy linket tartalmaz, amire, ha rákattint a felhasználó egy ártalmas weboldalra lesz irányítva. Ennek folyományaként kártékony program kerülhet telepítésre, vagy a támadó megszerezheti a felhasználó személyes akár banki adatait is. [10]

TOVÁBBI SOCIAL ENGINEERING ADATHALÁSZ FORMÁK ÉS ELNEVEZÉSÜK

Search engine phishing: Egy rendkívül nagy kedvezményt nyújtó vásárlási lehetőséget kínáló weboldal, mely azonnali vásárlásra buzdít és azonnali klikkelésre szólítja fel a gyanútlan felhasználót. Ezek között szerepelhet egy szerencsekerék megforgatása klikkeléssel, melynek segítségével 90%-os vásárlás kedvezményt nyer az illető, ha néhány percen belül felhasználja a nyeremény kupont. És amint klikkel a felhasználó, máris a támadó által létrehozott weboldalon landol.

Social data mining: A különböző social media felületeken, mint például a Facebook, Twitter, TikTok, Instagram, YouTube sok felhasználó posztol magáról és magával kapcsolatosan mindenféle privát információt, amit egy későbbi támadás során fel tud használni egy támadó. Gyakran a pontos helymeghatározást is nyilvános adattá teszik magukról és ezáltal könnyedén nyomon követhető válik, hogy mely helyeken fordul meg gyakrabban, mikor merre járt külföldön, vagy milyen ételeket, italokat fogyaszt szívesen az illető. Ezek az adatok nyilvánosan elérhetők és ez a tevékenység önmagában nem illegális, hiszen a felhasználók saját akaratuk szerint osztanak meg magukról információkat, viszont nagyon hasznos információkkal szolgálhat egy későbbi kibertámadáshoz.

Böngésző előzményeken alapuló adatgyűjtés és automatikus kitöltés funkció kihasználása: Ha az eszközünkhöz, melyet napi tevékenységeink során használunk, hozzáférhet más személy, akkor könnyedén rá tud keresni, mely oldalakon jártunk korábban. Akár hónapokra visszamenően is. Ezekből az előzményekből szintén megismerhetőek vagyunk, szokásaink, ízlésünk, gyakran látogatott weboldalaink alapján feltérképezhetővé válik, milyen módon lehet a legkönnyebb módon a közelünkbe férkőzni. Az inkognitó mód használatával (Chrome felületen: control + shift + n billentyűkombináció), el tudjuk kerülni, hogy az általunk látogatott oldalak megjelenjenek a böngészési előzményekben. [11]

ÖSSZEFOGLALÁS

A tanulmányban bemutatásra kerültek a social engineering különböző technikái és definiálásra kerültek a témához kapcsolódó alapfogalmak. A kiberbiztonság a 21. század egyik legkritikusabb jelensége, mely magánszemélyeket, kis és középvállalatokat, nagy cégeket, országokat és nemzeteket egyaránt érint. A tudatos digitális jelenlét és eszközhasználat kiemelkedően nagy hangsúlyt kap, elmulasztása egyaránt okozhat lényeges anyagi, mentális és presztízs veszteséget. Az online térben elkövetett illegális tevékenységek

ugyanúgy bűnözének minősülnek, mintha a boltban lopna vagy adót sikkasztana valaki. Sajnos a kiberbűnözést még mindig nem kezeljük megfelelő hozzáállással a társadalmunkban. A tetten érés nagyon nehéz a legtöbb esetben, ebből kifolyólag a kellő szankcionálás is. A legtöbb hétköznapi ember nem fordít elegendő odafigyelést az adatainak a védelmének érdekében. Ahogy az a tanulmányban bemutatásra került gyakran előfordul, hogy a legalapvetőbb biztonsági intézkedéseket sem tesszük meg, mint a kártyás fizetés során a pin kód eltakarása, vagy a bizalmas jellegű információk megbeszélése telefonálás során a megfelelő közegben, mások által nem hallható helyen. A legtöbben nincsenek a tudatában, hogy menynyire fontos a naprakész védelem minden eszközön és minden felületen. A legtöbb kibertámadás emberi mulasztás vagy gondatlanság miatt sikeres. Hiába találnak ki a szoftverfejlesztők nagyszerű programokat és alkalmazásokat, különböző tűzfalakat, vírusírtókat az adatok védelme érdekében, ha az átlagos emberek nincsenek tudatában az alapvető megelőzési technikákkal. A tudatos életvezetés minden aspektusban kiemelkedően fontos, így az online térben is. A programok rendszeres frissítése, a megfelelő erősségű jelszavak használata és gyakori cseréje, a nyílt és közös hálózatok használatának mellőzése, megfelelő vírusirtók és tűzfalak használata, kémprogram eltávolító alkalmazások, illetve a két lépcsős azonosítás használatával már sokat tehetünk önmagunk és adataink védelme érdekében. A figyelem felkeltése, a gyakori és ismétlődő tudatosítás kiemelkedően fontos szerepet kap a kiberbiztonság területén.

FELHASZNÁLT FORRÁSOK

[1] „Mitnick Security,” [Online]. Available: (https://www-mitnicksecurity-com.translate.goog/about-kevin-mitnick-mitnick-security?_x_tr_sl=en&_x_tr_tl=hu&_x_tr_hl=hu&_x_tr_pto=sc. [Hozzáférés dátuma: 02. 05. 2024.].

[2] „444.hu,” 2023. [Online]. Available: https://444.hu/2023/07/21/meghalt-kevin-mitnick-a-korai-internet-legendas-hackere. [Hozzáférés dátuma: 02. 05. 2024.].

[3] K. D. Mitnick és S. L. William, A legendás hacker A megtévesztés művészete, Budapest: Perfact, 2003.

[4] K. D. Mitnick és S. L. William, A legendás hacker a behatolás művészete, Budapest: Perfact, 2006.

[5] „HVG.hu,” 2023. [Online]. Available: https://hvg.hu/tudomany/20230720_Kevin_Mitnick_meghalt_hekker_amerika. [Hozzáférés dátuma: 02. 05. 2024.].

[6] K. D. Mitnick és S. L. William, A legkeresettebb hacker, Budapest: HVG, 2012.

[7] G. Kaczur, Spear phishing, Budapest: NKE, 2018.

[8] I. Psenakova, „Ne hagyd magad becsapni!,” Lélektan és hadviselés - Interdiszciplináris folyóirat, II. évf., pp. 55-65, 2020/1.

[9] A. P. Bodó és N. Zámbó, A közreműködők kötelezettségei a célzott támadások elhárításában az IBTV. szerint, in: Célzott kibertámadások: NKE, 2018.

[10] C. Kollár és Á. Zakar , „A social engineering és a manipulációs technikák és módszerek,” Biztonságtudományi Szemle II. évf. 2. sz., pp. 23-38, 2020.

[11] L. Kovács és E. Terták , „A kiberbűnözés legjobb ellenszere a pénzügyi műveltség 11. évf. 1. sz.,” Gazdaság és Pénzügy, pp. 6-29, 2024.