HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A NYÍLT FORRÁSÚ INFORMÁCIÓSZERZÉS SZEREPE A KIBERTÁMADÁSOK VÉGREHAJTÁSA SORÁN

THE ROLE OF OPEN SOURCE INTELLIGENCE ON THE IMPLEMENTATION OF CYBER ATTACKS

DEÁK Veronika

(ORCID: 0000-0001-9220-2002)

deak.veronika@uni-nke.hu

Absztrakt

A mindennapi életünk során kulcsfontosságú szerepet töltenek be a különféle adatok, információk, ennek következtében ezek megszerzése és hatékony felhasználása is rendkívül fontos a napi rutin feladataink megoldása és a kibertámadások végrehajtása folyamán egyaránt, ugyanis a megfelelő információk megszerzése éppúgy elengedhetetlen a hétköznapi tevékenységeink elvégzéséhez, mint egy kibertámadás kivitelezéséhez. Az információszerzés a kibertámadások lebonyolításának nélkülözhetetlen eleme, tulajdonképpen az első lépéseként is értelmezhető. Az információszerzés alkalmas a támadás célpontjának megismerésére, ezáltal a különböző sérülékenységek, sebezhetőségek és kockázatok feltárására is, hiszen ezen hiányosságok felfedésével jelentősen növelhető a támadás eredményes végrehajtásának esélye. Továbbá a kibertámadások egyes szakaszainak hatékony megvalósításához számos olyan tervezési, szervezési és végrehajtási tevékenység kapcsolódik, amely során a releváns információk megszerzésével, összegyűjtésével, illetve felhasználásával sokkal eredményesebben, hatékonyabban és gyorsabban kivitelezhető egy ilyen támadás. Jelen tanulmányban áttekintésre kerülnek nyílt forrású információszerzés lehetséges eszközei, formái és a kibertámadásokban betöltött szerepe is.

Kulcsszavak: *nyílt forrású információszerzés, OSINT, kibertámadás, információ*

Abstract

In our daily life, the various data and information play a key role, and as a result, their acquisition and efficient use are crucial to solving our daily routine tasks and during the implementation of cyber attacks, since getting the right information is just as essential to do our everyday activities as to initiate a cyber attack. The acquisition of information is an indispensable element of the implementation of cyber attacks and can be interpreted as its first step. The acquisition of information is a good way to get to know the target of the attack, and to explore the various vulnerabilities and risks, as discovering these shortcomings can significantly increase the chance of a successful attack. In addition, several planning, organizational and enforcement activities are associated with the effective implementation of certain sections of cyber attacks, whereby such an attack can be performed much more efficiently, effectively and faster by acquiring, collecting and using relevant information. This paper reviews the possible tools and forms of open source intelligence and its role played in cyber attacks.

Keywords: *open source intelligence, OSINT, cyber attack, information, cyber defence*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.20.

BEVEZETÉS

Napjainkban az információ központi szerepet tölt be életünkben, hiszen jelenleg információs társadalomban élünk, amely azt jelenti, hogy az információ a mindennapi élet alapvető mozgatórugója. Ez a társadalom alapjában véve az információs technológiára épül, működéséhez elengedhetetlenül szükséges ennek megléte. Az általunk felhasznált információk típusainak száma és mennyisége a korábban rendelkezésünkre állókhoz képest a sokszorosára nőtt, tárolásuk pedig igen nagy koncentrációban történik. Az információ a mindennapi tevékenységeink nélkülözhetetlen szereplőjévé vált, többek között jelen van a kommunikációban, a döntéshozatalokban, valamint a különféle folyamatok, eljárások lebonyolításában is. Továbbá a megfelelő információk birtokában a különböző döntések bizonytalansága csökkenthető, ezzel együtt a döntéshozatali folyamat gyorsítható, valamint a többi erőforrás felhasználásának eredményessége és hatékonysága is növelhető, illetve a belső és külső hatásokra való gyors reagálás kulcsfontosságú feltétele. [1] Ezáltal aki a megfelelő információkhoz hozzáfér, óriási előnyhöz juthat. A megfelelő információk megszerzésével információs fölény érhető el, amely lehetővé teszi, hogy a birtoklója az infokommunikációs rendszereit és azok képességeit kihasználva, az élet számos területén előnyre tegyen szert, emellett képes az őt érintő helyzeteket úgy irányítani, hogy ezalatt a másik felet megfossza ezen képességektől. [2]

Az információ értékének növekedésével együtt jár a különböző információk megszerzésére irányuló törekvések megjelenése is, függetlenül attól, hogy az adott információ bizalmasnak tekinthető-e vagy sem. Manapság már mindenkinek lehetősége van a különféle külső, nyílt források segítségével információkat szereznie, amely azonban akár rosszindulatú célra is felhasználhatóak, illetve ezen információk tekintetében a visszaélés lehetősége is fennállhat. Összességében elmondható, hogy a felhasználások céljai nem változtak alapjaikban, viszont tömegessé váltak a különféle információ lopások és az illegális felhasználásuk is. Ennek köszönhetően az információk kezelőinek jelentősen megnövekedett a felelőssége, különösen az állami szerveknél, ahol mind a gazdaság résztvevőiről, mind az állampolgárokról, mind az állami szervekről óriási mennyiségű adat, információ összpontosul.

Az információk számos módon megszerezhetők attól függően, hogy milyen forrásban állnak rendelkezésünkre az adatok. A következőkben a nyílt forrású információszerzés fontossága, céljai, illetve a különféle módszerei, eszközei kerülnek bemutatásra.

A NYÍLT FORRÁSÚ INFORMÁCIÓSZERZÉS

Ahhoz, hogy értelmezni tudjuk az információszerzés célját, egyes módszereit, a megvalósítás lépéseit, illetve ezen módszerek elleni védekezés, vagyis a bizalmas információink védelme érdekében tett intézkedéseket, mindenképpen ismernünk kell az alapvető fogalmakat, jelenségeket.

Az információszerzés típusától függetlenül elsőként azt szükséges tisztázni, hogy mire irányulnak ezen információszerzések, tehát mi a tárgya ennek a tevékenységnek. Ebben az esetben a tevékenység központi célja az adatok, információk gyűjtése, majd pedig saját célra történő felhasználása. Az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. [3] Az információ értelmezésére számtalan definíció létezik, nincs egységes meghatározása. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerint az információ bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott tapasztalat, megfigyelés, vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét átalakítja, megváltoztatja, illetve befolyásolja, továbbá bizonytalanságát csökkenti vagy megszünteti.[3] Egy másik definíció szerint az információ olyan új ismeret, adat, tény, amelynek megismerésekor olyan plusz tudásra teszünk szert, amely addig nem volt a birtokunkban.[4]

A következő fontos fogalom a nyílt forrás (Open Source), hiszen ez fejezi ki az információk származásának eredetét. A nyílt forrás magába foglalja azokat a nyilvánosan elérhető forrásokat, amelyekhez legálisan, törvényes eszközökkel hozzáférhetünk, például megfigyelés, előfizetés, személyes megkeresés, megvásárlás, lekérdezés, internetes keresés által. Ilyen forrásnak tekinthetők a bárki által szabadon elérhető információ-hordozók, például a hagyományos publikált anyagok, könyvek, tanulmánykötetek, napilapok, folyóiratok, fényképek, rádió-és televízióadások, médiahírek, konferenciák, személyek beszámolói, illetve az Internet és egyéb digitális tartalmak is. A nyílt források tárháza igen sokrétű, de napjainkban az Internet robbanásszerű és folyamatos fejlődésének és számtalan előnyének köszönhetően a legtöbb információszerzés az Interneten keresztül valósul meg. [5:13]

Nyílt forrású információnak (Open Source Information) minősülnek mindazon adatok, amelyek az előbb említett források segítségével megszerezhetők, elérhetők. Ilyen információnak tekinthető a még nem feldolgozott, nyomtatott, kisugárzott, szóban közölt, digitális vagy más formájú dokumentum, tény, ismeret, fogalom, meghatározás, tájékoztatás, amelyek a nyílt források által biztosítottak. [5:13]

A nyílt forrású információszerzés (Open Source Intelligence – OSINT) definícióját hazánkban először a hírszerzés és a katonai felderítéstől elkülönítve Lévay Gábor határozta meg, mely definíció szerint az „*OSINT katonai felderítés és a hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti*.” [6]

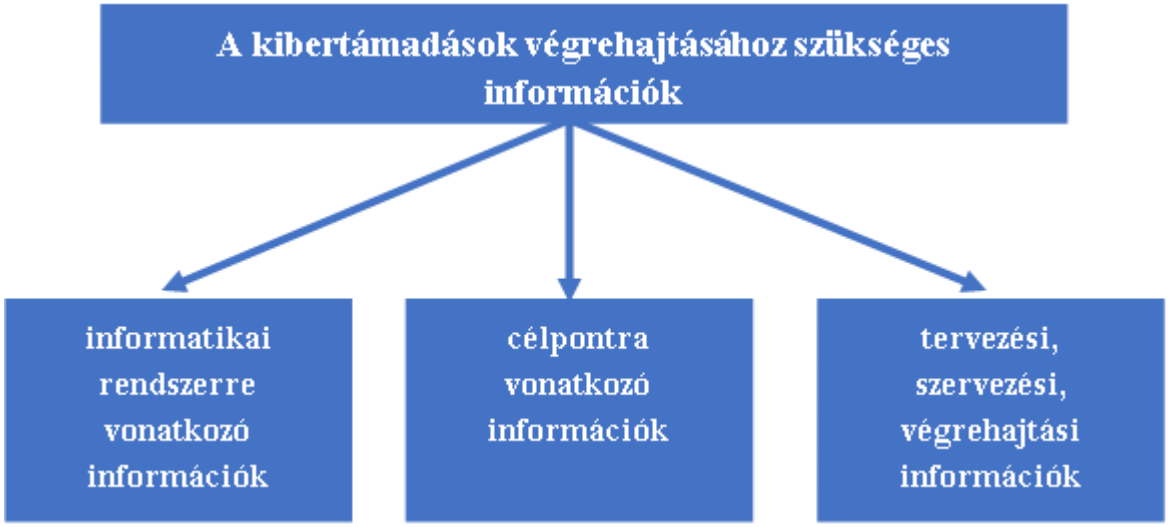
Összegezve tehát az OSINT olyan információgyűjtő eljárás, mely során az információk megszerzése bárki által szabadon hozzáférhető forrásokból történik. Napjainkban az OSINT széles körben elterjedt, gyakran alkalmazzák a mindennapi élet és a kibertámadások előkészítése és végrehajtása során is, azt azonban mindenképp ki kell emelni, hogy ezen módszer segítségével rengeteg információ megszerezhető, így az esetek jelentős részében nem elég csak összegyűjteni az információkat, ezt követően szűrni, szelektálni, rendszerezni, elemezni és értékelni is kell a felhasználás előtt. [7]

A nyílt forrású információszerzés elsődleges célja, hogy a felhasználó információigényeire minél pontosabb teljesebb, hitelesebb választ, visszajelzést tudjon biztosítani. Továbbá, hogy a felhasználó szándékának megfelelő információt szolgáltasson, függetlenül attól, hogy a felhasználó mire használja azt a továbbiakban. A felhasználók céljai sokfélék lehetnek, többek között az információszerzést felhasználhatják tájékoztatásra, döntéselőkésítésre, döntéshozatalra, üzleti célok megvalósítására, terrorcselekmények eredményes megvalósítására, vagy akár a kibertámadások előkészítésére és megvalósítására. [8] Jelen tanulmányban a nyílt forrású információszerzés kibertámadások végrehajtásában betöltött szerepe kerül bemutatásra.

A KIBERTÁMADÁSOK VÉGREHAJTÁSÁHOZ SZÜKSÉGES INFORMÁCIÓK

A kibertámadások nélkülözhetetlen elemeként értelmezhető az információszerzés, hiszen minden támadás alapja a támadás sikeres végrehajtásához szükséges információk megszerzése. Az, hogy pontosan milyen információk megszerzése a cél, az attól is függhet, hogy mi a konkrét támadás motivációja. Egy kibertámadás céljai igen sokrétűek lehetnek, többek között irányulhatnak információk gyűjtésére, módosítására, megváltoztatására, zárolására, törlésére, illetve megsemmisítésére, szolgáltatás, infrastruktúra akadályozására, korlátozására, gazdasági, politikai előny szerzésére, álhírek terjesztésére, hírnévrontásra, károkozásra, bizalomvesztés generálására, vagy akár vallási célok elérésére is. A kibertámadások során az információszerzés célja olyan információk gyűjtése, amelyek biztosítják a támadás céljától függően a sebezhetőségek, kockázatok és sérülékenységek feltárását. Egy kibertámadás alapjául szolgáló információszerzés alapvetően az alábbi ábrán látható információkat célozza. Az információszerzés irányulhat az informatikai rendszerre vonatkozó jellemzőkre és a célpontra vonatkozó információkra,

amelyek kapcsán elsődlegesen a sebezhetőségek, gyenge pontok feltárása a cél, majd ezek alapján következhet a tervezési, szervezési és végrehajtási információk összegyűjtése, rendszerezése.



1.ábra A kibertámadások végrehajtásához szükséges információk
(Saját szerkesztés)

Az *informatikai rendszerre vonatkozó információk* tartalmazzák az adott rendszer felépítésére, működésére vonatkozó adatokat, és a rendszerhez csatlakozó eszközök jellemzőit. Ezen információk megszerzése azért fontos, mert, ha a támadónak sikerül azonosítania az informatikai rendszer vagy az infokommunikációs eszközök sebezhetőségeit, akkor az információk segítségével meghatározható, hogy a rendszer mely pontján kell megvalósítani a támadást a sikeres végrehajtás érdekében. Nem létezik tökéletes biztonság, naponta jelennek meg újabb és újabb támadási módszerek, biztonsági rések, ennek következtében minden kockázatra kiterjedő védelemről sem beszélhetünk. Éppen ezért a technológiai sérülékenységek feltárása minden esetben kulcsfontosságú, hiszen ezek segítségével azonosíthatók az információs rendszerek vagy azok elemeinek gyenge pontjai, és ezáltal a sebezhetőségek orvoslása is időben elkezdődhet. Egy informatikai rendszer esetében kockázatnak tekinthetők többek között a különféle biztonsági rések, lehetséges szoftverhibák, hibás beállítások, gyenge jelszavak, a különböző szintű jogosultságok beállításának a hiánya, illetve hibás hozzáférési szintek megállapítása, a titkosítás hiánya vagy hibája, alkalmazás szintű hibák, mint például a hitelesítési, logikai hibák vagy akár az alkalmazások frissítéseinek elmulasztása. [9] Ezek alapján a fentebb példaként említett sebezhetőségekre és számos további, az informatikai rendszer gyenge pontjaira vonatkozó információk sorolhatók ebbe a csoportba.

A *célpontra vonatkozó információknak* két típusát különböztethetjük meg. Az egyik csoportba tartoznak azok az adatok, amelyek egy *szervezetre jellemzőek*, míg a másik csoportot a személyre utaló információk alkotják. A szervezettel kapcsolatos adatok magukba foglalják a szervezet tevékenységével, munkavállalóival, struktúrájával, illetve elérhetőségeivel kapcsolatos adatokat, amelyek tökéletes kiindulási alapot jelenthetnek a támadó számára a megfelelő személy kiválasztásához, aki rendelkezik a számára szükséges információkkal, vagy esetleg, akit megszemélyesíthet a későbbiekben további információk gyűjtéséhez vagy a konkrét támadás végrehajtásához. A szervezetre utaló információk kapcsán mindenképpen szükséges kitérni a szervezet fizikai jellemzőivel, védelmével összefüggő ismeretek megszerzésére is. Ennek során az információszerzés irányulhat például a szervezet belépési biztonságára, illetve arra, ho-

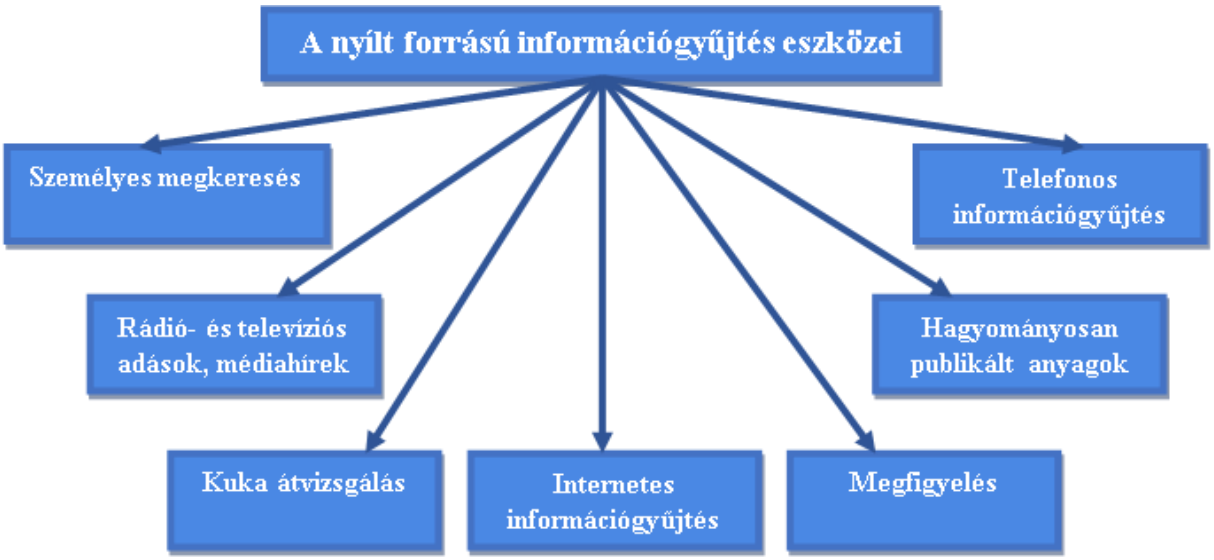
gyan történik a belépési jogosultságok ellenőrzése, milyen beléptető rendszer van a szervezetben, milyen szinten történik a szervezet épületeibe való bejutás ellenőrzése, illetve arra, hogy figyelik-e a szervezet alkalmazottainak indokolatlan bent tartózkodását, valamint, hogyan történik a szervezeten kívüli személyek beléptetése.

A *személyre utaló információk* megszerzése elősegíti a tökéletes célpont kiválasztását, aki a későbbiekben a támadó segítségére lesz a támadás megvalósításában. Ezen információk megszerzése során kerül sor a felhasználók biztonságtudatosságának felmérése, vagyis annak vizsgálatára, hogy mely alkalmazott nem rendelkezik megfelelő szintű információbiztonsági tudással és ezáltal mely munkavállaló segítségével szerezhetők meg a szervezetre vagy az informatikai rendszerre vonatkozó adatok, vagy mely célszemély alkalmas például egy kártékony program aktiválására, működésbe hozatalára. Ezen információk megszerzése során egyfajta profilozás is történik, hiszen az információk megszerzését követően a támadó célja, hogy az összegyűjtött ismeretekből következtetéseket vonjon le a célszemély gyenge pontjait illetően. A gyengeségek azonosítása azért rendkívül fontos, mert ezen ismeretek tudatában megtalálható az a személy, aki a kibertámadás megvalósításában a támadó segítségére lehet, vagy akitől bizalmas információkat lehet megszerezni. Ennek kapcsán az információszerzés kiterjed a célszemély személyes tulajdonságaira, amelyek a támadó által könnyedén kihasználhatók. Ilyen tulajdonságok többek között segítőkészség, naivitás, kíváncsiság, nyitottság, befolyásolhatóság, fáradtság vagy túlterheltség. Vannak olyan jellemzők is, amelyek jelentősen kapcsolódnak az áldozat munkahelyéhez is, ettől függ kialakulásuk, ilyen például, hogy ha valaki napi rutin munkát végez, minden nap ugyanolyan típusú problémát old meg, akkor sokkal nehezebb tesz különbség egy napi rutin feladat és a támadó kérése között. [10: 18-21] Ilyen tulajdonságnak tekinthető még az elégedetlenség, a lefizethetőség vagy például a megzsarolhatóság is, hiszen, ha a munkavállaló nem elégedett a munkájával, (esetleg a munkakörnyezetével, megbecsülésével vagy például a fizetésével) akkor a támadó akár megvesztegetheti vagy befolyásolhatja is az áldozatát, további információk kiadása érdekében. A támadó számára az is előnyös lehet, ha a kiszemelt áldozata szabadságon vagy betegállományban van, hisz ilyenkor a helyettesítő kollégának azt is mondhatja, hogy a betegállományban vagy szabadságon lévő személy ígérte meg neki bizonyos információk kiadását, így, ha a helyettesítő munkavállaló nem ellenőrzi ezt le, a támadó számos értékes információkkal gazdagodhat. Vannak olyan esetek, amikor az felhasználó szakképzetlenségét, jelszóhasználatát, a biztonságtudatosságának hiányát vagy a hanyagságát, illetve az ezekből adódó mulasztásokat használja ki a támadó, éppen ezért az információszerzésnek erre mindenképpen ki kell terjednie. [11]

A célinformációk harmadik nagy csoportját a *tervezési, szervezési, végrehajtási információk* alkotják. Ezen információk magukba foglalják a konkrét támadás kivitelezéséhez szükséges technikai, személyi, tárgyi és pénzügyi feltételeire vonatkozó ismereteket. Ezek egy része külön információszerző tevékenységet igényel, míg másik része a már korábban megszerzett másik két célinformáció csoport alapján kerül meghatározásra. A támadás végrehajtásához szükséges technikai feltételek tartalmazzák az infrastruktúra meglétét, többek között a különféle hálózati eszközöket (router, tűzfal), vezeték nélküli hálózatokat, VPN-t és az energiát is. A személyi feltétel magába foglalja a támadás megvalósításának egyik elengedhetetlen feltételét, vagyis azt a személyt, aki a magas szintű technikai tudásának köszönhetően képes végrehajtani az adott támadást. A tárgyi feltételek a támadás kivitelezéséhez szükséges eszközöket, berendezéseket, szervereket és szoftvereket jelentik. A pénzügyi feltételek az előbb említettek beszerzéséhez, megszervezéséhez szükséges anyagi forrásokat jelölik. Ezen információk megszerzését követően lehet összeállítani a támadás konkrét végrehajtási tervét, amely az előbbiek alapján tartalmazza a támadást kivitelezők körét, az ehhez szükséges technikai, infrastrukturális, tárgyi, pénzügyi feltételeket, a támadás konkrét időpontját, helyét, cselekvési tervét és a támadás konkrét célját.

A NYÍLT FORRÁSÚ INFORMÁCIÓSZERZÉS MÓDJAI, ESZKÖZEI A KIBERTÁMADÁSOK ELŐKÉSZÍTÉSÉBEN

Az információszerzés céljainak ismertetését követően mindenképpen ki kell térni, hogy mely eszközökkel, milyen módszerek segítségével valósítható meg a különféle információk megszerzése. Az alábbiakban az OSINT gyakran alkalmazott módszerei, eszközei kerülnek bemutatásra. A következő ábra a nyílt forrású információszerzés általam vizsgált egyes eszközeit mutatja, a teljesség igénye nélkül, hiszen ezeken kívül számos további módszer alkalmazható.



2.ábra A nyílt forrású információgyűjtés egyes eszközei
(Saját szerkesztés)

Napjainkban a technológia rohamos fejlődésének és az internetszolgáltatás elterjedésének köszönhetően az esetek döntő többségében az Internet segítségével valósítják meg az információszerzést. Ennek oka, hogy rövid idő alatt nagy mennyiségű információ gyűjthető kevés erőforrás felhasználásával, költséghatékonyan. A technikák első nagy csoportja alapvetően az *Internet* nyújtotta lehetőségeket kihasználva teszik lehetővé az adatok gyűjtését.

Az Internet adta lehetőségeknek köszönhetően az egyik legelterjedtebb információszerző és gyűjtő módszer az *internetes keresőrendszerek* alkalmazása. A keresőrendszerek olyan offline vagy online szoftverek, amelyek képesek a különféle adatok, információk találati listáját megjeleníteni a felhasználók számára. A konkrét keresés során különböző tartalmak többek között weboldalak, képek, videók, különféle fájltípusok, adatbázisok és számos további a támadó számára hasznos tartalom jeleníthető meg. A keresőrendszerek egyik típusát a webes keresőszolgáltatások alkotják, a másik csoportba pedig az emberi erőforrás által épített adatbázisok sorolhatók. [12]

Az emberi erőforrás által épített adatbázisok lényege, hogy az emberi tényező segítségével készül el az adatgyűjtemény, így, ha valamilyen változás következik be az adatok tekintetében, akkor azt manuálisan kell felvezetni. Annak ellenére, hogy ez a típus nem minden esetben tekinthető a legnaprakészebb forrásnak, mégis sokszor előfordul, hogy a támadók ezek segítségével gyűjtenek információt. Ilyen adatállományoknak tekinthetők az anyakönyvi, céginformációs vagy akár a telefonszámokat, elérhetőségeket tartalmazó adatbázisok. [12]

A webes keresőszolgáltatás működése három nélkülözhetetlen elemből áll. Az első lépésben a keresőmotor a webpásztázás során összegyűjti az adatokat a weboldalak tartalmáról a weboldalakon található hivatkozásokon keresztül, majd az így összegyűjtött tartalmat a következő lépésben az indexelés folyamatában elemzi és rendszerezi. A már korábban begyűjtött tartal-

makat metaadatokkal látja el, majd egy indextáblát készít, amely segítségével a keresési kritériumok ismeretében gyorsan elkészíthető a hatékony találati lista. A harmadik lépés a keresés, amely megvalósulhat a felhasználó, de akár egy program kérésére is. Ekkor az indexlistából a felhasználó által beírt vagy más programtól kapott kulcsszóhoz, illetve keresőkifejezéshez tartozó weboldalak rekordjainak kikeresése történik. [13: 39] Webes keresőszolgáltatásnak tekinthető a Bing, a Google, a Search vagy akár a Yahoo! is.

Napjaink legnépszerűbb és leggyakrabban alkalmazott keresőszolgáltatása a *Google* világszerte. A Google operátoraival történő keresést Google Hackingnek is nevezik, hiszen segítségével olyan részletes keresésre van lehetőség, amellyel akár a véletlenül nyilvánosságra hozott információk is felkutathatók, és amelyek a támadók számára hasznos információkat szolgáltathatnak. Többféle információt is találhatunk ezzel a technikával a jelszavaktól (felhasználók jelszavai, adminisztrátor jelszavak, alapértelmezett jelszavak) kezdve, elérhetőségeken, a belső használatra szánt anyagokon át, egészen a címlistákig szinte bármit. [13: 56-57] Ezen kívül a Google keresés során számos esetben tártak fel személyes adatokat (személyazonosításra alkalmas információk, bankszámlaszám, cím, telefonszám), e-mail címeket, felhasználóneveket, és a hozzá tartozó jelszavakat, hálózati adatokat, korábbi információbiztonsági auditok jegyzőkönyveit, illetve belsős anyagokat is. Továbbá a Google segítségével személyre szabott keresést valósíthatunk meg, rákereshetünk akár különféle fájltípusokra, képekre, videókra, könyvekre, illetve kereshetünk egy konkrét szövegben, címben vagy URL címben is. A Google Hacking Database egy hackerek által alkalmazott lekérdezéses adatbázis, aminek segítségével információk nyerhetők ki weboldalakról (hálózatbiztonsági információk, bejelentkezési oldalak stb.). Ez az adatbázis az internet segítségével valamilyen módon nyilvánosságra hozott, kiszivárgott, ezáltal a Google által is elérhető információkat, keresési kifejezéseket tartalmazza, a korábban indított lekérdezések katalogizálása által. [14]

A *Google* kapcsán mindenképp meg kell említeni a Street View, vagyis *Utcakép* funkcióját [15], amelynek lényege, hogy a 360 fokos panorámaképek segítségével egyfajta virtuális valóságként magunk előtt láthatjuk a keresett helyet. Ez rendkívül hasznos a támadó számára, mert a vizuális tartalomnak köszönhetően teljesen pontos és aprólékosan kidolgozott képet kaphat például a célszemély tartózkodási helyéről vagy éppen a támadás céljaként szolgáló szervezet fizikai adottságairól. Természetesen ezek a képek nem minden esetben szolgáltatnak naprakész információt, de kiindulási alapként tökéletesen alkalmazhatóak.

Az internetes keresőrendszerekkel kapcsolatban mindenképpen érdemes kiemelni azon keresőket, amelyek *konkrét személy megtalálására is alkalmasak*. Ezen keresők lehetőséget biztosítanak arra, hogy a legkülönfélébb variációkra, mint például vezetéknév, keresztnév, becenév, felhasználónév vagy akár ezek rövidített változatára is rákeressünk. Erre tökéletes példaként szolgálhat a Spokeo, [16] amely olyan kereső szolgáltatás, mely a nyilvános adatbázisok, nyilvántartások, közösségi hálózatok segítségével képes a célszemélyre vonatkozóan információ szolgáltatására. A Spokeo weboldalán történő kereséssel számos hasznos információhoz juthat a támadó a célszeméllyel kapcsolatban, így információt szerezhet a személy címéről, (amelyet egy Google térkép segítségével szemléltetnek) telefonszámáról, koráról, neméről, vallási, politikai meggyőződéséről, családtagokról, az elvégzett képzésekről és számos további személyes jellemzőiről. A Spokeo egyelőre még csak az Egyesült Államokban élő személyek keresésére alkalmas, de előfordulhat, hogy a világ többi részén is elérhetővé válik majd. Ezen kívül konkrét személyek megtalálására is használhatók a különféle közösségi oldalak (pl. Facebook, LinkedIn, Twitter stb.) és internetes keresőrendszerek (pl. Google).

Az Internet alapú információszerzés következő típusát a *közösségi oldalak* alkotják. A népszerűbb közösségi oldalak kitűnő kiindulópontot jelenthetnek, hiszen a kiszemelt áldozatról számos személyes információ begyűjthető. [17] A közösségi hálózatok általi információszerzés különösképp kedvező a támadó számára, hisz ezek segítségével kis költséggel nagy mennyi-

ségű információ szerezhető meg. Éppen ezért és az egyre növekvő alkalmazási kör miatt tökéletes kiindulási alapként szolgálnak egy kibertámadás előkészítéséhez vagy akár megvalósításához is. A támadó nem csak a célszemély személyes adatait és elérhetőségeit (e-mail cím, esetleg telefonszám, lakhely), hanem számos egyéb információt is megszerezhet. Gondoljunk csak arra, hogy első kézből láthatja az ismerőinek, családtagjainak, barátainak nevét, akik nevében egy kártékony programmal megfertőzött üzenetet is küldhet. Sokan megjelenítik a születési dátumukat, és gyakran posztolnak a családtagjaikról, kedvenc háziállatukról, amelyek akár az áldozat jelszavára is utalhatnak. Vannak, akik feltüntetik érdeklődési körüket és szabadidős tevékenységeiket is, így a támadó ennek birtokában tudja, hogy milyen tartalmú veszélyes csatolmánnyal ellátott üzenet küldjön, vagy esetleg a kapcsolatteremtés fázisába hogyan építse ezt be, mint például közös érdeklődési kört. Fontos megemlíteni azt is, hogy a közösségi portálok nem csak az információgyűjtésre alkalmasak, hanem kártékony program csatolására, például egy üzenetben elküldött link vagy fájl formájában, amire, ha rákattint a felhasználó, már aktiválódik is a kártékony program. Sok esetben még a célszemély pontos tartózkodási helye is fellelhető a közösségi oldalakon. Ezen kívül számos információ megszerezhető a leendő áldozat munkahelyi helyzetéről, politikai nézetéről, vallási meggyőződéséről, de akár a családi, párkapcsolati életére vonatkozóan is. A közösségi oldalak további előnye, hogy ha a támadónak nem sikerül hozzáférnie a célszemély biztonsági beállításainak köszönhetően adatlapjához, profilinformációkhoz akkor számos további lehetősége akad, akár információk gyűjtésére, de akár a kapcsolat kiépítésére és fenntartására is, hiszen profil létrehozásával rendelkezésére állnak a különféle fórumok, csoportok és a közvetlen üzenetváltás lehetősége is.

A közösségi oldalak kapcsán mindenképpen érdemes megemlíteni a különféle *párkereső oldalakat* és *alkalmazásokat* is. Ezen felületek is rendkívül sok személyes információt tartalmazhatnak a célszemélyről, a személyes adatoktól kezdve, az érdeklődési körön át, egészen a tartózkodási helyig számos a támadó számára hasznos információ fellelhető ezek segítségével.

Az internet alapú információszerzés további eszköze a *geolokációs helymeghatározást megvalósító applikációk*. Ilyen például a Creepy [7] alkalmazás, amely a földrajzi helyhez kapcsolódó információkat (időpont, hely) gyűjti online forrásokból, a közösségi médiában megjelenő bejegyzésekből, illetve képes azonosítani egy meghatározott IP cím fizikai tartózkodási helyét is. Ez lehetővé teszi meghatározott személyek mozgásának nyomon követését, és további következtetések levonását is, mint például a saját, a család, barátok lakhelyére vonatkozóan. Sok esetben mikor egy közösségi oldalt használunk és különféle bejegyzéseket, képeket, videókat osztunk meg, nem csak az előbb említett tartalmak kerülnek megosztásra, hanem ezzel együtt például a bejegyzés vagy kép készítésének konkrét helye is. A Creepy pontosan ezeket az információkat gyűjti össze és jeleníti meg egy térképen. Az alkalmazás információ szolgáltatásához használja többek között a Twitter, Instagram és a Flickr közösségi platformokat.

A kiszemelt áldozat megismerésének egyik legnyilvánvalóbb módszere az adott *szervezet/cég honlapjának* megtekintése, hiszen manapság már a legtöbb nagyvállalat, állami és nem állami szervek egyaránt rendelkeznek szervezeti weboldallal, amely nem csak a fő profiljuk, tevékenységük bemutatására alkalmas, hanem az ügyfelekkel való kapcsolattartásra is használható. A vállalati weboldalra gyakran kerülnek fel információk a vezetőkről, az alkalmazottakról, sok esetben még e-mail címekkel és telefonszámokkal együtt. Sőt, az is előfordulhat, hogy belső szervezeti ábra vagy telefonkönyv is elérhető a holnapon, ami jelentősen megkönnyíti a támadó számára a megfelelő személy kiválasztását, aki rendelkezik a számára szükséges információkkal, vagy esetleg, akit megszemélyesíthet. Abban az esetben, ha az e-mail címeket is feltüntették az oldalán, akkor akár egy veszélyes mellékletet tartalmazó levelet is küldhet a támadó. [17]

A következő csoportot az *elektronikus levelezés* általi információgyűjtés alkotja. Napjainkra az e-mail az egyik legelterjedtebb kommunikációs formává vált, amelyet az üzleti életben és a saját személyes ügyeink intézésére egyaránt használunk, hiszen leegyszerűsíti az üzenetküldést,

sokkal gyorsabb, költséghatékonyabb szolgáltatást valósít meg, továbbá már nem csak szöveget és képeket küldhetünk, mint a hagyományos levelezés során, hanem elektronikus dokumentumokat, fájlokat is. Az email-en keresztül történő megkeresés során általában a támadó valamilyen kérdőívet töltet ki, amelynek kérdései közé belecsempészi a számára szükséges információra irányuló kérdéseket. A kérdőívezés során a támadó elsősorban a személyes adatokra, születési dátumra, érdeklődési körre kérdez rá. [17]

A fentebb nevesített módszerek mindenféle informatikai, technikai tudás nélkül bárki által szabadon alkalmazhatók, de ezek mellett elérhetőek ingyenes információszerző szoftverek és programok, weboldalak, amelyek segítségével rengeteg olyan további információ gyűjthető, amely a támadás során felhasználható. Ilyen például a Shodan, amely az Internetre kötött infokommunikációs eszközök keresőszolgáltatása. A Sodan keresőmotort úgy tervezték, hogy képes legyen feltérképezni az Internetet, továbbá megpróbálja azonosítani és indexelni az Internetre kapcsolt eszközöket. A kereső lehetővé teszi a felhasználók számára, hogy különböző szűrőket alkalmazva feltárják az Internethez csatlakozó eszközöket (pl. számítógépeket, okostelefonokat, tableteket, szervereket, webkamerákat és azok videóit stb.), illetve még akár azok tartalmát, részletes adatait, sebezhetőségeit is. A Shodan nem csak a mindennapjaink során alkalmazott infokommunikációs eszközök tartalmához fér hozzá, hanem még akár az Internetre csatlakozott ipari vezérlőeszközökéhez is, amely ezáltal rendkívül nagy biztonsági kockázatként is értelmezhető. [18] Egy másik eszköz a theHarvester[7], amely segítségével e-mail fiókok, aldomain nevek, hosztok nyitott portok, bannerek és számos további az informatikai rendszerre vonatkozó információ gyűjthető. Ezen információkat különféle keresőmotorok, (Google, Bing) és más webhelyek, mint például a közösségi oldalak (LinkedIn) segítségével szerzi meg. A fentebb említett alkalmazásokon, szoftvereken kívül rengeteg más ingyenes elérhető program alkalmazható nyílt forrású információszerzésre.

Az Internet alapú OSINT-en kívül az egyik leghatásosabb, de egyben a legveszélyesebb módszer az áldozat *személyes megkeresése*, ugyanis ekkor a legmagasabb a lebukás kockázatának veszélye. Az áldozat közelébe férkőzve számos fontos információt megtudhat a támadó, mint például egy irodai körbenézés során, amikor is a különböző időbeosztások, szervezeti ábrák, szabadságolások, helyettesítések, számlák, infokommunikációs eszközök vagy esetleg a kiragasztott jelszavak is elérhetővé válnak a támadó számára. [10:57] Ezen kívül számos további a szervezet informatikai rendszerére, védelmére és tevékenységére vonatkozó belső és bizalmas információ is megtudható egy személyes beszélgetés által.

A személyes megkereséshez hasonló módszer a *megfigyelés*, amely esetén azonban nem történik meg a kapcsolatfelvétel, ehelyett a célszemély, célpont, vagy akár a szervezet fizikai megfigyelése valósul meg. Ennek előnye, hogy a személyes interakció hiányában a lebukás veszélye is kisebb, emellett rengeteg információ megszerezhető ezáltal. A megfigyelés segítségével információ gyűjthető a célszemély szokásairól, tartózkodási helyéről, szabadidős tevékenységeiről és a munkahelyi tevékenységére vonatkozóan is következtetések vonhatók le. A megfigyelés során a szervezet fizikai jellemzőivel, védelmével kapcsolatos információk is gyűjthetők, például hogyan történik a belépési jogosultságok ellenőrzése, illetve milyen beléptető rendszer van a szervezetben.

Igaz, hogy az Interneten keresztül manapság már szinte minden információt megtalálunk, azonban, ha ez mégsem lenne elegendő, akkor további információkat gyűjthetünk a *telefonos megkeresés* [10: 57] segítségével. Ebben a módszerben a támadó kiadhatja magát ügyfélnek, új munkatársnak, belső munkatársnak vagy egy partner szervezet/cég munkatársának, de akár egy felsőbb vezetőnek is. Az, hogy a támadó kinek a bőrébe bújik, az attól függ, hogy milyen információt akar megszerezni. Sok esetben a támadó célja az adott területen illetékes munkatársak nevükről, elérhetőségükről, hatáskörükről való tájékozódás, de a telefonos segítség kérése vagy az informatikai rendszer védelmének feltérképezése is lehet a cél.

Az információszerzés egy további hatékony módja *kuka átvizsgáló technika*, amelynek keretében számos hasznos információt tudhatunk meg az áldozatról. Az emberek bele se gondolnak, hogy milyen értékes információkat tudhat meg rólunk a támadó az irodai vagy otthoni szemetesünk átvizsgálásával. [10:37-38] Elég csak kidobni egy hivatalos levelet, bankszámla részletezőt, a támadó már tudomást is szerzett a személyes adatainkról, címünkről. De elég, ha csak a jelszavas cetli belekerül a kukába, és máris tudják a belépésünk adatait. Ezeken kívül számtalan olyan egyéb információt kidobhatunk, amelyek a támadónak segítséget nyújt például a személyiségünk ellopásához, vagy kényes információk esetében a zsaroláshoz is.

További információkhoz juthat a támadó a *leselejtezett informatikai eszközök átvizsgálásával* is. Napjainkra már számos olyan szoftver elérhető, amely segítségével a törölt adatok, információk, fájlok könnyedén visszaállíthatók.

Az Internet előnyeinek köszönhetően a nyílt forrású információszerzés az esetek döntő többségében ezen a felületen zajlik, de a *hagyományosan publikált anyagok* (könyvek, tanulmánykötetek, napilapok, folyóiratok) vagy például a *rádió-és televízióadások, médiahírek* segítségével is gyűjthetők hasznos információk, azonban napjainkban egyre kevésbé fordul elő alkalmazásuk. [7]

Az információszerzés lehetőségei rendkívül sokrétűek, azonban az igazán nagy veszélyt az jelenti, hogy a különböző helyről különböző módon összegyűjtött információkat összekapcsolják, és ezt használják a célpont ellen.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Az sebezhetőségek, sérülékenységek feltárása azért kiemelkedő jelentőségű, mert ennek tudatában a támadó fel tudja mérni, hogy a támadást pontosan hol kell végrehajtani. Abban az esetben, ha az információszerzés során sikerül feltárni a célpont sebezhetőségét, például az informatikai rendszerében vagy akár a szervezet egy alkalmazottjában, akkor a támadó egy sokkal személyre/szervezetre szabottabb támadást tud megvalósítani. A mai modern világunkban a különböző informatikai eszközök és rendszerek védelme már nagyon fejlett, így a támadó, ha például nem talál sebezhetőséget a felsőbb szinteken, mindig egy szinttel lejjebb fog menni, és addig csinálja ezt, amíg nem talál egy olyan pontot, ami sebezhető. Így például, ha a célpont informatikai eszközei és rendszerei magas szintű védelemmel vannak ellátva, akkor a támadó egy szinttel lejjebb, a szervezet alkalmazottai között keres sebezhetőséget. Ez azt jelenti, hogy ebben az esetben a támadó olyan munkavállalót keres, aki segítségével könnyedén bejuthat a szervezet rendszereibe, hálózataiba, információt szerezhet a szervezet sérülékenységeiről vagy akár, ha a támadás egy konkrét információ megszerzésére irányul, akkor ennek megszerzése is megvalósulhat az alkalmazott megtévesztésével, kihasználásával. Azokat a támadásokat, amelyek az emberi tényező kihasználásra, megtévesztésére irányulnak, social engineeringnek hívjuk. A social engineer a manipulálás, a befolyásolás, a megtévesztés és a meggyőzés segítségével irányítja áldozatát a céljai elérése érdekében. A támadások céljai igen sokrétűek, irányulhatnak többek között bizalmas információk megszerzésére, módosítására, illetve törlésére, a sérülékenységek és sebezhetőségek feltárására, a célszemély viselkedésének befolyásolására, a belső hálózati hozzáférés, jogosultság megszerzésére, különféle infokommunikációs eszközök rosszindulatú programmal történő megfertőzésére vagy akár egy komplex kibertámadás előkészítésére egyaránt. Éppen ezért a social engineering támadási technikák tökéletesen alkalmazhatók a kibertámadások végrehajtását megelőző információszerzésre.

A különféle infokommunikációs eszközök használata mindennapos tevékenységeink nélkülözhetetlen részévé vált, számtalan előnye mellett azonban a hátrányait és a hozzájuk kapcsolódó veszélyeket is szükséges megismerni. Elengedhetetlen, hogy mindennapjaink során megvédjük az információinkat a jogtalan hozzáféréstől, illetve az esetleges kiszivárgástól vagy megsemmisítéstől. Ahhoz pedig, hogy ez a védelem sikeres lehessen, úgy gondolom fontos, hogy mindenki megismerje az információk megszerzésére irányuló módszereket, hiszen csak

ezek tudatában lehet meghatározni, hogyan tudjuk megelőzni, megakadályozni a bizalmas információinkhoz való jogosulatlan hozzáférést, illetve hogyan kell reagálnunk, a már bekövetkezett eseményekre.

FELHASZNÁLT IRODALOM

[1] BOGNÁR L.: *Az információ fontossága, az információs rendszerek*. 2015. http://slideplayer.hu/slide/2117606/ (A letöltés ideje: 2018.04.02.)

[2] HAIG Zs., KOVÁCS L.: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* 2012. http://hdl.handle.net/11410/285 (A letöltés ideje: 2018. 04. 02.)

[3] 2013. évi L. törvény *az állami és önkormányzati szervek elektronikus információbiztonságáról.*

[4] KRASZNAY Cs.: *Az információbiztonság alapjai*. 2007. http://krasznay.hu/presentation/elte_01.ppt (2018.04.02.)

[5] FERENCZY G. Z.: *Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása.* 2007. http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2007/ferenczy_gabor.pdf (A letöltés ideje: 2018.04.02.)

[6] LÉVAY G.: *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés*. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2006.

[7] CHAUHAN, S., PANDA, N. K.: *Hacking Web Intelligence*. Open Source Intelligence and Web Reconnaissance Concepts and Techniques. 2015. https://doi.org/10.1016/B978-0-12-801867-5.00006-9 (A letöltés ideje: 2018. 05. 21.)

[8] KOBOLKA I. (szerk.): *Nemzetbiztonsági alapismeretek.* Budapest: Nemzeti Közszolgálati Egyetem, 2013.

[9] DOLÁNSZKY Gy.: *Informatikai rendszerek sérülékenységvizsgálata*. 2013. http://users.nik.uni-obuda.hu/poserne/ibst/Frissitett_anyagok_2013/20130508_Serulekenysegvizsgalat_eSec_KURT_DGY.pdf (A letöltés ideje: 2018. 04.17.)

[10] OROSZI E.: *Social Engineering*. Budapest: Budapesti Corvinus Egyetem, 2008.

[11] DEÁK V.: *A social engineering humán alapú támadási technikái*. 2017. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (A letöltés ideje: 2018. 04. 17.)

[12] MINORICS D.: *Internetes keresők*. 2016. https://thepitch.hu/internetes-keresok/ (A letöltés ideje: 2018. 04.22.)

[13] BÓTA L.: *Internetes keresőrendszerek működése*. Eger: Eszterházy Károly Egyetem, 2011.

[14] *Védekezés a GHDB* (Google Hacking Database) *ellen*. https://blackcell.hu/acunetix-web-serulekenyseg-vizsgalo/ (A letöltés ideje: 2018. 04. 22.)

[15] CROSS, M., HARRINGTON, M.: *Google Earth Forensics*. Waltham: Syngress, 2015.

[16] ANDREWS, L.: *I know who you are and I saw what you did. Social Networks and the Death of Privacy*. New York: Free Press, 2011.

[17] LEITOLD F.: Sebezhetőségvizsgálatok a gyakorlatban. Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[18] BODENHEIM, R., BUTTS J., DUNLAP, S., MULLINS, B.: Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection*. 7.2. https://doi.org/10.1016/j.ijcip.2014.03.001A letöltés ideje: 2018. 05. 21.)