Informatikai behatolások és felismerésük

(IT Enumeration and Their Recognition)

A tanulmány a KÖFOP-2.2.2-VEKOP-16-2016-00001

„KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése”

című projekt keretében készült.

NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Tartalomjegyzék

Absztrakt

A különböző informatikai rendszerek felhasználói széles skálán helyezkednek el mind szakmai ismeret, mind a felhasználás módja, mind pedig biztonságtudatosság tekintetében. A támadó azonban mindig a leggyengébb pontot fogja kiválasztani ahhoz, hogy bejusson a rendszerbe. Az incidensek számának és a károkozások mértékének csökkentése érdekében szükséges megismerni alapszinten a támadások felépítését, illetve a védekezési lehetőséget mindenkinek, legyen szó átlagos felhasználóról, üzemeltetőről vagy a biztonságot kiépítő szakemberről. E tudás hiányában könnyebben áldozatul eshet bárki akár a magánéletében, akár a munkahelyén. A tanulmányban bemutatom a különböző kiberbiztonsági támadásokat, illetve azokat a módszereket, melyek segítenek felismerni, ha egy támadás már elindult ellenünk.

1. Bevezetés

A tanulmány kifejezetten azt a célt hivatott elérni, hogy átfogó képet nyújtson a különböző kiberbiztonsági kihívásokról és technikákról, hiszen anélkül, hogy tudomásunk lenne a támadó oldalról, nem lehetséges védekezni. Nem célja egy-egy technika mélyebb szintű ismertetése, annak legapróbb részleteinek bemutatása. Ismertetem egy általános támadás menetét a kibertérben a célpont kiválasztásától kezdve a különböző passzív és aktív támadásokon keresztül a nyomok eltüntetéséig. Bemutatom a különböző malware típusok, illetve néhány közismert támadásról is szót ejtek. Ezeket követően különböző eszközök, technikák, információbiztonsági kontrollok használatának segítségével a védelem kialakításának idealizált kiépítésének bemutatása következik. Fontos hangsúlyozni, hogy – mint ahogy a támadások is nagyon szerteágazó palettán mozognak – nem létezik egy olyan út, melyet követve egy szervezet teljes biztonságban lenne. Egyfelől nem létezik 100%-os védelem, másfelől minden szervezet más infrastruktúrát használ, más területen tevékenykedik, így a különböző fenyegetések mértéke eltér. Fontos látni, hogy az adott szervezet érettségi szintjének, illetve az üzleti oldal igényeinek figyelembevételével alakíthatók ki észszerűen a biztonsági védvonalak.

A szerző felhívja a figyelmet arra, hogy az itt leírtak a tájékoztatást szolgálják, és nem cél, hogy ezáltal bárki illegális tevékenységet hajtson végre. Kifejezetten felhívja a figyelmet arra, hogy aki valamilyen módon szeretne ezekkel a technikákkal mélyebben megismerkedni, az a különböző etikus hacker, illetve más információbiztonsági képzések keretén belül tegye ezt meg, ahol szabályozott körülmények között szerezhet tapasztalatot és mélyebb tudást a következőkben leírtakról.

2. A közelmúlt kiberbiztonsági esszenciája

30 éve, 1988. november 2-án este kezdte el tevékenységét az interneten az első számítógépes kártevő, a Morris-féreg. [1] Akkoriban főként az egyetemek, valamint a katonaság eszközeiből állt a hálózat. Noha mindenki tisztában volt azzal, hogy a rendszer nem tökéletes, és vannak hibái, mégsem gondolták, hogy kárt lehetne benne okozni. Ugyan a féreg nem okozott hatalmas pusztítást, mégis bebizonyította, hogy nem szabad meggondolatlanul feltételezésekre alapozni. [2] A Morrist a Cornell Egyetemen alkotta meg Robert Tappan Morris Jr. kísérleti szándékkal. A féreg egy háttérben futó folyamat sérülékenységét kihasználva puffer-túlcsordulást okozott, majd kihasználva a levelezőrendszert, távoli számítógépeken demonstrálta a jelszóval védett fájlok feltörését. [3]

1988 óta azonban a különböző rosszindulatú kódok kiléptek a kísérleti világból, és a támadók élesen is alkalmazzák őket. A négy jól elkülönülő fenyegetést a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés jelenti. Míg a bűnözői csoportok haszonszerzési szándékkal követik el támadásaikat, addig az általában kisebb csoportokban működő hacktivisták és kiberterroristák fő célja, hogy ideológiájukkal minél több emberhez jussanak el az általuk elkövetett tettekről szóló hírek médiában történő megjelenéseinek segítségével. [4] Az állami és ipari hírszerzés eszköztárába az elmúlt 30 évben bekerültek a digitális teret kihasználó számítógépes kódok is. Fő törekvésük, hogy minél tovább tudjanak egy célrendszerben észrevétlenül rejtőzni, hogy így folyamatosan információt szivárogtassanak ki. Állami szinten azonban nemcsak a kémkedésben, de a hadviselésben is teret kaptak a különböző digitális támadások. [5]

Annak ténye, hogy 2001. november 23-án Budapesten aláírták az úgynevezett Cybercrime Egyezményt [1] (Számítástechnikai Bűnözés Elleni Egyezmény), megmutatja számunkra, hogy a kiberbűnözés egy olyan formája az illegális pénzszerzésnek, mellyel globálisan is foglalkozni kell. A szervezett bűnözés egyre közkedveltebb módszereivé válnak a különböző internetes csalások, a jogtalan felhasználások, illetve például a DDW (Deep and Dark Web) lehetőségeit kihasználó illegális fegyver-, kábítószer- stb. kereskedelem. Ennek egyik módja a TOR[2] (The Onion Router) böngészőn keresztüli hálózati kapcsolódás. Az alapvetően anonim böngészést kínáló megoldás mögé sok illegális tevékenység rejtőzik. Az elmúlt időkben gyakorlatilag minden olyan területen, ahol digitális pénz cserél gazdát, megjelentek a kiberbűnözők. Ilyenek lehet például a különböző elektronikus fizetési eszközök hamisításától kezdve, a telekommunikációs cégek szolgáltatásainak átverésén át, a mobilbank csalásokig terjedő esetek egyaránt, derül ki a ThreatMetrix 2018 első negyedévében közölt riportjából. [6] Nem szabad megfeledkezni az elmúlt évek zsarolóvírus-kampányairól és a kriptovaluták botnetekkel történő bányászásáról sem, melyek kifejezetten a közelmúltban nyertek igazán teret. [7] A felsoroltakon kívül számos más területet is lehetne említeni, ahol a kiberbűnözők jelen vannak.

A Hacktivista csoportok tagjai a kibertérben hajtanak végre olyan cselekvéseket, melyek segítségével valamilyen módon ki tudják fejezni politikai, nemzeti, szociális vagy más világnézeti véleményüket. Lehet ez pro vagy kontra egyaránt. Egy-egy csoport tevékenysége sokszor nem megy tovább különböző weblapok kompromittálásán vagy egy túlterheléses támadással történő elérhetetlenné tételén túl. Jó példa erre a fenyegetésre az Anonymous hackercsoport. Több különböző témában hallatták már a hangjukat. Volt köztük politikai véleménynyilvánítás (például 2017 áprilisában Magyarország kormánya ellen hirdettek háborút), de 2015-ben a terrorizmust vették górcső alá, amikor hadat üzentek az Iszlám Állam (ISIS) terrorszervezetnek a közösségi médián keresztül.

[1] https://net.jogtar.hu/jogszabaly?docid=A0400079.TV
[2] https://www.torproject.org/

A kiberterrorista csoportok, párhuzamban a hacktivistákkal, véleményük hangoztatására használják a kiberteret. Céljuk főleg valamilyen vallási, ideológiai eszme radikális kinyilvánítása, melyet más terrorista cselekvények mellett vagy azokat kiegészítve hajtanak végre. A kibertéren keresztül ezek a szervezetek, karöltve a fizikai síkon működő terrorszervezetekkel, propagálják tevékenységüket, de itt toboroznak, különböző képzéseket tartanak. Ezt a csatornát használják kommunikációra vagy a működésükhöz szükséges adományok gyűjtésére egyaránt. Előfordulnak konkrétan végrehajtott támadások is, melyből főleg a pszichológiai hadviselés a legmeghatározóbb. [8] Jó példa volt erre 2016. júliusában az ISIS-hez tartozó United Cyber Califhate, amelynek tagjai Egyesült Államok és Egyiptom ellenes plakátokat helyeztek el. [9]

Ugyan az OSINT-nak (Open Source Intelligence – nyílt forrású hírszerzés) és a SIGINT-nek (Signal Intelligence – rádióelektronikai felderítés) jellemzően a kibertéren keresztül történő információgyűjtés a fő eleme, a kiberkémkedés a tanulmány szempontjából a CYBINT (Inteligence gathered from Cyber Space – kiberhírszerzés) területe nyújtja az elsődleges fókuszt. Ez esetben a támadók fő célja, hogy nyílt vagy zárt számítógépes hálózatokból védett információkat szerezzenek közvetlenül vagy közvetetten (kisugárzott jelek visszafejtésének segítségével). [10] A kibertérben zajló leghatásosabb hírszerzési műveletekről értelemszerűen nincsen tudomásunk, hiszen (a támadó fél szerencséjére, az áldozat szerencsétlenségére) ezek még nem kerültek napvilágra. Ennek ellenére már ismertek olyan kevésbé hatékony esetek, ahol már valamilyen, általában nem hivatalos forrásokban szivárogtak ki információk. Ilyen például 2018 elején a holland titkosszolgálat megfigyelő tevékenykedése az orosz kormányhoz köthető Cozy Bear hackercsoport ellen.

Nem elhanyagolhatók a hadviseléshez köthető kibertevékenységek sem. [11] Itt különböző műveletekről lehet beszélni, attól függően, hogy a kibertéri képességeket milyen célok eléréséhez használják. Megkülönböztethetünk támadó, védelmi, illetve katonai információs hálózati műveleteket. [12] A hadviselés egyik nagyon fontos részét képezik az információs műveletek, melyeknek egyik alappillére a számítógép-hálózati hadviselés. [13] A védelmi műveletek azokból az eljárásokból tevődnek össze, melyek segítségével egy-egy rendszert vagy hálózatot próbálnak a lehető legbiztonságosabbá tenni. Támadó oldalról jelentőséggel bírnak a különböző túlterheléses támadások (DoS/DDoS), melyek során az ellenséges fél rendszerét vagy annak egy részét kívánják elérhetetlenné, működésképtelenné tenni. Ilyen eset például az orosz–grúz háború. [14] Akármennyire egyértelműnek is tűnhet egy kibertámadás, csak akkor beszélhetünk hadműveletekről, ha azt a támadó egyértelműen magára vállalja. Jó példa volt erre 2007-ben Észtország esete. 2005-ben a NATO 5. hadszínterévé nyilváníttatta a kiberteret [15], két évvel később oroszországi és ukrán IP címekről túlterheléses támadás érte az észt kormányzati rendszereket, miután egy orosz emlékművet eltávolítottak korábbi helyéről. Mivel a két ország között nem volt hivatalos konfliktus, és Oroszország tagadta az ellene felhozott érveket, ezért a NATO nem lépett fel ellene. [16]

A hivatalos katonai műveletek ellenére hidegháború zajlik a világban, ahol valószínűsíthetően államilag támogatott kiberfegyvereket tesztelnek. Ezzel párhuzamosan egyfajta erőfitogtatás is zajlik. A fent említett eseteken kívül az elmúlt időszakban több globális támadás is történt. Az iráni atomdúsító elleni, Stuxnet néven elhíresült sikeres szofisztikált támadás az ipari rendszerekben okozott fizikai kárt úgy, hogy a dúsító motorjait túlpörgette. Ennek hatására Irán atomprogramja, a szakértők szerint, több évre visszaesett. [17] 2014-ben és 2015-ben áram nélkül maradt Ukrajna egy része a BlackEnergy nevű támadás következtében,[3] majd 2017-ben két globális méretű zsarolóvírus-támadás (ransomware) pusztított szerte a világon. Először a WannaCry titkosított le több országban különböző rendszereket. Áldozatul esett például az Egyesült Királyságban több kórház is. [18] Ezt követően nem sokkal a

[3] https://www.kaspersky.com/resource-center/threats/blackenergy

NotPetya – vagy más névvel FakePetya – okozott hatalmas károkat, főleg Európában, azon belül is Ukrajnában. [19]

3. A behatolások tipikus szakaszai

Annak ellenére, hogy a támadások számosak és változatosak, mégis, a legtöbb esetben jól el lehet különíteni bizonyos szakaszaikat. A tanulmány ezen fejezete az EC-Council által gondozott Certified Ethical Hacker (CEH) képzés alapjául szolgáló tananyagban szereplő terminológiát [20] követi, amely a következő lépésekből áll:

- A célpont kiválasztása
- Passzív információgyűjtés (Footprinting)
- A támadási felület feltérképezése (Scanning)
- Behatolási kísérletek (Enumeration)
- Rendszerbe történő bejutás (System Hacking)
- A jogosultság növelése (Escalation of privilege)
- A nyomok eltüntetése (Covering tracks)

E lépések kifejtésén kívül bemutatom az úgynevezett social engineering technikákat, illetve néhány gyakran alkalmazott más támadási módszert.

3.1. A célpont kiválasztása

Minden támadás azzal kezdődik, hogy a támadó valamit el szeretne érni. Bejutni egy rendszerbe, és ott kárt tenni, pénzt vagy információt szerezni, zsarolni stb. A cél kiválasztása után a célpont kijelölése következik. Ez után felmérik, hogy milyen szaktudás, erőforrás áll rendelkezésükre. Egy államilag támogatott támadáshoz rendelt pénz, személyi állomány, tudás összehasonlíthatatlan egy tizenéves fiatal azon törekvéseivel, hogy megmutassa, ő mennyire ügyesen tud hackelni. A jól érezhető különbségek ellenére egyik sem elhanyagolható veszélyforrás.

A célpontok többféle entitásból kerülhetnek ki. A támadó kiválaszthat egy konkrét személyt. [21] Itt nyilvánvalóan arról van szó, hogy ennek az embernek szeretnének kárt okozni: lerombolni a róla kialakult képet, információt szerezni róla, pénzt kicsalni tőle stb. Lehetséges célpontok például politikai nézet, faji hovatartozás, nemi identitás, földrajzi elhelyezkedés, anyagi helyzet alapján kiszemelt kis vagy nagy csoportok. Jó példa lehet erre valamilyen politikai befolyásoló támadás, ahol a felhasználói viselkedési minták alapján, célzottan egy adott térség bizonyos korosztályának tudnak eljuttatni hamis híreket, információkat. [22][23] A 2016-os amerikai elnökválasztás eredménye kapcsán számos ilyen vád látott napvilágot Donald Trump hatalomra kerülését követően. [24] Nem csak magánszemélyek, hanem jogi személyiség vagy valamilyen objektum is lehet a kiszemelt célpont. Ezekben az esetekben sincs érdemi eltérés a technikák között.

3.2. Passzív információgyűjtés (Footprinting)

A passzív információgyűjtés az alapja minden támadásnak. Számos forrásból lehet olyan információkat szerezni a szervezetről, a megtámadni kívánt személyről, melyek elősegítik egy célzott támadás kivitelezését. Hasznos adatokat szerezhet a támadó a célrendszerről és a hálózatról egyaránt ezekkel a módszerekkel. Ezek az eszközök azért nagyon hatásosak, mert alkalmazásuk az áldozat számára alapesetben nem tűnik fel.

Az egyik ilyen alapmódszer az internet böngészése, a kereső felületek használata. Sima böngészéssel is sok érdekes információhoz juthat a támadó, azonban a keresőmotorok megfelelő alkalmazása hatékonyabbá teheti ezt a folyamatot. Az egyik legnagyobb kereső, a Google mechanizmusainak

kihasználhatóságát az úgynevezett Google Hacking Database (GHDB) gyűjtemény tartalmazza.[4] Itt számos olyan hasznos keresési feltétel található, amellyel egy adott vállalatról specifikusan egy kijelölt weboldalon összegyűjtött, előre meghatározott fájlformátumú eredmények listázódnak ki. Ez csak egy alappélda, számos más módon használható ez az adatbázis támadó tevékenységekre, de hasznos lehet a mindennapi élet elősegítésére is.

A közösségi médiában számos információt osztanak meg magukról az emberek. Ezek egy része öncélú, másik része pedig az üzleti életben elengedhetetlen. A magánéletről megosztott tartalmak segítenek a támadóknak, hogy célzott támadást készítsenek elő, míg például az álláskereső oldalak, üzleti közösségi platformok segédkezet nyújtanak a támadónak, hogy a kiszemelt szakmai tudásáról, annak elérhetőségeiről tájékozódjanak. Mivel a mindennapi életünk részei ezek az felületek, ezért nem a kerülésük a megoldás. A rendeltetésszerű, tudatos használat segíthet az esetleges támadások minimalizálásában. [25]

Nemcsak személyekről, de cégekről, vállalatokról is rengeteg információt ismerhet meg az, aki ártó szándékkal közeledik. A különböző céges adatbázisok (például cégjegyzékek vagy a Crunchbase felülete[5]) hasonlóan informatívak, mint a privát életben használt közösségi média felületek. Itt tájékozódni lehet például az alapítókról, tőkéről, de adott esetben a befektetőkről, támogatókról is. Nagy esély van arra, hogy a támadó megismerje a célponthoz köthető elérhetőségeket, de akár információt gyűjthet a telephelyekről is, amelyek megismerése a későbbiek folyamán segítheti a támadások hatásfokát a megszerezhető adatok korrelálásával (például a cégvezetők ellenőrzése a közösségi média felületeken: Facebook,[6] LinkedIn[7]). Ha a szervezetnél nincsenek megfelelően védve a különböző technológiák, azok is könnyen kompromittálódhatnak. Az internetre kötött eszközöknek lehetnek olyan sérülékenységeik, amelyeket kihasználva a támadó egyéb információkat tudhat meg. Ilyen lehet egy rosszul konfigurált hálózaton lévő IP kamera. Több olyan platform is található az interneten, ahol céges, ipari kamerák képeit lehet online követni. Ugyanígy hozzáférhetők közterületeken található eszközök képei is.

A technikai információk megszerzésére ugyanolyan mértékben szüksége van a támadónak, mint az eddig leírt általános adatokra. Passzív módon is lehetséges olyan képet kapni egy rendszerről, ami elegendő ahhoz, hogy abból fel lehessen építeni a támadások alapjait. Az úgynevezett whois rekordok például segítenek egy domainhez tartozó alapinformációkat megismerni, mint például:

- a domain neve;
- a domain azonosítója;
- mely szerveren van az adott domain;
- a weblapot regisztráló vállalat URL-je;
- az regisztráció dátuma;
- az utolsó módosítás dátuma;
- a nyilvántartás lejártának dátuma;
- a weblapot regisztráló cég neve;
- a weblapot regisztráló cég IANA azonosítója;
- a weblapot regisztráló cég kapcsolati adatai (e-mail, telefonszám);
- a domain állapotai;

[4] https://www.offensive-security.com/community-projects/google-hacking-database/
[5] https://www.crunchbase.com/
[6] www.facebook.com
[7] www.linkedin.com

- a névszerverek;
- illetve egyéb megjelölt információk is előfordulhatnak.

Ezek mind hasznosak lehetnek a támadónak. E felületeken kívül például a PING csomagok is segíthetnek kideríteni, hogy elérhető-e az adott host. Ez a legegyszerűbben Windows-os eszközön a parancssor (CMD) megnyitását követően a „ping weblapcím" paranccsal lehetséges. Ezt azonban mindig fenntartásokkal kell kezelni, hiszen nem minden esetben ad hiteles képet.

A technikai információszerzés célja, hogy a támadó például IP (Internet Protocol) címeket, privát weboldalakat, futó TCP (Transmission Control Protocol)/UDP(User Datagram Protocol) alapú szolgáltatásokat, VPN (Virtual Private Protocol) vagy VoIP (Voice over IP) információkat gyűjtsön. Fontos az is, hogy a használt operációs rendszerről tudjon meg minél többet (verziószám, architektúra, felhasználói információk stb.). Az így megszerzett információkat érdemes a NIAC (National Infrastructure Advisory Council) kutatásai alapján létrehozott sérülékenységeket összegyűjtő CVSSv3.0 (Common Vulnerability Scoring System version 3.0) adatbázissal[8] korrelálni.

A passzív információgyűjtés során megszerezhető információkhoz nem csak az interneten keresztül juthatnak hozzá a támadók. Nyílt napok, kiállítások alkalmával hasznos információkra lehet szert tenni, de jól működhet a célobjektum közelében lévő éttermekben történő hallgatózás is. Az emberi naivitást, hiszékenységet kihasználó információszerzés módszerével, a social engineeringgel olyan információkat tudhatunk meg, amelyekhez az interneten sem tudunk hozzájutni.

3.3. Támadási felület feltérképezése (Scanning)

A passzív információgyűjtés alatt megszerzett adatok felhasználásának segítségével sokszor még további feltérképezési lépésekre van szükség. Főleg a rendszer és a hálózat megismerésére nem elegendőek mindig a nyílt információk. Ilyen esetekben különböző szkennelési eljárások alkalmazandóak. Ezekből többféle létezik, melyeket legegyszerűbben 3 típusba lehet sorolni. Első csoport a port szkennek, ahol többnyire a közismert portokon futó alkalmazások felderítése történik valamilyen módon. A második csoport a hálózat feltérképezését célzó feltérképező eljárások. Ebben az esetben a célhálózat aktív elemeinek megismerése a cél. A harmadik csoportba a rendszer sérülékenységeinek a felfedezésére irányuló felderítéseket soroljuk.

A támadás e szakaszában nagyon hasznos ismerni az nmap[9] különböző parancsait. E program segítségével a célnak megfelelő felderítést lehet eszközölni. A szkenneléseknek számos típusa létezik. A legtöbb ilyen jellegű támadás azon alapszik, hogy a különböző kommunikációs protokollok (TCP/UDP) hogyan épülnek fel, a kommunikáció során használt csomagok miként követik egymást bizonyos szituációkban. A szabályszerűségeken és a protokollok gyengeségein alapszanak ezek a támadások. Az nmap segítségével nemcsak a hálózatot tudjuk tesztelni, de az operációsrendszerről is tudhatunk meg információkat. Abban az esetben, ha elegendő információval rendelkezünk már, következő lépésként az úgynevezett bannerek megszerzésével kideríthetjük azt is, hogy mely szolgáltatások mely gépeken futnak.

Külön érdekes kérdés a vezeték nélküli hálózatok témaköre. A megtámadni kívánt személyek laptopjai, telefonjai, tabletjei stb. által használt Wi-Fi, Bluetooth hackelési technikái külön figyelmet érdemelnek. Ezeket az információkat könnyen beszerezhető eszközökkel, automata programok segítségével bárki megszerezheti. Előfordulhatnak olyan esetek, amikor a rossz telepítés, konfigurálás miatt a támadó könnyen hozzá tud férni egy megfelelően irányított antenna segítségével a hálózathoz relatíve nagy

[8] https://www.first.org/cvss/specification-document
[9] https://nmap.org/

távolságból is. Ez után, ha nincsenek megfelelően szegmentálva a VLAN-ok, akár a teljes hálózathoz is hozzáférhet.

3.4. Behatolási kísérletek (Enumeration)

A támadás ezen szakaszához főleg azok a technikák tartoznak, amelyek segítségével a támadók hozzá tudnak férni egy-egy rendszerhez. Jóval célzottabb tevékenységről van már szó, mint a korábbi szakaszokban, hiszen itt már jó eséllyel rendelkezésre állnak az alap hálózati és rendszerinformációk. Ebben a szakaszban a hozzáférések megszerzése a cél. Tipikusan a felhasználónevek és jelszavak megszerzése az egyik fő cél ebben az esetben. Az e-mailekből, az SNMP és az SMTP protokollok kihasználásával kinyerhető információkból is számos hasznos és releváns adat ismerhető meg. A támadónak egy operációs rendszerben meg kell ismernie, hogy milyen felhasználói csoportok érhetőek el, illetve azt, hogy azok korlátozott felhasználói vagy adminisztrátori jogosultságokkal vannak-e ellátva. Akár Windows, akár Linux rendszerről beszélünk, a támadónak a lehető legtöbb tulajdonságot kell begyűjtenie a felhasználói csoportokról. Fontos információval bírnak, hogy milyen futó alkalmazások vannak használatban lokálisan vagy esetleg rendszerszinten.

A hálózati forgalomban a TCP/UDP porok számozása három csoportba lett felosztva, amelyek ismeretében még több információt lehet kinyerni. 0–1023-ig a gyakran használt portok, 1024–49151-ig az úgynevezett regisztrált portok és a 49152–65535-ig terjedő tartományban a dinamikus, illetve privát portok lelhetők fel. A különböző jól ismert (Well Known Ports) és egyéb portokon futó alkalmazások tesztelésének eredménye további hasznos információval szolgál a támadóknak. Egy szervezet üzemeltetője, fejleszthetője dönthet úgy, hogy megváltoztatja ezeket, azonban jó eséllyel a legtöbb rendszernél az alapértelmezett kiosztás lesz használatban. A következő táblázatban találhatók meg a leggyakrabban használt portok és a hozzájuk kapcsolt szolgáltatások listája. A gyűjtés a teljesség igénye nélkül az IANA (Internet Assigned Numbers Authrity) kiosztása[10] alapján készült:

TCP port	UDP port	Megnevezés
TCP 21	-	FTP (File Transfer Protocol)
TCP 22	UDP 22	SSH (Secure Shell)
TCP 23	-	Telnet Protocol
TCP 25	UDP 25	SMTP (Simple Mail Transfer Protocol)
TCP 53	UDP 53	DNS (Domain Name System)
-	UDP 69	TFTP (Trivial File Transfer Protocol)
TCP 80	-	HTTP (HyperText Transfer Protocol)
TCP 88	-	Kerberos
TCP 110	-	POP3 (Post Office Protocol version 3)
TCP 135	UDP 135	RCP (Remote Procedure Call)
TCP 137	UDP 137	NetBIOS – name service
TCP 139	UDP 139	NetBIOS – session service
TCP 156	UDP 156	SQL Service
TCP 161	UDP 161	SNMP (Simple Network Management Protocol)
TCP 162	UDP 162	SNMPTRAP (Simple Network Management Protocol Trap)
TCP 389	UDP 389	LDAP (Lightweight Directory Access Protocol)

[10] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

TCP 443	-	HTTPS (Hypertext Transfer Protocol over TLS/SSL)
TCP 445	-	Microsoft-DS (Directory-Service: AD, SMB)

Megfelelő ismeretekkel ezekből a különböző szolgáltatásokból kinyerhetőek olyan adatok, amelyek a rendszer mélyebb szintjére történő bejutáshoz szükségesek. Azonban nemcsak a különböző protokollok gyengeségei, de az emberi tényező kihasználhatósága is könnyen sikerre vihet egy támadást a már említett social engineering technikák segítségével.

3.5. A rendszerbe történő bejutás (System Hacking)

A három korábbi lépés (passzív információgyűjtés, támadási felületek feltérképezése, behatolási kísérletek) alapos elvégzése után már sokkal összetettebb, komplexebb és többnyire mélyebb szaktudást igénylő feladatok következnek. Az interneten elérhető számos információ, tananyag, videó és más forrás, ahol megmutatják a készítők, hogyan lehet feltörni bizonyos rendszereket, hogyan lehet oda bejutni. Ez az ismertető azonban egy komplex támadáshoz nem mindig elég. Tudni kell, hogy egy-egy lépés mit eredményez a rendszerben, mint ahogy azt is célszerű megtervezni, hogy először olyan módszereket alkalmazzanak, amelyek kevésbé észrevehetőek a célpont számára.

Az egyik hacking technika a jelszavak törése. Többféle módszer van erre, a minden lehetséges opciót kipróbáló brute force megoldástól kezdve, a potenciális jelszavakat tartalmazó, szótár alapú törésekig. Azonban vannak más módok, hogy jelszavakat szerezhessen meg a támadó. A következőkben a teljesség igénye nélkül mutatunk be néhányat. A hálózati forgalomban megbújó különböző csomagok rejthetnek magukban belépéshez szükséges adatokat. Manapság a legtöbb belépési felület már titkosított (HTTPS) csatornán keresztül végzi az autentikációt. Ez nem garancia a biztonságra, de egy lépés a védelem felé. A mai napig vannak olyan weboldalak, ahol nyílt szövegben jutnak egyik helyről a másikra ezek az információk. Ilyenkor egy célszoftverrel (például a Wireshark alkalmazással) könnyen ki lehet olvasni a felhasználónevet és a hozzátartozó jelszót. Azonban vannak más protokollok, amelyeken keresztül egy támadó hozzájuthat belépési adatokhoz. Potenciális veszélyforrás lehet a Telnet, az SMTP, a rlogin, illetve az SNMPv1 is. Ha ezek a módszerek sem vezettek eredményre, a támadónak továbbra is fennáll a lehetősége, hogy a kiszolgáló és a felhasználó közé álljon a hálózati forgalomban, azaz úgynevezett Man-in-the-Middle (MitM) támadást hajtson végre. Több különböző támadást foglal magában ez a kifejezés, ilyen például a titkosított weboldalak ellen használt SSL Strip, de a Burp Suite és a Browser Exploitation Framework (BeEF) is a MitM alkalmazásokhoz tartozik. Ha ezen technikák alkalmazása után a támadó nem rendelkezik a kívánt jelszavakkal, akkor egyéb megoldásokhoz kell folyamodnia. Ez lehet például valamilyen trójai vagy kémprogram, esetleg keylogger adott rendszerbe történő bejuttatása, de a jelszavak hashének bejuttatása (hash injecting) is hozhat eredményt.

A rendszerbe történő bejutáshoz nem kizárólagos út a jelszavak megszerzése. A különböző autentikációs folyamatok sérülékenységei jó belépési pontokat jelenthetnek a támadóknak. Microsoft platformokon az úgynevezett SAM (Security Account Manager) adatbázisban tárolt jelszavak LM, illetve NTLM hashelő algoritmusa lehet egy kerülő út, de a Kerberos protokoll szimmetrikus kulcsú titkosításának hackelésére is van mód.

Minden esetben az elsődleges cél az, hogy egy olyan hátsó kaput (backdoor) tudjon nyitni a támadó, melyen keresztül nemcsak egy alkalommal, hanem szükségszerűen többször hozzáférjen a megadott rendszerhez. Itt lehet szó valamilyen biztonsági hiányosság kihasználásáról, vagy egy erre specifikált rosszindulatú kód (például RAT – Remote Acces Trojan) alkalmazásáról. Hátsó kapunak tekinthető egy-egy beállítás megváltoztatása (például egy új felhasználó létrehozása), vagy valamilyen reverse shell segítségével rendszerszintű parancsok futtatásának a képessége is.

3.6. A jogosultság növelése (Escalation of privilege)

Miután a támadónak valamilyen módon lehetősége van egy adott rendszerbe bejutni, a következő célja, hogy a rendelkezésére álló teret a lehető legjobban tudja szélesíteni. A köztes lépés a továbbiakban az lesz, hogy a céljainak (például információszerzés, a rendszer rombolása stb.) megfelelő legmagasabb szintű jogokkal rendelkezzen. A folyamat alapvetően kétirányú. Lehetséges oldal irányban terjeszkedni, hogy minél több hasonló jogosultsággal rendelkező felhasználó nevében tudjon műveleteket elvégezni. Ez tipikusan a helyi hálózaton vagy egy rendszeren belül történő terjeszkedést célozza meg, illetve hogy minél több érzékeny rendszerhez férhessenek hozzá a támadó, így növelve a hatásfokot. A másik cél, hogy vertikálisan, a magasabb jogosultsággal rendelkező felhasználókat tudja kihasználni. Ebben az esetben nagyobb valószínűséggel tud a támadó adatokat módosítani, kiszivárogtatni, de más lépéseket is egyszerűbben tud elvégezni egy távoli cél elérése érdekében.

3.7. Nyomok eltüntetése (Covering tracks)

Egy professzionális támadó próbál minél jobban, a lehető legtovább elrejtőzve maradni, hacsak nem az a konkrét célja, hogy láttassa magát. Azért, hogy esetleg a jövőben is ki tudja használni az áldozat infrastruktúráját, a támadás kivitelezése után megpróbálja minél jobban eltüntetni azokat a digitális nyomokat, amelyeket tevékenységével hagyott a rendszerben. Teszi ezt azért is, hogy elkerülje a bonyodalmakat az esetleges nyomozati szervek tevékenysége kapcsán. Arról van szó, hogy ha lehetséges, mindent visszaállít az eredeti állapotába, mindezt olyan kivitelezéssel, hogy a jövőbeli bejutás biztosított legyen. A másik fontos lépés, hogy eltüntesse az árulkodó bejegyzéseket az előzményekből, a registry-ből, a naplóállományokból, illetve az ezeket kezelő rendszerekből.

4. Informatikai támadások

Különböző módon lehet támadásokat kivitelezni. Megtámadható egy rendszer a sérülékenységeit kihasználva az interneten keresztül, alkalmazhatók különböző rosszindulatú kódok, de magát az embert is ki lehet használni. E fejezetben olyan tipikus technikákat mutatunk be, amelyekkel könnyen találkozhat bárki akár különböző médiumokban is.

4.1. Social engineering

A bemutatott lépések mellett azonban fontos említést tenni a social engineeringről is, amely valamilyen formában mindegyik ponthoz kiegészítésként köthető. Ennek a fogalomnak a megismerése mindenki számára hasznos lehet, aki informatikai eszközöket használ magáncélra vagy munkája elvégzésére. De mit is foglal magában ez a kifejezés? Christopher Hadnagy, a téma egyik szakértője a következőként fogalmaz *Social Engineering – The Art of Human Hacking* című művében:

„…social engineering a művészete, még inkább a tudománya annak, hogy gyakorlatias műveletekkel befolyásoljuk az emberi lényeket, azért, hogy a célunk érdekében cselekedjenek az életük néhány helyzetében…" [26]

Alapvetően nem negatív cselekedetekről van szó. A kisbaba, amikor nyalókáért sír és toporzékol a bolt közepén, ugyanúgy használja – tudattalanul – ezeket a technikákat, mint az orvos, amikor páciensét szaktudásának megfelelő módon terelgeti. Ezek a technikák azonban a rossz szándékú támadó kezében is hatásosak, hiszen az emberi lény hiszékenységét, jószándékát, naivitását és sok más tulajdonságát használja ki. Azért tudnak ezek az alapvetően információszerzésre irányuló technikák jól működni, mert információval telített gyors életünktől éppen csak annyiban térnek el, hogy az áldozat az adott pillanatban vagy ne vegye észre, vagy ne tulajdonítson neki jelentőséget. Kevin D. Mitnick, a legendás hacker így írja körül a social engineeringet *A megtévesztés művészete* című könyvének előszavában:

„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy a nélkül – képes az embereket információszerzés érdekében kihasználni." [27]

4.1.1. Humán alapú technikák

Mitnick idézetéből is jól kivehető, hogy két csoportba lehet sorolni a támadó technikákat: humán és technikai alapúakra. Az elsőbe tartoznak azok, amelyekhez alapvetően nem szükséges semmilyen technológiai eszköz. Ezekben az esetekben sokszor elegendő, ha valakinek az identitását lopják el, és a támadó másnak adva ki magát tud információkhoz vagy különböző rendszerekhez hozzáférni. Leggyakrabban valamilyen álruhába bújva próbálkoznak. Ilyen lehet egy pizzafutár, egy szerelő, egy rendőr személyiségének a felvétele. Céges környezetben több megszemélyesítési mód is működhet: például egy ismeretlen alkalmazott, új munkaerő, gyakornok, magas pozíciójú vezető, IT szakértő, rendszergazda vagy a partnercég munkatársa, de egy auditori vagy egy ellenőri szerep is lehet hatásos bizonyos szituációkban. Érdekes, de működő megoldás lehet az úgynevezett Tombstonetheft,[11] amikor a támadó egy olyan elhunyt személy nevében cselekszik, akinek a tragédiájáról az adott környezet még nem szerzett tudomást.

Sokszor működő megoldás, hogy a social engineer először megtesz valamit az áldozatnak, hogy utána cserébe „jogosan" kérhessen ellenszolgáltatást, például néhány apró információt vagy egy pendrive csatlakoztatását nyomtatási szándéknak álcázva. Cél lehet olyan helyzet megteremtése, amikor az

[11] http://www.social-engineer.org/framework/Social_Engineers:_Identity_Thieves#Tombstone_Theft

áldozat azt gondolja, hogy önszántából kér segítséget a támadótól, holott ez előre előkészített szituáció. Egy forgatókönyv lehet erre a szituációra, hogy a támadó beszélgetésbe elegyedik, és szimpatikussá teszi magát [28] valamilyen rendezvényen a potenciális áldozattal, akinek mesél szakértelméről, tudásáról (például remek rendszergazda). Néhány nappal később a támadó szándékosan olyan hibát idéz elő az áldozatnál, amelynek a kijavításához pont ő ért, ezért nagy valószínűséggel egy megkeresést fog kapni a hiba javításához. Ez után sokkal könnyebb lehet hozzáférni a rendszerhez.

A humán alapú technikák közé sorolhatjuk a jelszavak kitalálását. Az emberek sokszor használnak érdeklődési körükből következtethető (például kedvenc sportcsapat, sportoló, együttes, előadóművész, családtag vagy háziállat neve stb.), számukra releváns évszámoknak megfelelő (például családon belüli születési dátumok, évfordulók stb.) jelszavakat, de az alapértelmezett (például admin) és a gyakori (például 1234, 12345678, qwerty, asdf, password stb.) kifejezések is használatban vannak sok helyen. A támadónak nincs más dolga, mint egyesével kipróbálgassa ezeket, vagy építsen egy specifikus szótárfájlt, amit egy erre alkalmas programmal végigfuttat egy rendszeren. Ha esetleg egyik sem működik, még mindig ott a lehetőség, hogy úgynevezett brute force (nyers erő) módszerrel minden lehetséges kombinációt végigpróbáljon a támadó abban bízva, hogy kellően rövid jelszóval van dolga ahhoz, hogy belátható időn belül feltörje. Érdemes megemlíteni a jelszavak, kódok valamilyen eszközön (például: klaviatúra, érintőképernyő stb.) bevitelkor történő lelesését is. Ezt a szaknyelv shoulder surfingnek nevezi.

Az épületbe történő illetéktelen bejutásnak több módszere van, ebből kettőt szükséges mindenképpen kiemelni. Az egyik technika az úgynevezett tailgaiting, amikor a támadó egy csoporthoz csatlakozik, és a tömegben elvegyülve jut be az épületbe, helyiségbe. Illetve piggybackingnek nevezzük azokat a módszereket, amikor az otthon maradt kulcs vagy belépőkártya történetét használják fel a jogosulatlan belépéshez.

A humán alapú technikák egyik, ha nem a leghatásosabb módszere a dumpsterdiving, azaz kukabúvárkodás. A felelőtlen felhasználók számos olyan papír- vagy más alapú szemetet dobnak ki, amelyből az értő szem messzemenő következtetéseket tud levonni: hasznos információkat tudhat meg egy-egy vállalatról vagy személyről különböző dokumentumokból, levelekből. Nem is beszélve azokról a leírt napi rutinokról, kapcsolatokról, esetleg jelszavakról, amelyeket a jegyzettömbre írnak fel az emberek, hogy ne felejtsék el őket, majd miután már nincs rá szükségük, felelőtlenül kidobják azokat. Ez a social engineerek aranybányája. Jó védekezési megoldás lehet a papíralapú adathordozóknak az iratmegsemmisítővel történő ledarálása, ám ebből is olyat érdemes használni, ami nemcsak vertikálisan, hanem horizontálisan is elvágja a lapot. Van az az információ, amiért érdemes hosszú időt eltölteni a ledarált papírdarabok összeillesztésével, ezért célszerű megnehezíteni a támadók dolgát.

4.1.2. IT alapú technikák

Az IT alapú technikák közé lehet sorolni a 3.2. fejezet információgyűjtési technikáit: a weboldalak, a közösségi platformok, blogbejegyzések, vlog és más multimédia-tartalmak átvizsgálását és a Google Hackinget is. Rengeteg információval szolgálhat egy védelemmel el nem látott laptop vagy más mobil eszköz (például okostelefon, tablet, PDA stb.) eltulajdonítása. Manapság egy-egy ilyen eszközhöz történő hozzáférés a támadót a lehető legközelebb engedi célpontjához. Ezeken az alapvetően passzív, illetve fél-aktív megoldásokon kívül léteznek olyan technikák is, amelyekhez a támadó kreativitására, ügyességére nagyobb szüksége van.

A legelterjedtebb ilyen technika az adathalász (azaz phishing) levelek használata. Itt minden esetben az a célja a támadónak, hogy elhitesse a célponttal, hogy legitim e-mailt kap. Ennek a támadásnak két célja lehet. Egyrészt valamilyen malware bejuttatása az áldozat számítógépére. Ezt a támadó úgy éri

el, hogy olyan hihető szöveget ír a fogadó félnek, hogy az a levél rosszindulatú kódot rejtő csatolmányát megnyissa, vagy a szövegben szereplő fertőzött weboldalra mutató linkre rákattintson. Másrészt lehetséges, hogy a támadó valóban adatokat (felhasználónevet, a hozzá tartozó jelszót vagy más személyes jellegű információkat) szeretne nem túl szofisztikált módon megszerezni. Ilyenkor egy legitimnek tűnő weboldalra irányítja az áldozatot a phishing levél szövegének a segítségével, ahol rákérdez a szükséges adatokra, a legtöbb esetben valamilyen kérdőívnek álcázott megoldással. A támadás létezik más, nem csak e-mailes formában is. Ilyen közvetítő felület lehet egy chat alkalmazás, sms (smishing), DNS szerver (pharming). A kifejezetten cégvezetők ellen irányuló támadásokat whalingnak nevezzük. A phishing célzott típusát spear phishingnek nevezzük. Ilyenkor kifejezetten egy ember vagy embercsoport ellen tervezi meg a támadó a csali levelet, annak biztosítása érdekében, hogy az áldozat a legnagyobb valószínűséggel sétáljon be a csapdába. A spear phishinget általában alaposabb információgyűjtés előz meg, ami alapján a támadó megismerheti a megtámadni kívánt személy vagy csoport érdeklődési területét, illetve az ehhez kapcsolódó szakszavakat, terminológiát, szokásos stílust. Ezekre a hitelesség növelése miatt van szükség.

A social engineer különböző kártékony kódokat, trójai programokat juttathat a céleszközre. Lehet ez valamilyen játéknak vagy más szoftvernek álcázott program, egy flash játék vagy egy torrent oldalon elhelyezett, ingyenessé tett célszoftver is. Az ilyen jellegű megoldások több célt szolgálhatnak. Az egyik lehetőség lehet olyan úgynevezett keyloggerek telepítése, melyek célja, hogy folyamatosan rögzítse a billentyűzet-leütéseket, az egér mozgását és kattintását, de akár megadott időnként képernyőképet is készítsenek. Keyloggerből léteznek fizikai megoldások is, melyeket például egy klaviatúra csatlakozójának toldalékaként lehet elképzelni. Ez az eszköz a számítógép és a periféria közé illesztve rögzíti a rajta átfolyó tartalmat.

úgy el egy frekventált vagy célirányú helyen, hogy az elhagyott eszköznek tűnjön. A CD/DVD-k hőskorában például a „Kedvenc képek/filmek” felirat lehetett hívó szó, amit a gyanútlan áldozat a számítógépébe helyezve saját eszközét fertőzte meg. Manapság ezt a technikát a jelenleg sokkal jobban elterjedt memóriakártyák és USB pendrive-ok segítségével hajtják végre. Az emberi kíváncsiságot, segítő szándékot kihasználva lehet így bejuttatni a kártevő kódot, akár egy alapvetően zárt rendszerbe is.

Minden technikát lehet a másikkal ötvözni, legyen szó humán vagy technikai alapú támadásról. A lényeg az, hogy az alapvető emberi tulajdonságokat használja ki, és a lehető legjobban illeszkedjen a hétköznapokhoz. Annyira egyszerű megoldások is sikeresek lehetnek, mint egy weblap címében a kicsi „L” betű kicserélése az egyes számra. A következő példában az első címben a normál betű, míg a másodikban pedig a szám szerepel: http://www.valami.com; http://va1ami.com. Jó eséllyel bárkit megtévesztene egy ilyen domain mögé bújtatott kártékony oldal. Szerencsére a böngészőket is kezdik felkészíteni ilyen jellegű esetekre, és már van, ahol olyan karakterkészleteket használnak, amelyekben a karakterek különbözősége miatt a felhasználó nagyobb eséllyel veszi észre az eltéréseket.

4.2. Malware-ek

A támadások egy részét az úgynevezett rosszindulatú szoftverek, azaz malware-ek (malicious software) segítségével tudják a támadók kivitelezni. Ezek a programkódok különböző formában vannak jelen. Ször Péter több nyelven megjelent, *A vírusvédelem művészete* című kötetében az önreprodukáló automatáktól kezdve foglalja össze a malware-ek történetét. [29]

A következő táblázat fő jellemzőikkel együtt mutatja be a különböző platformokon (Windows, Linux, UNIX, Android, IoS stb.) előforduló malware típusokat. A táblázat összegyűjti Ször Péter 30 éves

kutatása alatt összegyűjtött, témához kapcsolódó eredményeit [30], illetve a halála óta megjelent új típusokat [31]:

A malware típusa	**Fő jellemzők**
Ször Péter: *A vírusvédelem művészete* című kötete alapján	
Vírusok	Saját magát vagy önmagának egy fejlettebb változatát másoló kód. Fájlokat, rendszerterületeket fertőznek meg.
Férgek	A vírus olyan speciális változata, amely elsősorban a hálózaton terjed. Általában önmagától terjedő programkód, ritkán emberi indikáció szükséges a fertőzés elindítására. (Altípusai: levélférgek, polipok, nyulak.)
Logikai bombák	Normál szoftverbe a programozó által beépített működési anomália.
Trójai falovak	Valamilyen más programnak vagy annak egy részének álcázzák magukat. (Altípusai: hátsóajtó-programok, jelszólopó vírusok)
Baktériumok	Kezdetleges vírusfajták.
Alkalmazáshibát kihasználó vírusok (Exploit vírusok)	Egy program sebezhető pontját/pontjait támadják célzottan.
Letöltők	Más rosszindulatú programok telepítésében segítenek.
Tárcsázók	Fizetős szolgáltatásokra irányító kód.
Dropperek	Például a rendszerindító szektorba települő vírusok telepítéséért felelős kódok.
Injektorok	A dropper speciális változatai, amelyek a memóriában aktív állapotban helyezik el a vírusokat.
Automatizált jogosultságszerzők	Magas jogosultságszerzésre alkalmasak, általában exploit vírus segítségével.
Kitek (vírusgenerátorok)	Vírusok generálására alkalmas programok.
Spammer programok	Kéretlen levelek küldésére alkalmas programok.
Flooderek	Szolgáltatás-leálláshoz vezető, többlet adatforgalmat generáló programok.
Billentyűzetnaplózók (keyloggerek)	A billentyűzet-leütéseket, adott esetben monitorképet, más beviteli perifériák tevékenységét rögzítő malware-ek. (Létezik hardver változat is.)
Rootkitek	Rendszergazdai jogosultságú, akár kernelszintű hozzáférést biztosító programcsomagok.
Spyware	Felhasználói (például internetes) tevékenységet kutató programok.
Hirdető programok	Kéretlen reklámokat jelenítenek meg például a böngészőkben. Rendszerint más kárt nem okoznak.
A szerző korábbi munkássága alapján	

Ransomware (zsaroló vírus)	Olyan malware-ek, melyek visszaállítható vagy visszaállíthatatlan módon titkosítanak a célrendszerben, majd váltságdíjat kérnek a feloldókulcs megadásáért.
Kripto vírusok	A kriptovaluták lopására alkalmas kártékony kódok.
Destructoware	A trójai falovak egy fajtája. A legitim szoftver valamilyen funkcióját kihasználva kifejezetten romboló hatást ér el.

A különböző malware-eket csoportosíthatjuk a fertőzés módja szerint is. [32] Ebben az esetben megkülönböztetünk a bootszektort célzó, úgynevezett boot vírusokat, amelyek a rendszer bootoláskor töltődnek be úgy, hogy magukat másolják be az indításkor. Mivel ezek a kártevők a legtöbbször rendszerszintű változásokat hoznak létre, sokszor igen hatékonyak. A következő csoportba a fájlvírusok tartoznak, amelyek a futtatható állományok segítségével érik el céljukat. A különböző Microsoft Office programokat kihasználó, makro nyelven megírt kártevők az úgynevezett makrovírusok. A helyi, illetve kiterjedtebb (például internet) hálózatok protokolljait a hálózati vírusok segítségével tudják kihasználni a támadók. Létezik a polimorf, mutálódó, öntitkosító vírusok kategóriája is, amelynek tagjai önmaguktól képesek saját kódjukon változtatni.

A malware-ek ellen történő védekezés többféleképen lehetséges. [33] Első, alapvető formája a mintaalapú keresések, ahol egy jól ismert vírusminta alapján keresik az egyezőségeket az antivírus gyártók adatbázisaival. (Célszerű lehet gyanús tevékenységnél olyan adatbázisokba feltölteni a kártékonynak vélt kódot, mint például a www.virustotal.com, ahol több gyártó motorja is be van építve.) Egy másik kereső eljárás a programkódokban található vírusfunkciókra utaló mintákat célzó, úgynevezett heurisztikus keresések. Ezek a fajta detektálási módok csak akkor hatékonyak, ha van már korábbról jól ismert minta. Noha a gyártók folyamatosan frissítik saját adatbázisukat, a még fel nem fedezett, nulladik napi (zero-day) sérülékenységek ellen hatástalanok. Ilyen esetekben a változás tényét fogja a védelmi szoftver felismerni, ami által még mintával nem rendelkező malware-ek ellen is hatékonyabb megoldást nyújthat.

4.3. Támadási technikák

Számos támadás létezik a kibertéren keresztül. A különböző rosszindulatú kódok (malware-ek) más és más célra alkalmasak. Sok esetben nincs is értelme kiragadni az adott környezetből a behatolásra használt programot. Egy számítógép akár bűncselekmény tárgya lehet a tulajdonos tudta nélkül is. Előfordulhat, hogy a támadó nem új fertőzést szeretne egy gépen eszközölni, hogy hozzáférést szerezzen vagy oda bejuttasson valamilyen rosszindulatú kódot. Ilyen lehet, ha egy korábban saját maga vagy más által zombi-hálózat (botnet) részévé tett eszközökkel szeretne túlterheléses támadást kivitelezni valamilyen rendszer ellen. A példánál maradva, az sem mindegy, hogy mi a szándéka a támadónak. Lehet, hogy egyszerűen csak fel szeretné hívni a figyelmet magára (például egy hacktivista csoport), vagy adott esetben a célrendszer valamilyen sebezhetőségén keresztül egy túlterheléssel olyan műveleteket kíván véghez vinni, melyet normál működés alatt nem lehet. Lehetséges továbbá az is, hogy egy-egy támadást előre megtervezve különböző lépéseken keresztül juthat be a támadó. Ezt beszállítói lánc (Supply Chain Attack) támadásnak hívjuk. [34] Jó példa erre a korábban már említett, iráni Siemens urándúsítók motorja elleni Stuxnet támadás, ahol a kód már korábban megfertőzött számos USB pendrive-ot, és a célrendszerben hajtotta végre a konkrét támadást.

Másik példa a – többnyire felhasználói vagy személyes adatok gyűjtésére szolgáló – adathalász támadások egy része. Számos olyan esetről van tudomásunk, ahol a támadást nem előzi meg

semmilyen előkészület, és sok esetben utólag sem történik újabb művelet. Az úgynevezett nigériai levelek kiküldésénél a csalók, miután megírták az üzenetek szövegét, és kiküldték azokat a nagyvilágba, csak vártak, hogy valaki bedőljön a csalásnak. Nem szerettek volna mélyebben más rendszerekhez hozzáférni, csupán pénzt szerettek volna szerezni. Nem mindegy tehát, hogy a támadónak mi a célja, hogy célzottan valaki(k) ellen szeretnének elkövetni egy támadást, vagy halászó módon annyi a lényeg, hogy valaki áldozatul essen. Az embereket érő nagy adatmennyiségben (Big Data-ban) [35] egyszerűen tud bárki áldozatul esni.

Az internet felől érkező támadások a rosszindulatú cselekvések nagy részét képzik, mivel nem szükséges hozzá személyes jelenlét, így a támadó könnyebben el tud bújni. Mivel az állami, az üzleti és a magánszektor számos internetre kötött eszközt, rendszert használ, így adja magát, hogy ezeknek a kihasználásával sikereket lehessen elérni a támadó oldalon. Nem nehezíti meg a dolgukat az a trend, miszerint az emberek a hétköznapjaik során is rengeteg időt töltenek az interneten, amire például a We Are Social elemző cég riportja[12] is rávilágít. E fejezetnek nem célja, hogy bemutasson minden támadási technikát, csupán néhány ismertebbet sorol fel a jól ismert sérülékenységeket kihasználó megoldások közül.

4.3.1. DoS/DDoS

A két technika között az alapvető különbség az, hogy míg a DoS (Denial of Service) az egy adott gépről induló csomagokat jelenti, addig a DDoS (Distributed Denial of Service) támadást több, általában botnetbe rendeződött eszközök hajtják végre. A túlterheléses támadások alapvetően két célt szolgálnak. Egyrészt lehet általánosan egy hálózati kommunikáció ellehetetlenítése (például a SYN csomagokkal történő elárasztás technikájával, az úgynevezett SYN flood támadással), vagy a támadók akár célzottan egy szolgáltatás megfelelő működését próbálják meggátolni. [36]

4.3.2. XSS

Az XSS, azaz Cross Site Scripting a különböző oldalakon keresztül történő scripthívást foglalja magában. A phishing támadásoknál használt, link alapú, nem perzisztens fajtája során magába az URL-be illesztették be az adott scriptet (például java script). Egy támadónak az is lehet a célja, hogy úgy helyezze el a kódját egy oldalon, hogy az minden betöltéskor fusson le. Példa erre egy blog alatti kommentként történő beillesztés. Ennek a módszernek alapfeltétele, hogy a weboldal írója a készítés során ne akadályozza ezt meg valamilyen szűréssel. A minden megnyitáskor lefutó XSS változatát hívjuk perzisztensnek. [37]

4.3.3. SQL injection

Ez a támadási mód a webes alkalmazások mögötti adatbázisok ellen irányul. A dinamikusan összeálló lekérdezések lehetőséget biztosítanak a támadónak, hogy a programozók előre megalkotott kereteit, megszorításait kikerülhessék, a nem hitelesített biztonsági réseket kihasználhassák. Egy tudatosan használt, megfelelően parametrizált kérés futtatásával, azaz „befecskendezésével" olyan adatok nyerhetők ki a háttér adatbázisból a webes alkalmazásokon keresztül, amelyekre eredetileg nem volt jogosultsága a támadónak. E technikával akár a teljes adatbázis tartalma is megismerhető. [38]

4.3.4. Cookie poisoning

A bejelentkezések és a folyamatok azonosításához a weblapok úgynevezett sütiket, azaz cookie-kat használnak. A támadó célja az lehet a sütimérgezéssel, hogy ezeket valamilyen módon manipulálja,

[12] https://wearesocial.com/blog/2018/10/the-state-of-the-internet-in-q4-2018

módosítsa, hogy így elkerülje a különböző biztonsági mechanizmusokat. Ezzel a támadással illetéktelen információkhoz juthatnak más felhasználókról, illetve ellophatják személyazonosságukat. [39]

4.3.5. Forráskód elemzés, weboldal tükrözés

Dokumentumként lementve a weboldalak forráskódját, akár online kapcsolat nélkül is elemezheti a támadó a megtámadni kívánt weblapot. Az elemzés következtében megismerheti az oldalon található sérülékenységeket. Az elemzését követően akár egy meghamisított weblapra is könnyen letükrözheti az eredeti design-t, melyet egy social engineering, phishing támadás során tud felhasználni. [40]

4.3.6. Túlcsordulás előidézése

Érdemes megemlíteni az egyébként jellemzően nem webes alkalmazások programozási hibáit kihasználó technikát. Ez esetben olyan mennyiségű adat kerül használatra a program futtatása közben, hogy az meghaladja a számára fenntartott területet. Ilyen esetekben könnyen összeomlás is eredményezhető például egy olyan nem megfelelően megírt webszerver-szolgáltatás esetében, amely paramétereket vár a felhasználótól. Erre egy példa lehet, ha a támadó a cookie userid változóban helyezi el kódot (cookie injection), amit a webszerver rosszul kezel, és így túlcsordulás miatt eszközölhető távoli kód futtatása. Ha a támadónak van megfelelő ismerete a háttérben futó alkalmazásról, akár rosszindulatú kód befecskendezését is végre tudja hajtani. Ez által lehetséges egy adott számítógép felett átvenni az irányítást, vagy annak a felhasználónak a nevében parancsot futtatni, akihez a sérülékeny program volt rendelve. [41]

5. Behatolások elleni védekezés

A támadások elleni védekezés kiépítése egyáltalán nem egyszerű feladat, mivel a korábban felsorolt különböző támadási indítékok és módszerek ellen teljeskörűen nem lehet védekezni. A megoldást a réteges, kockázat alapú biztonsági megoldások, kontrollok jelenthetik, amelyeket megfelelően képzett szakemberek, jól kidolgozott folyamatok mentén tudnak kialakítani, működtetni és fejleszteni.

5.1. A védendő információk kategorizálása

A behatolás elleni védekezést többféleképen meg lehet közelíteni. Az egyik legfontosabb tisztázni való kérdés – a tervezés során –, hogy mi a védekezés fő célja. Az információbiztonság kiemelten 3 tulajdonsággal foglalkozik az információs rendszerek védelmével kapcsolatban. Az egyik legfontosabb tényező a bizalmasság (Confidentiality) fenntartása. Itt a cél az, hogy az adott információkhoz, rendszerekhez csak azok férhessenek hozzá, akik valóban jogosultak rá. A sértetlenség (Integrity) fenntartásánál a szakemberek azt próbálják biztosítani, hogy illetéktelenül ne lehessen módosításokat eszközölni különböző beállításokban, adatokon. A harmadik a rendelkezésre állás (Availability). A cél az, hogy egy adott rendszer az elvárt időtartamban elérhető legyen. Célszerű, ha e három tulajdonságot folyamatosan fenn tudjuk tartani a megfelelő arányban. A fókusz azonban eltérő lehet különböző szektorok, szolgáltatások esetén.

A három fő tulajdonság mellett azonban vannak más olyan tulajdonságai az adatoknak, amelyeket érdemes biztosítani, védeni. A letagadhatatlanság (Non-repudiation) megteremtése során a cél az, hogy a feladó, szerző ne tudja letagadni az adat eredetét. A hitelesség (Authenticity) azt hivatott biztosítani, hogy minden kétséget kizáróan megállapítható legyen a feladó fél személye. Végül pedig a tevékenység jogszerűségének (Legality) biztosítása jelenthet kihívást az információbiztonság megteremtésekor.

Végig kell gondolni, hogy milyen kontrollok bevezetésével lehetséges a legkönnyebben a céloknak megfelelő hatást elérni. Beszélhetünk fizikai, logikai és adminisztratív fajtákról. Míg az elsőnél az a cél, hogy fizikailag tudjuk lehetetlenné tenni az ártó szándékú vagy figyelmetlenségből adódó károkozást, addig a logikai intézkedések a rendszeren belül akadályozzák meg azt, hogy valaki jogosulatlanul tevékenykedjen. Legalább ennyire fontos az is, hogy szabályzatokkal, nyilvántartásokkal, szerződésekkel, jogszabályokkal biztosított legyen az adminisztratív szabályozás. Egy másik megközelítés a CISSP [42] szerint: a kontrollokat detektív (Detective), korrekciós (Corrective), elrettentő (Deterrent), helyreállító (Recovery) és kompenzáló (Compensating) módon célszerű csoportosítani.

Bármelyik módon is tervezünk védelmet biztosítani a rendszernek, fontos, hogy a kialakítás nem egy statikus tevékenység, amit ha egyszer elvégeztek, akkor azzal többet nem kell foglalkozni. A környezeti körülményeket figyelembe véve állandóan fejleszteni kell a rendszert és a folyamatokat a mindenkori fenyegetéseket szem előtt tartva. [43] A fejlesztés mindig a tervezési (Plan) szakasszal kezdődik, amely célszerűen kockázatelemzésen alapszik. Ezután a konkrét cselekvés (Do) következik, amikor kialakítják a kontrollokat. Egy bizonyos idő után mindenképpen valamilyen formában (például audit, sérülékenységvizsgálat stb. segítségével) ellenőrizni (Check) szükséges, hogy megfelelő védelmet nyújtanak-e az általunk bevezetett megoldások. Ahol nem kielégítőek az eredmények, ott be kell avatkozni (Act) azért, hogy a lehető legmagasabb védelmi szintet érhessük el. Ez a PDCA ciklus, melynek követése folyamatos karbantartást, fejlesztést eredményez.

5.2. Adatvagyon

Az információ- és adatvédelem kialakításánál törekedni kell a költség és a védelmi célok arányának fenntartására. Manapság a különböző biztonsági megoldások fejlettségi foka és számossága lehetővé teszi, hogy egy rendszer a megfelelő biztonságban legyen. A management értelemszerűen nem fog forrást allokálni olyan beruházásokra, amelyeket pénzkidobásnak értelmez. Ezért (is) szükséges úgy megtervezni a bevezetni, fejleszteni kívánt megoldásokat, hogy arányban legyenek a védendő értékkel. Ennek meghatározására a szervezetnél található adatvagyon megismerése és értékelése szükséges. Ennek első lépése, hogy a szervezet üzleti igényeknek megfelelően kialakítja saját kárérték tábláját. Itt meghatározza, hogy a különböző rendszerekben található adatok vagy azoknak egy optimális elv mentén csoportba rendezett körének (például szerződések, ügyféladatok stb.) bizalmasságának, sértetlenségének, rendelkezésre állásának sérülése milyen kárt okozna a cég számára. Ezt sávos formában szükséges elkészíteni, melyeket általában egytől ötig terjedő skálán szoktak elhelyezni.

Egy cég életében azonban többféle kár is keletkezhet. Előfordulhat anyagi kár, amikor például egy csőtörés következményeként a nem jól kialakított szerverszobát eláztatja a víz, és új eszközöket kell vásárolni. De ugyanúgy kieséssel jár, ha a cég fő bevételi forrását jelentő szolgáltatás nem érhető el hosszú ideig. Jó példa erre egy online webshop.

Sok esetben azonban a jó hírnéven esett csorba nagyobb veszteség lehet, mint maga az elszenvedett összeg. A banki szektort ért támadásokat nem véletlenül nem publikálják minden alkalommal. Annak ellenére, hogy elemzési adatok szerint [44] az online banki csalások mindennaposak, mégsem halljuk a sajtóban, hogy megint megtámadtak egy bizonyos pénzintézetet. E szervezetek kifejezetten ügyelnek arra, hogy a lehető legkevesebb negatív megjelenést kapják a sajtóban, hiszen az ügyfeleik máskülönben bizalmukat vesztenék, és egy másik banknál intéznék pénzügyeiket.

Abban az esetben, ha a személyes adatok kezelésében egy elégedetlen ügyfél hibát talál, könnyen be is perelheti az adott vállalatot, így okozva annak jogi kárt például a büntetési tétel kifizetésével. Azt, hogyan is néz ki egy ilyen kárhatástábla, a következő példa szemlélteti:

Kárjelleg	1 (minimális)	2 (csekély)	3 (közepes)	4 (jelentős)	5 (kritikus)
Anyagi kár	1 mFt-ig	1–5 mFt	5–15 mFt	15–30 mFt	30 mFt felett
Jogi kár	1 mFt-ig	1–5 mFt	5–15 mFt	15–30 mFt	30 mFt felett
Presztízskár	1–5 negatív komment a közösségi médiában, mely nem kelt visszhangot	1–5 negatív komment a közösségi médiában, melyekhez max. 10-10 megosztás társul	5–50 negatív komment a médiában, melyekhez több megosztás társul, de 1–3 nap után megszűnik a további tartalom generálás	A közösségi média felületeken 1 hétig folyamatos negatív hangvételű tartalom-generálást eredményez.	1 hétnél tovább a közösségi médiában újabb és újabb negatív hangvételű tartalom-generálást eredményez.

A kárhatás-táblára nincs általánosan elfogadott szabvány, amely szerint el kellene készíteni azt. Igény szerint változtatható a sorok száma, illetve a tartalom is. Célszerű követni az egytől-ötig terjedő skálát, mert a legtöbb helyen ezt használják, így ha egy külső auditor vagy egy jövőben érkező munkatárs tartja a kezében, akkor könnyen átlátja és megérti. De ez sem kötelező érvényű.

Egy példa kedvéért érdemes elgondolkozni azon az eseten, hogy ha egy adott adatkörbe tartozó valamilyen adat nyilvánosságra kerül, akkor milyen károk érik a szervezetet. Legyen jelenleg ez a felső vezetők fizetési adata. Közvetlen anyagi kár, ha a versenytársak ennek hatására átcsábítják ezeket a kulcsembereket egy magasabb fizetési ígérettel. Jelentsen ez a táblázat szerint egy 3-as (közepes) kárértéket. Szélsőséges esetben azonban annyira magasak a fizetések az adott szervezetnél, hogy mindenféle pletykák kezdenek el terjedni a közösségi médiában, és a közvélemény egy hétig napirenden tartja a témát, amire a sajtóban megjelenő cikkek is erősítik. Ez a táblázat szerint 4-es (jelentős) szintet jelent. A példában tehát szerepel kettő darab különböző érték: 3, 4. Ezekben az esetekben a kontrollokat úgy kell kialakítani, hogy a 4-es szinthez rendelt biztonsági megoldásokkal legyen védve, azaz a legnagyobb kárhatást szükséges minden figyelembe venni. Mint ahogy a PDCA modell is mutatja, ezt nem elég egyszer elkészíteni, folyamatosan célszerű naprakészen tartani és időnként felülvizsgálni.

5.3. Az információbiztonsági kontrollok

Amint a szervezetnél elkészült egy mindenre kiterjedő adatvagyonleltár, szükséges kialakítani egy rendszert, mely a megfelelő védelmi szintnek felel meg. Több szabvány, keretrendszer, ajánlás foglalkozik a témával. Jelen esetben a szerző az ISO 27001 szabvány [45] „A” mellékletét tekinti alapul.

5.3.1. Információbiztonsági politika

Anélkül, hogy a felsővezetés el ne kötelezné magát az információbiztonság mellett, gyakorlatilag esélytelen megfelelően működő rendszert kialakítani és fenntartani. Ennek módja egy kinyilatkoztatás, azaz az információbiztonsági politika publikálása. Ez a kulcs a szakemberek számára, amire hivatkozva kérhetnek erőforrást (emberi és anyagi) a költségvetésből. Emellett fontos, hogy elkészüljön egy kockázatelemzésre alapuló stratégia is, amely rövid, közép- és hosszú távú információbiztonsági célokat tartalmaz. Ezt leképezve, de még mindig magas szinten az információbiztonsági (esetleg vírusvédelmi, mobil eszköz használati stb.) szabályzat jelöli ki a vonatkozó követelményeket, az alkalmazandó kontrollokat és védelmi intézkedéseket. Részletesebben egy-egy folyamathoz tartozó konkrét lépéseket az eljárásrendek definiálnak. [46]

5.3.2. Az információbiztonság szervezete

A megfelelő feladat-, szerep- és felelősségi körök meghatározása nélkül nem lehetséges az információbiztonság működtetése. Nemcsak a szervezeten belüli együttműködés kialakítására van szükség, de a külső szakmai partnerekkel, hatóságokkal, egyéb szervezetekkel is fontos az információk folyamatos megosztása. Lényeges a különböző szintek kialakítása. Célszerű az információbiztonságot a felső vezetés közvetlen felügyelete alá vonni, így biztosítva egy-egy esetleges incidensre történő reagálás gyorsaságát. Érdemes elválasztani a különböző információbiztonsági területen dolgozó munkatársakat, és jól elkülönített munkaköröket, felelősségeket bízni rájuk. Egy nagyobb számú biztonsági csapatban a következő munkaköröket célszerű alkalmazni:

- Biztonsági vezető (CSO – Chief Security Officer)
- Információbiztossági vezető (CISO – Chief Information Security Officer)
- Tervező (architect)
- Mérnök (engineer)
- Tanácsadó (consultant)
- Elemző (analyst)
- Adminisztrátor

A felsorolt pozíciókon kívül érdemes lehet foglalkozni információgyűjtéssel, hírszerzéssel (intelligence), de más speciális szerepkörök (például folyamatgazdák, erőforrásgazdák) meghatározása is fontos lehet.

5.3.3. Az emberi erőforrások biztonsága

Onnantól kezdve, hogy a szervezettel kapcsolatba lép egy személy, a szervezet biztonságát szükséges szem előtt tartani. A kiválasztás folyamatát úgy kell meghatározni, hogy a lehető legkevésbé jelentsen a leendő munkatárs biztonsági kockázatot a vállalat számára. Különös elővigyázatosság szükséges a kritikus, bizalmas pozíciók betöltése előtt. A privátszektor számára kevés eszköz áll rendelkezésre az állásinterjúkon kívül. Indokolt esetben az erkölcsi bizonyítvány bekérése lehet egy olyan megoldás, mellyel szűrést tudnak alkalmazni. Az általános módszer – a közösségi médiában történő ilyen célú keresés – sem jogszerű az Általános Adatvédelmi Rendelet célhoz kötöttség elvének megfelelően. Ha a munkavállaló hozzáférhet nemzeti minősített adatokhoz, akkor a nemzetbiztonsági átvilágítás után ki kell állítani számára az ehhez szükséges tanúsítványt.

A munkavállalókra oda kell figyelni, nemcsak a felvételük előtt, de addig is, amíg a szervezetnél dolgoznak. Sok kárt okozhatnak az elégedetlen, bosszúvágytól fűtött belsős személyek. Az is fontos kockázati tényező, hogy átlagosan egy évi fizetésükkel az emberek könnyen korrumpálhatók. Ez az összeg rendelkezésére állhat egy támadónak. Azokon a helyeken, ahol nem megfelelő a fizetés vagy a cég iránti lojalitás, a támadó könnyűszerrel nyúlhat ilyen eszközökhöz. A munkavállalók tudatosságának képzése, figyelmének folyamatos fenntartása jelentősen növelheti a cég biztonsági szintjét. Az ilyen jellegű oktatásoknál, kampányoknál meg kell találni azt az optimumot, ahol kellő cégspecifikusság mellett érdekes, figyelemfelkeltő tudás adható át úgy, hogy a lehető legtöbb embernél meg is maradjon. Nem célszerű azonban túl sokszor terhelni ezzel a munkavállalókat, mert könnyen kontraproduktív lehet a folyamat.

Az emberi erőforrások biztonságát akkor is figyelembe kell venni, amikor az elbocsátási folyamatokat alakítja ki a szervezet. Mivel a legtöbb embert negatívan érinti, ha elbocsátják, ezért ebben az időszakban van a legnagyobb a kockázata annak, hogy még az utolsó pillanatban illetéktelenül eltulajdonítja a cég adatait. Ezért kell például megfelelő jogosultságkezelést és hozzá tartozó folyamatot kialakítani.

5.3.4. A vagyontárgyak biztonsága

A szervezet számára fontos lehet a vagyontárgyak kezelése. Érdemes leltárt vezetni a különböző eszközökről, melynek segítségével könnyen nyomon tudjuk követni, hogy melyik munkavállalónál milyen eszközök találhatók. Ezt érdemes aláírnia mind a két félnek, hogy az elszámoltatás ne lehessen vita tárgya. Külön figyelmet kell fordítani a hordozható adattárolókra. Célszerű kidolgozni a használat mellett a szállítás és főleg a selejtezés folyamatát. A nem megfelelő törlés alkalmazása mellett ugyanis számos adat maradhat az adott eszközön. Lopás esetén vagy ha valaki véletlenül elhagyja azt, könnyen hozzáférhetővé válnak olyan tartalmak, amelyek illetéktelenek kezébe kerülve kárt okozhatnak a szervezet számára. Megoldást jelenthet az adathordozók titkosítása, ahol viszont a jelszavak megfelelőségét kell kidolgozni. Azonban nem csupán materiális vagyontárgyak védelméről kell gondoskodni. Az adatvagyon biztonsága, karbantartása legalább ekkora jelentőséggel bír. A saját eszközök céges környezetben történő alkalmazására az úgynevezett BYOD (Bring-Your-Own-Device) megoldások jelenthetnek jó alternatívát.

5.3.5. A hozzáférés ellenőrzése

Nem csak az adathordozók hozzáférésének kezelését kell megoldani, hanem általánosságban véve minden informatikai rendszert és eszközt célszerű úgy védeni, hogy csak azok férhessenek hozzá, akik erre jogosultak. Beszélhetünk itt fizikai szeparálásról (például zárható iroda) vagy logikai jogosultságkezelésről. Ha nem mindenki férhet hozzá ezekhez, természetes, hogy engedélyt kell adnunk azok számára, akiknek korábban még nem volt (például az új munkavállalóknak). Az viszont sokszor nem természetes, hogy ha egy munkavállaló elmegy a cégtől, az ő jogosultságai megfelelően legyenek letiltva. Pláne nem jól működő folyamat sok helyen, ha a beszállítói oldalon történik változás a munkavállalók között. Egy szoftvergyártó partnernél elbocsájtott munkatárs könnyen tehet kárt, ha nincs megfelelően kezelve. Az ilyen eseteket célszerű a szerződésben kikötni, így károkozás esetén a beszállítót terheli egyértelműen a kár. Akkor megfelelő egy céges jogosultságkezelés, ha az alapjául szolgáló jogosultsági mátrix folyamatosan karban van tartva. A hálózatokhoz történő szabályozást az AAA valósítja meg, mely rövidítés az azonosítás (Authentication), a jogosultságkezelés (Authorization) és a felelősségre vonhatóság (Accountability) angol megfelelőinek kezdőbetűjéből áll. E három feltétel biztosítja, hogy megfelelően történjen a folyamat.

Az informatikai rendszerekhez történő hozzáférés azonosítására különböző módszerek vannak. Az azonosítást három kategóriába tudjuk sorolni, így három különböző faktort iktathatunk be a folyamatba. Az első faktor a tudás alapú azonosítás, mely azokat a kulcsokat foglalja magában, amelyek az agyunkban keletkeznek. Ilyen lehet például egy jelszó vagy egy PIN kód. Célszerű ezeket észben tartani és nem leírni. Ha mégis szükség lenne ezek rögzítésére, azt jól elkülönített, mások által nem hozzáférhető helyen kell tartani. Elektronikus megoldásként olyan jelszószéfeket célszerű használni, amelyek megfelelő kriptográfiával vannak ellátva. A második faktor a birtoklás alapú azonosítás. Ezek jellemzően olyan fizikai síkon megfogható eszközök, mint egy token vagy egy beléptető kártya. Ezek hátránya, hogy ellophatók, vagy akár figyelmetlenség miatt otthon is hagyhatók. Harmadik faktor a tulajdonság alapú azonosítás, amely valamilyen egyedi mintát használ a jogosultság megállapítására. Jellemzően ezek biometrikus adatokon, mint például ujjnyomaton, íriszmintán, erezetmintán alapulnak. A három faktort lehet, sőt ha van rá lehetőség, ajánlott kombinálni.

A hozzáférés biztonságát az RBAC (Role-based access control) keretrendszer alkalmazása is elősegítheti. Ebben az esetben különböző szerepekhez rendelődnek a rendszeradminisztrációs folyamatok. Például amíg az egyik felhasználó a fájlrendszert kezeli, addig egy másik a felhasználói fiókok létrehozását engedélyezi. Érdemes továbbá úgy kiosztani a jogosultságokat, hogy érvényesüljön a legkisebb hozzáférés elve, azaz mindenkihez csak a valóban szükséges jogok legyenek hozzárendelve. Így megelőzhető az esetleges szándékos vagy véletlen károkozás. A rendszer megfelelő működéséhez hasznos lehet a megfelelő összeférhetetlen jogkörök rendszerének kialakítása, így elkerülve a jogosultság halmozás problémáját.[13]

5.3.6. Kriptográfia

A kriptológia a titkosítás tudománya, amely az információ bizalmasságát, hitelességét, sértetlenségét biztosító algoritmusok és protokollok fejlesztésével foglalkozó kriptográfiából és az ezek megfejtését célzó kriptoanalízisből tevődik össze. Léteznek szimmetrikus és aszimmetrikus kulcsú titkosító eljárások. Az első esetben ugyanaz a kulcs hivatott mind az enkriptálásra, mind a dekriptálásra, míg a második típusnál publikus és privát kulcsokból álló kulcspárokon alapszik az algoritmus. [47] Az aszimmetrikus kulcsú titkosításon alapszik például a hitelességet és integritást garantáló digitális

[13] https://www.ibm.com/support/knowledgecenter/hu/ssw_aix_71/com.ibm.aix.security/rbac_elements_of.htm

aláírás. Ahhoz, hogy mind két fél meg tudjon bízni az algoritmusban, a kulcspárok generálását erre szakosodott tanúsító szervezetek (CA – Certificate Authority) állítják ki.

Az eszközök és a rendszerek biztonságos használatához minden esetben olyan algoritmusokat kell alkalmazni, amelyek minimum az adott korban elérhető számítási kapacitással belátható időn belül nem törhetők fel. Az elterjedt algoritmusokban előfordulhat, hogy sérülékenységet fedeznek fel. Ilyen esetekben, ha a szervezetnél használatban vannak, érdemes felülvizsgálni, hogy ezek miként válthatók ki. Jelenleg a matematikusok dolgoznak olyan kriptográfiai algoritmusokon, amelyek a kvantumszámítógép elterjedésével is kellő biztonságot nyújtanak a törési kísérletek ellen.

E témakörbe tartoznak a hash algoritmusok, amelyek alapja egy olyan függvény, melynek futtatása után egy lenyomat képződik, melyet az integritás ellenőrzésére lehet használni. Fő tulajdonsága, hogy bármilyen hosszú bitsorból mindig egy meghatározott hosszúságú bitsorozat képződik. Ezek az algoritmusok egyirányúak (könnyű lenyomatkészítés, nehéz visszafejtés), illetve általában – hash típustól függően – ellenállóak az ütközéssel (nehéz ugyanazt a lenyomatot két külön bitsorhoz rendelni).

5.3.7. Fizikai és környezeti biztonság

Az eszközök, a hálózat és minden más infrastruktúra védelmére szükséges kialakítani a fizikai biztonság fogalomkörébe tartozó különböző védelmi megoldásokat. Idetartozik a mechanikai védelem (például megfelelő minőségű vastagságú falak, rácsok stb.), az élőerős őrzésvédelem, illetve az elektronikus jelzőrendszerek (például CCTV, behatolásjelző, beléptető, járőrkövető, tűzjelző rendszerek) kialakítása az éppen hatályos jogszabályoknak, illetve más előírásoknak (például a MABISZ – Magyar Biztosítók Szövetsége). A fizikai beléptetési pontok védelme legalább annyira fontos, mint az IT, információbiztonság szempontjából kritikus területeké vagy a szállítási, rakodási tereké. Ezeket a helyeket biztosítani kell a környezeti fenyegetések ellen (például tűz, robbanás, elektromágneses behatások, árvíz, belvíz, rezgés, villám stb.), mint ahogy meg kell akadályozni, hogy mérgező, korrozív vagy nukleáris anyagok kerülhessenek az erre nem felkészített terekbe, helyiségekbe. A biztonságos munkavégzés feltételeinek kialakítása elengedhetetlen részét képezi az intézkedéseknek. Az informatikai munkát végzők számára főleg az érintésvédelem megfelelősége az elsődleges. Az objektum és a benne található személyek, eszközök számára szükséges közműszolgáltatások (például villamos energia, távközlés stb.) folyamatos biztosítására célszerű redundáns, tartalékellátást biztosító rendszereket kiépíteni. Bármelyik felsorolt kontrollt (eszközt) alakítják ki, az üzemszerű működéshez elengedhetetlen a folyamatos ellenőrzés és karbantartás.

5.3.8. Üzemeltetési biztonság

Ahhoz, hogy az üzleti folyamatok megfelelően működjenek, az azokat kiszolgáló egységek folyamatos működése szükséges. Azonban egy informatikai rendszer nem statikus. Ha másért nem, azért fog cserélődni az eszközpark, mert elhasználódik, vagy nem fog megfelelni az új számítási és munkaigényeknek. Az ad-hoc módon történő fejlesztés egy nagy rendszerben nem megengedhető. Az üzemeltetők emlékezete korlátos, ráadásul a fluktuáció miatt egyáltalán nem biztos, hogy az a munkavállaló lesz jelen egy változásnál, aki ott volt a telepítésnél. A különböző dokumentációk (telepítési, fejlesztési leírások, tesztelési tervek, jegyzőkönyvek), illetve a megfelelően kialakított folyamatok (például a változásmenedzsment, a kapacitásmenedzsment, a fejlesztési, a tesztelési és az üzemeltetési folyamatok szétválasztása) naprakész karbantartása lehet a legjobb védekezés. Az üzemeltetési biztonsághoz hozzátartozik a malware-ek elleni védelem, illetve a biztonsági mentés és a naplózás menedzselésének a tervezése, üzemeltetése. Ezeknél a folyamatoknál az optimum megtalálása a cél. Egy mindenre kiterjedő malware védelem irreálisan drága lehet, és valószínűleg kivitelezhetetlen is. Ha mindenről georedundáns biztonsági mentés készül, akkor az olyan nagy

tárhelyet igényel, melynek biztosítása valószínűleg nem oldható meg. A céltalan naplózás pedig azt eredményezheti, hogy hiába van meg a releváns esemény bejegyzése, a hatalmas adattömegben az nem fog az elemző számára szemet szúrni.

5.3.9. Kommunikációbiztonság

Manapság egy modern vállalat mindennapi működéséhez nélkülözhetetlen az elektronikus kommunikáció mind a munkavállalók, mind a hálózatba kötött eszközök között. A hálózati forgalom védelme érdekében jó megoldást nyújthat a különböző szegmensek megfelelő elválasztása. Érdemes az alhálózatainkat külön szervezni funkcionalitás és biztonsági szint szerint. Tovább növelhető a védelem, ha a megfelelő eszközöket (például tűzfalat, IDS/IPS-t, proxyt, application firewallt, SIEM-et stb.) telepítik. Ezek integrálása a rendszerbe azonban könnyen hamis biztonságiérzetet generálhat a vállalat menedzsmentje, de akár biztonsági szakemberei számára is. Sok esetben nem történik meg a telepítés után a leglényegesebb lépés, a testre szabás, illetve az alapértelmezett jelszavak megváltoztatása. Az eszközök alapértelmezett beállításainak, szabályainak alkalmazása olyan biztonsági résként működhet, amely egy hozzáértő támadó számára könnyű bejárást eredményezhet a rendszerbe.

Hasonló probléma a vezeték nélküli hálózati elemek védelme. Mivel alapvetően a kommunikáció sokkal könnyebben lehallgatható (például egy irányított antennával), mint a hagyományos vezetékes kapcsolaté, ezért a titkosításnak, szegmentációnak még nagyobb jelentősége van. Az üzleti kommunikáció alapját jelentő e-mail forgalom különböző szintű védelme (például titkosítás, elektronikus aláírással történő ellátás, spam szűrés, black és white list készítése stb.) elősegítheti az üzleti folyamat fenntartása és az információbiztonság szintjének növelését. Lényeges lehet mind a levelezésnél, mind a szóbeli és papíralapú kommunikációnál meghatározni, mi minősül üzleti titoknak, illetve érdemes meghatározni, hogy milyen körben terjeszthető (nyílt, korlátozottan terjeszthető, bizalmas, szigorúan bizalmas) az adott adathordozón szereplő információ.

A kommunikáció biztonságának növelését különböző megoldások bevezetésével, illetve bizonyos protokollok használatával tehetjük meg. A távoli munkamenet védelmét, illetve a vezeték nélküli hálózatok használatát a virtuális magánhálózatokkal (VPN) biztosíthatjuk. Ennek két fajtája van. Az első megoldásnál egy szolgáltató biztosítja a védett kapcsolatot. Ezt nevezzük trusted VPN-nek. A másik fajtája a secure VPN, ahol külső féltől függetlenül biztosítható a biztonságos kapcsolat. Védelmet nyújthat a lehallgatás ellen az IPSec csatorna vagy átviteli módjának használata, a PPTP (Point-to-Point Tunneling Protocol) és az L2TP (Layer 2 Tunneling Protocol) protokollok használata. A biztonságos internetes kommunikációhoz a jelenleg TLS-t (Trasport Layer Security) érdemes használni, melynek elődje az SSL (Secure Socket Layer). Az e-mailes kommunikáció előtt pedig érdemes lehet egy aszimmetrikus kulcsú titkosítás használata, melynek egyik formája a PGP, azaz Pretty Good Privacy. [48]

5.3.10. Az információs rendszerek beszerzése, fejlesztése és karbantartása

Bármilyen okból is történik változtatás egy adott rendszerben, célszerű előre gondolkodni. Minden esetben lényeges lehet, hogy az aktuális védelmi szintet a változtatás ne csökkentse. Tételezzük fel, hogy egy beszerzésnél ugyanolyan eszközt vásárolunk, amilyen az előző termék volt. Típusra, gyártmányra megegyezőt. A probléma az, hogy ettől még az új eszköz bármikor meghibásodhat. Ha az adott beszállítóval kötött szerződésben nincs meghatározva, hogy mennyi időn belül köteles javítani, pótolni az így kiesett eszközt, akár fontos üzleti folyamatok is kárt szenvedhetnek. Igaz lehet ez egyedi gyártású szoftver esetén is. Bármikor előfordulhat, hogy a használat során egy korábban fel nem fedezett hiba miatt működésképtelenné válik a program. Ezeket a lépéseket célszerű alkalmazni új hardver vagy szoftver beszerzésénél vagy azok fejlesztésénél. Érdemes lehet karbantartási szerződést

is kötni, még az esetleges plusz költségek ellenére is, mivel a ráfordítás közvetve vagy közvetlenül valószínűleg meg fog térülni.

Szükség lehet bizonyos esetekben a különböző vállalatok számára egyedi kontrollok kifejlesztése, bevezetése, megkövetelése, melyek segítségével saját infrastruktúrájuk védelmét tudják magasabb szintre emelni.

5.3.11. Beszállítói kapcsolatok

A beszállítókkal történő együttműködés felügyelete nem csak abban merül ki, hogy próbáljuk megvizsgálni, hogy megbízható személyeket engedjünk a cég közelébe, illetve hogy szerződésben rögzítjük, mennyi időn belül cseréljenek ki egy meghibásodott eszközt, amit ők illesztettek be a rendszerünkbe. Ezeket nevezzük a szerződésekben szolgáltatási szinteknek, SLA-knak (Service Level Agreement). De ugyanannyira fontos minden velük kapcsolatos folyamatot kidolgozni és be is tartatni, mint a szervezet saját munkavállalói esetében. Lényeges, hogy a különböző változások megfelelően legyenek menedzselve, hogy kellő mértékben kontrolláljuk, monitorozzuk az ő munkájukat. Erre nyújthatnak megoldást a különböző hatékonyan meghatározott teljesítménymutatók (KPI-ok – Key Performance Indicators). Ezekkel a mérhető értékekkel lehet mérni a beszállítói hatékonyságot. (Hasonlóképp, léteznek KPI-ok a munkavállalók teljesítményének mérésére.)

5.3.12. Az információbiztonsági incidensek kezelése

Ahhoz, hogy incidensmenedzsmentről lehessen beszélni az információbiztonság szempontjából, az adott vállalatnak meg kell határoznia, hogy mit tekint incidensnek. Alapvetően arról van szó, hogy valamilyen, a normálistól eltérő esemény történik, mely potenciálisan fenyegetést hordoz magában. Ez hatással lehet az üzletmenet folyamatosságára vagy az informatikai, illetve információs rendszerek üzemszerű működésére. A következő lépés, hogy meg legyen határozva, az adott ellenintézkedés kinek a felelőssége. Egyértelműeknek kell lenniük azoknak az eljárásrendeknek, amelyeket az adott pillanatban követni kell. Miután valamilyen sikerességgel reagáltak az illetékesek az adott problémára, szükséges az eset kommunikálása a vezetőség felé. Ez után döntést kell hozni, hogy miként történjen meg a kármentesítés, illetve adott esetben a bizonyítékok begyűjtése. Egy szervezetben az információbiztonság akkor tud a legjobban fejlődni, ha képes a hibáiból tanulni és változtatni. Az incidensekből le kell vonni a következtetéseket, tanulságokat, és fel kell használni azokat a védelem megerősítésére.

5.3.13. Üzletmenet-folytonosság menedzsment (információbiztonsági aspektusa)

A különböző kontrollok bevezetése és úgy általában a biztonság, így a kiberbiztonság sem öncélú tevékenység. Ezek a beruházások mind azért kellenek, hogy a digitalizált világban üzemelő infrastruktúrák, melyek a pénzszerző fő tevékenységeket szolgálják, védve legyenek. Ezért szükséges, hogy a felsővezetés kötelezze el magát a biztonság megteremtése mellett. Szükséges megmutatni, hogy mely üzleti folyamatok kiesése mekkora veszteséget jelenthet a szervezetre nézve, és a legkritikusabb esetekre előre fel kell készülni. Ennek egyik módja az üzletmenet-folytonossági terv (Business Continuity Plan, BCP) elkészítése. Ez olyan lépéseknek az egymásutániságát foglalja magában, melyeket követve egy adott incidens megtörténése esetén a lehető legkisebb kár éri a vállalatot. A katasztrófa-helyreállítási tervben (Disaster Recovery Plan, DRP) pedig olyan folyamatokat rögzítenek, amelyeket végrehajtva minél hamarabb visszaállítható a normál üzem. Célszerű minél több esetre felkészülni, de hiába van számtalan BCP-nk vagy DRP-nk, ha soha senki nem próbálta ki, hogy valóban lehetséges-e velük elérni a céljukat. Nagyon fontos, hogy tesztelve legyenek a lépések, és ha szükséges, újra kell gondolni azokat.

5.3.14. Megfelelőség

Utolsó pontként az ISO 27001 A melléklete a megfelelőségre tér ki. Ez vonatkozik a különböző jogszabályokra, önkéntesen vagy szükségszerűen vállalt szabványokra, de ugyanúgy a szerződésekre is, melyeket a szervezet valamilyen más természetes vagy jogi személyiséggel kötött. [49] Érdemes lefedni nemcsak a vállalatok jogi kötelezettségeit, de valamilyen sérülékenység- vagy behatolás-vizsgálattal a technikai, műszaki megfelelést is ellenőrizni. Az ezekre vonatkozó vizsgálatokat egy szervezet a fejlődése szempontból önmaga is elvégezhet, azonban a gyakorlatban külső, független fél ellenőrzése a mérvadó és elfogadott.

5.4. A felismerés szerepe a védelemben

Egy kellő mértékben kialakított védelmi struktúra az, amelyben a különböző védelmi rendszerelemek és jól átgondolt biztonsági folyamatok mentén tevékenykedő szakemberek folyamatos kontroll alatt tudják tartani a rendszert. Ha ezek adottak, lehetséges bizonyos jelek alapján detektálni egyes támadásokat. A biztonságban az idő nagyon fontos tényező. Ezért alakítanak ki egyre több helyen helyileg vagy vesznek igénybe szolgáltatásként Security Operation Centereket (SOC), ahol folyamatos monitorozás mellett igyekeznek a lehető legrövidebb időn belül észlelni az offenzív tevékenységet.

Egy jól kialakított incidensmenedzsmenttel azok a maradványkockázatok, amelyeket a biztonsági rendszer kialakításánál a cég vezetése felvállalt, kellő mértékben kezelhetők. Egy-egy korrektív intézkedés meghozatala egy gyanús szituációban megmentheti a vállalatot a károkozástól.

6. A behatolások felismerésének módszerei

A behatolás felismerésére több különböző eszköz segítségével van lehetőség: Elsősorban a védelmi eszközök monitorozásával, a logok elemzésével, illetve utólagosan különböző forensic módszerekkel. A reagálás minden esetben azon múlik, hogy az adott eszköz milyen módon van bevéve az incidensmenedzsmentbe. Lehet bármilyen jó megoldás egy szervezetnél, ha senki nem figyeli, akkor semmit sem ér. A modern védelmi megoldások kialakításánál már az úgynevezett rétegzett struktúrát érdemes követni, melynek egyik módszere lehet a fuzzy logikán alapuló módszerek. [50]

6.1. Hálózat- és host alapú behatolás elleni védelmi megoldások

Alapvetően kétféle módon lehet védekezni a különböző támadások ellen. Egyrészt a különböző hálózatok felől érkező támadásokat kell megakadályozni, másrészt arról kell gondoskodni, hogy ha a támadó közel kerül az infrastruktúrához, akkor ott legyen lehetősége kárt okozni.

6.1.1. Hálózati alapok

A hálózat felől érkező támadások egy jelentős részére van megfelelő védelem, azonban ezek ismertetése előtt szükséges áttekinteni, hogy milyen nemzetközi szervezetek foglalkoznak a különböző hálózatok szabványosításával, illetve egy hálózat miként is épül fel. [51] A szabványosítással az alábbi szervezetek foglalkoznak:

- ANSI (American National Standards Institute – Amerikai Nemzeti Szabványügyi Intézet)
- ETSI (European Telecommunications Standards Institute – Európai Távközlési Szabványügyi Intézet)
- IEEE (Institute of Electrical and Electronics Engineers – villamosmérnököket és informatikusokat egyesítő szervezet)
- IETF (Internet Engineering Task Force – az internet fejlesztésének szervezete)
- ISO (International Organization for Standardization – Nemzetközi Szabványügyi Szervezet)
- ITU (International Telecommunication Union – Nemzetközi Távközlési Egyesület)

A hálózatokon különböző protokollok alkalmazásával történik az adatcsere. A nagy bonyolultságú hálózati forgalmat célszerű különböző rétegekbe szervezni, melyre a leginkább elterjedt a hét rétegből álló OSI (Open System Interconnect) és a négyrétegű TCP/IP modell. E kettőt általában egymás mellett szokták szerepeltetni, mivel egymásnak megfeleltethetők.

OSI modell	TCP/IP modell
Alkalmazás réteg (7)	Alkalmazás réteg (4)
Megjelenítési réteg (6)	
Viszony réteg (5)	
Szállítási réteg (4)	Átviteli réteg (3)
Hálózati réteg (3)	Internet réteg (2)
Adatkapcsolati réteg (2)	Hálózati hozzáférési réteg (1)
Fizikai réteg (1)	

A hálózati kommunikáció felépülése az OSI modell szerint a fizikai réteggel kezdődik, ahol bit szinten történik a binárisok átvitele. Ez után következik az adatkapcsolati rétegben a fizikai címzés (jellemzően MAC címek), majd a hálózati rétegben a logikai címzés (IP címek). A végpontok közötti kapcsolatot (a

portok segítségével) a szállítási réteg, míg a csomópontok között a viszony réteg biztosítja. A végső alkalmazási réteg előtt a megjelenítési rétegben történik az adatok kódolása, dekódolása.

A következő táblázat [52] összefoglalja, hogy az OSI modell egyes szintjein milyen ismertebb protokollok léteznek, és milyen gyakori támadások vannak ellenük:

A különböző szinteket más és más hálózati eszköz tudja biztosítani. Az OSI modell első rétegében az ismétlők (repeater) és ezek több portos változatai (hub) működnek. A következő szintet, az adatkapcsolati réteget a hidak (bridge) és a kapcsolók (switch) szolgálják ki. A harmadik rétegben az útválasztók (router) és az e szintnek megfelelő kapcsolók (layer 3 switch) találhatók. A felsőbb rétegekben már nem találunk külön eszközöket, ezeket már az alkalmazások kezelik.

OSI modell	Ismertebb protokollok	Gyakori támadások
Alkalmazás réteg (7)	DNS, DHCP, HTTP, FTP, IMAP, IRC, LDAP, NTP, POP3, Radius, SSH, SMTP, SNMP, SCP, SFTP, HTTPS, Telnet, TFTP	DNS mérgezés, Adathalászat, befecskendezéses támadások, Spam/Scam
Megjelenítési réteg (6)	SSL, TLS (kommunikáció)	SSL MItM, SSL DOS, SMB támadás
Viszony réteg (5)	SMB, NFS, Socks, SSL, TLS (kézfogás)	session eltérítés, L2TP támadás, SIP támadás
Szállítási réteg (4)	TCP, UDP, DCCP, SCTP, RSVP	TCP támadások, Útválasztó támadások, SYN flood, Lehallgatás
Hálózati réteg (3)	IP (IPv4, IPv6), ICMP (ICMPv6), IGMP, IPSec, GGP, OSPF, RIP	Ping/ICMP Flood
Adatkapcsolati réteg (2)	PPP, PPTP, Token Ring, Wifi, Ethernet, ATM, X.25, ARP	ARP spoofing, MAC flooding, VLAN hopping, DHCP támadások, Hamisításos (spoofing) támadások, Lehallgatás
Fizikai réteg (1)	RJ45, BNC	kábel elvágása, networktap, signaljammer

6.1.2. Védelmi eszközök

A különböző hálózati szinteken különböző megoldásokat érdemes és szükséges alkalmazni. Az internet felől az első védelmi vonalat egy olyan hálózati szeparáció jelentheti, ahol a nem biztonságos szolgáltatásokat helyezzük ki. Ezt nevezzük demilitarizált zónának, azaz DMZ-nek. Ennek kompromittálódása esetén a támadó még nem férhet hozzá a belső hálózathoz. A következő védvonalat a különböző hálózati tűzfalak (firewall) jelentik, amelyek valamilyen szabályrendszer szerint engedik át a kommunikációs csomagokat. Működésüket tekintve több különböző típussal lehet találkozni. Léteznek állapotmentes csomagszűrő tűzfalak (stateless packet filtering), állapotmegőrző tűzfalak (stateful packet filtering), proxy tűzfalak, dinamikus csomagszűrő tűzfalak (dynamic packet filtering) és kernel proxyk.

A támadások elleni újabb biztonsági eszköz lehet egy mézescsupor, azaz honeypot, amelyből többet egyszerre használva honeynetről beszélünk. Ennek az a lényege, hogy a hálózat egy külső szegmensében elhelyezve odacsalogatja a támadót, hogy az ne a valós rendszert kezdje el feltörni. Mivel ez a támadás felismerésének eszköze elsősorban, ennek a védekezési formának akkor van főleg értelme, ha a defenzív oldalon a jelzést érdemben le is tudják kezelni. Tovább nehezíthetjük a támadó a dolgát a hálózati csomagok késleltetésével. Ennek a technikának az eszközét tarpitnak nevezzük.

A behatolások felismerésére készültek el a különböző erre specializálódott jelzőrendszerek, az IDS-ek (Intrusion Detection System). Léteznek olyan változatai, melyek egy adott eszközön vizsgálják a

rendellenes tevékenységet, ezeket nevezzük HIDS-nek (Host-based Intrusion Detection System). A hálózatalapú NIDS (Network-based Intrusion Detection System) pedig a hálózati forgalomban keres anomáliákat a különböző előre megadott minták, szignatúrák vagy viselkedés alapján. Célszerűbb azonban – szakmai meggyőződéstől függően – egy IPS (Intrusion Protection System) használata, mely nemcsak figyelmeztet, de be is avatkozik bizonyos esetekben. Ennek az eszköznek az alkalmazásánál azonban kiemelten fontos, hogy megfelelő szakértelemmel legyen telepítve, üzemeltetve és folyamatosan ellenőrizve, mivel könnyen nem várt hibákat generálhat. Az IDS-ek és IPS-ek (illetve más hálózati eszközök) logjainak kezelésére, elemzésére szolgálnak az úgynevezett SIEM (Security information and Event Management) rendszerek. Ezek megfelelő, előre beállított módon értékelik a beérkező naplóállományokat, amelyekből különböző szinten lévő munkavállalóknak (például vezetőség, elemző stb.) tudnak igény szerint kimutatásokat készíteni.

A felsorolt megoldásokon kívül léteznek más védelmi eszközök is, mint például az elszeparált környezetet biztosító sandbox környezetek, az elektronikus levelezést biztonságosabbá tévő spam (levélszemét) szűrők vagy a túlterheléses támadások (DoS/DDoS) detektálását végző eszközök. A malware-ek, kémprogramok ellen Anti-malware, Anti-spyware, Antivirus stb. programok lehetnek hasznosak. A megfelelő frissítések kezelésére alkalmasak a patch managerek, a webalkalmazások szűrésére pedig az alkalmazás-tűzfalak (WAF – Web Application Firewalls). Ha az adatszivárgás ellen szükséges védekezni, a DLP (Data Loss Prevention) eszközök nyújthatnak megfelelő védelmet, míg lopás ellen az Anti-theft alkalmazásokkal biztosíthatjuk a magasabb szintű biztonságot.

Bármely megoldást is vezetik be, a legfontosabb, hogy az egy adott célt szolgáljon, ne csak a bevezetés, de a tervezés során is. Végig kell gondolni, hogy a hálózaton belül hogyan helyezzük el a különböző védelmi pontokat. Más funkcióval bír egy külső tűzfal, mint egy belső. Meg kell vizsgálni, hogy miként védekezzünk a titkosított adatforgalmon keresztül érkező támadásokkal szemben, illetve miként kezeljük az egyes rendszerek által adott fals pozitív, negatív jelzéseket. De arra is érdemes odafigyelni, hogy a csatlakoztatható eszközök segítségével terjedő kártékony kódok ellen a tűzfalak nem megfelelőek. A belülről érkező emberi károkozás ellen pedig teljesen más megközelítés szükséges. Nincs általánosan jó megoldás. Minden esetben a hálózattól és a rendszertől függően külön kell megtervezni a biztonságot a ráfordítható (emberi és anyagi) erőforrások figyelembevételében.

Érdemes lehet azon is elgondolkodni, hogy a biztonságot mint szolgáltatást vegye igénybe egy vállalat. Vannak kifejezetten tanácsadó cégek, akik segítenek a különböző aspektusokban, de akár folyamatos felügyeletet is nyújtanak a kiépített SOC-okban. Mivel a szakmában folyamatos a jó szakemberek hiánya, így relatíve magas azok fizetési aránya. Ezért nem biztos, hogy állandó jelleggel kell egész csapatot fenntartani, azonban minden esetben egy felelős személy ki kell hogy legyen jelölve.

6.2. Egyéb felismerési módszerek

A védelmi eszközökön kívül számos olyan mód van, melyeket alkalmazva nincs szükség feltétlen külön eszközökre. Érdemes lehet odafigyelni az árulkodó jelekre. Egy letöltéskor például hatásos lehet a fájl hash-ének ellenőrzése, vagy ha a szokásostól eltérőt tevékenységet észlelünk egy rendszerben, akkor is élhetünk a gyanúperrel, hogy nincs minden rendben. Már a 2000-es évek elején is felhívták a figyelmet [53] arra, hogy milyen jelek utalhatnak egy malware jelenlétére. Ezek jellemzően a mai napig érvényes szabályok, melyek észlelésénél érdemes rendszergazdához, IT biztonsági szakemberhez fordulni:

- A korábban megszokott memória hirtelen nem lesz elegendő, jelentős lassulás látszódik egy program futtatásánál.
- Megmagyarázhatatlan módon elfogy a korábban szabad lemezterület.

- Váratlan programhibák lépnek fel a különböző, korábban használt, jól működő alkalmazások futtatása közben.
- Lelassul vagy leáll az adott program.
- A monitoron szokatlan ábrák, szövegek, üzenetek jelennek meg.
- Szokatlan médiatartalmak indokolatlan lejátszása.
- Szándékunktól független módon bizonyos tartalmak (fájlok, mappák stb.) elérhetetlenné válnak.
- Szándékunktól független módon új tartalmak (fájlok, mappák stb.) jelennek meg.
- Váratlan újraindulások tapasztalhatók.
- Váratlan növekedés a levélforgalomban.
- Illetve természetesen, ha az eszközön futó védelmi szoftver, például Anti-malware program jelez, hogy kártékony tartalmat talált.

6.3. A hatályos jogszabályok alapján kötelezően kialakítandó védelmek

A hatályos jogszabályok különböző formában kívánják szabályozni a kiberbiztonsági teret. [54] Először a legmagasabb szinten érdemes megvizsgálni Magyarországra vonatkozóan az Európai Unió törekvéseit. [55] Az Európai tanács 2003-ban elfogadta az *Európai biztonsági stratégia – Biztonságos Európa egy jobb világban* című dokumentumot, ahol megnevezték a kiberbiztonság növelésének szándékát mint potenciális fenyegetés elleni védelem. Ezt a stratégiát 2008-ban felülvizsgálták,[14] mely fő változtatásként a témával kapcsolatban a kritikus infrastruktúrák és azok informatikai rendszereinek védelmét nevesítette, melyet 2009-ben meg is erőstett egy közleménnyel.[15] Itt meghatározták az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (a továbbiakban: ENISA) hatókörének kiterjesztése, illetve az Európa szintű reagálóképesség növelése. 2010-ben az Europa 2020 Stratégia[16] megalkotásával a döntéshozók növelni kívánták a digitális eszközök és technológiák ismertségének szélesítését a polgárok számára, az adatvédelem megerősítését és az internetes biztonság növelését. E stratégiának köszönhetően 2012-ben kiadták *A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé* az Európai Parlament állásfoglalása, melyben meghatározták az eseménykezelő központok (CERT-ek) [56] együttműködési kötelezettségei. 2013-ban *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* című Európai Unió stratégiában fő helyet kapott a defenzív képességek növelése, a kiberbűnözés elleni intézkedések erősítése, egy EU-s kibervédelmi politika kidolgozása, a szükséges erőforrások allokálása, előteremtése. 2017-ben Jean-Claude Juncker, az Európai Bizottság elnöke ezekre reagálva egy új stratégiai szintű változtatás szükségességét jelentett be.

Az Europa 2020 program elvei és irányai mentén Magyarországon is leképződött 4 irány (Digitális infrastruktúra, Digitális kompetenciák, Digitális gazdaság és Digitális állam) mentén a stratégiai gondolkozás. A megvalósítás érdekében először a 1631/2014. (XI. 6.) Kormány határozat[17] mentén létrejött a Digitális Nemzet Fejlesztési Program, amit a jelenleg is tartó, 2012/2015. (XII. 29.) Kormány határozat[18] alapján kialakított Digitális Jólét Program követett.

Az adat és információbiztonsági törekvések európai uniós új irányzatának két, 2016-ban elfogadott, korszakalkotó jelentőségű rendelete az Általános Adatvédelmi Rendelet (GDPR – General Data

[14] http://www.consilium.europa.eu/media/30811/qc7809568huc.pdf
[15] http://ec.europa.eu/transparency/regdoc/rep/1/2009/HU/1-2009-149-HU-F1-1.Pdf
[16] http://ec.europa.eu/eu2020/pdf/1_HU_ACT_part1_v1.pdf
[17] https://hirlevel.egov.hu/2014/11/08/a-kormany-16312014-xi-6-korm-hatarozata-a-digitalis-nemzet-fejlesztesi-program-megvalositasarol/
[18] https://net.jogtar.hu/jogszabaly?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT

Protection Regulation),[19] illetve a hálózat- és információbiztonságot szabályzó NIS (Network and Information Security) direktíva.[20] Míg az első főleg a személyes adatok európai szintű kezelésének kialakítását szolgálja, addig a NIS irányelvek a biztonsági minimumok előírásával a nemzeti szabályok közös nevezőre hozását irányozzák elő. [57]

Jelenleg a következő hatályos jogszabályok kapcsolódnak az információbiztonsághoz, illetve a különböző rendszerekbe történő behatoláshoz:

Jogszabály neve	**Internetes elérhetősége**
Hazai hatályos jogszabályok	
65/2013. (III. 8.) Korm. rendelet A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról	https://net.jogtar.hu/jogszabaly?docid=A1300065.KOR
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról	http://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf
2013. évi L. (IV. 15.) törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról	https://net.jogtar.hu/jogszabaly?docid=A1300050.TV
233/2013. (VI. 30.) Korm. rendelet Az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről	https://net.jogtar.hu/jogszabaly?docid=a1300233.kor&getdoc=1
187/2015. (VII. 13.) Korm. rendelet Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról	https://net.jogtar.hu/jogszabaly?docid=A1500187.KOR
A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény	https://net.jogtar.hu/jogszabaly?docid=A1100128.TV
Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól 2015. évi CCXXII. törvény	https://net.jogtar.hu/jogszabaly?docid=A1500222.TV
A nemzeti adatvagyon körébe tartozó állami nyilvántartások védelméről szóló 2010. évi CLVII. törvény	https://net.jogtar.hu/jogszabaly?docid=A1000157.TV
38/2011. (III. 22.) Korm. Rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról	https://net.jogtar.hu/jogszabaly?docid=A1100038.KOR
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről	https://net.jogtar.hu/jogszabaly?docid=A1200166.TV
Európai uniós szabályozások, szerződések	
Zöld Könyv a kritikus infrastruktúra védelemről	https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52005DC0576

[19] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

Kritikus Információs Infrastruktúra Védelme (COM(2009)149)	https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:52009DC0149
Convention on Cybercrime. CETS No.: 185, Számítástechnikai Bűnözésről Szóló Egyezmény	https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról	https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32004R0460
Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA)	https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32013R0526
Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió Kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér, 2013	https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52014JC0012
Az Európai Parlament és a Tanács 2013/40/EU Irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról	https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32013L0040
Az Európai Parlament és Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről	https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN
Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)	https://eur-lex.europa.eu/legal-content/HU/TXT/ELI/?eliuri=eli:reg:2016:679:oj

7. Összegzés

Általánosságban kijelenthető, hogy a kiberbiztonság témaköre igen összetett. A különböző védelmi szintek tervezése, bevezetése és működtetése egyáltalán nem triviális művelet. Számos környezeti körülményt kell figyelembe venni a különböző kontrollok bevezetésénél. Törekedni kell a kockázatarányosságra, hiszen a véletlenszerű intézkedések nem hozzák meg a megtérülést, amelyet az üzleti oldal támaszt. Meg kell találni azt az optimumot, ahol a különböző támadási formák ellen még hatékony a védelem, de a ráköltött összeg arányban van a cég érettségi szintjével, illetve támadási potenciáljával. A támadó és védekező oldal folyamatos versenyében az offenzív oldal mindig lépéselőnyben lesz, hiszen számára az idő nem a legfontosabb szempont. Ezzel szemben a biztonsági szakemberek által úgy kell kialakítani a folyamatokat, illetve bevezetni védelmi megoldásokat, hogy a lehető leggyorsabban tudják észlelni az incidensgyanús eseményeket, és azokra reagálni is tudjanak. Általában a biztonságra igaz, hogy nem statikus állapot, hanem dinamikus, folyamatosan fejlesztendő terület. Ez az állítás hatványozottan igaz a jelenleg rohamosan fejlődő digitális világ veszélyei ellen megoldást nyújtani kívánó kiberbiztonságra.

Irodalomjegyzék

[1] Spafford, Eugene H.: *The Internet Worm Program: An analysis.* Purdue Technical Report, CSD-TR-823. 1988. https://spaf.cerias.purdue.edu/tech-reps/823.pdf (2018. 11. 10.)

[2] Szőr Péter: *A vírusvédelem művészete.* SZAK Kiadó, Bicske, 2010, pp. 376–378.

[3] Szőr Péter: *A vírusvédelem művészete.* SZAK Kiadó, Bicske, 2010, p. 351.

[4] Hambrick, David Z. – Marquardt, Madeline: *Cognitive Ability and Vulnerability to Fake News.* 2018. Scientific America 2018. 02. 06. https://www.scientificamerican.com/article/cognitive-ability-and-vulnerability-to-fake-news/ (2018. 11. 10.)

[5] Krasznay Csaba (2012): *A polgárok védelme egy kiberkonfliktusban.* Hadmérnök VII. évfolyam, 2012, 4. szám, pp. 143–144. http://hadmernok.hu/2012_4_krasznay.pdf (2018. 11. 10.)

[6] ThreatMetrix: *Q1 2018 Cybercrime Report.* https://www.threatmetrix.com/wp-content/uploads/2018/05/q1-2018-cybercrime-report-1526659517.pdf (2018. 11. 10.)

[7] Malwarebytes Labs: *Cybercrime tactics and techniques: Q2 2018.* https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf (2018. 11. 10.)

[8] Bányász Péter: *Kiberbűnözés és közösségi média.* Nemzetbiztonsági Szemle, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, 2017/4. pp. 55–74. https://www.uni-nke.hu/document/uni-nke-hu/nemzetbiztonsagi-szemle-2017-4-szam.pdf (2018. 11. 10.)

[9] Zerzri, Mayssa: *The threat of cyber terrorism and recommendations for countermeasures.* Center for Applied Policy Research Tunisia. 2017. pp. 2–3. https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf (2018. 11. 10.)

[10] Vida Csaba: *A hírszerzés szerepe, jelentősége, az információgyűjtés fajtái és formái.* In: Kobolka István (szerk.): Nemzetbiztonsági alapismeretek. Nemzeti Közszolgálati Egyetem, Budapest, 2013, pp. 102–105.

[11] Berki Gábor: *Kiberháborúk, kiberkonfliktusok.* http://real.mtak.hu/80322/1/246_kiberhaboru16182.pdf (2018. 11. 10.)

[12] Kovács Zoltán: *Védett vezetők hordozható infokommunikációs eszközeinek védelme a rádiófrekvenciás tartományban.* Bolyai Szemle, XXIII. évfolyam, 4. szám Budapest, 2014, p. 63.

[13] Haig Zsolt – Várhegyi István: *Hadviselés az információs hadszíntéren.* Zrínyi Kiadó, Budapest, 2005, p. 198.

[14] Lattmann Tamás: *A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén.* https://www.academia.edu/8028014/A_nemzetközi_jog_lehetséges_szerepe_az_informatikai_hadviselés_területén (2018. 11. 10.)

[15] Molnár Dóra: *Egységes európai kibertér? Az Európai Unió Kiberbiztonsági Politikájának fejlődése.* Hadmérnök, 2017/1. http://hadmernok.hu/171_20_molnar2.pdf (2018. 11. 10.)

[16] Lattmann Tamás: *A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén.* https://www.academia.edu/8028014/A_nemzetközi_jog_lehetséges_szerepe_az_informatikai_hadviselés_területén (2018. 11. 10.)

[17] Shakarian, Paulo – Shakarian, Jana – Ruef, Andrew: *Introduction to Cyber-Warfare.* Elsevier Inc. Waltham, 2013, pp. 223–239.

[18] Mattei, Tobias A.: *Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack.* World Neurosurgery 2017/8, pp. 972–974. https://www.sciencedirect.com/science/article/pii/S1878875017309968 (2018. 11. 10.)

[19] Mattei, Tobias A.: *Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack.* World Neurosurgery 2017/8, pp. 972–974. https://www.sciencedirect.com/science/article/pii/S1878875017309968 (2018. 11. 10.)

[20] Oriyano, Sean-Philip: *CEHv9: Certified Ethical Hacker Version 9 Study Guide; Figure 1.2.* Joh Wiley & Sons Inc., Indianapolis, 2016.

[21] Kiss Dávid – Váczi Dániel: *A vállalatok és a kritikus infrastruktúrák humánhálózata ellen irányuló támadások veszélyei a komplex hálózatok elemélete alapján.* Hadmérnök, 2018/1, pp. 151–168. http://real.mtak.hu/77916/1/HT20181_153_170_u.pdf (2018. 11. 10.)

[22] Solon, Olivia – Siddiqui, Sabrina: *Russia-backed Facebook posts 'reached 126m Americans' during US elecition.* The Guardian, 2017. 10. 31. https://www.theguardian.com/tech-nology/2017/oct/30/facebook-russia-fake-accounts-126-million (2018. 11. 10.)

[23] Fehér Katalin – Király Olívia: *Álhíresülés – a hamis hírek dinamikája a médiában.* Századvég, 2017/2, p. 44. https://szazadveg.hu/uploads/media/59888870e25b0/szazadveg-84-alhirek-201708.pdf (2018. 11. 10.)

[24] JAR-16-20296. *Grizzly Steppe – Russian Malicious Cyber Activity.* US Department of Homeland Security and Federal Bureau of Investigation [online] 2016. 12. 16. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (2018. 11. 10.)

[25] Klausz Melinda: *Megosztok, tehát vagyok.* Antheneum Kiadó, Budapest, 2017.

[26] Hadnagy, Cristopher: *Social Engineering – The Art of Human Hacking.* Wiley Publishing, Indianapolis, 2011, p. 10. – fordította: Sörös Tamás, Váczi Dániel

[27] Mitnick, Kevin D.: *A legendás hacker – A megtévesztés művészete.* Előszó. Perfact-Pro, Budapest, 2003.

[28] Hadnagy, Cristopher: *Social Engineering – The Art of Human Hacking.* Wiley Publishing, Indianapolis, 2011, p. 162–172.

[29] Szőr Péter: *A vírusvédelem művészete.* SZAK Kiadó, Bicske, 2010, pp. 4–5.

[30] Szőr Péter: *A vírusvédelem művészete.* SZAK Kiadó, Bicske, 2010, pp. 25–34.

[31] Váczi Dániel: *Célzott támadások módszertana.* Célzott kibertámadások. Nemzeti Közszolgálati Egyetem, Budapest, 2018, pp. 66–67.

[32] Dreilinger Tímea: *Vírusvédelem.* Panem Könyvkiadó, Budapest, 2004, pp. 19–23.

[33] Dreilinger Tímea: *Vírusvédelem.* Panem Könyvkiadó, Budapest, 2004, pp. 25–29.

[34] Kenny, Steven: *Strengthening the network security supply chain.* Computer Fraud & Security, 2017/12, pp. 11–14. https://www.researchgate.net/publication/321846131_Strengthening_the_network_security_supply_chain (2018. 11. 10.)

[35] Viktor Mayer-Schönberger, Kenneth Cukier (2014): Big Data, HVG Kiadó Budapest

[36] Fehér Krisztián: *Kezdő hackerek kézikönyve.* BBS-INFO Kiadó, Budapest, 2016, pp. 202–204.

[37] Fehér Krisztián: *Kezdő hackerek kézikönyve.* BBS-INFO Kiadó, Budapest, 2016, pp. 178–184.

[38] Fehér Krisztián: *Kezdő hackerek kézikönyve.* BBS-INFO Kiadó, Budapest, 2016, pp. 184–192.

[39] Fehér Krisztián: *Kezdő hackerek kézikönyve.* BBS-INFO Kiadó, Budapest, 2016, pp. 192–202.

[40] Fehér Krisztián: *Kezdő hackerek kézikönyve.* BBS-INFO Kiadó, Budapest, 2016, pp. 163–165.

[41] Fehér Krisztián: *Kezdő hackerek kézikönyve.* BBS-INFO Kiadó, Budapest, 2016, p. 205.

[42] Gregory, Peter: *CISSP Guide to Security Essentials.* pp. 55–61. https://books.google.hu/books?id=IRp-mgJVy40C&pg=PA56&lpg=PA56&dq=cissp+controls&source=bl&ots=B4GwBSxgGq&sig=dNluyljdIjQLY-RzIkwxrThXRT4&hl=de&sa=X&ved=2ahUKEwjJv8yB3tTeAhXSLlAKHTDFAbM4ChDoATAFegQIABAB#v=onepage&q=cissp%20controls&f=false (2018. 11. 10.)

[43] Check Point: *Stepping Up to Gen V (5th Generation) of Cyber Security.* 2018. https://www.checkpoint.com/downloads/product-related/brochure/gen_v_brochure-.pdf (2018. 11. 10.)

[44] Europol: *The Internet Organised Crime Threat Assesment 2016.* Europol, Hága, 2016. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (2018. 11. 30.)

[45] MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági-Irányítási Rendszerek. Követelmények.

[46] Oroszi Eszter Diána: *Információbiztonsági stratégia és vezetés.* https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsagi-strategia-es-vezetes.original.pdf (2018. 11. 10.)

[47] Buttyán Levente – Vajda István: *Kriptográfia és alkalmazásai.* Typotex, Budapest, 2004.

[48] Frész Ferenc – Kálovics Tamás – Puha Gábor: *Hálózatok biztonsága.* pp. 19–22. https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/halozatok-biztonsaga.original.pdf

[49] Szádeczky Tamás: *Információbiztonsági szabványok.* Nemzeti Közszolgálati Egyetem, Budapest, 2014. https://lipusz.hu/pedagogia_tanulas/nke_eiv/informaciobiztonsagi-szabvanyok.original.pdf (2018. 11. 10.)

[50] Bederna Zsolt: *Fuzzy-based Intrusion Detection.* Hadmérnök, X. évfolyam, 2015, 1. szám, március. http://hadmernok.hu/151_14_bedernazs.pdf (2018. 11. 10.)

[51] Frész Ferenc – Kálovics Tamás – Puha Gábor: *Hálózatok biztonsága.* https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/halozatok-biztonsaga.original.pdf (2018. 11. 10.)

[52] Frész Ferenc – Kálovics Tamás – Puha Gábor: *Hálózatok biztonsága.* p. 34. https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/halozatok-biztonsaga.original.pdf (2018. 11. 10.)

[53] Dreilinger Tímea: *Vírusvédelem.* Panem Könyvkiadó, Budapest, 2004, pp. 13–14.

[54] Bodó Attila Pál – Zámbó Nóra: *Újdonságok a kibervédelmi szabályozásban.*

[55] Munk Sándor: *Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interoperabilitással.* http://www.hadmernok.hu/180kofop_12_munk.pdf (2018. 11. 10.)

[56] Európai Hálózat- és Információbiztonsági Ügynökség: *Részletes leírás a CSIRT-Csoportok létrehozásáról.* 2006. https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-hungarian/at_download/fullReport (2018. 11. 10.)

[57] Molnár Dóra: *Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése.* http://hadmernok.hu/171_20_molnar2.pdf (2018. 11. 10.)

Ajánlott irodalom

- Fehér Krisztián: *Kezdő hackerek kézikönyve.* BBS-INFO Kiadó, Budapest, 2016.
- Fehér Krisztián: *Hackertechnikák.* BBS-INFO Kiadó, Budapest, 2018.
- Hadnagy, Cristopher: *Social Engineering – The Art of Human Hacking.* Wiley Publishing, Indianapolis, 2011,
- Mitnick, Kevin D.: *A legendás hacker – A megtévesztés művészete.* Perfact-Pro, Budapest, 2003.
- Mitnick, Kevin D.: *A legendás hacker – A behatolás művészete.* Perfact-Pro, Budapest, 2006.
- Rodé Magdolna: Virtuális rabszolgaság. Kolor Optika Bt., Budapest, 2018.
- Szőr Péter: *A vírusvédelem művészete.* SZAK Kiadó, Bicske, 2010.
- Warren, Peter – Streeter, Michael: *Az internet sötét oldala.* HVG Könyvek, Budapest, 2005.

Táblázatjegyzék

Kifejezés- és rövidítésjegyzék

- AAA (Authentication – azonosítás, Authorization – jogosultságkezelés, Accountability felelősségre vonhatóság)
- AD – Active Directory
- analyst – Elemző
- ANSI – American National Standards Institute (Amerikai Nemzeti Szabványügyi Intézet)
- architect – Tervező
- Authenticity – hitelesség
- Automatizált jogosultságszerzők – rosszindulatú szoftver fajta
- Availability – rendelkezésre állás
- Backdoor – hátsó kapu
- Baktériumok – rosszindulatú szoftver fajta
- BCP – Business Continuity Plan
- BeEF – Browser Exploitation Framework
- Blacklist – fekete lista (tiltok elemek listája)
- Botnetet – zombi-hálózatot
- Bridge – hidak (hálózati eszköz)
- Brute force – nyers erő

- CA – Certificate Authority (tanusító szervezet)
- CCTV – Closed-circuit television (zárt-láncú kamera rendszer)
- CEH – Certified Ethical Hacker
- CERT – Computer Emergency Response Team (eseménykezelő központok
- CIA triad – BSR triád
- CISO – Chief Information Security Officer (Információbiztossági vezető)
- CISSP – Certified Information Systems Security Professional
- CMD – parancssor
- Compensating – kompenzáló
- Confidentiality – bizalmasság
- Consultant – Tanácsadó
- Cookie – süti (dinamikus webes tartalom)
- Corrective – korrekciós
- Covering tracks – Nyomok eltűntetése
- CVSSv3.0 – Common Vulnerability Scoring System version 3.0
- Cybercrime egyezmény – Számítástechnikai Bűnözés Elleni Egyezmény
- CYBINT – Inteligence gathered from Cyber Space (kiberhírszerzés tűzfal)
- CSO – Chief Security Officer (Biztonsági vezető)
- DDoS – Distributed Denial of Service
- DDW – Deep and Dark Web
- Destructoware – rosszindulatú szoftver fajta
- Detective – detektív)
- Deterrent – elrettentő
- DLP – Data Loss Prevention
- DMZ – demilitarizált zóna
- DNS – Domain Name System
- DoS – Denial of Service
- Dropperek – rosszindulatú szoftver fajta
- DRP – Disaster Recovery Plan
- Dumpsterdiving – kukabúvárkodás
- Engineer – Mérnök
- Enumeration – Behatolási kísérletek
- Escalation of privilege – Jogosultság növelése
- ETSI – European Telecommunications Standards Institute (Európai Távközlési Szabványügyi Intézet)
- Exploit vírusok – Alkalmazáshibát kihasználó vírusok
- Exploitation – kihasználás
- Féreg – rosszindulatú szoftver fajta

- Flooderek – rosszindulatú szoftver fajta
- Footprinting – Passzív információgyűjtés
- FTP – File Transfer Protocol
- GDPR – General Data Protection Regulation (Általános Adatvédelmi Rendelet)
- GHDB – Google Hacking Database
- HIDS – Host-based Intrusion Detection System
- Hirdető programok – rosszindulatú szoftver fajta
- Honeynet – Több egyszerre alkalmazott Honeypot
- Honeypot – mézes csupor (hálózatbiztonsági eszköz)
- HTTP – HyperText Transfer Protocol
- HTTPS – Hypertext Transfer Protocol over TLS/SSL
- Hub – több portos repeater (hálózati eszköz)
- IANA – Internet Assigned Numbers Authrity
- ID – azonosító
- IDS – Intrusion Detection System
- IEEE – Institute of Electrical and Electronics Engineers
- IETF – Internet Engineering Task Force (az internet fejlesztésének szervezete)
- Injektorok – rosszindulatú szoftver fajta
- Integrity – sértetlenség
- Intelligence – hírszerzés
- IP – Internet Protocol
- IPS – Intusion Protection System
- ISIS – Iszlám Állam
- ISO – International Organization for Standardization (Nemzetközi Szabványügyi Szervezet)
- IT – Information Technology
- ITU – International Telecommunication Union (Nemzetközi Távközlési Egyesület)
- Keylogger – billentyűzet leütő
- Kitek (vírusgenerátorok) – rosszindulatú szoftver fajta
- KPI – Key Performance Indicators
- Kripto vírusok – rosszindulatú szoftver fajta
- L2TP – Layer 2 Tunneling Protocol
- Layer 3 switch – 3. szintű kapcsolók (hálózati eszköz)
- LDAP – Lightweight Directory Access Protocol
- Legality – jogszerűségének
- Letöltők – rosszindulatú szoftver fajta
- Logikai bombák – rosszindulatú szoftver fajta
- MABISZ – Magyar Biztosítók Szövetsége
- Malware – malicious software (rosszindulatú szoftver)

- MitM – Man-In-The-Middle
- NIAC – National Infrastructure Advisory Council
- NIDS – Network-based Intrusion Detection System
- NIS directive – Network and Information Security Directive
- Non-repudiation – letagadhatatlanság
- OSINT – Open Source Intelligence (nyílt forrású hírszerzés)
- PDCA (Plan – tervezés, Do – cselekvés, Check –ellenőrzés, Act – beavatkozás)
- PGP – Pretty Good Privacy
- Piggybacking – jogosulatlan belépés
- Plain text – nyílt szöveg
- PoC – Proof of Concept
- POP3 – Post Office Protocol version 3
- PPTP – Point-to-Point Tunneling Protocol
- Ransomware – zsarolóvírus
- RAT – Remote Acces Trojan
- RBAC – Role-based acces control
- RCP – Remote Procedure Call
- Recovery – helyreállító
- Repeater – ismétlők (hálózati eszköz)
- Rootkitek – rosszindulatú szoftver fajta
- Router – útválasztók (hálózati eszköz)
- SAM – Security Account Manager
- Scanning – Támadási felület feltérképezése
- SIEM – Security information and Event Management
- SIGINT – Signal Intelligence (rádióelektronikai felderítés)
- SLA – Service Level Agreement
- SMB – Service Message Block
- SMS – Short Message Service
- SMTP – Simple Mail Transfer Protocol
- SNMP – Simple Network Management Protocol
- SNMPTRAP – Simple Network Management Protocol Trap
- SOC – Security Operation Centereket
- Social Media – Közösségi média
- Spammer programok – rosszindulatú szoftver fajta
- Spyware – rosszindulatú szoftver fajta
- SQL – Structured Query Language (strukturált lekérdezőnyelv)
- SSH – Secure Shell
- SSL – Secure Socket Layer

- Switch – kapcsolók (hálózati eszköz)
- SYN – a bannerek egy fajtája
- System Hacking – Rendszerbe történő bejutás
- Tailgaiting – bejutás a tömeggel együtt
- Tárcsázók – rosszindulatú szoftver fajta
- TCP – Transmission Control Protocol
- TFTP – Trivial File Transfer Protocol
- TLS – Trasport Layer Security
- TOR – The Onion Router
- Trójai falovak – rosszindulatú szoftver fajta
- UDP – User Datagram Protocol
- URL – Uniform Resource Locator
- Vírus – rosszindulatú szoftver fajta
- VoIP – Voice over IP
- VPN – Virtual Private Network (virtuális magánhálózat)
- VPN – Virtual Private Protocol
- WAF –Web Application Firewalls (WEB alkalmazás tűzfal)
- Well Known Ports – jól ismert portokon
- Whitelist – fehér lista (engedélyezett elemek listája)
- XSS – Cross Site Scripting