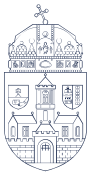


ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK	Hallgató neve:	**Major Gábor László**
2021	Hallgató törzskönyvi száma:	**T/008053/FI12904/N**

Óbudai Egyetem
Neumann János Informatikai Kar
Kiberfizikai Rendszerek Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Major Gábor László**
Törzskönyvi száma: T/008053/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

Személyre szabható digitális önvédelem kialakítása
Personalized Digital self defense

Intézményi konzulens: Balázsné Dr. Kail Eszter
Külső konzulens:

Beadási határidő: 2022. május 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének biztonsága
IT hálózatbiztonság

A feladat

Napjainkban az internet megkerülhetetlen, behálózza az életünket. Ebben a kibertérben rengeteg adat és információ található, mérete napról napra nő. Az internet használatával olyan információkat is megosztunk magunkról, melyek hatalmas veszélyeket rejtenek.
A szakdolgozat célja, hogy bemutassa az alapvető digitális önvédelmi technikákat, ezek személyre szabhatóságát, illetve segítse a biztonságtudatosság fejlesztését. Segítségével kialakítható a digitális biztonság azon állapota, mely nem hátráltatja a mindennapi életben az internet és ahhoz csatlakoztatott eszközök használatát, de kielégítő biztonságot nyújt a felhasználónak.
A feladat során a hallgató tanulmányozza a ma használt legnépszerűbb platformok, szolgáltatások biztonságát, megtervezi és bemutatja ezek biztonságos használatának lehetőségeit, kiemelve azon részeket, ahol a felhasználók kritikus adatokat tehetnek nyilvánossá anélkül, hogy tudatában lennének vele. Az implementációt követően teszteli annak biztonságát, összegzi tapasztalatait, számba veszi továbbfejlesztési lehetőségeit.

A dolgozatnak tartalmaznia kell:

- veszélyforrások bemutatását a kibertérben és azon kívül,
- leggyakrabban elkövetett hibák ismertetését, melyek információszivárgáshoz vezetnek,
- OSINT technikák bemutatását,
- gyakran használt online szolgáltatások összehasonlító biztonsági elemzését,
- az alkalmazható digitális (ön)védelmi technológiák bemutatását,
- egy biztonságos rendszer és szolgáltatások implementációját,
- az implementált rendszer validálását,
- a tesztelés során szerzett tapasztalatok összefoglalását,
- továbbfejlesztési lehetőségek vizsgálatát.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * 1. Budapest

.....
Dr. habil. Lovas Róbert
intézetigazgató

A szakdolgozat elévülésének határideje: **2024. május 15.**
(OE TVSz 55.§ szerint)

A dolgozatot beadásra alkalmasnak tartom:

.....
külső konzulens

.....
intézményi konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

HALLGATÓI NYILATKOZAT

Alulírott hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatomban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja.

Budapest, 2021. május 15.

.....

hallgató aláírása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: Major Gábor László

Neptun Kód: [redacted] .

Tagozat: Levelező

Telefon: [redacted]

Levelezési cím (pl.: lakcím): [redacted] .

Projektmunka címe magyarul:

Szermélyre szabható digitalis önvédelem kialakítása

Projektmunka címe angolul:

Personalized Digital Self Defense

Intézményi konzulens: Balázsné Dr. Kail Eszter

Külső konzulens: .....

Kérjük, hogy az adatokat nyomtatott nagy betűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2022.02.07	Feladatok meghatározása	Kail
2.	2022.02.19	Szakirodalom áttekintése	Kail
3.	2022.03.22	Dokumentum struktúrálása	Kail
4.	2022.05.02	Elkészült dokumentum áttekintése	Kail

A Konzultációs naplót összesen 4 alkalommal, az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a Projektlabor 1. / 2. / 3. / Záródolgozati projekt[1] tantárgy követelményét teljesítette, beszámolóra/védésre[2] bocsátható. A javasolt érdemjegy: 5

Kail

.....

Intézményi konzulens

Budapest, 2022 május 13.

---

[1] A megfelelő bekarikázandó/aláhúzandó!

[2] A megfelelő aláhúzandó!

Tartalomjegyzék

1. KÖSZÖNETNYILVÁNÍTÁS

Köszönöm Balázsné Dr. Kail Eszter konzulensem bíztatását, segítségét, tapasztalatát és tudását, melyet megosztott velem a szakdolgozat elkészítése és a képzés során, valamint a az Óbudai Egyetem valamennyi munkatársának, akik segítségével sikeresen teljesíthettem a Kiberbiztonsági Szakmérnök képzést!

2. BEVEZETÉS

Napjainkra az infokommunikációs technológiák összességét egy határokon átívelő közüzemi szolgáltatásnak tekinthetjük. Elterjedtsége, bonyolultsága és magas felhasználói száma, valamint az elkövetett kibertámadások miatt a digitális önvédelem éppoly fontossá vált, mint maga a technológia. A modern infokommunikációs technológia még viszonylag fiatal, viszont rendkívül dinamikusan fejlődik, emiatt még nem alakult ki minden felhasználóban a veszélyforrásokkal kapcsolatos felhasználói félelemérzet és a biztonságtudatosság. A veszély érzékelésének képessége, élményszerű felismerésen alapul, mely során kialakul a szubjektív félelemérzet, vagy ahogy Kézdi Anikó fogalmazott „ A félelmek gyökerének tudatosítása, vagyis annak megértése, hogy mitől lett az adott helyzet olyan félelmetes a számunkra, milyen gyerekkori vagy későbbi tapasztalatok okozták...” [1] A félelemérzet tehát idővel tapasztalati úton alakul ki. A kibertérben ez nem egyszerű feladat, mert a támadásokat olyan eszközök használatával hajtják végre azok, akik mélyebb ismeretekkel rendelkeznek az információs technológiák terén - azok sérelmére, akik csupán felhasználói ismeretek birtokában vannak - melyek nem tartoznak az informatikai általános tudás témakörébe A fizikai világtól eltérően, itt nem észlelhető a felénk irányuló támadás, csak ha az már elérte az első védelmi vonalunkat, az ISP modemet, vagy a Wifi hálózatot, mely sok esetben a lakáson kívülről is elérhető. Emiatt kijelenthetjük, hogy senki nincs folyamatos biztonságban. Ez ahhoz hasonlítható, amikor az utcán a támadót akkor észleli az áldozat, amikor az első ütést már megkapta. Azonban a támadások korábban is észlelhetőek, az előjelek felismerhetőek. Ehhez szükséges az általános felhasználói szintű IT biztonsági tudás bővítése.

A kibertér fenyegetéseiről szóló hírekkel egyre többször találkozunk. Sajnos többek között a korábban említett okok miatt még mindig túl misztikusnak, távolinak érzik ezt a fenyegetettséget a felhasználók. Nem sejtik, hogy milyen veszélyeket rejt ez a technológia adta kényelem és az eszközök, amiket nap, mint nap használnak. Avatatlan szem képtelen felismerni az adathalász e-maileket vagy oldalakat, rosszindulatú kódokat tartalmazó alkalmazásokat, hardveres sérülékenységeket. Ezekről legtöbbször csupán a baj bekövetkezte után szerez tudomást az áldozat, ami jobb esetben lehet egy tönkrement eszköz, emiatt bekövetkező adatvesztés, így legalább nem kerültek illetéktelenek birtokába, és nem használható fel ellene. Sajnos rosszabb esetben illetéktelen kezekbe kerülő adatok, dokumentumok, fényképek, videók, bankszámláról a pénz, személyazonosító adatok.

Dolgozatom két fő témára koncentrál, az első rész bemutatja azokat a ráutaló magatartási szokásokat a fizikai és kibertérben, melyekkel bárki veszélybe sodorhatja saját magát és közvetetten másokat is, természetesen ajánlásokat is tesz, melyekkel csökkenthető a veszély mértéke, ez a humán faktor a digitális magatartás humán tűzfala.

A második részben az infokommunikációs eszközöket, így a felhasználókat érintő veszélyeket mutatja be. Láthatjuk, miként képesek mások vezérelni készülékeinket, melyekkel megfigyelhetnek minket akár a saját otthonunkban is. A készülékeink biztonsági beállításainak és helyes használatának segítségével csökkenthetjük a veszély mértékét, de teljesen ki nem tudjuk iktatni, emiatt az adataink biztonsági mentésének lehetőségeivel is foglalkozunk. Ezek után az otthoni hálózatunk biztonsági kérdéseit, veszélyeit tárgyaljuk, valamint ezek kijavítását, a felhasználó számára elrhető eszközök, módszerek segítségével. Mindezek után az internetes kommunikációt és a népszerűbb online szolgáltatások biztonsági beállításait végezzük el a hozzá tartozó kellően erős bejelentkezési azonosítók, jelszavak definiálásval, tárolásával együtt vesszük át. Dolgozatom célja, hogy az átlagos felhasználók számára adjon támpontot, amivel növelhetik a saját kiberbiztonságukat.

2.1. A probléma felvetése

A kiberbűnözők folyamatosan keresik a lehetőségeket és kiskapukat, hogy a számukra fontos adatokat megszerezzék, vagy irányításuk alá vonjanak internetre csatlakoztatott eszközöket, hogy ezeken keresztül hajtsanak végre támadásokat. Ezek a támadások egyre kifinomultabbak és bonyolultabbak, mert folyamatosan képezik magukat, hogy képesek legyenek egy lépéssel a kiberbiztonsági szakemberek előtt járni. Emiatt a felhasználóknak is képezniük kell magukat és egyre fontosabb elsajátítani azokat a módszereket, mellyekkel növelhetik a adataik biztonságát. A tömeges kibertámadások nagy része nem személyre szabott célzott támadások, a legnépszerűbb, legtöbb példányban használt szoftverek, hardverek és szolgáltatások sebezhetőségeit kihasználva igyekeznek minél több számítógéphez, szenzitív, értékes adathoz hozzáférni. Ezeken keresztül érik el a legtöbb olyan felhasználót, akik nem fordítanak sem figyelmet, sem energiát a saját kiberbiztonságukra, sőt akár még motiválhatóak is, hogy bizonyos dolgokat megtegyenek, mert hamis biztonságérzetük nem jelez, hogy bajba fognak kerülni. Sajnos ez inkább a támadókat segítik. A támadásokat jellemzően a kijavítatlan sérülékenységekre, így a helytelen felhasználói magatartásra építik. A kritikus emberi tényezőket a Social Engineering technikákkal képesek a támadók kihasználni. Ezeket általában megelőző támadásoknak tekinthetjük. A későbbi támadásokhoz szükséges információkat ekkor szerzik meg. Ezek jellemzően belépési adatok, olyan felhasználói fiókokhoz, ahol a támadók számára is értékes dolgokat tárolnak a felhasználók. Ezek lehetnek akár internetbank, pénzügyi vagy egyéb szolgáltatásokhoz tartozó hozzáférések, munkahelyünkön használt belépési adatok. Céljuk lehet továbbá az otthoni hálózatunkat felhasználva, más internetre csatlakoztatott eszközökkel együtt zombi hálózat kialakítása, mellyel nagyobb támadásokat hajthatnak végre. Ezzel a hálózattal képesek lehetnek túlterheléses támadást végrehajtani vagy kriptobányászatra felhasználni a hálózatra csatlakoztatott eszközöket.

3. A BIZTONSÁG ÉS VESZÉLY KÉRDÉSEK, VALAMINT A VESZÉLYEK LEHETŐSÉGEI

A korábbi tapasztalataink alapján kialakult digitális magatartásunk és a hamis biztonságérzet miatt árulunk el magunkról és eszközeinkről információkat. Internetes jelenlét során csupán a böngésző és a látogatott weboldalak sütijeinek használatával információkat osztunk meg magunkról, melyekből egyértelműen nem feltétlenül azonosítható egy személy (pl: böngésző típusa, verziója, használt nyelv, időzóna, böngésző kiegészítők, betűtípus és méret információk, képernyőfelbontás, egyéb böngésző beállítás, engedélyezett sütik, protokollok, IP cím, geolokáció, eszközinformációk, látogatott oldal, stb.), viszont a tevékenyég igen, ez illetve a látogatott weboldalon futó egyéb szkriptek által gyűjtött információk - melyek az oldal futásához elengedhetetlenek - kombinációjából kialakul egy profil. Ez a profil azonosíthat egy személyt, egy csoportot. A fenti lista tartalmazhatjaa az ISP által kisztott publikus IP címet és a pontos helyet ahol tartózkodunk. Tehát egy teljesen veszélytelennek tűnő linkre kattintva egy olyan oldalra juthatunk, ami elsőre nem különbözik a várt oldaltól, küllemét tekintve elsőre teljesen azonos az eredetivel, de mégsem az és tudtunkon kívül azokat az infomációkat osztjuk meg magunkról, eszközünkről, amit kihasználva támadást indíthatnak. A támadó lényegében tudja, hogy hova kell menjen és már csak az ajtót kell megtalálnia, amin keresztül bejuthat a belső hálózatunkba. Ezek lehetnek nyitott portok és egyéb védtelen, elavult és ezáltal sebezhető szolgáltatások.

Az internetes jelenlét nem merül ki csupán a böngészéssel. Számtalan egyéb lehetőség áll a kiberbűnözők rendelkezésére. Itt szeretnék némi párhuzammal élni. Ha eláruljuk, hogy hol lakunk könnyedén betörhetnek, azt tudjuk, hogy feltörhetetlen zár nincs ezért nem az a kérdés, hogy betörnek-e, hanem az, hogy mikor.

A publikus IP címünk ebben az esetben a saját lakcímünknek feleltethető meg. Az ISP által rendelkezésünkre bocsátott modem, gyakran magában foglalja a routert, switchet, vezeték nélküli hálózatot és a tűzfalat. Ez az ajtó, amin az ismert sérülékenységeket és a hibás konfigurációs beállítások által létrehozott sérülékenységeket kihasználva bejuthat a támadó a belső hálózatunkba. A digitális eszközeink sérülékenységeit későbbi fejezetek során részletezem. Kijelenthetjük, hogy feltörhetetlen rendszer nem létezik, csak olyan, melynek még nem találták meg a hatékonyan kihasználható gyenge pontját. Ezért az informatikai eszközöket, szolgáltatásokat csupán felhasználói ismeretekkel rendelkező felhasználók, hamis biztonságérzettel és erre építkező biztonságtudatossággal használják, így könnyen célponttá válhatnak. A hamis biztonságérzet tehát egy újabb veszélyforrás ránk és az adatinkra nézve. Székely Iván, Somody Bernadette és Szabó Máté Dániel cikkében [2] kifejtett biztonságérzet definíciója alapján tudjuk a biztonságérzet szoros kapcsolatban áll a tevékenységgel, valamint számos egyéb tényezővel, melyek összessége

váltja ki ezt az érzetet. A változók lehetnek helyzetértékelések, a veszélyek bekövetkezésének idejének és helyének valószínűségei, melyek saját megítélésen alapulnak, például vannak, akik félnek a kutyáktól és vannak, akik a pókoktól. Valamennyi esetben lehetnek közvetlen saját élményekre épülő alapja, de lehet ugyanez közvetett is. Előzetes tapasztalatok alapján extrapolált jövőbeni állapotra vonatkozó érzelem. Azok, akiknek volt saját közvetlen tapasztalatuk áldozati szerepben kibertámadást átélni, azok jobban félnek egy esetlegesen újból bekovetkező támadástól, mint akik nem rendelkeznek ilyen jellegű tapasztalattal. Azonban mások által megtapasztalt élmények is segíthetik a saját biztonságérzetünk érzékenyéségnek változtatását. Vagyis mások hibájából is tanulhatunk.

Ahhoz, hogy megértsük miért fontos az emberi oldalról megközelítenünk az informatikai biztonságot, vizsgáljuk meg! A leginkább illő megfogalmazás Muha Lajostól származik [3] „Az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértet-lensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.” Az informatikai rendszerre leginkább megfelelő megfogalmazás szintén Muha Lajostól [3] származik „ ...az adatok kezelésére használt elektronikus eszközök, eljárások, valamint az ezeket kiszolgáló és a felhasználó személyek együttese.” Melyből jól látszik, hogy a rendszer használata és karbantartása során eljáró személy is a rendszer része. Informatikai értelemben vett jelentése során tehát egy állapotot nevezünk meg, melyet folyamatosan fenn kell tartanunk. Az informatikai rendszerek elemeivel kapcsolatos sérülékenységek folyamatosan kerülnek napvilágra, melyek hibás működésre, hibás tervezésre, esetleg kivitelezésre, vagy felhasználói hibára vezethetőek vissza. Ezért dolgozatomban a biztonság egyik leggyengébb láncszemével a humán faktorral vagy más néven humán tűzfal bemutatásával folytatom, melyet szintén több részterületre bontva taglalom a veszélyek és ezek kivédésének egy lehetséges megoldásával.

4. A HUMÁN FAKTOR

Az informatikai eszközök biztonsági szempontból történő vizsgálata során felfedezhetünk olyan biztonsági réseket, melyek kiaknázásával sikeres támadások hajthatók végre. Saját személyiségünk, viselkedésünk esetében az eszközök biztonsági réseinek analógiáját felhasználva szintén felfedezhetünk biztonsági réseket, ezeket a social engineering segítségével aknázzák ki a támadók. A social engineering egy támadási forma, melyet a kiberbűnözők saját céljaik elérése érdekében alkalmaznak. A kihasználható emberi tulajdonságokat, gyengeségeket keresik a célpontokban, ezeket felhasználva az áldozat manipulálásával, megtévesztésével sikeres támadást készíthetnek elő vagy hajthatnak végre. Ezek alapvető emberi tulajdonságok, ami azt jelenti, hogy bárki célpont lehet, aki rendelkezik a következők közül legalább 1 tulajdonsággal, mint segítőkészség, hiszékenység esetleg naívság, befolyásolhatóság vagy épp bosszúálló. Ezen támadási formák ellen nehéz védekezni, viszont csökkenthetőek a sikeresen végrehajtott támadások. A vállalati környezetben jellemző social engineering veszélyekre nem térnék ki, ezt a témát Oroszi Eszter [4] részletesen feldolgozta. A hétköznapi életünk során előforduló esetekre koncentrálva, azonban a tartalmi korlát figyelembe vételével csupán 1-1 támadási formát illetve ezekre adható védekezési módszert mutatok be. A különböző támadásokkal kapcsolatban érdemes naprakész információkkal rendelkezni, melyeket a Nemzeti Kibervédelmi Intézet honlapján is [5] megtalálhatunk. Így ezek tudatában könnyebb felismerni a mintázatot, amivel a támadások kezdeti jeleit gyorsabban azonosíthatjuk és megtehetjük a szükséges lépéseket, hogy elkerüljük a támadást. A mintázatok jelen esetben azok a jelek, amik felismerése esetén fokozottan figyelünk értékeinkre, testbeszédünkre. Ez segíthet a biztonságtudatos digitális önvédelem kialakításában, ösztönösen és tanult viselkedési formaként a mindenapokban jól alkalmazható, hasonlóan a különböző önvédelmi módszerek elsajátításához.

Az információs technológia és a kiberbiztonsági megoldások folyamatos fejlődése mellett kulcsfontosságú a felhasználók kiberbiztonsági tudásának fejlesztése. Ha ez nem történik meg, akkor maga a felhasználó válhat a biztonság gyenge láncszemévé. Abban az esetben, ha a felhasználó nem alkalmazza a rendelkezésére álló alapvető biztonsági funkciókat, mint a megfelelően erős jelszó, többfaktoros azonosítás, adatainak egyértelműen struktúrált tárolása, biztonsági mentések alkalmazása, valamint az átgondolt internetes kommunikáció, ebben az esetben ezek által nyújtott biztonság kihasználatlan.

4.1. A biztonságtudatosság hiányának okai

Héder Klára [6] jegyezte meg, a biztonságtudatosság pszichés gátjainak több szempontból történő megközelítése alapján a felhasználók érzelmi és kognitív vonatkozásában számtalan módon viszonyulnak a témához. A túl bonyolult és hosszú képzések ellenérzést

válthatnak ki, ami a magabiztosság csökkenésével jár, és inkább feladja, megbékél azzal a tudattal, hogy adatait úgysem tudja megvédeni.

A biztonságtudatosság hiányának több oka lehetséges, ezek között szerepel a felhasználók védekezéshez szükséges ismereteinek hiányát. A második helyen a motiváció hiánya szerepel, aminek következtében nem tesz azért a helhasználó, hogy elsajátítsa ezeket az ismereteket. A harmadik lehetséges okaként a támadók ezene a területen magas kvalifikáltsága szerepel, amivel a felhasználók nem képesek felvenni a versenyt. A felhasználói társadalom számára, akik nem voltak elszenvedői kibertámadásnak, távolinak érzi és hibás feltételezés alapján gondolja, hogy nem is lesz áldozata ilyen incidensnek, vagy épp nem tartja értékesnek adatait, emiatt érdektelennek gondolja és minimálisra szorítkozik a biztonsági intézkedések terén, hogy a működőképes állapotot elérje. Erre lehet egy példáa amikor nincsenek megváltoztatva az alapértelmezett belépési adatok, az eszközök képesek működni, azonban a biztonság növelése nem történt meg. A különböző személyiségjegyek, attitűdök, és egyéb tényezők hosszan befolyásolhatják a biztonságtudatos hozzáállást. A támadók emiatt különböző célcsoportokat különböző módon célozzák meg. A célcsoportokra jellemző kihasználható tulajdonságok alapján. Az internetes jelenlét során a felhasználói társadalom különböző közösségi platformokon egyfajta önkifejezést gyakorol, ahol érzelmeket kifejezve ez lehet többek között düh, öröm, szomorúság, melyek az adott érzelmi állapot kihasználását célzó támadásokat segíti.

4.2. A veszély felismerésének hiánya

A felhasználói hozzáállás egyik kritikus része, hogy azt állítja, hogy a támadót nem érdeklem vagy nincs olyan adatom, ami értékes lenne a támadóknak..., ha mégis megtörténne a baj, akkor pedig abban a tévhitben van, hogy majd az IT biztonsági szolgáltatások megvédik. De ez tévedés, ezzel pontosan úgy viselkedik, ahogy azt a támadó akarja. A technológia önmagában nem képes megvédeni mindentől. A biztonság állapotának fenntartásához minden szereplőnek a lehető legtöbbet kell teljesítenie. A felelőtlen vagy figyelmetlen magatartástól nem véd meg semmi. Bizonos dolgokat a felhasználónak kell megtennie, hogy ne önmaga legyen a biztonság leggyengébb láncszeme. A következőkben néhány kihasználható tulajdonságot mutatok be, amit a támadók különféle módon képesek kiaknázni.

4.3. A segítőkészség

Az emberek legtöbbje szívesen segít másokon, ha az számára nem jelent problémát. Az utcai rablások sokszor kezdődnek segítségkéréssel. A kiszemelt áldozatot kizökkentve a saját fókuszából, a figyelme a segítségkérőre helyeződik át például útbaigazítást kérnek, esetleg a pontos idő megkérdezésével, stb. A kizökkentés állapotát úgy érdemes

elképzelni, mint a bemutatkozást. Első alkalommal nehezen jegyezzük meg a másik fél nevét, mert eredendően arra figyelünk, hogy a saját nevünket mondjuk és azt helyesen ejtsük ki, illetve feldolgozzuk a másik fél keltette első benyomást, a nonverbális kommunikációját, ami alapján bizalmat vagy ellenszenvet szavazunk. Míg a figyelmetlen áldozat a megoldást keresi egy másik támadó észrevétlenül eltulajdonítja az áldozat értékeit, melyek adattárolásra alkalmas informatikai eszközök, pénztárca, igazolványok, stb. A támadók motivációja jellemzően az eltulajdonított eszközök, személyi azonosító okmányok ezek értékesítésével, felhasználásával megszerzett anyagi vagy egyéb haszon. Azonban az eszközök tartalmaznak szenzitív adatokat melyeket értékesítve a személyi azonosító okmányokkal együtt felhasználva további előnyhöz juthatnak, az áldozat kárára. Nehezen kivédhető, mert a támadók legtöbbször meggyőző történettel, bizalomgerjesztő külsővel és testbeszéddel közelednek az áldozathoz. Ezekben az esetekben mindig figyeljünk, hogy az értékeink ne legyenek szem előtt és lehetőleg ne könnyen hozzáférhető helyen tároljuk őket, valamint figyeljünk a közvetlen környezetünkre, hányan és kik vesznek körül minket. Ne hagyjuk, hogy elvonják a figyelmünket. Így az a támadó, akinek az eltulajdonítás a feladata kevesebb lehetősége lesz észrevétlenül végrehajtani a feladatát.

4.4. A hiszékenység

A segítőkész áldozat tovább ronthatja saját helyzetét, ha elhiszi, hogy az áldozat valóban bajban van, mielőtt megyőződne annak valódiságáról. A telefonhívás erejéig kölcsönkért és átadott mobiltelefon is veszélyes lehet adatainkra, mégha az jelszóval, biometrikus vagy egyéb módon védett is. Ha az áldozat elhiszi, hogy valóban fontos a támadónak telefonálnia, mert bajban van, ezért a készülékét feloldva saját maga juttatja hozzá a támadót az adataihoz. Semmiképp ne adjuk át saját készülékünket a támadónak, helyette hívjunk mi segítséget, ha meggyőződtünk arról, hogy valóban bajban van az illető. Ne adjunk lehetőséget a támadónak hogy felmérje az értékeinket és a képességeinket, melyeket kihasználva további támadásokat intézhet.

4.5. A befolyásolhatóság

Az emberek könnyen befolyásolhatóak, melyeket a megtévesztéssel, megfélemlítéssel esetleg csalással ér el a támadó. Például többször hallhattunk olyan híreket, hogy egyenruhába öltözött csalók hajtottak végre sikeres támadásokat. Legtöbbször azért használnak egyenruhát, mert az emberek többsége egy megfelelő egyenruhába öltözött személyt előbb engednek a bizalmukba. Ennek a fentebb sorolt okai lehetnek, tehát elhiszi, hogy valóban az a támadó akinek kiadja magát, esetleg a hatalomtól és retorzióktól való félelem miatt. Ebben az esetben a figyelmetlen áldozat feltétel nélkül végrehajtja a támadó által kiadott utasításokat. Kivédése, illetve a károk minimalizálása érdekében, ha nincs közvetlen életveszély, figyelmesen mérje fel támadója egyenruháját, illetve kérje

meg, hogy azonosítsa magát. A támadó által említett szervezet telefonos elérhetőségén igazolja a támadó állításának valódiságát. A támadók erre nem hajlandóak, mert ezzel a cselekedetükkel felfednék magukat.

4.6. A bosszúállás

A bosszúállás is, mint az eddig említett tulajdonságok ötvözhető, egymásba ágyzható. A támadók céljaik elérése érdekében nem feltétlenül kell saját maguknak végrehajtani a támadást, számukra elegendő, ha információval rendelkeznek egy olyan személyről, aki kihasználva ösztönözhető egy vélt vagy valós sérelem bosszújára. Ez a személy könnyen befolyásolható, rávehető, hogy hajtson végre egy vagy több tevékenységet a valós támadó helyett, amit meg is fog tenni, ha elhitetik vele, hogy nem származik ebből semmilyen hátránya, emiatt segíteni fog a támadónak elérni a célját. Kivédése nehéz, mert érzelmileg aktivált állapotban rendkívül nehéz racionális döntést hozni. Érzelmileg aktivált állapotnak több szintje van, jelen esetben egy magasabb szélsőséges állapot esetén váltja ki a bosszúállást, mint a düh reakcióját. Ez az állapot egy erősen emócionális állapot mely gyenge hatékonyságot és kevéssé ellenőrzöztt viselkedést eredményez. Ezt részeletesebben Csépe Valéria, Győri Miklós és Ragó Anett Az általános pszichológia című könyve [7] tárgyalja

4.7. A figyelmetlenség

A mai felgyorsult világban rengeteg impulzus ér minket, ezért a figyelmünket nagyon könnyű elvonni, megosztani. Ennek a jelenségnek a kiaknázására szakosodott támadók a figyelmetlen áldozatot számos módon képesek kihasználni. A figyelmetlenség témája három fő részre osztható. Az első részben a különböző változatos impulzusok valamint a napi tevékenység során fokozott koncentrációt igénylő tevékenységünk miatt bekövetkező lehetőségeket vesszük számba. Erre az egyik legjobb példa egy zsúfolt utcán halaszthatatlan telefonbeszélgetést folytató figyelmetlen ember. Számára fontos, hogy megoldjon egy problémát, melyre koncentrál azonban az utca zaja, a tömeg megosztja a figyelmét, így a támadó könnyedén eltulajdoníthatja értékeit. A figyelmetlenség egy másik oldalról történő megközelítésére egy példa az autóban látható helyen felejtett értékek a támadók számára egy kiaknázható sérülékenység. A harmadik részt tekintjük az előbbi két halmaz uniójának. Erre a legjobb példa a zsúfolt utcán a dugóban az autójában ülő gépjárművezető mellől eltulajdonított táska. A támadók a helyszín gyors elhagyására alkalmas közlekedési eszközzel pl: kerékpárral vagy motorkerékpárral az autók között cikázva keresik a legmegfelelőbb áldozatot. Egy pillanat alatt képesek a gépjármű oldalsó üvegét betörni, majd egy gyors mozdulattal a táskát eltulajdonítani és ugyanilyen sebességgel a helyszínt elhagyni. Az áldozat a forgalomra koncentrál, de a hanyagul látható helyen elhelyezett érték miatt helyezi magát az áldozat szerepébe.

5. A HUMÁN TŰZFAL, VAGYIS AZ EMBERI TÉNYEZŐ VÉDELME

Az emberi tényezőkön alapuló támadások elleni védekezést a viselkedésünk megfigyelésével kell kezdenünk. Korábbi tanulmányaim során sokat foglalkoztam az emberi viselkedéssel, valamint annak befolyásolhatóságával. A nem várt hirtelen érkező ingerek a normálistól eltérő állapotot idéznek elő, mely esetben a normálistól eltérő válaszreakciókat adjuk. Ezekre építve befolyásolható a viselkedésünk, amit a támadók a saját céljaikra használhatnak. A következő részekben a felkészüléshez adok néhány gyakorlati segítséget, mellyel minimalizálható a kockázat és a bekövetkező kár. A védekezéshez nem szükséges feleslegesen drága és bonyolult eszközökre beruháznunk.

5.1. A stresszhelyzet

Tisztában kell lennünk azzal, hogy a támadók gyakorlottak és igyekeznek minél hitelesebbek lenni, hogy az áldozat számára, negatív vagy pozitív stresszhelyzetet teremtsenek. Ezzel képesek kizökkenteni az áldozatot a megszokott állapotából, amivel amegoszthatják a célpont figyelmét. Biztonságunk érdekében sokat tehetünk, ha tartunk egy önreflexiót és viselkedésünket tudatosan megfigyeljük. Ennek segítségévelMiként reagálunk bizonyos dolgokra, pl: egy ismeretlentől származó új e-mail-re, reklámokra, milyen információkat osztunk meg magunkról. Ha figyelmesek, és kellőképp gyanakvóak vagyunk, valamint tisztában vagyunk az aktuális támadásokkal, a legtöbb esetben képesek vagyunk észrevenni, hogy a fent tárgyalt emberi tulajdonságok közül épp melyiket célozzák meg a támadók. Ezt megtehetik közelről, személyes találkozó esetén, vagy távolról vagyis telefonon esetelg interneten keresztül. Természetsen sokat segít, ha tájékozódunk az épp aktuális támadásokról a hatóságok vagy a korábban említett Nemzeti Kibervédelmi Intézet honlapján, akkor könnyebben készülhetünk fel, így nem fog váratlanul érni egy támadás. Lényegében ugyanezt tesszük az időjárás esetén is, felkészülünk, hogy ne érjen meglepetés.

5.2. A negatív stresszhelyzet kezelése

A negatív stresszhelyzetre egy példa, amikor támadók banki alkalmazottnak kiadva magukat telefonon keresik fel az áldozatukat, ahol megkérik, hogy azonosítsa be megát az áldozat, hogy egy kitalált bankszámlával kapcsolatos probléma megoldása megtörténjen. Soha nem szabad átadni illetéktelen személyeknek semmilyen adatot. A legjobb védekezés ebben az esetben, ha nem esünk pánikba és adataink megadása nélkül minél több információt kiderítünk a felkeresés indokával kapcsolatban, majd tegyük le a telefont. Ezután hívjuk fel a bankot a weboldalukon található telefonszámon, majd kérdezzünk rá a korábbi hívásban említett problémára. Abban az eesetben, ha valódi volt

az indok, ami miatt felkerestek, úgy megoldhatjuk telefonon keresztül annak tudatában, hogy valóban a megfelelő személlyel beszélünk.

5.3. A pozitív stresszhelyzet kezelése

A pozitív stresszhelyzet esetén valamilyen nyeremény miatt keresik fel az áldozatokat a támadók, majd a nyeremény átvételéhez szükséges adatokat elkérve próbálnak meg hozzájutni a számukra fontos információkhoz. Ebben az esetben szintén érdemes higgadtnak maradnunk és hasonlóan a banki példa alapján minél több információt szerezzünk be és tegyük le a telefont. Ha valóban történt olyan eset, hogy részt vettünk egy nyereményjátékban, akkor általában emlékszünk, vagy van róla valamilyen bizonyíték. Ekkor érdemes az ott szereplő elérhetőségen felkeresni a megadott elérhetőségeken az illetékest, majd beszámolni a kapott információkról. Ha hiteles volt a megkeresés, akkor visszahívás után is releváns lesz az ok, amennyiben nem volt hiteles, úgy megbizonyosodhatunk róla, hogy sikeresen meghiúsítottunk és elkerültünk egy támadást.

Természetesen előfordulhatnak olyan helyzetek, amikor azonnal kell döntést hoznunk, és ezzel a csalók is tisztában vannak de az esetek többségében van gondolkodási idő, amit ne felejtsünk el kihasználni. Olyan eset nem fordul elő, hogy azonnal kell adatot szolgáltatnunk telefonon vagy interneten keresztül. Ha ilyennel találkozunk, akkor nagy valószínűséggel csalás van háttérben.

5.4. Az érzelmi befolyásoltság kötődése a biztonsághoz

A felhasználók által befolyásolható biztonság egyik pillére a jelszó. Ma is sok szolgáltatás van, ahol nem alkalmaznak kötelező jelszó kirtériumokat. Karen Renaud, Robert Otondo és Merrill Warkentin [8] kutatása megállapította, hogy a felhasználók érzelmi kötődés alapján is alkalmaznak jelszavakat, jelszógenerálási szabályokat. Ezeket a támadók kiasználhatják, mert nem túl erős, de könnyen megjegyezhetőek a jelszavak. Az érzelmi befolyás csökkentése és a biztonság növelése érdekében a jelszógenerálás és tárolás nehézkes feladatát egy erre alkalmas jelszókezelő alkalmazás segítheti. Ennek következtében a generált jelszavak nem kötődnek a felhasználóhoz olyan szempontból, hogy nem számára jelentős esemény, állapot, dátum, személy, kisállat, stb. adja a jelszót magát vagy egy részét, hanem az alkalmazás generálja. Ennek előnye, hogy a támadók adatgyűjtés közben nem tudják kihasználni a megszerzett információkból történő jelszavak kikövetkeztetését. Így a jelszavakhoz kötődő stressz, feloldható. A mindennapi használatot megkönnyíti, mert egyetlen helyen megtalálhatja az össszes jelszavát, amivel időt spórolhat, mindamellett a sikerélmény következtében az új képességek elsajátítása iránti motiváció, valamint a nyitottság is növelhető. A 5.1 táblázatban összegyűjtve látható néhány gyakoribb kihasználható emberi tulajdonság.

Kihasználható tulajdonságok	Támadás	Védekezés
Segítőkészség	Ismeretlen feladótól származó gyanús, szokatlan e-mail, melyben segítséget kérnek, főként pénzt, melynek többszörösét ígérik	Használjunk több e-mail fiókot különböző célokra. Keressünk rá az e-mail szövegére, feladóra az interneten. Találat esetén jelöljük kéretlennek.
Hiszékenység	Baljós e-mail, amiben jelzik, hogy felvétel készült az áldozatról, amit a támadók közzétesznek, ha nem fizet váltságdíjat	Takarjuk le a kamerát, ha nincs használatban és korlátozzuk az alkalmazások kamera jogosultságait.
Befolyásolhatóság	E-mail értesítés ami haonló egy banki levélhez, amiben belépési adataink megváltoztatását kérik	Ne adjuk ki adatainkat, mindig a hivatalos elérési útvonalat haználjuk.
Bosszúállás	Felkérés, hogy másnak továbbítsunk egy vírusos állományt e-mailben, amivel árthatunk neki	Mindennek nyoma van valahol, tehát, ha valakinek ártó szándékkal kárt okozunk, akkor mi kerülhetünk bajba
Figyelmetlenség	Jelszavak egyszerű szövegfájlban tárolva, vagy bejelentkezve maradni egy fiókban oylan eszközön, amihez más is hozzáférhet és eltulajdoníthatja.	Jelszókezelő alkalmazások használata, biztonsági mentések készítése

5.1. táblázat. Online és Offline jelszókezelő alkalmazások főbb funkciói

6. AZ ADAT AZ ÚJ ARANY

Szenzitív adatainkhoz, számítógépes magánszféránkhoz számtalan módon hozzáférhetnek a támadók. A hozzáférés lehetősége és nehézsége függ a támadó tudásától, az áldozat biztonságtudatos viselkedésétől, valamint az általa használt eszközök és hálózat biztonsági felkészültségének összességétől. A korábbi fejezetekben az emberi tényezőket vettük számításba, a továbbiakban áttérünk a használt eszközökre, ezek fenyegetettségeire.

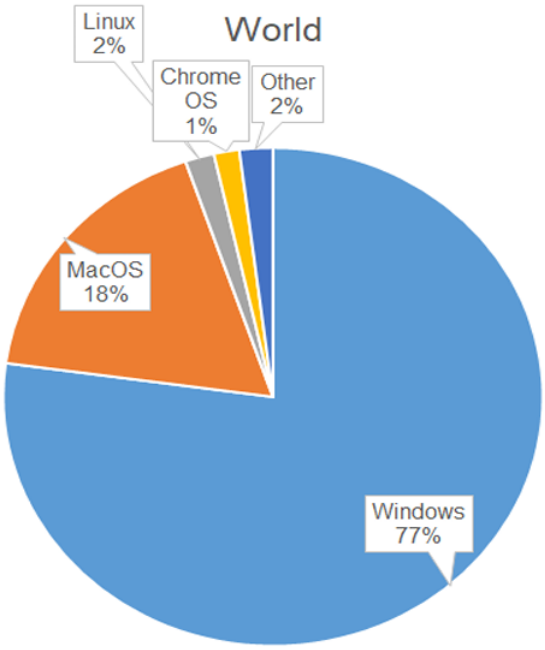
Ahogy az emberi viselkedés esetén, úgy a számítógépünk és minden internetre csatlakozott eszközünk esetén is számtalan sérülékenyésg létezik. Ezeket kihasználva lehetősége van a támadónak az áldozat adatait megszerezni, vagy egyéb kárt okozni, pl: tönkretenni a számítógépet, vagy akár kellemetlen helyzetbe hozni áldozatát azzal, hogy a nevében számára kínos tartalmakat oszt meg. Ha használjuk a korábban említett analógiát, miszerint a nonverbális kommunikációnk a fizikai világban például a testbeszédünk, a kibertérben ezt a szerepet az eszközeink és a használt szoftvereink töltik be. Minél nagyobb felületet adunk a támadásra, jelen esetben a ki nem javított sebezhetőségek, a rendszerünket fertőzni képes vírusok számossága, illetve a hibás konfigurációs beállítások, annál nagyobb veszélyben vannak adataink. Természetesen a kibertámadások elleni kitettség nem szűntethető meg teljesen, azonban jelentősen csökkenthető a veszély. Eddig a két fő téma közül azokat a fenyegetéseket vizsgáltuk, melyekhez nem feltétlen van szükség IKT vagy más néven információs és kommunikációs technológiára, eszközökre. Ezek voltak a humán tűzfal biztonsági kérdései. A következő fejezetekben a második fő területre fogunk koncentrálni, mely bemutatja egy vagy több eszköz, hálózat, szolgáltatás, veszélyforrásait és biztonsági kérdéseit. Mobil készülékek, PC-k, IoT és hálózati eszközök sérülékenységeit, melyeket a hardver, az operációs rendszer vagy egyéb telepített szoftver, esetleg a felhasználó okoz. A sérülékenységeket kereső támadók a felhasználói viselkedésekből és az eszközök elemzésének eredményéből indulnak ki.

7. SÉRÜLÉKENYSÉGEK ÉS VESZÉLYFORRÁSOK

A sérülékenységek következhetnek fejlesztési, tesztelési hiányosságokból, ami azt jelenti, hogy egy kiaknázható sérülékenység a fejlesztés és a teszt során nem derült ki. Amíg ez nem kerül javításra, addig az a támadó, aki képes kihasználni ezt a sérülékenységet, támadást indíthat az eszközünk ellen. Más sérülékenységek felhasználói okokra vezethetőek vissza. Ez azt jelenti, hogy gyári beállításokat, belépési adatokat beüzemeléskor a felhasználó nem változtatja meg, illetve nem aktiválja a biztonsági funkciókat. Viszont sok esetben találkozhatunk olyan esettel, amikor valamilyen kártékony kódot tartalmazó fájl, program, jut a számítógépre és ez használja ki a sérülékenységeket, vagy újakat hoz létre. Ez pedig az emberi sérülékenységek következtében történhet meg. Figyelmetlenül vagy kapkodva olyan linkre kattintunk, ami egy ismeretlentől származó e-mailben vagy annak csatolmányában van. Ez elindíthat egy folyamatot, ami során kártékony kód kerülhet a számítógépünkre.

7.1. Kártevők

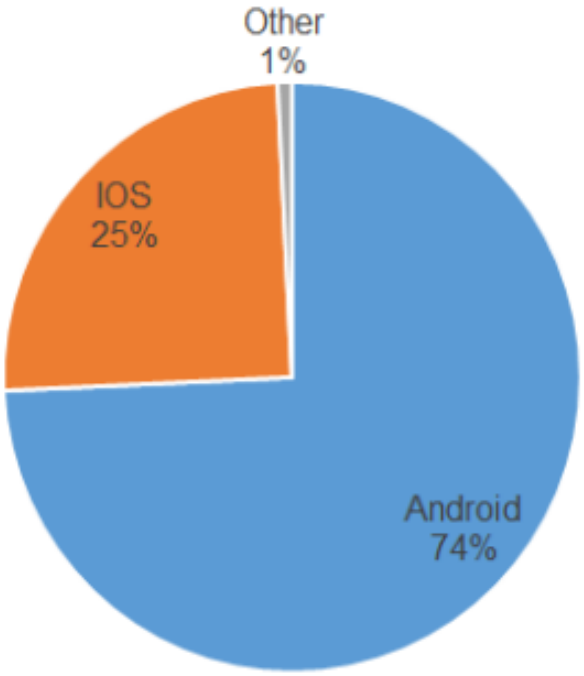
A kártékony kódok szinte minden operációs rendszerre elérhetőek. A különböző operációs rendszereket különböző kártevők képesek megfertőzni, azonban vannak kivételek, melyek képesek több fajta operációs rendszer megfertőzésére. A nem célzott támadások esetén, ahogy azt korábban említettem a legtöbb potenciális célpontra koncentrálnak a legtöbb kihasználható sérülékenységgel. A vírusok készítői emiatt a legnagyobb hasznot elérve a legkisebb energiabefektetéssel és a legnagyobb siker lehetőségével a legnépszerűbb operációs rendszerekhez készítettek kártevőket. Ezeket a kártevőket képesek úgy felhasználni, hogy az áldozat eszközére olyan kártevőt juttatnak, ami vagy rendszergazdai jogosultságot szerez, majd ezzel a jogosultsággal megnyit egy kiskaput a támadónak, aki a már megszerzett rendszergazdai jogosultsággal képes a számítógépünk felett átvenni az uralmat és lényegében azt csinál, amit csak akar. Más esetekben keyloggert vagyis billentyűzetfigyelőt küldenek, amivel láthatják a leütött billentyűket és megszerezhetik vele a belépési adatokat. Természetesen mindezt az áldozat előtt gondosan elrejtve. A legnépszerűbb és leggyakrabban használt platformokat támadják a biztos eredményn érdekében. Az amerikai HHS [9] (Department of Health and Human Services - Egészségügyi és Humánerőforrások Minisztériuma) által készített 2020-as globális méretű felmérés alapján, melyben az asztali számítógépeken és notebookokon futó operációs rendszerek piaci részesedését felmérték, a Microsoft Windows 77%, a MacOS 18%, a Linux 2%, az egyéb operációs rendszerek szintén 2%, valamint a Chrome OS 1% részesedéssel osztoztak a piacon, ahogy az a 7.1 ábrán is látható. A kártékony kódoknak több fajtája létezik, más-más céllal készültek.



7.1. ábra. Operációs rendszerek piaci részesedése a PC-k és notebookok piacán

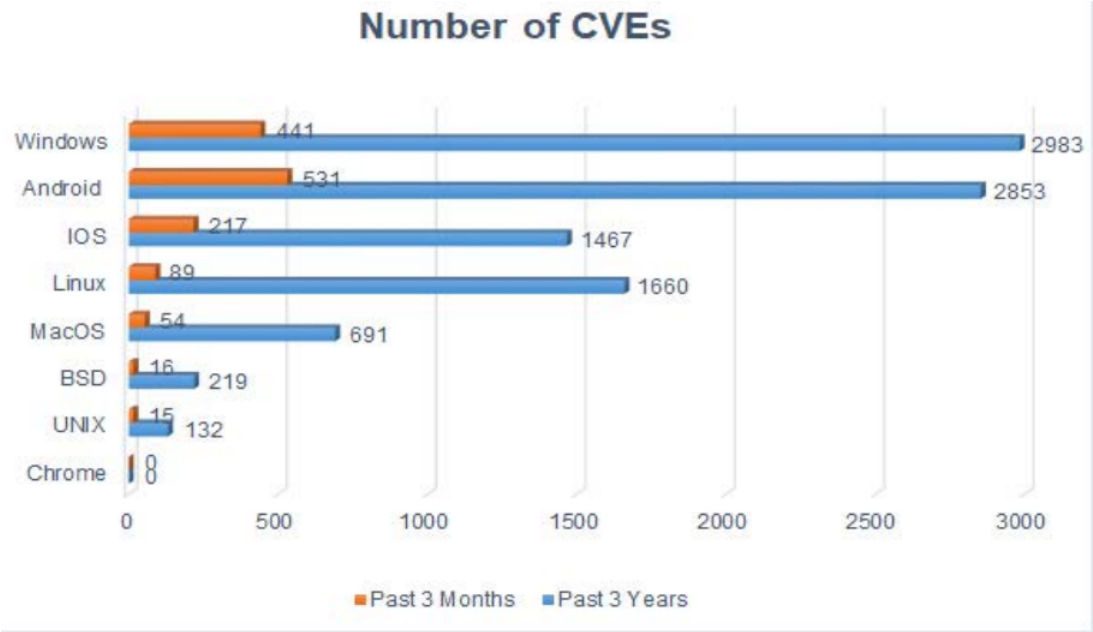
Ebből jól látható, hogy a legtöbb kártevő az asztali számítógépek esetén a népszerűsége miatt a Microsoft operációs rendszereit érinti. Az eddig tárgyaltak alapján, ha egy felhasználó, aki anélkül nyit meg egy levélben kapott linket, hogy ellenőriné a feladót vagy a levél helyességét, hitelességét, mert nincs tisztában azzal, hogy ez mekkora veszélyt jelent számára, valamint a Microsoft egyik operációs rendszerét használja hatékony vírusírtó szoftver nélkül, úgy fertőzheti meg a számítógépét, hogy erről nem szerez tudomást mindaddig, amíg nyilvánvalóvá nem válik számára, hogy ellopták az adatait, pénzét, egyéb értékeit.

A mobil készülékek piacán jelenleg Az Android operációs rendszert futtató készülékek 74%, az IOS operációs rendszert használó készülékek 25%, az egyéb rendszert használó készülékek 1% piaci részesedéssel rendelkeznek, ami a 7.2 ábrán is látható.



7.2. ábra. Mobil operációs rendszerek piaci részesedése

Ha számításba vesszük az operációs rendszerek elterjedtségét és a nyilvánosságra került sérülékenységeket, amik megtalálhatóak a CVE adatbázisában [10] is. A CVE adatbázis tartlmazza azokat a sérülékenységeket, amik eddig kiderültek és kiaknázhatóak, ha nem utólag nem lett befoltozva. A 7.3 ábra is jól szemlélteti, a legelterjedtebb és legnépszerűbb operációs rendszerek a leginkább érintettek, ezek pedig a Microsoft Windows és a Google Android különböző verziói. Ez természetesen nem azt jelenti, hogy az adott operációs rendszerek rosszak, hanem inkább azt jelenti, hogy ezek használata esetén fontos gondoskodni a sérülékenységek javításáról, a megfelelő védelmi szoftverek naprakészen tartásáról és a lehető legtöbb védelemmel ellátni az adott rendszert.



7.3. ábra. Operációs rendszerek sérölékenységei 2020-as adat

Emiatt a nem megfelelő célra felhasznált eszközök és szoftverek sérülékenységei szintén növelik a kockázatot. A nem hivatalos forrásból beszerzett szoftverek pedig tartalmazhatnak különböző kártevőket, melyeket különböző célokra szánnak a készítőik és a támadók.

7.1.1. Kémprogramok

A kémprogramot valamilyen másik ártalmatlannak tűnő fájlba vagy weboldalba ágyaznak a támadók, hogy a felhasználói tevékenységről, belépési azonosítókról és az általa használt eszközökről információt szerezzen. Ezek képesek képernyőmentéseket, billentyűleütéseket, a számítógép mikrofonjával és webkamerájával hangot és képet rögzíteni és elküldeni a támadó számára. Melyeket később akár zsarolásra is felhasználhatnak vagy ha sikerült megszerezni belépési adatokat, akkor azokat felhasználva további információkat lophatnak tőlünk, pl: hozzáférhetnek az internetbankhoz és pénzt vagy kriptovalutát lophatnak az áldozattól.

7.1.2. Adathalászok

Angolul phising-nek hívjuk őket, melyek a felhasználót igyekeznek manipulálni, pszichológiai megtévesztés útján próbál személyes adatokat, jelszavakat megszerezni. A megtévesztés kivitelezése során úgy tűnik, hogy az e-mail egy megbízhatónak tűnő feladótól származik. A levél kísértetiesen hasonlít arra, amit a valós feladó küldene. Általában bankokat vagy szolgáltatókat szoktak megszemélyesíteni és az ő formátumukat

próbálják használni. A levélben felhívják a célpont figyelmét, hogy meg kell tennie bizonyos lépéseket, mely segítségével valamilyen veszteséget kerülhetnek el. Ez lehet pl: felhívás egy adatszivárgásról szóló incidensre és megkérik a felhasználókat, hogy változtatssák meg a bejelentkezéshez használt jelszót. Természetesen a linken elérhető oldal szintén nagyon hasonlít a valódira, ahol ugyanolyan bejelentkezési felülletet lehet találni. Így a gyanútlan felhasználó az ijedtség miatt beírja a felhasználói azonosítóját, jelszavát. Miután elküldte az adatokat vagy nem történik semmi, vagy a valódi szolgáltató, bank bejelentkezési oldalára irányítja át. Az áldozat addig nem veszi észre az incidenst, míg nem lopják el a pénzét az internetbankból vagy meg nem változtatják a bejelentkezési adatokat és akár propaganda célokra fel nem használják mondjuk a közösségi oldalát.

7.1.3. Rootkitek

A rootkitek segítségével Windows operációs rendszereken rendszergazdai Linux alapú operációs rendszereken pedig root jogot szereznek. Ezekkel a jogosultságokkal képesek átvenni a számítógép felett az uralmat és bármit megtehetnek vele a támadók. Zombi hálózatot hozhatnak létre több egymáshoz kapcsolt számítógéppel, melyekkel célzott támadást hajthatnak végre vállalatok, bankok és kormányzati, infrastruktúrák ellen.

7.1.4. Ransomwarek

A kártevők egy másik fajtája képes a szímtógépen lévő állományok titkosítására, melyeket a támadók egy bizonyos összeg fejében feloldanak. Az áldozat számítóógépére került károkozó működésbe lépése után különös, szokatlan kiterjesztésű fájlokat fog találni, amik olvashatatlanok minden program számára. A felhasználó ilyenkor elveszíti minden adatát, ha a támadók a korábban említett, vagy más módszerrel eltulajdonították a felhasználó adaatait még a titkosítás előtt, akkor nem csak adatvesztés, hanem lopás is fennáll.

7.1.5. Trójai programok

A trójai programok, csalogató hasznos alkalmazásnak tűnnek, akár vírusírtó alkalmazásnak is kiadhatják magukat, ami nem végez vírusírtást vagy vizsgálatot, csak úgy viselkedik. Ebbe építenek be a korábban említett vagy más kártevőket, amik a program elindítása után a háttérben futnak. Szintén a megtévesztésre épít, hogy az áldozat a hamis biztonságérzete miatt nyugodtan elindítja és haználja az alkalmazást mit sem sejtve a valódi működéséről. Ezek jellemzően ellenőrizetlen hátterű szoftverek. Mobil alkalmazások között szintén sok példányban előfordul, amiket a felhasználók a telepítőfájl formájában egymásnak adnak.

7.1.6. Vírusok

A vírusok, ahogy a neve sugallja, gyorsan reprodukálódik és terjed, több fajtája létezik. Képesek beépülni egy programba és módosítani azt, majd további fertőzhető programokat és fájlokat, dokumentumokat keres a számítógépen, hálózaton, hogy újabb példányt készítsen magáról. Képes módosítani saját kódját, hogy a vírusírtók előtt rejtve maradhasson. Egy teljesen ártalmatlan e-mail formájában is képes bejutni a számítógépre, ahol megkezdi működését. Fajtái tekintve végrehajtható állományokba, vagy az operációs rendszer betöltéséhez szükséges boot szektorba is képes beírni magát, amivel a vírusírtó előtt képes elindulni, ha van ilyen a számítógépen. Ennek működését képes befolyásolni és észrevétlen maradni. Szkriptként vagy makroként is létezhetnek, melyek rendszerfájlokban, dokumentumokban, rejtőznek, fertőznek, és terjednek. Nem minden esetben történik tényleges rohngálás, ez a támadók céljától függ. Ilyen módszerrel feltérképezhető egy hálózat, nyomon követhetőek a felhasználók, vagy hozzáférst adhat a rendszerhez a támadó számára. Természetesen büntető funkciókat is elláthat, ekkor a cél, hogy a megbénuljon az áldozat számítógépe, hálózata.

7.1.7. Férgek

A férgek a vírusok egy fajtája, de nem szükséges számukra egy gazda fájl, melybe beépülnek. Felhasználói tevékenység nélkül képes terjedni, a kijavítatlan sérülékenységeket kihasználva.

7.2. Kártevők elleni védekezések

A kártevők elleni védekezéshez a korábban tárgyalt felhaználói attitűd transzformációján kívül, további alkalmazásokra is szükség van, valamint a rendszer biztonságát tovább növelhetjük vírusírtó alkalmazáson kívül, tűzfal, és különböző tartalomszűrő alkalmazással. A megfelelő vírusírtó, tűzfal és egyéb kártékony kódokat távoltartani és eltávolítani képes alkalmazások naprakészen tartása nem zárja ki teljesen a kártevők bejutását. Sajnos előfordulhatnak olyan esetek, hogy a vírusírtó alkalmazás által még nem ismert kártevőt nem azonosítja, vagy nem képes megállítani. A mai vírusírtó szoftverek kínálnak egyéb beépített szolgáltatásokat, melyekre nem mindig és nem mindenkinek van feltétlenül szüksége. A megfelelő szoftver kiválasztása komoly fejfájást tud okozni olyan felhasználók számára, akik nem rendelkeznek mélyebb ismeretekkel ezen a téren. Emiatt a leginkább javasolt módszer az, hogy vásárlás előtt tájékozódjunk. Az AV-TEST [11] Institute honlapján megtalálhatóak az összehasonlító tesztek, melyek alapján a legnagyobb pontszámot elért alkalmazást ajánlják a leginkább. A felhasználási környezet, operációs rendszer alapján is kiválasztható a megfelelő alkalmazás. Mindamellett a vírusírtó alkalmazások folyamatosan fejlődnek, ezért a helyezés folyton változik a listán. Természetesen nem jelenti azt, hogy folyton cserélni kell őket. Ahogy

korábban említettem a vírusírtó szoftverek szükségesek, de nem elégségesek. A National Cíbersecurity Alliance [12] által közzétett információk alapján általános felhasználás mentén haladva a legtöbb kártevő e-mail, reklám, nem hivatalos forrásból származó szoftverek, valamint USB eszközök csatlakoztatása esetén juthat a számítógépre. A megfelelő felhasználói magatartás ebben az esetben annyit tesz, hogy több e-mail fiókot használunk több különböző célra. Javasolt egy dedikált e-mail fiókot a hivatalos és fontos adatok használatára szánni, egy újabbat a különböző szolgáltatásokra fenntartani, egy újabbat pedig egyéb felületekre használni. A felhasználás csoportosítása egyéni preferencia lehetősége. Az elkülönített csoportosítás esetén a beérkező leveleket is könnyebben tudjuk azonosítani. Egy hivatalos vagy fontos levél nem érkezhet az egyéb célra fenntatott fiókba. Ha mégis találkozunk annak tűnő levéllel, akkor gyanakvásra adhat okot, vagyis kizárhatjuk annak lehetőségét, hogy megnyissuk a levélben szereplő csatolmányt vagy linket.

8. HOGYAN VÉDJÜK MEG AZ ESZKÖZEINKET

Adataink védelmének következő szintjét a megfelelő eszközök és szoftverek használatával erősíthetjük. Az adatok védelme nagy mértékben függ a létrehozásukra, feldolgozásukra, tárolásukra, továbbításukra, törlésükre használt hardverektől és szoftverektől is. A korábbi fejezetekben kitértünk a felhasználói viselkedésre, melyek veszélyt jelentenek az aktuális biztonság szintjére, ami egy állapot és folyton változik. Jelen fejezet a megfelelő eszköz választásra és kezelésre szorítkozik. Adataink biztonsága érdekében sokat tehetünk, ha megvizsgáljuk, hogy valóban milyen eszközökre és platformokra van szükségünk.

Vizsgáljuk meg, hogy az általános felhasználásra alkalmas 3 fő operációs rendszer a Microsoft Windows, a GNU/Linux alapú disztribúciók, és a Mac OS rendszere közül melyik képes kiszolgálni az igényeinket. Tökéletesen biztonságos rendszer nem létezik és minden feladatra alkalmas rendszer sem. Mindhárom rendszernek megvannak az előnyei és a hátrányai, azonban sokat segíthetünk, ha olyan rendszert használunk mely céljaink elérése érdekében a legkevesebb hátránnyal és a legtöbb előnnyel rendelkezik. Mindhárom rendszer különböző típusú, a Microsoft Windows és a Mac OS zárt rendszerű, a GNU/Linux alapú operációs rendszerek pedig nyílt forráskódú. A GNU/Linux továbbiakban Linux szabadon használható, terjeszthető, módosítható, melynek egyik nagy előnye, hogy a publikált szoftver forráskódját nem egy adott vállalat szakemberei fejlesztik, tesztelik, javítják, hanem egy hatalmas közösség, így bármely hiba esetén azt a közösség rugalmasabban és gyorsbban javítja, mint a zárt rendszerű operációs rendszerek esetében, ahol viszonylag kevesebb létszámú, megadott ütemtervhez között fejlesztői csapat végzi el ugyanezt a feladatot. Hátránya viszont, hogy könnyebb sérülékenységet találni a rendszerben, mert ismert a forráskódja. A zárt rendszerű operációs rendszereknek viszont az a nagy előnye, hogy nem ismert a rendszer forráskódja, ezért a kihasználható sérülékenységek keresése másképp zajlik, mint a Linux esetében. Ahogy tökéletes rendszer, úgy tökéletes hardver sem létezik a hibák és sérülékenységek folyamatosan kerülnek elő, melyeket a frissítések telepítésével javíthatunk.

8.1. A kibertér eszközei

A korábban említett Muha Lajostól származó informatikai rendszer definíciója [3] alapján a felhasználó és a rendszert kiszolgáló személyekkel foglalkoztunk. Most viszont térjünk át az eszközök és eljárások témakörére.

Jelen dolgozat a magánszférára, annak eszközeire és segítségükkel igénybe vett szolgáltatá-sok veszélyeire koncentrál. A COVID-19 okozta pandémia és lezárások miatt megnövekedett igény mutatkozott az online oktatás és home office használatára. A háztartásokban használt SOHO (Small Office Home Office rövidítése) hálózatokra

ugrásszerűen megnövekedett teher nehezedett, mint korábban. A hálózat és sávszélesség kihasználtsága növekedett, a támadások száma ezzel arányosan növekedett. Emiatt az információbiztonság ISO/IEC 13335 szabványban használatos CIA modell, mint az információbiztonság három alappillére a bizalmasság, sértetlenség, rendelkezésre állás (az angol rövidítések kezdőbetűi után nevezték el **CIA** elvnek. **C**onfidentality: bizalmasság, **I**nregrity: sértetlenség, **A**vailability: rendelkezésre állás) alapján ezek a SOHO hálózatok és a csatlakoztatott eszközök által kezelt adatok biztonságának, hatékonyságának növelése elkerülhetetlen. A hirtelen jött tömeges home office miatt azok a vállalatok, melyek nem voltak felkészülve a biztonságos távmunka lehetőségére, nem álltak rendelkezésre naprakész szabályok, a belső hálózat kívülről történő elérésének lehetősége, a jogosultsági koncepció, távmunkára vonatkozó működési szabályzat, biztonsági oktatások, sőt sok esetben eszközök. A támadóknak így lehetősége nyílt az otthonról dolgozó alkalmazottak hálózatán keresztül megtámadni a kevésbbé felkészült vállalat hálózatát. Ebben az időben elszaporodtak a zsarolóvírusok és az adathalász e-mailekkel történtő támadások. A tömeges e-mail küldések során a támadókank lehetőségük van például a házon kívüli értesítések által visszaküldött e-mailek fejlécének elemzésésvel a levelezőrendszerre vonatkozó információkat összegyűjteni és további támadásokat indítani. A fokozódó mértékű támadások miatt egyre szükségesebb az otthoni hálózat minden elemének biztonságának fokozása.

8.2. Számítógépünk védelme

Minden személyi használatra szánt asztali vagy hordozható számítógéphez szükség van egy operációs rendszerre. Jelenleg nincs olyan operációs rendszer, amihez ne tartozna valamenyni sérülékenység, melyeket kihasználhatnak a támadók, mindamellett a szoftvergyártók azon dolgoznak, hogy az újabb és újabb sérülékenységeket minél gyorsabban kijavítsák. Ma a legelterjedtebb a Microsoft Windows operációs rendszere, emiatt csak erre a rendszerre térek ki. A Microsoft is rendszeres időközönként közzéteszi a legújabb frissítéseket, melyek nem csak új funkciókat jelentenek a felhasználók számára, hanem sérülékenységek és egy hibák javítását is. Az átlagos felhasználásra szánt Windows esetén nincs lehetősége a felhasználónak megtagadni a frissítés telepítését, esetleg késleltetni azt. Ezzel a gyártó igyekszik automatikus módon javítani a hibákat. A magasabb szintű biztonság érdekében a felhasználóknak is javallott alkalmazni néhány védelmi intézkedést, amivel megnehezíthetik a támadók munkáját. Természetesen tökéletesen védett és biztonságos rendszer nem létezik.

A kártevők elleni védekezés nagy részét a vírusírtó ellátja, erre még később visszatérünk, viszont vannak olyan jellegű támadások, melyeket nem feltétlen észlel a vírusírtó szoftver. A BeEF vagyis a Browser exploitation Framework segítségével a böngészőn keresztül támadja a számítógépet, amin kiaknázható sérülékenységeket keres,

vagy figyelheti a billentyűleütéseket, amivel jelszavakat szerezhetnek. Vagy a Rubber Ducky nevű eszköz, ami egy USB Pendrivenak tűnő eszköz, biszont nem háttértárként észleli a számítógép, hanem billentyűzetként. Csatlakoztatás után azonnal egy előre beprogramozott folyamat zajlik le, ami lehet egy parancssor megnyitása, parancs lefuttatása, böngésző mgegnyitása, ami egy adott fertőzött oldalt megynyit, aminek segítségével távolról hozzáférhetnek a támadók a számítógéphez.

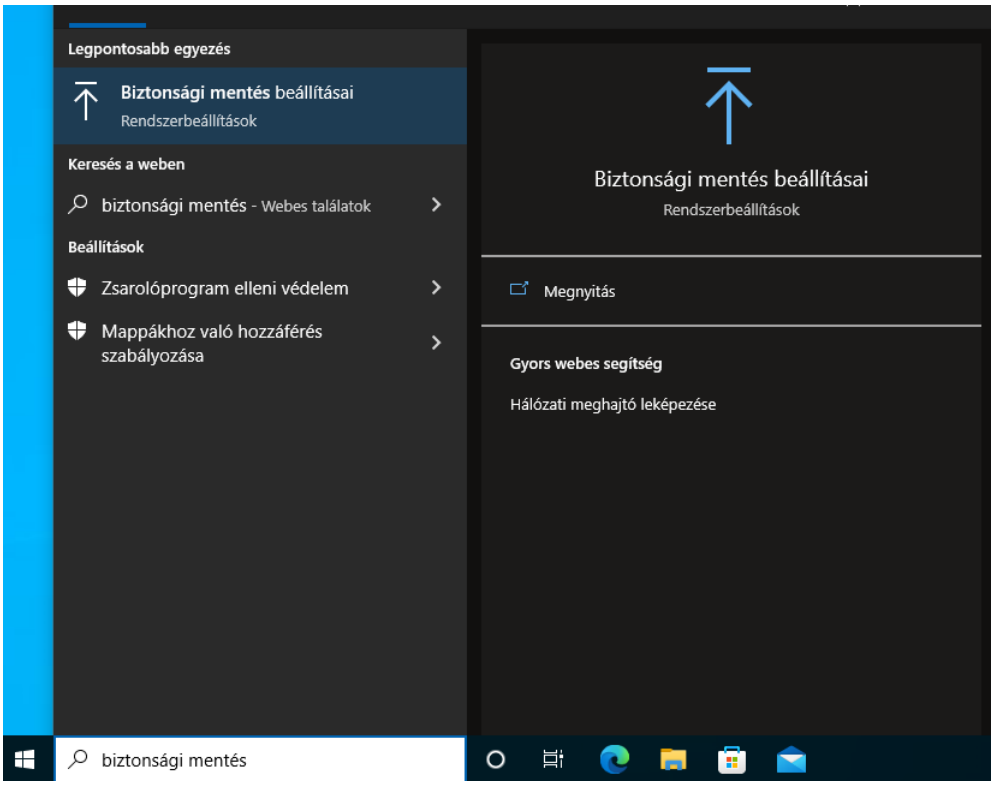
A tűzfallal lehetőség van az internet felől érkező kapcsolódásokat blokkolni, viszont a korábban említett támadás ellen nem véd csak a tűzfal és csak a vírusírtó. Ezért érdemes a következő lépéseket megtenni:

- Mindig a legfrissebb operációs rendszert és alkalmazásokat használjuk
- A szoftvereket csak hivatalos forrásból szerezzük be.
- Használjunk hivatalos forrásból származó vírusírtó alkalmazást, tűzfalat.
- Ne rendszergazda jogosultsággal használjuk a számítógépet, arra tartsunk egy külön usert, amely csak a minimálisan szükséges jogosultsággal rendelkezik.
- Ne jelentkezzünk fel a készülékkel nyilvános Wi-fi hálózatra.
- Új eszköz csatlakoztatás engedélyezését kössük adminisztrátori jogosultsághoz.
- A parancssor indításának lehetőségét kössük jelszóhoz.
- PowerShell kikapcsolása. A Windows-szolgáltatások program start menüből történő elindítása után a Windows PowerShell 2.0 melletti jelölőnégyzet kitörlése.
- Használjunk jelszókezelő alkalmazást, erre a későbbiekben kitérünk
- A Bitlocker lemeztitkosítást aktiváljuk.
- Rendszeresen végezzünk biztonsági mentést, erre szintén kitérünk a későbbiekben.

8.3. Biztonsági mentés készítése Windows 10 rendszerhez

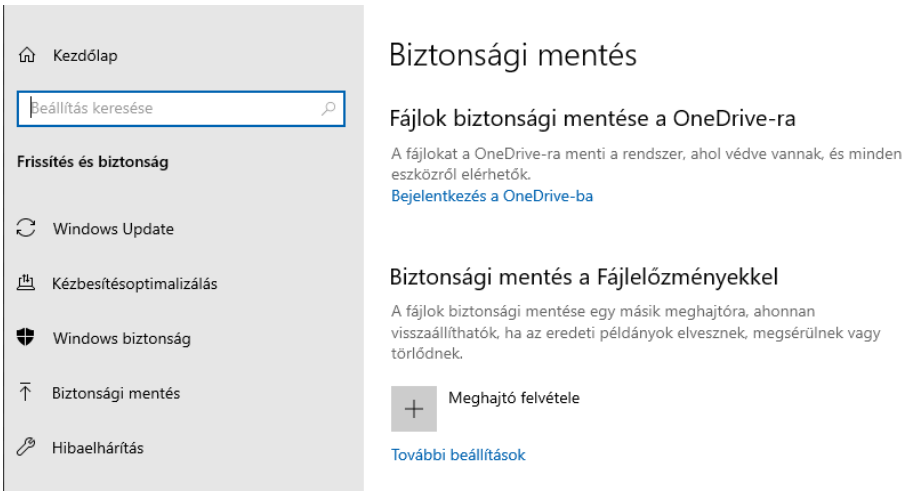
A Microsoft Windows 10 rendelkezik saját beépített biztonsági mentés készítő alkalmazással, így nem szükséges harmadik féltől származó szoftvereket vásárolnunk. Ezzel a lehetsőséggel élve a költségek csökkenthetők, mindamellett a biztonsági mentés elkészítéséhez szükség van egy megfelelő kapacitással rendelkező tárolóra, ami csak a mentés idejéig van a számítógéphez csatlakoztatva. Készítettem egy útmutatást, amit követve elkészíthető a mentés. Mielőtt elkezdjük a mentés konfigurálását, csatlakoztassuk a tárolót. Fontos megjegyezni, hogy a mentések tárolására használt meghajtó üres legyen.

1. A Start menü kereső mezőjébe írjuk be a biztonsági mentés szót, majd válasszuk ki a Biztonsági mentés beállításai opciót:



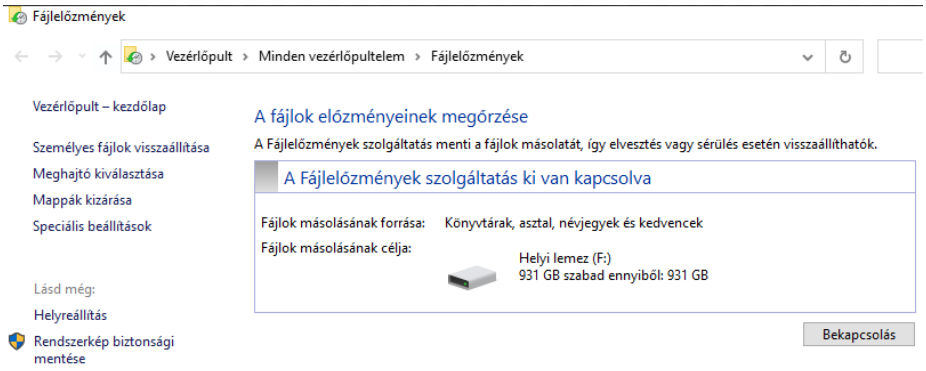
8.4. ábra. A biztonsági mentés beállításait ezen keresztül érhetjük el

2. Válassszuk ki a További beállítások opciót:



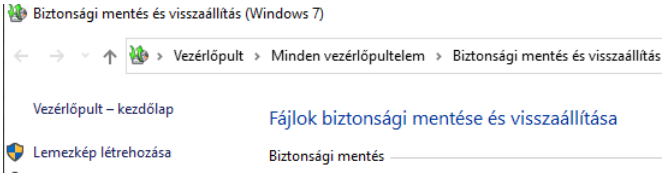
8.5. ábra. Itt a mentések tárolásának kiválasztása lehetséges

3. A Rendszerkép biztonsági mentése funkciót válasszuk ki:



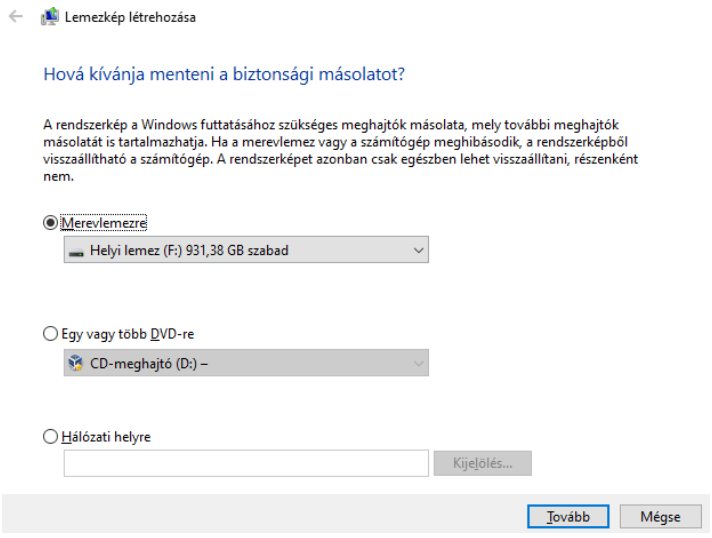
8.6. ábra. A mentéshez használható tárolók listája

4. A lemezkép létrehozása opciót válasszuk ki:



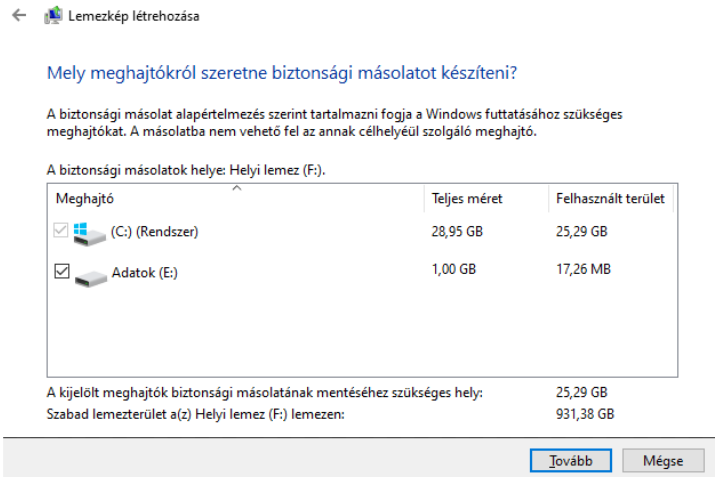
8.7. ábra. A lemezkép segítségével visszaállítható a teljes rendszerünk

5. Adjuk meg a mentés helyét:



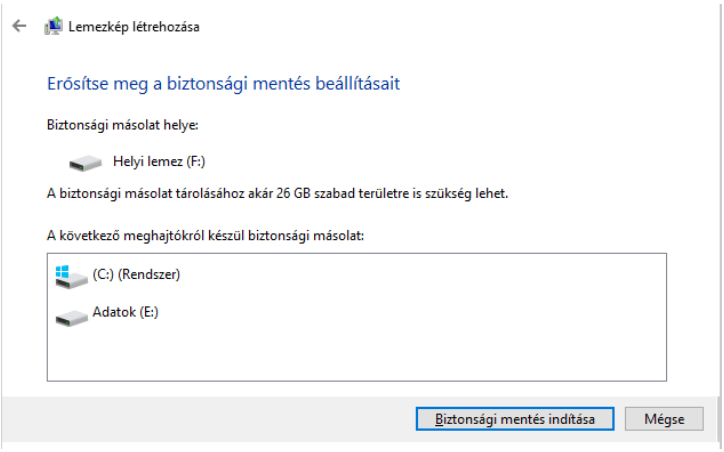
8.8. ábra. A megadott helyre kerülnek az adatok

6. Adjuk meg, hogy melyik meghatjóról szeretnénk mentést készíteni:



8.9. ábra. Jelöljük ki azokat a meghatjókat, amiről készüljön mentés

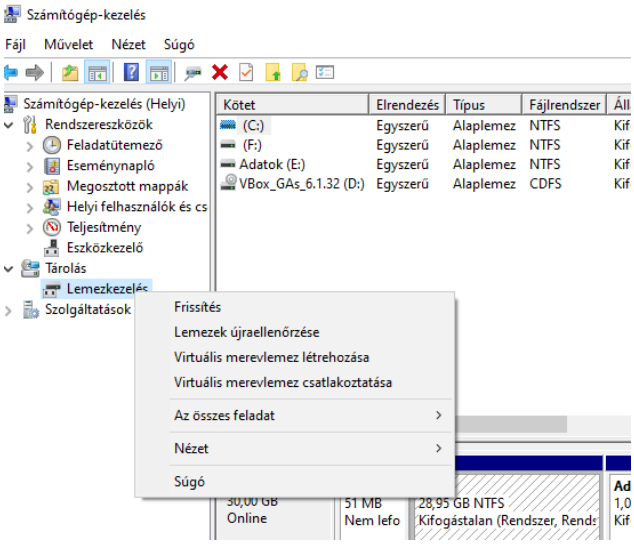
7. Az összesítő ablak látható, innen 1 kattintással indítható a mentés:



8.10. ábra. Jelöljük ki azokat a meghatjókat, amiről szeretnénk mentést

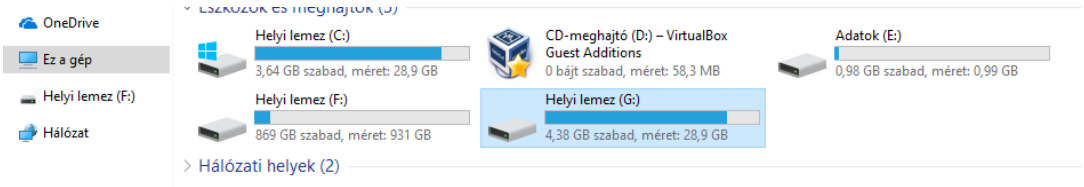
A mentést tesztelhetjük úgy, hogy felcsatoljuk a lemezképet, mint egy meghajtót. Ezt a lemezkezelő felületen tehetjük meg:

Az összesítő ablak látható, innen 1 kattintással indítható a mentés:



8.11. ábra. A virtuális merevlemez csatlakoztatása opcióval hozzáadható a mentés

A csatlakoztatott lemez mérete és kihasználtsága megegyezik a mentésről készített meghatjóval. Tallózva a tartalmát megnyithatjuk a mentett fájlokat. Ha sikeresen, hiba nélkül megnyitottuk a fájlokat, az azt jelenti, hogy a visszaállítás esetén is használhatóak lesznek.



8.12. ábra. A mentést tartalmazó meghajtó

8.4. Mobil eszközeink védelme

A mai okostelefonok teljesítménük alapján mini számítógépeknek számítanak, szintén futtatnak valamilyen operációs rendszert, amiknek szintén létezik sérülékenységük. Ezek javítását az operációs rendszer gyártója folyamatosan végzi különböző frissítések keretében. Mindazonáltal az összes sérülékenység javítása ebben az esetben sem lehetséges, ugyanis a számítógépekhez hasonlóan egyes sérülékenységek a beépített hardverekre vonatkoznak, más sérülékenységek javítás következtében elveszítheti funkcióinak részeit. Ez jelentheti azt, hogy nem lenne alkalmas SMS küldésre és fogadásra, vagy más jellegű kommunikációra, mivel egyes támadáshokhoz elegendő a támadó kód elküldése SMS-ben, ahogy az elhíresült Pegasus botrányban is megtörtént. Más esetekben e-mail útján képesek fertőzni a készüléket. Többek között a korábban említett BeEF szintén alkalmas erre. Ez természetesen nem jelenti azt, hogy ne lenne szabad ilyen készülékeket

használni, csupán javasolt a gyártó által nyújtott biztonsági funkciókat aktiválni, valamint néhány biztonsági intézkedést érdemes betartani.

- Mindig a legfrissebb operációs rendszert és alkalmazásokat használjuk
- A szoftvereket csak hivatalos forrásból, a gyártó alkalmazás boltjából szerezzük be.
- Használjunk hivatalos forrásból származó vírusírtó alkalmazást.
- Ne használjunk olyan készülket, ami Android esetén rootolt, iPhone esetén Jailbreakelt, vagyis rendszergazda jogosultsággal rendelkezik minden alkalmazás és felhasználó.
- Ne jelentkezzünk fel a készülékkel nyilvános Wi-fi hálózatra.
- Alkalmazzuk a képernyőzárat minél bonyolultbb jelszó kombinációval, vagy a biometrikus azonosítással.
- Aktiváljuk a gyártó által nyújtott titkosítási funkciót.
- Használjunk jelszókezelő alkalmazást, erre a későbbiekben kitérünk
- Rendszeresen végezzünk biztonsági mentést, erre szintén kitérünk a későbbiekben.

8.5. Informatikai eszközök felhasználói életciklusa

Az informatikai eszközeink életciklusa 3 részre osztható fel. Az első, mely során, bizonyos szempontok alapján kiválasztjuk a használni kívánt eszközt. A kiválasztás során az ár, a teljesítmény, egyéb funkciók és szolgáltatások játszanak túlnyomó szerepet. Az eszközök adatlapján, elhanyagolható mennyiségű információt találunk a biztonsági funkciókról. Az eszközök tervezése, gyártása során még nem észlelt biztonsági sérülékenység későbbi javításának lehetősége limitált. Ennek javítását a gyártók a teljesítményvesztés, valamint a hozzá tartozó presztízsvesztés miatt nem mindig vállalják. A sérülékenységek létezését, valamint kihasználásának módjának ismeretével a sikeres támadások esélye növelhető. A második terület az eszköz konfigurációja, használata. Ez idő alatt a fenti ”beépített” sérülékenységek kihasználása történhet meg. Ha a felhasználó nem gondoskodik megfelelően az eszköz megfelelő bitonságáról, mint megfelelő Operációs rendszer, felhasználói jogosultságok, tűzfal, vírusírtó, szoftverek, lemeztitkosítás, VPN és egyéb biztonsági szolgáltatások használatáról, a támadások sikeressége és a kiaknázható veszélyforrások miatt megnő az adatszivárgás és adatvesztés lehetősége. A harmadik rész az eszközök leselejtezése, tovább értékesítése. A leselejtezett eszközök tartalmazhatnak személyes, szenzitív adatokat. Több olyan hírrel is találkozhattunk, hogy új pendrive megvárálása után a pendrive tartalmazott adatokat. Az alkatrészek újrafelhasználása esetén előfordulhat, hogy nem inicializálják annak tartalmát. A továbbérétkesítés esetén szintén problémát jelent az eszköz nem megfelelő alaphelyzetbe állítáaa. Az új tulajdonos ebben az esetben az eszközön kívül az adatokhoz is hozzájuthat.

8.6. Papír alapú adatok veszélyforrássai, védelme

Adataink eltulajdonításához nem feltétlen van szükség intormatikai eszközre, internet hozzáférésre. Rendkívül sok adatra lehet bukkani az úgy nevezett kuka búvár módszerrel, melyet Kevin Mitnick sikeresen alkalmazott és a többek között a Hack and Stack című könyv is bemutat [13]. Gondoljunk bele milyen papírokat dobunk ki a szemétbe, azokon mennyi adat szerepel. Olyan adatokat, melyek segítségével egyértelműen azonosítható egy személy vagy, ezek segítségével elérhetővé válik az azonosításra használható adat, ezeket személyes adatoknak nevezzük. Szinte mindenkivel előfordult már, hogy kidobott a szemétbe egy olyan papírt, melyen szerepelt a neve, címe, telefonszáma, e-mail címe. A postán vagy futár szolgálaton kersztül érkező csomagok külső csomagolásán ezen adatok kivétel nélkül szerepelnek. Ugyanez az eset előfordul, ha régi saját névjegykártyát, dobunk a szemetesbe. A papír alapú lejárt, régi közüzemi számláink kötelező megőrzési időn túl szintén a szemetesben landolnak. Ezeken már partnerszámok és egyéb fontos azonosításhoz szükséges adatok is megtalálhatóak. Lejárt, kiváltatlan orvosi receptek a kukában szintén potenciális veszélyforrások. Egy olyan személy szemetesében ügyesen kiválogatott az egyén számára hulladéknak tűnő papírkötegből annyi személyes adatot lehet összegyűjteni, mellyel akár telefonon keresztüli megszemélyesítés vagy egyéb támadás áldozata is lehet. A kinyerhető adatok mennyisége és minősége nagyban függ attól, hogy ki mennyire figyelmesen semmisíti meg ezeket a nem szükséges iratokat. Ahogy már korábban hivatkoztam Oroszi Eszter dolgozatára [4], a vállalati adatok kezelésének szerves része a papír alapú szenzitív adatok megsemmisítésének egyértelműen definiált folyamata. Ahogy egy vállalat esetében úgy magánszemély esetén is egyaránt fontos tényező.

Személyes tapasztalatom, egyike volt, mikor egy barátom figyelmét felhívtam a lomtalanítás alkalmával gondatlanul kidobott papírok veszélyére. Állításom bizonyításaként, természetesen az Ő beleegyezésésvel sikerült ilyen módszerrel több helyen egyetlen telefon segítségével meglévő szolgáltatást módosítanom és új szolgáltatást megrendelnem. A beazonosításhoz mindössze az Ő nevére, születési idejére, helyére és édesanyja nevére volt szükségem. Szelektív hulladékgyűjtők esetében nagyobb sűrűséggel találhatóak olyan papírok, melyek tartalmaznak szenzitív vagy személyes adatokat.

Az ilyen jellegű adatszivárgás megelőzésére időt kell fordítanunk. Számunkra jól átláthatóan rendszerezetten tároljunk olyan papírokat, melyek tartalmaznak szenzitív, személyes adatot. Figyelmesen vizsgáljuk meg, hogy felismerjük, milyen papírokat kell külön kezelnünk a többitől. Egy idő után szokássá válik, melynek lesz egy olyan pozitív mellékhatása, hogy minden iratunkat rendszerezett tároljuk és mindig megtaláljuk, ha szükség van rájuk. A korábban említett barátomnak javasoltam az általam használt módszert. Természetesen ehhez is, mint minden biztonsági intézkedéshez szükség

van erőforrásra, jelen esetben időre. Minden olyan részt mechanikusan eltávolítok a papírról, melyen a korábban említett szenzitív jellegű adat megtalálható. Az eltávolított részek kisebb helyet foglalnak, melyeket útján semmisítek meg. A megmaradt részeket, melyek nem tartalmaznak olyan információkat, amivel beazonosítható vagyok az iratmegsemmisítővel feldarabolom, majd a szelekítv gyűjtőbe helyezem. Ezzel jelentősen csökkenthető az adatszivárgás.

Ugyanígy a lejárt bankkártyákat, hűség és egyéb plasztikkártyákat a kibocsátó szolgáltató átal az Általános Szerződési Feltétlekben leírt módon átveszi és megsemmisíti. Ha nem találunk erre vonatkozó leírást a mágnescsíkot, valamint a chippet és a kártya felületén szereplő adatok különválasztásával megsemmisíthetjük. Aktív normál és érintésmentes fizetésre alkalmas bankkártyákat minden esetben tároljuk rádiójelek blokkolására alkalmas tokban, melyeket néhány centért rendelhetünk interneten keresztül. Ezzel megakadályozhatjuk, hogy a kártyánkat illetéktelenek klónozzák és használják. Az utcán sétálva, vagy tömegközlekedési eszközön a támadóknak lehetőségük van olyan közel kerülni az áldozathoz, hogy az érintésmentes fizetésre alkalmas bankkártyáját lemásolják. Kivédése a fentebb említett tokozással eszközölhető. Ha fizetés esetén át kell adnunk a kártyát, minden esetben figyeljük a kártyát és kérjük meg a pénztárost, hogy jól látható helyen hajtsa végre a műveletet.

8.7. Elektronikusan tárolt adatok veszélyforrásai, védelme

Adataink tárolása már jó ideje eltolódott a papírlapú megoldásoktól az elektronikus megoldások irányába. Már hivatalos ügyeket is könnyedén intézhetünk az internet segítségével. Az elektronikuan tárolt adatok esetében is rengeteget tehetünk azért, hogy az adatszivárgást a lehető legkisebb mértékűre csökkentsük. A vállalati infrastruktúra esetében meghatározott szabályokat betartva dolgozhatunk az adatokkal. Ebben az esetben többek között a jogosultságokkal szabályozzák az adatokhoz való hozzáférést. Egy jól definiált jogosultsági koncepció az adott vállalat működését hatékonyan támogatja. Erre lehet egy példa: a lehető legkevesebb jogosultságot megadva a felhasználóknak, amivel még képesek ellátni a feladataikat. Ha az otthoni hálózatunk és eszközeink esetén nem létezik jól definiált szabály, melyet alkalmazva az adataink és eszközeink biztonságos kezelése megoldott, abban az esetben a hibalehetőségek, betörés és támadás okozta adatvesztés és adatszivárgás esélye magas. Több különböző sérülékenység kihasználásával, egymásba ágyazásával több lehetőségük van a támadónak elérni a céljukat. Egy példa, ha a SOHO routerünk konfigurációját portjait és alapértelemzett autentikációs azonosítóit, valamint a hozzá tartozó jelszavakat nem módosítjuk vagy tiltjuk le, könnyen a belső, védett hálózatunkhoz hozzáfér a támadó, mellyel minden eszközünket a saját céljaira használhat fel. A bejutás egyszerű, több erre a célra fejlesztett és használható nyílt forráskódú, tehát bárki számára elérhető programmal könnyedén végrehajtható ez a fel-

adat, mivel ezek használatáról ugyancsak megtalálhatóak leírások, amik lépésről lépésre mutatják be az eszközök haszná-latát. Természetesen a megoldáshoz ebben az esetben nem elegendő a fent javasolt nem használt portok letiltása, konfiguráció módosítása és az azonosító jelszó párok módosítása. Ahogy a vállalati IT rendszereknél, úgy az otthoni felhasználás esetén is jó megoldás többek között a mélységi védelem kialakítása, mely a védelmet nem egy határra helyezi, nem egyetlen eszközre vagy szolgáltatásra bízza, hanem minden eszközünknek rendelkeznie kell a lehető legnagyobb védelemmel, mely nem gátolja a használatuk segítségével elérni kívánt szolgáltatások minőségét jelentős mértékben. Ebben az esetben elkerülhető annak a lehetősége, hogy perimeter védelem esetén alkalmazott megoldás kiesése esetén védtelenné válik a hálózatunk, minden eszközünk és adatunk a támadókkal szemben. Így akár az adataink feletti kontroll is átkerülhet máshoz, emiatt fontos, hogy az otthoni vagy átlagos felhasználásra szánt környezet is rendelkezzen az elektronikus adattárolás esetén több biztonságos lehetőséggel. Általában a saját PC-nk háttértárolóján történő tárolás, külső tároló egység (USB HDD/SSD, Pendrive, CD/DVD, NAS), valamint a felhőszolgáltatás a jellemző. Az ipari környezet számára elérhető eszközöket most nem sorolom be egy kategóriába sem. Minden esetben számolhatunk előnyökkel illetve hátrá-nyokkal. Ezeket a későbbi szemeszterek során fejtem ki.

8.8. Adatok tárolása, kezelése, biztonsági mentése

Digitális önvédelmünk érdekében érdemes rendet tartanunk az eszközeinken, így fel tudjuk mérni, hogy mik a fontos és kevésbbé fontos adatok. Mindenkinek vannak olyan adata, fájljai, képek, videók, dokumentumok, stb., melyek elvesztése esetén azok pótolhatatlanok lennének. A biztonsági mentések mindig idő és költségigényes feladatok, azonban az első káresemény esetén megtérül a ráfordított idő, pénz és energia. Adataink elvesztése, megsemmisülése számtalan okból megtörténhet, ezek lehetnek például az eszközünk tároló egységének meghibásodása valamilyen fizikai behatás (vilámcsapás, tűz, víz, hardverhiba, természeti katasztrófa), hacker támadás, vírusok, ransomwarek, egyéb malwarek, valamint felhasználói hiba következtében. Mivel ezek bármikor megtörténhetnek, ezért kijelenthetjük a veszélyek függvényében, hogy adat addig nem is létezik igazán, míg nincs belőle legalább két példány.

Nagyon fontos, hogy számunkra jól struktúrált hierarchiában tároljuk adatainkat. A jól felépített könyvtárszerkezet kevesebb helyet foglal, mert a felesleges és nem szükséges állományokat nem tartalmazza, ezzel elkerülhetjük, hogy feleslegesen foglalják a tárolót és ne növeljék a biztonsági mentések méretét. Ennek egy pozitív oldala, hogy a számítógépen végzett tevékenységünk is hatékonyabbá válik, mert nem kell felesleges időt töltenünk egy használni kívánt állomány keresésével. Továbbá érdemes az adatainkat az operációs rendszertől elkülönítve tárolni egy második partíción, jobb esetben külön merevlemezen. Adatok, kezelésére, tárolására, megosztására számos lehetőség

közül választhatunk. A technikai fejlődésnek köszönhetően elterjedtek az elérhető árú hatalmas, akár több TB kapacitású tárolók. Egy mai átlagos otthoni felhasználásra szánt PC, NAS (Network Attached Storage) is rendelkezik ezzel a kapacitással, mindamellett a költséghatékonyság figyelembe vételével sok esetben elegendő lehet egy vagy két darab külső SSD vagy merevlemez, amin tárolhatjuk a biztonsági mentéseinket. A növekvő tárhelyre a szintén növekvő igény miatt volt szükség. Ezeken az eszközökön tárolt adatok mennyisége miatt a felhasználóknak a biztonság eléréséhez szükségük van egy koncepcióra. Egy jól definiált koncpeció segítségével hatékonyabban, biztonságosabban felhasználható a rendelkezésre álló tárterület. A legegyszerűbb és legolcsóbb megoldás, ha adataink terjedelmének megfelelően egy üzletben vásárolható egyszerű külső merevelemzre elkészítjük a fontosabb adatainkról a biztonsági mentést.Minél több adat biztonságáról kell gondoskodnunk, az annál nagyobb költséggel jár. Az adatok tárolásának veszélyeit és biztonsági kérdéseit két területre osztottam, melyeket a következő fejezetekben részletezem. Az első a papír alapon történő adattárolás és kezelés, a második az elektronikusan tárolt adatok.

8.8.1. Biztonsági mentések készítése

Számtalan stratégiát választhatunk biztonsági mentésként például:

- Online, ami lehet egy távoli kiszolgáló pl_: Google Drive, Microsoft OneDrive, Mega, iCloud számtalan egyéb szolgáltató közül választhatunk ingyenes és fizetős tárolókapacitást, ahova szinkronizálhatjuk adatainkat. Bár ebben az esetben az adatok feletti teljes kontroll nem a felhasználónál, vagyis nálunk lesz. Ez azt jelenti, hogy nem tudhatjuk, hogy pontosan mi történik az adatainkkal, ha egy támadó megszerzi a hozzáférésünket ezekhez a szolgáltatásokhoz. Kényelmes, de nem teljesen veszélytelen.
- Offline, amikor fontos adatainkról egy külső tárolóra készítjük a biztonsági másolatot. Ilyenkor az adatok feletti kontroll nálunk van, az online mentéssel ellentétben itt annyi példányban fog létezni a mentés, ahány példányban elkészítjük. Ha megsérül a mentés és nincs több példány belőle, szintén adatvesztés történik. Az online tárolt biztonsági mentés esetén az adatok több példányban, több helyen is léteznek, melyek földrajzilag is el vannak osztva. Emiatt nem vesszük észre, ha a szolgáltatónál meghibásodik néhány tároló. A meghibásodás és kártékony kóddal történő megfertőződés csökkentésének érdekében offline mentést olyan eszközre készítsünk, amit csak a mentés idejére csatlakoztatunk a PC-hez.
- Offline mentés több példányban, több helyszínen tárolva lehetőségünk van megakadályozni az adatvesztést, ha bármilyen ok miatt megsérül vagy működésképtelen lesz egy tároló. Ebben az esetben az adatok több példányban léteznek, több tárolón, de más helyszínen, elkülönítve őket egymástól. Azonban ez a megoldás több

időt vesz igénybe és több munkával is jár, mivel ebben az esetben a tárolókat el is kell szállítani, illetve a tartalmukat is figyelemmel kell követni. A mentéseket ráadásul nem elég csak elkészíteni, tesztelésre is szükség van. Ha nem teszteljük, hogy vissza tudjuk-e állítani a mentésből az adatokat, akkor nem lehetünk biztosak benne, hogy van biztonsági mentésünk van vagy egy halom értelmezhetetlen adat, amivel nem tudunk mit kezdeni.

A mentéseket elkészítésére rengeteg szoftvár áll a rendelkezésünkre, melyekkel akár ütemezetten is elkészíthetjük a mentéseket. A tesztelés mellett a másik fontos szempont a titkosítás. A mentéseket lehetőségünk van titkosítani, amivel elkerülhetők az illetéktelen kezekbe jutása esetén az adatok kiszivárgása. Erre számos eszköz létezik, a mentést készítő szoftverek nagy része képes titkosítani az adatokat. A Windows beépített biztonsági mentés készítő szftvere is nyújt erre lehetőséget.

9. OTTHONI HÁLÓZAT VESZÉLYEI BIZTONSÁGA

Ebben a fejezetben néhány az otthoni hálózatunkhoz csatlakoztatott eszközök és maga a hálózat veszélyeire hívom fel a feigyelmet. Egyes jellemző általános veszélyforrások a megfelelő konfigurációval és magatartással kizárható. Mielőtt bármilyen biztonsági beállítást módosítunk, mindenképp készítsünk biztonsági mentést a konfigurációról, így lehetőségünk van visszatérni a kiinudlási állapothoz. Így biztonsak lehetünk benne, hogy nem zárjuk ki magunkat a saját rendszereinkből.
Összehasonlítva egy átlagos otthoni hálózatot egy átlagos multinacionális vállalat hálózatá-val, különös tekintettel a hálózatbiztonságra, amit utóbbi esetén hatalmas költségek befektetésével terveznek és építenek ki szakemberek, mely az előbbi esetében nem mondható el. A vállalatoknál a legmodernebb ipari környezetbe szánt switchek, routerek, tűzfalak, IDS / IPS-ek, biztonsági szabályzatok ellenére is hallhatunk sikeresen végrehajtott hacker támadásokról. Az átlagos otthoni hálózat védelmét jellemzően egy ISP modem látja el. Ez az eszköz tölti be a router, a switch, a vezeték nélküli hálózat és tűzfal szerepét. Emiatt az eszközök operációs rendszerének naprakészen tartása, az adott típus ismert sérülékenységeinek kijavítása, folyamatos monitorozása rendívül fontos. 2019-ben a Cable Haunt nevű sérülékenység csak Európában több millió modemet érintett. Ennek kihasználása során a támadók képesek távolról kódok futtatására WebSocket kapcsolaton keresztül, miután az áldozatot egy rosszindulatú JavaScript kódot futtató weboldalra csalják. Ezt követően puffertúlcsordulást elérve a támadó hozzáférhet a modemhez a böngészőt futtató számítógép biztonsági mechanizmusait megkerülve DNS újrakötési támadást hajtanak végre [14]. Ezen kívül számtalan módszer létezik, mint pl: WPS elleni támadás, router konfiguráció felhőben tárolása, uPnP szolgátatás kihasználása. Azonban a gyártói oldalról az eszközök operációs rendszerének frissítését idővel leállítják és a készülék ettől a ponttól és a készülékkel kapcsolatos sérülékenység, ki nem javított hiba nyilvánosságra kerülésétől már nem tekinthető biztonságosnak az eredeti állapotában. Számos Open Source megoldás létezik, melyek Linux alapú operációs rendszerrel helyettesíti a gyárit. Ezek közül az Open-WRT és DD-WRT, erősebb hardver esetén a pfSense, RouterOS alkalmas a feladatok további ellátására. Az otthoni hálózat biztonsági fenyegetettségét 4 területre felosztva mutatom be, melyek a publikus hálózatról, internet felől érkező támadások, a hálózatra csatlakoztatott eszközök, a vezeték nélküli hálózat, és a munkahelyi hálózati kapcsolat.

9.1. Publikus hálózat felől érkező támadások

Minden internet kapcsolattal rendelkező SOHO hálózat kap az ISP-től egy publikus IP címet. A támadók ezeket a publikus IP címtartományokat monitorozzák. Ha az ISP modem válaszol a PING kérésre, abban az esetben nagy eséllyel alapbeállítással vagy helytelen konfigurációval ellátott modemet találtak. Ebben az esetben a 65536 TCP

és 65536 UDP port közül megkeresik, hogy melyik nyitott WAN irányban. További támadási felületet adhatnak pl távoli menedzsment funkción keresztül történő belépés, WAN irányba történő kommunikáció engedélyezése a hálózatra csatlakoztatott babaőr, vagy IP kamera, robotporszívó és egyéb eszköz használatához. Az IP kamerák, hálózati eszközök távoli menedzsment felület elérése, valamint alapértelmezett autentikációs adatok hatalmas veszélyt jelentenek.

9.2. Belső hálózatra csatolakoztatott eszközök veszélyei

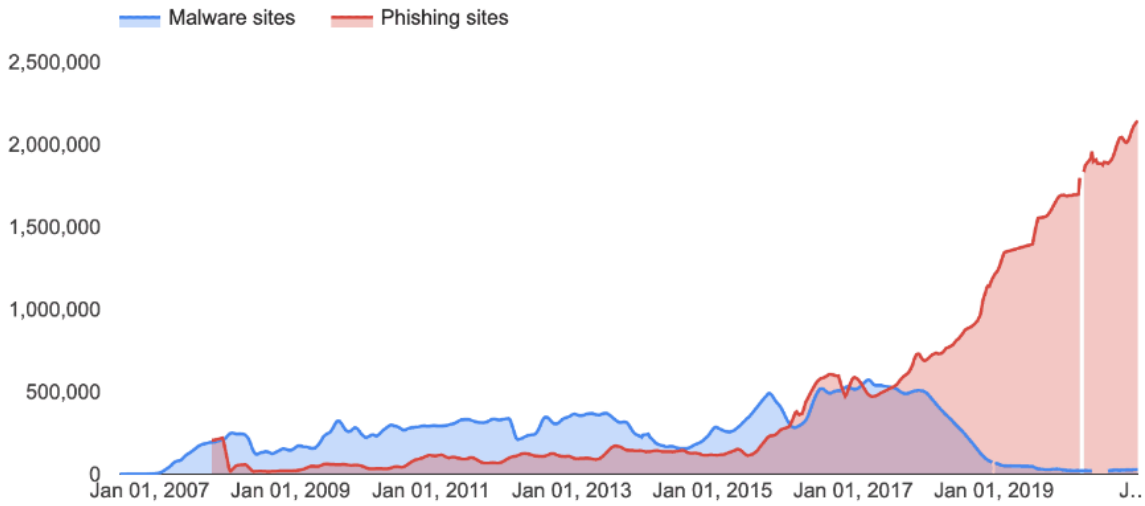
A belső hálózatra csatlakoztatott eszközök általában egy hálózatra vannak kapcsolva, melyek között előfordulhat ismeretlen, nem megbízható gyártótól származó IoT eszköz (okos LED izzó, okos kapcsoló, okos porszívó, stb., mely egy számunkra ismeretlen szerverrel kommunikál firmware letöltés, vagy kommunikáció létesítése a mobil készüléken található alkalmazással. Az eszközzel kapcsolatban álló ismeretlen távoli szerver szerepét átveheti egy támadó, mely az eszköz által letöltött módosított firmware segítségével a belső hálózathoz hozzáférhet.

9.3. Vezeték nélküli hálózat veszélyei

A vezeték nélüküli hálózat SSID azonosító alapértelmezett beállítása esetén a támadónak lehetősége van a router gyártója és típusa azonosítására, majd a típussal kapcsolatos sérülékenységek, alapértelmezett azonosítók után kutatva az interneten ezek ellen támadás indítása.

9.4. Munkahelyi hálózat felől érkező támadás

A jelenlegi vírushelyzet szülte hirtelen átállás távmunkára feladta a leckét a vállalatoknak. Azonnali megoldást kellett találniuk az üzlet folyamatos biztosítására, otthoni környezetből is. A vállalati domainbe léptetett PC-ket az otthoni hálózatból üzemeltetni a biztonság szintjének megtartásával több-kevesebb sikerrel megvalósult. Azonban az otthoni hálózatot is fel kell készíteni, mert a tömeges hirtelen átállás távmunkára növeli az otthoni hálózatok felé irányuló támadások kockázatát, A kiberbűnözők célpontjává válnak azok az eszközök, amik az alapértelmezett gyári konfigurációt futtatják, gyakran elavult szoftververziójú operációs rendszert futtató hálózati eszközöket. A Google Safe Browsing [15] által készített statisztika alapján generált 9.13 grafikonon látható, hogy arányaiban többszörösére ugrott a különböző malware és adathalász oldalak száma.



9.13. ábra. Malware és adathalász oldalak száma Google Safe Browsing statisztika

Mivel az otthoni hálózatunk is poenciális céponttá vált, ezért fontos, hogy felruházzuk a megfelelő védelmi rendszerekkel. Ennek pénzben, időben is kimutatható ára van. Az internet előfizetésen kívül egyéb a korábbi fejezetekben felsorolt akár havidíjas előfizetéses rendszerben megvásárolható szolgáltatásokra is szükség van. Jelen fejezet gyakorlati kivitelezését a következő szemeszter során tervezem kifejteni.

10. OTTHONI HÁLÓZATUNK VÉDELME

Az otthoni hálózatunk védelmét a mai trendeknek megfelelően érdemes inkább mélységi védelemmel ellátni, emiatt a védelmet nem bízzuk egyedül a routerre, hanem minden hálózatra csatlakoztatott eszköznek lesz valamilyen védelmi feladata.

10.1. Router és vezeték nélküli hálózati eszközök védelme

Az otthoni router, ami egyben a vezeték nélküli hálóatot is biztosítja, valamint egy kisebb switchként is használható. Több feladathiz, több biztonsági rés is társul, amikről a telepítés során javasolt gondoskodni. A használati célnak megfelelően konfigurált routerrel azon felül, hogy akár jobb átviteli sebesség is elérhető, a biztonság is növelhető. Az alábbi beállítási lehetőségek a routerek többségén megtalálható és javasolt aktiválni őket. A beállításhoz szükséges dokumentációt az eszöz típusának ismeretében könnyen megtalálhatjuk a gyártó honlapján.

- A bejelentkezési adatok megváltoztatása, mert az interneten bárki által fellelhető adatbázisban az alapértelmezett adatok megtalálhatóak, amivel átveheti az uralmat. Javasolt minél hosszabb és bonyolultabb jelszót válsaztani, amit a jelszó kezelő alaklamzás generál.
- Tiltsuk le a WAN management funkciót, hogy az internet irányából ne legyen lehetőség a bejelentkezésre. A hálózat adminisztrációját, a belső hálózat felől végezzük.
- WPS autentikáció inaktiválása. A használatával ugyan egyszerűbb az eszközök csatlakoztatása, mindamellett a támadók is számítanak arra, hogy a felhasználók használják ezt a funkciót. Brute-force, vagyis a nyers erő alkalmazásával a PIN kódot képes felderíteni és csatlakozni ahálózathoz. Ha nem használjuk, ezzel a lehetőséggel nem tud élni.
- Aktiváljuk a https bejelentkezés kikényszerítését. Ezzel a lehetőséggel a routerünket biztonságos kapcsolaton keresztül érhetjük el.
- Az SSID vagyis a vezeték nélküli hálózat nevének megváltoztatása, olyan névre, ami nem utal a hardver gyártójára és típ usára. Ezzel megnehezíthető a támadó számráa az eszköz pontos típusának kiderítése, arra jellemző sérülékenységek kihasználása.
- A rejtőzködés az otthoni hálózat esetén hasznos védekezés lehet. Tiltsuk le az SSID kijelzést. Ugyan a képzett támadók képesek lehetnek megtalálni a hálózatot, de ezzel a lépéssel is növelhetjük a biztonságot.
- Ha a készülék támogatja, a vezeték nélküli hálózat lefedettségét is be tudjuk állítani. Ezzel elkerüljünk, hogy az ingatlanon kívülről csatlakozzanak a hálózathoz.

- A WPA2-AES titkosítás használata szintén véletlenszerű karakterket tartalmazó jelszóval, lehetőleg minél hosszabb, akár 20 vagy több karakter hosszú jelszó is lehet. Ezt a jelszót az eszközünk első csatlakoztatásakor kell használnunk, így nem lesz kényelmetlen a használata.
- Aktiváljuk a vendég hálózatot, ahova a vendégek tudnak csatlakozni és teljesen el van szeparálva a saját belső hálózatunktól.
- A DHCP szerver kikapcsolása, hogy a támadónak nehezebb legyen kideríteni, hogy milyen IP cím tartományt használunk. Inkább kézzel adjuk meg az összes eszközünknek egy IP címet.
- SPI tűzfal engedlyezése. Ez jellemzően csak egy jelölő négyzet. Ezzel csak azt a kapcsolatot engedélyezi, ami a belső hálózatunkból kezdeményeztünk.
- Rendszeres időközönként ellenőrizzük, hogy elérhető-e frissítés az eszközhöz, ha igen, alkalmazzuk, mert az időközben kiderült biztonsági rések befoltozása ezen keresztül történik meg.
- Minden hálózatra csatlakozni képes eszköz rendelkezik egy MAC címmel. Készítsünk egy listát a saját eszközeink MAC címéről és ezeket vigyük fel a routerbe, létrehozva ezzel egy fehér listát, ami az adott MAC címmel rendelkező eszközöket engedi kapcsaolódni a hálózatra. Ez othoni környezetben, amikor nem 0-24 csatlakozik eszköz a hálózathoz segítség lehet, mert a támadók nem tudják kideríteni, hogy milyen MAC címet állítsanak be az eszközüknek, ha épp nem csatlakozik a mi eszközünk közül egy sem. Ha nem vagyunk otthon, tiltsuk le a vezeték nélküli hálózatot, így nem tudnak csatlakozni a támadók. Ezt egyes routerek akár időzítve is képesek végrehajtani.
- Az UPnP protkollt kapcsoljuk ki, amivel meggátolhatjuk, hogy megnyithasson egy portot bármelyik eszköz a routeren. Ha kártékony kód jut be a hálózatunkba, ezzel a funkcióval képes utat nyitni a támadónak.

Azt láthatjuk, hogy az otthoni hálózat esetén a rejtőzködés segítségünkre lehet a biztonságunk növelése érdekében. A vállalatokkal ellentétben az otthoni hálózaton az átlag felhasználó nem üzemeltet olyan szolgáltatásokat, melyeket kívülről is el kell érni, így jobb azt a látszatot kelteni, hogy nem is létezik a hálózat.

A fenti beállítások betartása esetén, ha a támadó megtalálja a hálózatot és sikerül azt feltörni, a MAC cím szűrő tovább nehezíti a célja elérésében, mert meg kell találnia az engedélyezett MAC címeket, ami időbe telik. Ha ezt is sikerül megoldania, akkor az IP cím tartományt és a használt IP címek listáját kell meghatároznia, hogy kommunikálhasson a hálózaton. A támadás időtartama tovább tarthat, mint arra számított a támadó, emiatt akár fel is adhatja a támadást, mert nem éri meg a befektetett munka, vagy eléri azt az időt,

amikor a vezeték nélküli hálózatot lekapcsoljuk, mert nem tartózkodunk otthon. Így nem képes tovább folytatni a munkáját.

10.2. Mire jó a VPN?

Biztosan találkoztunk már olyan videóval, amiben VPN szolgáltatást reklámoznak. A VPN valóban hasznos, azonban több fajátja létezik és mindegyiket másra használjuk. Ahhoz, hogy el tudjuk dönteni, hogy melyikre van szükségünk, meg kell ismernünk őket. A VPN vagyis a virtuális magánhálózat, aminek a segítségével elrejthető a valós IP címünk és bizonyos típusú VPN-ek esetén az adatforgalom titkosítására is lehetőségünk van. Tehát bizonyos mértékben megvédheti az online magánszférát. A VPN önmagában nem képes megoldani az összes kiberbiztonsági problémát. Használatával például hozzáférhetünk olyan streaming tartalmakhoz, amik a saját régiónkban nem elérhetőek. Érdemes áttekinteni a különböző VPN szolgáltatók kínálatát és összehasonlítani őket amjd egyeztetni a saját igényeinkkel. Azonban amit érdemes szem előtt tartani, hogy a választásnál szempont kell legyen, hogy valóban teljesíti mindazt, amit ígér és megfelelő sebességet tudjon biztosítani a használata közben.
A biztonsággal kapcsolatban a minimum elvárás:

- Az AES 256 bites titkosítás.
- A Kill switch funkció.
- A valóban naplózásmentes szolgáltatás.
- Az IPv6 és DNS szivárgás elleni védelem.

Annak ellenére, hogy VPN-t használunk, a sütiken keresztül több weboldal is képes követni online tevékenységünket, mint azt gondolnánk. Titkosíthatjuk az adatforgalmat, de a szerveren tárolt adatokról pl: login információk, stb. nem áll módunkban rendelkezni. Sok esetben nincs más választásunk, vagy megbízunk az adott weboldalban vagy inkább nem használjuk.
A Kill switch lényege, hogy leállítja az adatforgalmat, ha megszakad a VPN kiszolgálóval a kapcsolat. Ez segít megőrizni az anonimitást és az adatszivárgás ellen is véd, mert megakadályozza az adatforgalom titkostatlan csatornán.
A naplózásmentesség szintén hozzájárul a biztonsághoz, mert nem tárolnak előzményeket a használat közbeni tevékenységről.
Ha a VPN szolgáltatás során a DNS kérések titkosításra kerülnek, akkor az internetszolgáltatónk előtt is titkosítva vannak ezek az információk, mindaddig amíg a DNS és IPv6 elleni szivárgás aktív. A sebesség és felhasználhatóság szempontjából fontos a kiterjedt szerverhálózat, hogy minél több IP címet biztosítson a számunkra. Ezzel kiküszöbölve az IP cím ismétlődést. A VPN használata közben lassabb sávszélességre számíthatunk, azonban ez szolgáltatótól is függ, hogy milyen mértékben lassul az internet

sebesség. Ez a mindennapi használat miatt szempont, hogy kellően nagy sávszélességgel tudjunk kihasználni és ne kelljen lekapcsolni a VPN-t, hogy bizonyos feladatokat végre tudjunk hajtani. A VPN használathoz jellemzően nem szükséges egyéb hardver, tehát szoftveres úton is megoldható a használata. Ennek 2 csoportját tudjuk meghatározni. Az egyik az erre alkalmas saját otthoni routerünkön tudjuk futtatni, így az összes eszköz, ami a router belső hálózatára van csatlakoztatva képes használni a VPN szolgáltatást. A másik, csaoport, ahol a különböző készülékeken egyesével állítjuk be a VPN klienst. Ebben az esetben a szolgáltató választás esetén fontos, hogy milyen platformokat támogat. Személyes javaslatom, hogy a VPN szolgáltatók között érdemes úgy választani, hogy a támadók fejével gondolkodunk. Melyik szolgáltató esetén van lehetőség nagyobb adatforgalom elkapására. Egyes titkosítással nem rendelkező szolgáltató igazi aranybányaként szolgál a támadóknak. Személyes javaslatom, hogy a VPN-re, mint egy célszerszámra tekintsünk és ne úgy, mint a digitális önvédelem egyetlen eszközeként.

11. ADATBIZTONSÁGOT NÖVELŐ ESZKÖZÖK

A biztonságos állapot minél magasabb szintjének fenntartása érdekében használhatunk különböző eszközöket. A megfelelő hardver és operációs rendszerek, biztonsági mentéseken túl a különböző típusú veszélyforrások elleni védekezés érdekében alkalmazhatunk újabb hasznos eszközöket, amik a biztonság növelésén túl másodlagos haszonként időt takaríthat meg nekünk. Ezeket az eszközöket ajánlott hivatalos forrásokból beszerezni, mert csak ebben az esetben garantálja a gyártó a specifikációban leírtak szerinti működést.

11.1. Szoftverforrások

Eszközeinknek szoftverek nélkül nem sok hasznát vesszük, ezért mindenképp szükségünk van operációs rendszerre, különböző felhasználói igényeket kielégítő alkalmazásokra. Rengeteg lehetőség közül választhatunk, hogyan és honnan szerezzük be ezeket. A nem megbízható és nem ellenőrzött forrásból beszerzett szoftvereket nem tekinthetjük biztonságosnak. Ezek az alkalmazások tartalmazhatnak olyan kártékony kódokat, amik veszélyt jelenthetnek az adatainkra. Ezek kiszűrését megfelelő szoftverek képesek elvégezni, azonban csak erre hagyatkozni nagy hiba. A vírusírtó szoftverek sem képesek minden kártevőt kiszűrni, ezért fontos, hogy minden bejövő e-mail, link, weboldal, telefonhívással kapcsolatban legyünk szkeptikusak. Ne feledjük, hogy a támadók folyamatosan alkalmazkodnak a technolódiai változásokhoz és újabbnál újabb lehetőségeket keresnek és találnak, hogy elérjék céljaikat. Ezért nem javasolt kétes és nem ellenőrzött torrent és weboldalakról beszerezni a szükséges szoftvereinket. A szoftvereket nagyjából két fő részre oszthatjuk, nyílt forráskódú és zárt forráskódú. Az előbbit egy közösség ellenőrzi és nyilvános a forráskód, így bárki ellenőrizheti a szoftver viselkedését és meggyőződhet arról, hogy tartalmaz-e kártevőt vagy van-e negatív nem várt hatása a használatának. Az utóbbi forráskódja ismeretlen, emiatt meg kell bíznunk a szoftver gyártójában, aki különböző tanúsítványokkal tudja bizonyítani az előbbieket, természetesen ezek javarészt nem ingyenes alkalmazások.

11.2. Adatbiztonság a hardverek függvényében

A valódi igényeinknek megfelelő hardverek kiválasztása szintén javít a biztonságon. Ne feledjük, ahogy azt korábban kifjtettük, hogy a biztonság egy állapot, amelyet folyamatosan fenn kell tartanunk. Eddig számba vettük az emberi tényezőket, valamint a megfelelő eszközök témakörét érintettük a potenciális kártevők és sérülékenységek oldaláról. Az eszköz kiválasztása szintén emberi tényezők szempontjai szerint valósul meg. Szinte minden választás megindokolható, például a bekerülési költségek, vagy a jól hangzó marketing. A megfelelő eszköz kiváasztása esetén mindkét indok igaz. Ez a dokumentum nem a

vállalati informatikai biztonsággal és digitális védelem témakörét taglalja, sokkal inkább a személyes digitális önvédelmet. Azonban sok esetben, ahogyan most is van átfedés a kettő között. Az informatikai eszközöket, jelen esetben az asztali számítógépek és laptopok kategóriáját két részre érdemes bontanunk. Fontos tudni, hogy az otthoni felhasználásra szánt eszközök és az üzleti felhasználásra szánt eszközök között jelentős különbségek fedezhetők fel az üzleti kategóriás eszközök javára, mivel ezeket 24/7 vagyis folyamatos üzemre tervezték, minimum 5 év, de jellemzően hosszabb élettartam mellett. Ellenben az otthoni felhasználásra szánt eszközök nem képesek ilyen igény kielégítésére. Ezt az eszközökben található alkatrészek minősége és teljesítménye is tükrözi. A 11.14 ábra jól szemlélteti a különbséget a két eltérő kategóriájú laptop processzor hűtője között. Az üzleti kategóriás alkatrész masszívabb vaskosabb, erősebb, addig az olcsóbb kategóriájú, kisebb, vékonyabb.

11.14. ábra. Balra egy olcsóbb, jobbra pedig egy üzleti kategóriás laptop CPU hűtője

A vállalati környezetben az adatok képeznek értéket az azt tároló eszközzel szemben, viszont felépítéséből adódóan alkalmasak a vállalat számára értékes adatok kezelésére, feldolgozására, továbbítására és az üzletmenet hatékony támogatására ellentétben az otthoni felhasználásra szánt eszközökkel. A minőségi különbség az eszközök bekerülési költségében is megjelenik, az üzleti felhasználásra szánt eszközök jobb minőségőek, emiatt magasabb áron vásárolhatóak meg, azonban a készüléken túl ebben az esetben a support is gyorsabb. Az üzleti szériás eszközök életciklusa egy vállalatnál általában 3 év, ezután felújításra és újkori árának töredékéért újraértékesítésre kerülnek, otthoni felhasználásra továbbra is tökéletesen alkalmas. Moduláris felépítésének köszönhetően egy bizonyos mértékig fejleszthetőek, ezáltal életciklusuk meghosszabbítható. Védelmi képességei (bizonyos mértékig ütés-, és folyadékálló jellemzően fém, általában magnézium és nagyobb igénybevételnek ellenállóbb műanyag borítással rendelkeznek), magasabb biztonságot és megbízhatóságot jelent. Beépített biztonsági chipek például a TPM, biometrikus azonosításra alkalmas szenzorok, fizikai kapcsolók kamerához és egyéb adatok biztonságáért felelős megoldások, szintén a biztonságot növelk. Az Apple készülékei szintén tartalmaznak biztonsági chipet. Ezzel szemben az otthoni felhasználásra szánt készülékek nagy része nem bővíthető, főbb alkotóelemeik nem

javíthatóak, alaplapra forrasztott hardverekből áll össze, gyenge minőségű anyagok felhasználásával kialakított burkolattal és gyenge minőségű hardverekkel rendelkeznek. Előnyük csupán az áruk. Nem vagy minimális védelmi eszközökkel rendelkeznek. A vállalati készülékek biztonsági arzenálját otthoni körülmények között is igénybe tudjuk venni. Hardvereit szinte az összes népszerűbb operációs rendszer támogatja, mivel megbízható ismert gyártó termékei kerültek beépítésre. Az asztali számítógépek sem különbznek a hordozható számítógépektől. Esetükben ugyanúgy megkülönböztethetünk otthoni és üzleti kategóriás eszközöket.

12. HOGYAN VÉDJÜK MEG MAGUNKAT AZ INTERNETEN

Az internet használata közben szintén szükség van a megfontolt magatartásra, mellyel megnehezíthetjük a támadók dolgát. A költséghatékonyság és az egyszerűség érdekében az otthoni felhasználók esetében az alapvető eddig említett védelmi megoldásokon, eszközökön felül a tudatos hozzáállás célravezető lehet, hogy növeljük a biztonságot. Adataink védelméért sokat tehetünk, ha kerüljük a támadók figyelemének felkeltését és minél kevesebb ellenünk felhasználható információt osztunk meg magunkról. Ezek lehetnek a rendszerünkre vonatkozó információk, melyek alapján képesek keresni különböző sérülékenységeket illetve olyan kártékony kódot, amivel elérhetik a céljukat. Mindezeken túl az online szolgáltatások használatához szükségünk van regisztrációra. A regisztrált fiókok védelmét többek között megfelelően erős jelszavakkal és többfaktoros azonosítással, valamint alternatív bejelentkezési módok használatával is védhetjük.

13. JELSZAVAK, AUTENTIKÁCIÓS MÓDSZEREK

Az imént említettem a megfelelő jelszavakat és a többfaktoros azonosítást. Az autentikáció során ellenőrizzük, hogy egy adott személy vagy eszköz hozzáférhet-e az adott rendszerhez, szolgáltatáshoz. Napjainkban az autentikáció során gyakran használunk jelszavakat és egyéb módszereket. Ez esetben 3 fontos dolgot kell megjegyezni. Valamit tudni, amit csak mi tudhatunk, ez a jelszó, valami amit csak mi birtokolhatunk, ez lehet egy smart card vagy egy hardverkulcs, mely egyedi jellemzőkkel rendelkezik, illetve valaminek lenni, ami csak mi lehetünk, ebben az esetben a biometrikus azonosítást értjük, olyan egyedi jellemző alapján történő azonosítás, mely minden egyes egyén esetén egyedi, ez lehet az ujjlenyomat vagy írisz. Az imént felsorolt 3 dolgot kombinálhatjuk amit többfaktoros és többlépcsős azonsoításnak hívunk. A többfaktoros és többlépcsős azonosítás hasonlóak ugyan, de nem ugyanazt jelentik, ráadásul különböző területen is használhatjuk őket. A többfaktoros azonosításról akkor beszélünk, ha a fentebb felsorolt 3 tényező közül legalább 2 felhasználásra kerül. A legegyszerűbb példa a kézpénzfelvétel. Ebben az esetben az adat, amit csak mi tudhatunk az a PIN kód, amit pedig birtokolunk az a bankkártya, mely egyedi jellemzőkkel bír. Csak akkor vehetünk fel készpénzt egy ATM-ből, ha a megfelelő PIN kódot adtuk meg miután a hozzá tartozó bankkártyát behelyeztük az ATM-be.

A többlépcsős azonosítás esetén szintén tudnunk kell valamit, amit csak mi tudhatunk, ez a felhasználónév és a hozzá tartozó jelszó. A rendszer a megfelelő adatok megadása után a következő lépésként generál egy e-mailt, mely tartalmaz egy kódot vagy linket melyet a belépés következő lépéseként meg kell adnunk, vagy a linkre kattintva megerősíthetjük a belépési szándékunk illetve a személyazonosságunk. A rendszer a többlépcsős azonosítás beállítása során megadott e-mail címre vagy telefonszámra küldi az e-mailt, illetve az SMS-t. A különbség a többfaktoros azonosítással szemben, hogy a két faktorra nem egy időben van szükség. A megadott felhasználónév és jelszó páros megadása váltja ki azt az eseményt, mely egy másik csatornán keresztüli azonosításra szólítja fel a felhasználót. Amennyiben lehetséges mindig alkalmazzuk a többfaktoros és többlépcsős azonosításokat, melyek egy kellően hosszú és bonyolult jelszóval kombinálva növelhető a biztonság. Milyen a biztonságos jelszó? Hol tároljuk a jelszavakat? Biztonságos-e, ha beírjuk a jelszót a jelszó mezőbe? Mi történik a háttérben miután megadtuk a jelszavunkat? Van-e támadónak lehetősége a hálózati kommunikáció lehallgatására, azonosítók megszerzésére? Miyen egyéb lehetőségek léteznek? Ezekre a kérdésekre térjönk vissza később. A jelszavak használatával kapcsolatban rengeteg ajánlással találkozhatunk az interneten a dolgozat írásának pillanatában (2021 április) a password szóra több, mint 2 milliárd találat volt elérhető. Tehát a Jelszavak használata a mindennapi életünk része. Olyan, mint a fogkefe, vagyis jót választunk, naponta használjuk, nem adjuk kölcsön senkinek és időnként cseréljük. A kibertámadások nagy

részét általában tömegesen hajtják végre, a támadásra leginkább érzékeny platformok, szolgáltatások és felhasználói fiókok ellen. A szolgáltatások és felhasználói fiókok védelme érdekében az egyik legfontosabb védelmi intézkedés, ha megfelelő jelszót és többfaktoros azonosítást alkalmazunk. Erre a későbbi fejezetekben még kitérünk. A jelszavakat vizsgálatuk során többféle képpen lehet csoportosítani. Jelen esetben használatuk módjára vonatkozóan 4 csoportra osztom őket. Az első csoport a jelszavak egyéb azonosító nélkül történő használata, a második csoport a jelszavak egy azonosító, mely lehet felhasználónév, vagy e-mail cím párossal történő használata, a harmadik csoport az előzőhöz hasonlóan a jelszavakat felhasználónév, e-mail cím, stb. páros illetve többfaktoros azonosítás egy módszerével történő használata, a negyedik csoport a jelszavak nélküli autentikáció. A különböző típusú jelszavak feltöréséhez szükséges időt a Hive Systems [16] által készített 13.15 táblában láthatjuk. Jól látható, hogy egy kellően erős jelszó legalább 12 karakterből áll, tartalmaz kis-, és nagybetűket, speciális karaktereket, valamint számokat. Ennek feltöréséhez egy RTX2080 típusú GPU felhasználásával 34 ezer évre van szükség.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tm years	100tn years	7qd years

13.15. ábra. A feltöréshez egy RTX2080 GPU-t használtak

13.1. Jelszavak használata egyéb azonosítók nélkül

Egyes esetekben a jelszavakat önállóan használjuk felhasználói azonosító nélkül, melyek lehetnek ajtókon található zárak, lakatok, mobiltelefonok és táblagépek feloldó kódjai, riasztókhoz tartozó jelszavak, egyszerűbb szoftverek beépített titkosítással, pl: irodai al-

kalmazások, fájltömörítők. Az azonosítás sikeressége ebben az esetben a helyes jelszó ismeretétől, valamint az azonosító eszköz hozzáférhetőségétől függ. Feltörésük ideje több tényezőn múlhat, ezek a használt jelszó hosszától, jelszóban használt karakterek különbözöségétől, sokszínűségétől, a karakterek ismétlődésétől, a titkosítás módjától, a feltörésre használt erőforrástól, valamint zárak esetén a feltörés során észrevétlenül eltöltött időtől és a zárszerkezettől függ. Több online szolgáltatás szakosodott jelszavas védelemmel ellátott fájlok feltörésére, így maximalizálni tudja a profitot, mert a kihasználatlan erőforrásait ezen feladatokkal képes lekötni. Jellemzően néhány $10-tól indulnak a szolgáltatások költsége, ami kellőképpen alacsony összeg, annak reményében, hogy hozzáférhetünk védett, számunkra is értéket képviselő adatokhoz. A támadónak nem szükséges hatalmas kapacitásokkal, jelszólistákkal és egyéb eszközökkel rendelkeznie, hogy hozzáférhessen az információhoz. Ha a jelszóval védett fájlt megszerezte, az adatokhoz nagyobb anyagi és idő ráfordítás nélkül férhet hozzá. Ebben az esetben mindenképp ajánlott olyan jelszót, vagy PIN kódot alkalmazni, mely semmilyen szempontból sem kötődik a használójához. Javasolt kerülni a nevezetes dátumokat, pl: szöletésnap és egyéb fontosabb események, személyek, tárgyak neveinek használatát. A fentebb tárgyalt emberi tényezők között kitértem arra, hogy ezen információkat mások is tudhatják, kikövetkeztethetik vagy észrevétlenül akár keresztkérdések segítségével is megszerezhetik. PIN kódok esetében segítséget nyújthat, ha a

13.2. Jelszavak felhasználó azonosító párossal történő használata

A jelszavak azonosító párossal történő használatából következtethetünk, hogy a használni kívánt rendszer alkalmas egynél több felhasználó kezelésére. Ezek jellemzően Operációs rendszerek, online szolgáltatások. Ebben az esetben valós felhasználónév és jelszó páros esetén lehetséges a belépés. A támadások sikeressége függ felhasználónév jelszó páros több szolgáltás esetén történő használatától, a használt szolgáltatások biztonságától, a jelszó bonyolultságától, hosszától, valamint a felhasználó biztonságtudatosságától. Ha a támadó sikeresen hozzáfér az azonosításhoz szükséges adatokhoz, minden szolgáltatásba képes bejelentkezni, ahol ezek használatban vannak. Tehát egy egyszerű jelszóval védett szöveges fájlban tárolt jelszóadatbázis illetéktelen kezekbe kerülése komoly biztonsági kockázatot jelent, ha figyelembe vesszük, hogy az előző alfejezetben taglaltak alapján könnyedén feltörhető a jelszóval védett fájl.

13.3. Jelszó azonosító páros használata, többfaktoros azonosítással

Többfaktoros azonosítás esetén az autentikálás során az előző módszerhez hasonlóan szükség van a felhasználónév jelszó párosra. Ezek érvényessége esetén következik a második faktor, mely lehet egy egyszeri SMS-ben vagy e-mailben elküldött karaktersor vagy mobilkészülékünkon használt autentikátor alkalmazás által generált több karakterből

álló rögzített időközönként generált jelszó. Ennek bevitelére általában limitált idő áll rendelkezésünkre. Ha lejár a beviteli idő, az autentikálást újra kell kezdeni. Ez a megoldás sem tökéletes, az SMS-ek elfogására is léteznek megoldások, valamint nagyban függ a mobilkészülékünk biztonságától.

Az autentikátor alkalmazásoknak szintén vannak előnyeik és hátrányaik, melyeket érdemes figyelembe venni mielőtt használjuk őket. Viszonylag sok alkalmazás áll rendelkezésünkre a többlépcsős azonosításhoz. Azonban mielőtt használjuk őket érdemes közelebbről is megvizsgálni. Ezeket az alkalmazásokat általában mobilkészüléken használjuk, amit könnyedén elhagyhatunk. Ebben az esetben a mobilkészüléken tárolt és általa hozzáférhető online fiókok és adatok hozzáférhetősége a készüléken alkalmazott biztonsági beállításoktól függ. Ha sikerül a készülék feloldása, a Google authenticator alkalmazásban regisztrált fiókok is hozzáférhetővé válnak, mert az alkalmazás futtatása nincs azonosításhoz kötve. Természetesen nem azonnal férhetnek hozzá a fiókokhoz az illetéktelen behatolók, de megkönnyíti a dolgukat. A bizotnság így az SMS-ben kapott kóddal egyenértékű, mert az SMS nem titkosított csatornát használ és elfoghatóak az üzenetek. Ha az előbbi példánál maradunk, vagy a mobilkészülékünk használhatatlanná válik és egy új készülékre váltunk de nem tudunk belépni a Google fiókunkba, az authenticator alkalmazás tartalma nem állítható vissza, kivéve, ha a biztonsági kódokat egy biztonságos helyen eltároltuk.

Természetesen léteznek alternatív lehetőségek is, például az Authy, ami az előbb említett két sérülékenységgel nem rendelkezik. Az alkalmazás használata PIN kódhoz köthető, így elkerülhető az illetéktelen behatolás. Az Authy támogatja a több eszköz használatát, tehát nincs megkötés, és asztali PC-n is futtathatjuk. Előnye, hogy, elveszett, megrongálódott készülék esetén is hozzáférünk az ott regisztrált szolgáltatások többlépcsős azonosításához. A felhőben történő tárolás szintén kockázattal jár, azonban alkalmi használat esetén segítségünkre lehet. A szinkronizáció bármikor aktiválható és inaktiválható. Egy másik lehetőség a Microsoft Authenticator, ami szintén támogatja a futtatás PIN kód, vagy biometrikus azonosítóhoz kötését. iPhone esetén lehetség van a tartalmat menteni iCloud tárhelyre, így könnyen visszaállíthatóvá teszi a tartalmát. Egy harmadik lehetőség is a rendelkezésünkre áll, ami a fizikai kulcsot jelenti. Ez egy pendrive-hoz hasonlító fizikai kulcsot jelent. Több gyártó többféle terméke közül választhatunk. Személyes javaslatom a Yubico termékei [17], a Yubikey kulcsai. Ha hardveres kulcs mellett döntünk azért javaslom a Yubikey kulcsait, mert széles körben használható, számos szolgáltatása mellett, lehetőség van több típusú csatolakozóval is rendelni, így a lehető legtöbb eszközünkkel használhatjuk. Szinte az összes operációs rendszerhez elérhető az segédprogramjai, amivel a használni kívánt célra konfigurálhatjuk, valamint rendelkezik authenticator alkalmazással is, így nem sükséges

a felhőben tárolnunk ezeket az adatokat, tehát felettük a kontroll végig a mi kezünkben van. Fizikai behatásoknak kellőképp ellenáll, meghibásodása esetén rendelkezésünkre áll alternatív azonosítási mód. Személyes javaslatom azonban, hogy legalább 2 ilyen eszközzel rendelkezzünk, így egy esetleges hiba esetén sem kell változtatnunk az azonosítási módszereken. A 13.2 táblázat bemutatja a többfaktoros azonosítás és az egyfaktoros azonosítás közötti különbséget.

	Többfaktoros azonosítás használata	Többfaktoros azonosítás nélkül
Jelszó publikussá válik	A második faktor ismerete nélkül nem léphet be a támadó	Felhasználónév és jelszó ismeretében beléphet a támadó
Adathalász jellegű támadás esetén	A második faktor ismerete nélkül nem léphet be a támadó	Felhasználónév és jelszó ismeretében beléphet a támadó
Beállítás és használat ideje	Több időt igényel a belépéshez	Gyorsabb belépést biztosít
Elhagyás esetén	Egyszer használatos biztonsági kódok védelméről gondoskodni kell	Jelszó emlékeztető
Költségek	Ingyenes és fizetős	Ingyenes
Biztonság	Jogosultlan belépés esetén lehetőség van megtagadni a belépést	Sok esetben nincs értesítés a belépésről sem

13.2. táblázat. Többfaktoros vs. egyfaktoros hitelesítés

A biztonság további növeléséhez lehetőség van szeparálni a különböző többfaktoros azonosítási megoldásokat, tehát a felhazsnálási célnak megfelelően használhatjuk azt a megoldást, amit az adott szolgáltatás támogat. Sőt adott esetben lehetőség van akár MFA-ként vagyis multifaktoros azonosításként ezek összevont használata is, ami azt jelenti, hogy a jelszó megadása után több egymás utáni faktor sikeres abszolválása után léptet be a rendszer. A felhasználókban felmerülő ellenérzés transzformációjához segítségül szolgálhat, ha a belépések bonyolítása és megnehezítéseét aképp értelmezzük, hogy a támadó belépési lehetőségeit azzal korlátozzuk, hogy a belépéshez szükséges információk lehető legnagyobb részét nem tesszük számára elérhetővé. Ennek egyik módja lehet, hogy a többfaktoros azonosításhoz olyan módszert használunk, mely adott időben, adott helyen, csak az arra jogosult számára érhető el. Erre alkalmas lehet egy hardverkulcs használata, melyet távolról nem képes manipulálni a támadó. A legtöbb hardverkulcs, mint pl: a Yubikey kulcsainak firmware-e nem módosítható, így nem lehet felülírni manipulált firm-

warerrel sem. A biztonság növelése érdekében, a megfelelő kulcs választáshoz segítségül szolgáhat a 13.3 táblázat.

Többfaktoros azonosítás	Yubikey 5	Authy	Google Authenticator
Ár	$45	Ingyenes	Ingyenes
Biztonsági elvesztés esetén	Egyszer használatos biztonsági kódok, egyszerre több kulcs használható	Készíthető biztonsági mentés	Nincs biztonsági mentés
Beállítás és használat ideje	A konfiguráció nehezebb, mint a másik kettő	Egyszerű beállítani	Egyszerű beállítani
Tárolás	Lokálisan	Felhőben	Felhőben
Biztonsági funkciók	Zárolható PIN kóddal	Zárolható PIN kóddal	Nincs applikáció zárolás
Protokoll	Esemény és időalapú, statikus jelszó. Több, mint 12 protokoll	Idő-, és hash alapú hitelesítés	Idő-, és hash alapú hitelesítés
Platform	Windows, Mac, Linux, Andorid, iOS	Windows, Mac, Linux, Andorid, iOS	Chrome bővítményként, Android, iOS
Dokumentáció	Több nyelven elérhető	Több nyelven elérhető	Több nyelven elérhető

13.3. táblázat. Többfaktoros hitelesítéshez használható eszközök

A különböző eszközök által nyújtott biztonsági és kényelmi funkciók alapján látható, hogy a legszélesebb funkcionalitást nyújtó megoldás nem ingyenes, mindamellett szükséges lehet oktatóvideók és dokumentumok a beállításhoz, cserébe viszont megadja azt a kényelmet, hogy minden adat a felhasználónál tárolódik, ellentétben a szoftveres megoldásokkal, ahol szükség van egy felhasználói azonosító regisztrációjára. Ebben az esetben az adatok egy része, nem a felhasználónál tárolódik, cserében a használatuk könnyebb, de mindenképp szükséges egy mobiulkészülék a használatukhoz, aminek biztonságáról szintén a felhzasnálónak kell gondoskodnia.

13.4. Biztonságos jelszókezelés

A Dashlane [18] által készített kimutatás alapján egy átlagos felhasználó körülbelül 150 jelszóval rendelkezik, ami 300-ra, vagyis a duplájára fog emelkedni 2022-re. A jelszavak generálásával, kezelésével kapcsolatos probléma egyik oka innen eredeztethető. Nehéz, időigényes és fárasztó minden jelszót megjegyezni, és naprakészen tartani, ezért sokan sajnos könnyen megjegyezhető és egyszerű jelszavakat alkalmaznak, melyek nem növelik a biztonságot. Gondoljunk bele, hogy az eddig megismert veszélyek, amik az eszközökre és a viselkedésre vonatkoznak, mekkora veszélyt jelent egy kibertámadás esetén, ha a használt jelszavak szintén nem tartoznak a kellően erős jelszavak kategóriájába.

Úgy javíthatunk a jelszavak biztonságán, ha a használt jelszó nem egy értelmes szót alkot, nem tartalmaz két azonos karaktert, kis- és nagybetűket, numerikus és speciális karaktereket, valamint kellően hosszú, ami 12-15 karakter hosszúságú. Ha mindehhez hozzávesszük, hogy a mindennapi élet során is használhatóak legyenek, tehát könnyen megjegyezhetőek, akkor nincs könnyű dolgunk. A jelszavakkal használatával kapcsolatban fontos megjegyezni, hogy egy jelszót, csak egyszer érdemes használni. Ez segít csökkenteni a kockázatot. Abban az esetben, ha egy jelszó publikussá válik, és jó esetben csak egyszer használtuk, akkor csak egy adott fiók esetében kell azt megváltoztatni. Amennyiben egynél több helyen is használuk ráadásul ugyanazzal a felhasználói azonosítóval vagy e-mail címmel, akkor az összes olyan fiók veszélyben van, ahol ezeket a párosokat alkalmaztuk. Ebből kiindulva látható, hogy a biztonság növelhető az egy jelszó egy fiók alkalmazásával, viszont ez fokozható, ha az egy fiók egy felhasználói azonosító és egy jelszó hármast alkalmazzuk. Ennyi egyedi adatot képtelenség naprakészen és fejben tartani. Szerencsére léteznek léteznek erre a célra alkalmazható eszközök, melyeket jelszókezelő alkalmazásokank hívunk. A jelszókezelő alkalmazásokra érdemes úgy tekinteni, mint egy célszerszámra. Természetesen egy egyszerű titkosítatlan szöveges állomány is képes tárolni a jelszavakat, viszont ennek megvannak a veszélyei, egyáltalán nem biztonságos, ahogy a papíron tárolt jelszavak sem azok. Ezek tartalma könnyedén megváltoztatható, törölhető vagy lemásolható. A jelszókezelő alkalmazások többsége kínál többféle szolgáltatást, melyek segítenek a jelszavak hatékony adminisztrálásában. Különböző riportokat képesek készíteni, mint pl: többször használt adatok kigyűjtése, jelszó erősség ellenőrzése, valamint az online jelszókezelők egyik nagy előnye, hogy képes az internetes adatbázisok monitorozására és jelez, ha az adatbázisunkban szereplő bármely jelszó publikussá vált. A különböző szolgáltatások különböző jelszó komplexitást követelnek. Léteznek olyan követelmények, ahol nem használható speciális karakter vagy limitált a jelszó minimális hossza. Ebben az esetben érdemes a minél hosszabb jelszóra törekedni.

A jelszókezelő alkalmazások szintén képesek megadott paraméterek alapján jelszót generálni. A jelszókezelő alkalmazásokat gyakran alkalmazzák vállalati környezetben is, mert egyes alkalmazások képesek több felhasználót is kiszolgálni, így jogosultságokhoz köthető az adatbázis különböző tartalmainak elérése, módosítása, vagy akár a jelszó felfedésének mellőzése mellett a jelszóhoz tartozó szolgáltatás használata. A jelszókezelő alkalmazásoknak két fajtája létezik, az offline és az online, melyek közül az utóbbi például a LastPass képességei között találjuk meg a korábban említett funkciót, mely az adatbázisban található publikussá vált, kompromittált jelszavakat képes megjelölni és felhívni a felhasználó figyelmét a jelszó mielőbbi megváltoztatására. Ebben az esetben is vannak előnyök és hátrányok. Az online jelszókezelő bármilyen okból történő kompromittálása esetén kikerülő jelszavak magas kockázatot jelentenek. Ha nincs az adatbázis a birtokunkban, hanem egy távoli szolgáltató távoli szerverén van, akkor limitáltak a lehetőségeink illetve az ismeretenik, hogy mi történik az ott tárolt adatokkal, azonban több példányban is létezik biztonsági mentés formájában, melyek több különböző szerveren tárolódnak, így a tárolására használt adathordozó esetleges hibája nem jelent kockázatot. Offline adatbázis esetén például a KeePass, ami nyílt forráskódú, általában nincs lehetőség a kompromittált jelszavak internetes monitorozására és a biztonsági mentésről is a felhasználónak kell gondoskodnia, amire később még visszatérünk, azonban egyik nagy előnye, hogy az adatbázis a felhasználó birtokában van, mindaddig amíg azt nem egy felhőtárhelyen tárolja. Illetve testreszabhatóbb felületet biztosít és szinte minden platformon elérhető. Szerencsére léteznek olyan felületek, ahol ezeket a jelszókezelőket összehasonlítják és segítséget nyújtanak a megfelelő termék kiválasztásához, ilyen például a CyberNews [19] összehasonlítása. A 13.4 táblázat bemutatja a két különböző típusú jelszókezelő alkalmazás közötti különbséget, segítségével kiválasztható a felhasználási igénynek megfelelő alkalmazás.

Jelszókezelők	Offline (KeePass)	Online (LastPass)
Kétlépcsős hitelesítés	Bővítménnyel érhető el	Alapértelmezett
Több eszköz szinkronizációja	Bővítménnyel érhető el	Alapértelmezett
Jelszógenerátor	Alapértelmezett	Alapértelmezett
Támogatás	Közösségi	E-mail (csak angolul)
Alkalmazások	Android, iOS, Windows, MacOS, Linux	Android, iOS
Adatbázis helye	Felhasználónál	LastPass szerverein tárolja,
Költségek	Ingyenes	Limitált ingyenes (max. 50 jelszó) / Prémium: $4 /hó

13.4. táblázat. Online és offline jelszókezelő alkalmazások főbb funkciói

14. NÉPSZERŰBB ONLINE SZOLGÁLTATÁSOK

Az internet elérhető különböző szolgáltatások térnyerésével megnövekedett a támadások lehetőségének számossága. Az online szolgáltatások esetén egy átlag felhasználó számára nem feltétlenül egyértelmű a biztonság felelősségének kérdése. A szolgáltatáshoz tartozó EULA, ami az End User Licence Agreement rövidítése, jelentése: végfelhasználói licenszszerződés, valamint a TOS, ami a Terms of Services rövidítése, a szolgáltató és a szolgáltatást igénybe vevő közötti megállapodást jelenti. Ezeket terjedelmük és nehéz értelmezhetőségük miatt az átlag felhasználók nem tanulmányozzák, emiatt nincsenek tisztában a felelősségek kérdésével. A népszerűbb online szolgáltatások, mint a banki szolgáltatás, video streaming, közösségi média, levelező szolgáltatások, fájlok online megosztása, tárolása, webshopokon keresztül vásárlás, és számtalan szolgáltatás használa során megosztott adataink biztonsága már több tényezőtől függ. A szolgáltatások használata során a felhasználó által megosztott nyilvánosan elérhető adatok gyűjtésére számtalan módszer áll a rendelkezésünkre. Az adatok nyilvánossága a felhasználó magatartásától és a használt szolgáltatás biztonságától, hálózati kommunikáció típusától függ. A data breach vagyis adatszivárgás kifejezésre a kereső több, mint 141 millió találatot ad. Ezek egy része a már kiderült adatszivárgásokról a másik része, pedig ezek lehetőségeiről, megvalósításáról szól. A nem nyilvánosan elérhető, védett, bizalmas adatok illetéktelen kezekbe jutnak, nyilvánosan elérhetővé válnak. A közösségi oldalak esetén, mint pl: a Facebook, Instagram, Twitter számára bevételi forrást jelentő felhasználói adatok a támadók számára szintén értékesek. Ezek többek között a helyadatokra vonatkozó információk, harmadik féltől származó alkalmazások által használt adatok, a platformok használata során a megosztásokra, posztokra vonatkozó paraméterek, valamint a felhasználókat érintő további adatok és a személyes profilunkat elérő célzott reklámok. Későbbi fejezetben az OSINT technikákra is kitérünk, melyek a fenti nyilvánosan elérhető adatok megszerzésében adnak segítséget a támadóknak.

A népszerűbb közösségi média platformok (Facebook, Instagram, LinkedIn, Twitter, stb.) támogatják a kétfaktoros hitelesítést, melyet erősen ajánlott bekapcsolni és használni. Ezzel növelhető a fiók biztonsága és sértetlensége, ahogy azt korábban a jelszavaknál kifejtettem. A legtöbb esetben ezt a funkciót a Profil beállításokkal kapcsolatos menüben érhetjük el jellemzően a Biztonság és Adatvédelem almenü alatt. Ezzel az adott fiók védelméért tettünk egy lépést. A fiókok összekapcsolása is lehetséges, bár ezt személy szerint kerülném. Az összekapcsolt fiókok ugyan kényelmesebb használatot eredményeznek, viszont biztonsági szempontból kockázatos. Ha kompromittálják a felhasználói fiókot, akkor az összekapcsolt fiók adatiahoz is hozzáférést szereznek. Az elsődleges fiók pl: Facebook rendszerhibája vagy szolgáltatáskimaradása esetén, előfordulhat, hogy nem férünk hozzá az összekapcsolt fiókhoz, mert nem lehetséges az

autentikáció. Amennyiben kerüljük az összekapcsolást, ezeket a hibákat elkerülhetjük. A többfaktoros és többlépcsős azonosítás lehetőségét érdemes minden egyes szolgáltatás esetén ellenőrizni. A fiók és személyes adatok veszélyeivel és védelmével a kovetkező fejezetek foglalkoznak.

14.1. Felhasználói fiókok

Az átlag felhasználó rengeteg magára hagyott felhasználói fiókkal rendelkezik. Ha közelebbről megvizsgáljuk, ezeket a fiókokat, akkor látható, hogy miért veszélyes ez. Érdemes megnézni, hogy a magára hagyott fióknál használt jelszó vagy felhasználónév hol szerepel még. Ha nem követjük figyelemmel, hogy az adott oldalnál, vgy szolgáltatásnál legutolsó bejelentkezésünk óta történt-e bármillyen kiberbiztonsági incidens. Ha igen, és máshol is használtuk az azonosítót vagy a jelszót, azt felhaználhatják későbbi támadásokhoz. Léteznek szintén OSINT alkalmazások, amik segítségével ellenőrizhetőek a népszerű online szolgáltatásoknál regisztrált azonosítók. Ha létezik, akkor a publikussá vált jelszóval próbálnak belépni. Sok esetben ezzel könnyű bejutni más fiókokba.
Emiatt érdemes tehát a nem használt fiókokat megszűntetni, leiratkozni olyan hírlevelekről, amik nem relevánsak számunkra. Ezzel időt is megtakaríthatunk, mert csökkenthető a levélszemét és az általuk az eszközeinkre juttatott kártékony kódok. A korábban javasolt jelszóadatbázisban viszont érdemes megtartani a bejegyzést, az aktuális bejegyzséektől elkülönítve. Ennek előnye, hogy később monitorozhatjuk, ha bármilyen általunk használt azonosító vagy jelszó komprmittálódott-e vagy sem.
Egyszerű, akár Google keresővel, a saját felhasználói azonosítóinkra rákeresve szembesülhetünk, hogy mennyire könnyen elérhetőek ezek az adatok. Természetesen megfelelő célszerszámmal, OSINT eszközök felhasználásával még több információ gyűjthető össze. Személyes javaslatom, hogy mindig csak annyit mutassunk meg, amivel nyerhetünk...

14.2. E-mail kommunikáció

Egy e-mailt megírni és elküldeni nem egy bonyolult folyamat, viszont adataink biztonsága érdekében szükséges néhány részlettel tisztában lenni és a szükséges biztonsági intézkedéseket eszközölni. Kezdjük rögtön az e-mail fiókok számával. Egy felmérés [20] alapján kiderült, hogy átlagosan 1,75 e-mail fiókja van egy embernek. Természetesen ez világszinten értendő átlag. Miért fontos a biztonság szempontjából, hogy hány e-mail fiókkal rendelkezünk? Ha mindenhol ugyanazt az e-mail címet adjuk meg és regisztráljuk külnböző internetes szolgáltatások során, előbb vagy utóbb be fog kerülni egy adatbázisba, amit fel fognak használni különböző támadásokra. Az e-mail szolgáltatók, fiókok és felhasználók gyakran szerepelnek célpontként. Adathalász, kártékony kódot, vagy fertőzött oldalra irányító linket, amire kattintva automatikusan letöltődik a kártékony

kód, tartalmazó e-maileket küldenek tömegesen. Ehhez e-mail címekre van szükségük, amiket többféleképpen szerezhetnek meg. Dark weben megvásárolják, OSINT technikákkal, erre a célra kifejlesztett nyilvános adatbázisokban kereső szolgáltatások és szkriptek segítségével összegyűjtik, vagy egy megfertőzött e-mail fiókon keresztül az e-mail fiók összes névjegyét letöltve és újra fertőzve építenek fel hatalmas mennyiségű e-mail címeket tartalmazó adatbázisokat.

14.2.1. Támadások

Az E-mail fiók védelme több szempontból is fontos. Ha egy szolgáltatásra az e-mail címünkkel regisztrálunk, akkor a szolgáltatásba a támadók az e-mail fiókunkon keresztül is bejuthatnak. A jelszó alaphelyzetbe állításával érkezik egy link az e-mail fiókunkba, aminek segítségével a támadók megadhatnak egy új jelszót, ezzel pedig átveszik a fiók felett az irányítást. Természetesen ehhez az e-mail fiók felett is át kell venniük az irányítást.

- Az e-mail fiókunk segítségével megszemélyesítéses támadást hajthatnak végre a támadók a nevünkben. A kiszemelt célpont az e-mail címünkről érkezett e-mail alapján gyanakvás nélkül nagyobb eséllyel tölti le a fertőzött csatolmányt, vagy nyitja meg a kártékony kódot tartalmazó linket.
- Online automatizált eszközökkel publikus adatok között kutatva akár Sherlock [21], Hunter.io [22], stb. segítségével rátalálhatunak a támadók az e-mail címünkre, még könnyebb dolguk van akkor, ha azt valamilyen publikus felületen közzétesszük. Emellett a felhasználónévhez tartozható jelszavakat is keresnek, melyek valamilyen okból nyilvánossá váltak, majd ezek párosításával a támadók megpróbálnak belépni a fiókunkba.
- Ha az előbbi esetben nem járnak sikerrel, kapcsolatba léphetnek velünk, másnak kiadva magukat a bizalmunkba férkőzni. Ha ezt sikeresen teljesítették, küldhetnek fertőzött e-mailt, amit például egy metasploitot felhasználva készítenek, a tartalmát megnyitva a mi számítógépünkön lefutva kapcsolatot épít ki a támadók által irányított szerver között és ezen a csatornán keresztül billentyűfigyelés vagy más eszköz segítségével megszerezhetik a jelszót.

14.2.2. Védjük meg e-mail fiókunkat

E-mailben érkező támadások esetén lehetőségünk van védekezésre azonban a megfelelő körültekintő viselkedés elengedhetetlen. Több e-mail fiók használata esetén lehetőségünk van az e-maileket fiókonként csoportosítva rendezni, amivel kizárhatunk néhány támadást. Lehetőség szerint kategorizáljuk a fiókokat a kommunikáció és adattartalom alapján. Miért fontos, hogy több e-mail cím legyen? Ha csak egy címmel rendelkezünk és azt a különböző oldalakon egy adott felhasználónévvel osztjuk

meg például fórum, önéletrajz, közösségi média, akkor könnyebben beazonosítható a használója. Ez a támadóknak segít célzott támadást indítani. Tehát több e-mail cím más-más célra, lehetőleg más és más névvel, ami nem hasonlít a többi e-mail címre. A kategorizálás is egyén és felhasználói szokástól függ például számlák, ügyfélkau, közösségi médiák, vásárlás, stb. Néhány e-mail címet megosztunk másokkal, néhányat viszont nem. Így csökkenthetőek a spam e-mailek, amik jobb esetben a spam mappában gyűlnek, azonban kizárólag csak erre sem hagyatkozhatunk. Nagyon jól felépített és a felhasználót können megtévesztő e-mailek is bekerülnek a bejövő mappába

14.2.3. A jó e-mail fiók

Keressünk olyan e-mail szolgáltatót ahol a biztonság kiemelkedő szerephez jut. A Cybernews [23] kimutatása alapján a Protonmail-t jegyzi a legbiztonságosabb email szolgáltatónak. A többfaktoros autentikáción kívül a végpont-végpont közötti titkosítás mellett hatékony spam szűrővel rendelkezik. A spam küldő szolgáltatások nyiulvánosságra került felhasználónevekből készítenek maguknak saját listát lehetséges e-mail címekkel, ahova a szolgáltató tehát a @ utáni domaint behelyettesítik a legnépszerűbb szolgáltatásokéval. A protonmail jelenleg még nem annyira népszerű, mint a Gmail vagy a Yahoo, emiatt még nem fókuszálnak annyira erre a szolgáltatóra.

14.2.4. A védelem 4 lépése bejövő e-mail esetén

1. Az első, hogy vizsgáljuk meg az e-mailt, amit kaptunk. Ebbe a fiókba vártuk az e-mailt? Ezt az e-mail címet használtuk a regisztrációhoz? Nyelvtanilag és formailag helyes az e-mail? Ha nem, akkor biztosak lehetünk benne, hogy támadás és nem valódi a tartalma. Kitől kaptuk az e-mailt, tőle vártuk?
2. Az egeret húzzuk a link fölé, ami az e-mailben szerepel. A böngésző bal alsó sarkában ilyenkor megjelenik a valódi internet cím. Ha ez a link nem ismert oldalra visz, vagy IP cím látható, akkor biztosak lehetünk benne, hogy e-mailben történő támadás célpontjai vagyunk. Nem várt címről érkező e-mailben érkező csatolmányt ne nyissunk meg.
3. Rövidített link esetén lehetőségünk van például az Expand URL [24] szolgáltatással megnézni, hogy milyen oldalra vezet a rövidített cím. Spam levélre ne válaszoljunk, hogy ezzel elkerüljük a megerősítést, hogy az e-mail cím valós és használatban van.
4. Ha releváns számunkra a link, és nem találtunk semmi gyanúsat, megnyithatjuk azt.

14.2.5. Védelem kimenő e-mailek esetén

Mielőtt elküldjük az e-mailt, érdemes átnézni árulkodó jelek után. Ilyen lehet például az e-mail aláírás is. Ha be van állítva, alapértelmezett aláírásként, hogy jelenítse meg, hogy

milyen vírusírtó szoftver vizsgálja át a levelet, akkor azt mindenképp kapcsoljuk ki. Ez az információ is adhat támpontot egy támadáshoz. Ha tudják a hackerek, hogy milyen vrusírtóval rendelkezünk, akkor kihasználhatják annak gyengeségeit. Sőt, ha az adott vírusírtó verziószáma is szerepel, akkor még precízebb támpontot adhat a támadóknak kihasználni az adott vírusírtó sérülékenységeit. A virustotal egy online felület, ahol szabadon átvizsgálható egy adott fájlt, hogy tartalmaz-e vírust vagy sem. Ezt az oldalt ahsználva a támadók, addig finomíthatják a vírust, amíg az adott vírusírtó, amiről már tudnak ne ismerje fel és kihszanálhassa az áldozat eszközeinek gyenge pontjait. Amennyiben szükségünk van titkosításra használhatunk akár erre alkalmas PGP kompatibilis alkalmazást is, melynek használatát később fogom kifejteni.
Akár az általunk elküldött e-mailekre válaszolva vagy bármi előzmény nélkül kaphatunk e-mailt. Mielőtt megnyitjuk a levelet jó, ha megvizsgáljuk a feladót, az e-mail fejlécét és árulkodó jelek után kutatunk. A rohanó és impulzusokkal teli mindennapokban is ajánlott erre időt szakítani, mert egy árulkodó vagy hibás nyelvhasználat felismerése is megmenthet attól, hogy kiadjuk jelszavunkat, vagy egy kártékony kódot tartalmazó számlának tűnő pdf fájlt megnyissunk.

Egyes esetekben jó szolgálatot tehetnek az eldobható e-mail címek, amiket egy bizonyos célra használunk fel például vásárlás, regisztráció meglététől függö adatokhoz való hozzáférés, stb. Később ezeket törölhetjük. Az Apple is kínál olyan szolgáltatást, ahol egy véletlenszerű e-mail cím mögé rejthetjük el a saját valódi e-mail címünket, vagy a ”throwaway e-mail” kulcsszóra rákeresve találhatunk szolgáltatókat, ilyen például a mailbox.org, ahol akár 25 alias e-mail címet is használhatunk.

14.3. Közösségi média felületek

A különböző célra kifejlesztett közösségi média platformok különböző felhasználói kört céloznak meg szolgáltatásaikkal. A legtöbb ilyen szolgáltatás úgymint a Facebook, Instagram, Twitter, LinkedIn alapvető védelemként javasolja, hogy felhasználóként tegyünk meg mindent a fiókunk védelme érdekében. A szolgáltatások által kínált biztonsági funkciók használatán kívül figyelnünk kell arra, hogy mit osztunk meg másokkal. Nem szabad figyelmen kívül hagyni, hogy minden, amit nyilvánosan megosztunk, azt minden kereső beindexeli és nyilvánosan elérhető és felhasználható lesz. A közösségi médiával kapcsolatosan ki kell térnünk néhány dolgra, melyek hozzátartoznak az adatok biztonságos kezeléséhez.

14.3.1. Helyadatokra vonatkozó információk

A közösségi oldalak, és számos weboldal extra funkcionalitást tesz lehetővé, ha megosztjuk a pontos helyadatainkat az oldallal. Segítségével megcímkézhetjük a földrajzi adatokkal a megosztott képeket, vagy a hozzánk közelebb eső használni kívánt szolgáltatást

és annak elérhetőségeit kínálja fel, azonban a helyadataink kiadásával nyilvánossá válik jelenlegi tartózkodási helyünk, vagy az utazási célként megjelölt hely. Ennek segítségével extrapolálhaó a támadók számára a távollét ideje, mely időablakot kihasználva betöréses, besurranásos lopás áldozataivá válhatunk. Egyes közösségi oldalak, pl: a Facebook arcfelismerő funkciója képes beazonosítani és megjelölni mindenkit egy adott fotón, amely egyrészről kényelmes, másrészről a név és a hozzá tartozó profil elérhető a támadók számára, ahonnan további adatokat gyűjthetnek az áldozatról. Léteznek OSINT eszközök, melyek IP címünk segítségével viszonylagos pontossággal behatárolható a tartózkodási helyünk. A közösségi adatokon keresztül megosztott helyadatok, képek, szöveges tartalmak elemzésének segítségével pontosítható ez az adat. Ezeket a funkciókat érdemes kerülni, ha mégis szükséges a használata, akkor tudatosan és jól megfontoltan használni. Lehetőség van az adatok láthatóságának szabályozására, ezek lehetnek publikus, vagyis bárki számára látható vagy csak ismerősök számára látható, vagy csak a fiók tulajdonosa, illetve adott személyek számára a hozzáférés letiltása illetve engedélyezése.

14.3.2. Harmadik féltől származó alkalmazások által használt adatok

A közösségi oldalakon használt harmadik féltől származó alkalmazások közül számtalan alkalmazás kér a szükségesnél több engedélyt eszközeinkhez. A híres Face App, mely a mobilkészüléken található fotók manipulálása miatt vált népszerűvé. Funkciója betöltéséhez hozzáférésre van szüksége a kamerákhoz és a fotókhoz. A fényképek manipulálása nem a saját eszközünkön történik, ehhez az alkalmazásnak fel kell töltenie őket egy felhőtárhelyre, ahol a manipuláció megtörténik. A felhőtárhelyre feltöltött képek törlésére a felhasználóknak nincs lehetőségük. Törlésükről a szolgáltató gondoskodik, melyről a felhasználó nem tud meggyőződni. Az alkalmazások funkicóinak sokszínűsége miatt, óvatlanul átadhatjuk az irányítást a kamera, telefonkönyv, üzenetek és egyéb adatok irányítása felett. Az alkalmazások testreszabásához számos adatot kérhet tőlünk, egészségügyi, érdeklődési kör, és egyéb felhasználható adat, melyek a specifikus és irányított funkciók hatékonyságnövelését eredményezhetik. Azonban az adatok felhasználhatóak tevékenységeink monitorozására. Mennyi időt és hol töltünk a nap folyamán, érdeklődési körünkkel kapcsolatos témával kezdeményezett kapcsolatfelvétel, vagy a fentebb tárgyalt social engineering technikák segítségével. A támadók által megszerzett adatokkal az áldozat részletesebb profilját képesek kialakítani. Vagy ahogy Dobák Imre és Tóth Tamás fogalmazott „ ...az egyes adathalmazokban megjelenő metaadatok, amelyek komplex elemzése és értelmezése, majd további adatbázisokkal történő kiegészítése akár szenzitív jellegű adathalmazok létrehozását is jelenthetik, például profilozás vagy kapcsolati hálók megalkotása során.” [25] következtethetnek bizonyos jövőben bekövetkező cselekedetekre. Ahogy a többfaktoros azonosításra is egyre több helyen van lehetőség, úgy harmadik féltől származó úgy nevezett 3rd alakalmazások jogosultságainak felülvizsgálatára is van lehetőség. A nem használt vagy

elavult alkalmazások adatainkhoz való hozzáférését javasolt megvonni, és csak akkor engedélyezni a működésüket, amikor valóban szükséges.

14.3.3. Megosztásokra, posztokra vonatkozó paraméterek

A közösségi platformok használata során a felhasználók posztokat, képeket, videókat oszthatnak meg a többi felhasználókkal. Ezek egyik paramétere a láthatóság, és a megjelölés lehetősége, melyek segítségével beállítható, hogy ki láthatja a posztot és ki jelölhet be egy adott poszt alatt. Támadási felületet adhat ez a funkció, ha a beállítások hanyag kezelése során, olyan posztokban jelölnek be felhasználókat, melyek tartalmaznak kétes, vírust tartalmazó weboldalakra vezető linket, melyre kattintva a felhasználó saját magát sodorja veszélybe. A támadók egy ilyen lehetőséggel tömegeket vehetnek célba. A célszemélyek eszközeinek további biztonsági beállításától - minimum egy naprakész vírusírtó és tűzfal - függ, hogy milyen feladatra használhatják fel a támadók a megszerzett erőforrást. Ezek lehetnek kripto bányászat, proxy chain, személyes adatok felhasználása és számtalan egyéb feladat. 2020-ban az ausztrál miniszterlenök Tony Abbott Instagramon posztolt beszállókártyájáról egy képet, majd 45 perccel később egy etikus hacker Alex Hope megszerezte a telefonszámát és az útlevele legfontosabb adatait. [26]

14.3.4. Felhasználókat érintő további adatok

A közösségi média használatához meg kell adnunk az e-mail cím, telefonszám, születésnap, lakóhely, valamint egyéb személyes adatokat. A platform az adatokat az általa nyújtott szolgáltatás magasabb színvonala miatt kéri. Segítségével az ismerősök könnyebben azonosíthatják be egymást. Azonban, a fenti adatok mellett a felasználóknak lehetőségük van bizonyos személyeket külön státuszban megjelölni, rokoni, családi állapot alapján. Tehát a támadónak lehetősége van az áldozat kapcsolati hálójának feltérképezésére, bizonyos személyeket kihasználni megszemélyesítéses támadás segítségével, valamint telefonos azonosítással a megfelelő adatok, mint születési hely, idő, anyja neve, lakcím megadásával az áldozat nevében eljárni.

14.3.5. Facebook

A Facebook viszonylag széles tevékenységi lehetőségeket nyújt a felhasználóinak, emiatt rengeteg adatot osztanak meg, rendelkeznek kapcsolati hálóval, üzenetekkel, küldhetnek egymásnak fájlokat, képeket, videókat, és egyéb szenzitív jellegű adatokat, telefonszámok, e-mail és lakcímek. A kapcsolati hálót felhasználhatják arra, hogy könnyebben küldjenek, terjesszenek olyan linkeket, melyek egy fertőzött kódot tartalmazó oldalra irányítja azt, aki rákattint. A Facebook esetén, ha olyan személy küld üzenetet, aki nem szerepel a kapcsolati hálóban, akkor az egyéb kategóriába kerül az üzenet, amit nem jelez rögtön a Facebook, viszont a kapcsolati hálón belülről jövő üzenet esetén, azonnal

éretsítést kap a felhasználó. Emiatt szükséges a támadók számára, hogy hozzáférjenek az adott fiókhoz. Ha a felhasználó megnyitja az ismerőstől kapott linket, a lefutott támadó kód irányítása alá vonhatja a felhasználó eszközét, adatot szerezhet meg róla, további támadást indíthat. A szenzitív adatok megszerzésével, pedig zsarolhat, pénzt kérhet a fiókért vagy az adatokért cserébe. Hogyan védjük meg a Facebook fiókunkat?

- Gondoskodjunk arról, hogy minden eszközünkön alkalmazzuk az elérhető legmagasabb védelmet.
- Mobilkészülékünk rendelkezzen csak számunkra könnyen, demások számára nehezen kitalálható képernyőzárral, vírusírtó alkalmazással, és zároljuk az alkalmazást.
- Bejelentkezéshez használjuk a hivatalos linket vagy alkalmazást.
- Számítógépünk legyen erős jelszóval védett és naprakész vírusírtó alkalmazással rendelkezzen.
- Ne mentsük a bejelentkezéshez használt jelszót a böngészőben.
- Minden ezsközünk a lehető legfrissebb operációs rendszert használja.
- Egyedi megfelelően erős jelszót használjunk, amire korábban a jelszavak kezeléseénél kitértünk.
- Alkalmazzunk többfaktoros azonosítást, Authenticator alkalmazás, hardveres kulcs, vagy ezek kombinációit.
- Állítsunk be megbízható kontaktokat, akik segítségével visszaállíthatjuk a fiókunkat, ha támadás esetén nem férnénk hozzá.
- Vizsgáljuk meg, hogy milyen posztokhoz és adatokhoz férhetnek hozzá rajtunk kívül. Mit láthatnak mások.
- Ne fogadjunk el ismeretlenektől származó kapcsolati kérést.
- Ha rövidített linket tartalmazó üzenetet kapunk, ne nyissuk meg őket.
- Harmadik féltől származó alkalmazásokat ne kapcsoljunk a Facebook fiókhoz.
- Ne kössük össze Facebook fiókunkat semmilyen szolgáltatással, így elkerüljük Facebook fiókunk kompromittálása esetén, hogy felhasználják a csatolakoztatott fiókokban tárolt adatokat.

14.3.6. Instagram

Az Instagram a Facebook tulajdonában áll, a kínált biztonsági azonosak. A támadók a Facebook támadáshoz hasonló módon képesek hozzájutni felhasználói fiókokhoz. Ugyan Instagram fiókunk kevesebb adatot tart nyilván, mint a Facebook, de a támadók számára ez az adatok ugyanúgy értékesek. A platform a Facebookhoz hasonlóan népszerű,

emiatt könnyen találhatnak olyan célpontokat a támadók, akik nem könnyebben kihasználhatóak. A keresőmotorok hasonlóan a Facebook tartalmakhoz ugyanúgy képesek beindexelni és nyilvánosan kereshetővé tenni azokat a tartalmakat, melyeket nyilvános profilok osztottak meg. Hogyan védjük meg a Instagram fiókunkat?

- A profil legyen privát.
- Az aktivitás megjelenítését rejtsük el.
- Gondoskodjunk arról, hogy minden eszközünkön alkalmazzuk az elérhető legmagasabb védelmet.
- Mobilkészülékünk rendelkezzen csak számunkra könnyen, demások számára nehezen kitalálható képernyőzárral, vírusírtó alkalmazással, és zároljuk az alkalmazást.
- Bejelentkezéshez használjuk a hivatalos linket vagy alkalmazást.
- Számítógépünk legyen erős jelszóval védett és naprakész vírusírtó alkalmazással rendelkezzen.
- Ne mentsük a bejelentkezéshez használt jelszót a böngészőben.
- Minden eszközünk a lehető legfrissebb operációs rendszert használja.
- Egyedi megfelelően erős jelszót használjunk, amire korábban a jelszavak kezeléseénél kitértünk.
- Alkalmazzunk többfaktoros azonosítást, Authenticator alkalmazás, hardveres kulcs, vagy ezek kombinációit.
- Ha rövidített linket tartalmazó üzenetet kapunk, ne nyissuk meg őket.

14.3.7. Twitter

Hasonlóan az Instagramhoz a Twitter esetén sincs olyan kapcsolati háló, mint a Facebooknál. Ebben az esetben is követések, megjelölések vannak. A megosztott információk követések alapján válnak elérhetővé, így követés után bárki hozzáférhet egy megsoztáshoz, ebben az esetben tweethez. Hogyan védjük meg a Twitter fiókunkat?

- A követések engedélyhez kötését aktiváljuk
- Szűkítsük azok körét akik küldhetnek Üzeneteket.
- Gondoskodjunk arról, hogy minden eszközünkön alkalmazzuk az elérhető legmagasabb védelmet.
- Mobilkészülékünk rendelkezzen csak számunkra könnyen, demások számára nehezen kitalálható képernyőzárral, vírusírtó alkalmazással, és zároljuk az alkalmazást.
- Bejelentkezéshez használjuk a hivatalos linket vagy alkalmazást.

- Számítógépünk legyen erős jelszóval védett és naprakész vírusírtó alkalmazással rendelkezzen.
- Ne mentsük a bejelentkezéshez használt jelszót a böngészőben.
- Minden eszközünk a lehető legfrissebb operációs rendszert használja.
- Egyedi megfelelően erős jelszót használjunk, amire korábban a jelszavak kezeléseénél kitértünk.
- Alkalmazzunk többfaktoros azonosítást, Authenticator alkalmazás, hardveres kulcs, vagy ezek kombinációit.
- Ha rövidített linket tartalmazó üzenetet kapunk, ne nyissuk meg őket.
- Harmadik féltől származó alkalmazásokat ne kapcsoljunk a Facebook fiókhoz.

14.3.8. LinkedIn

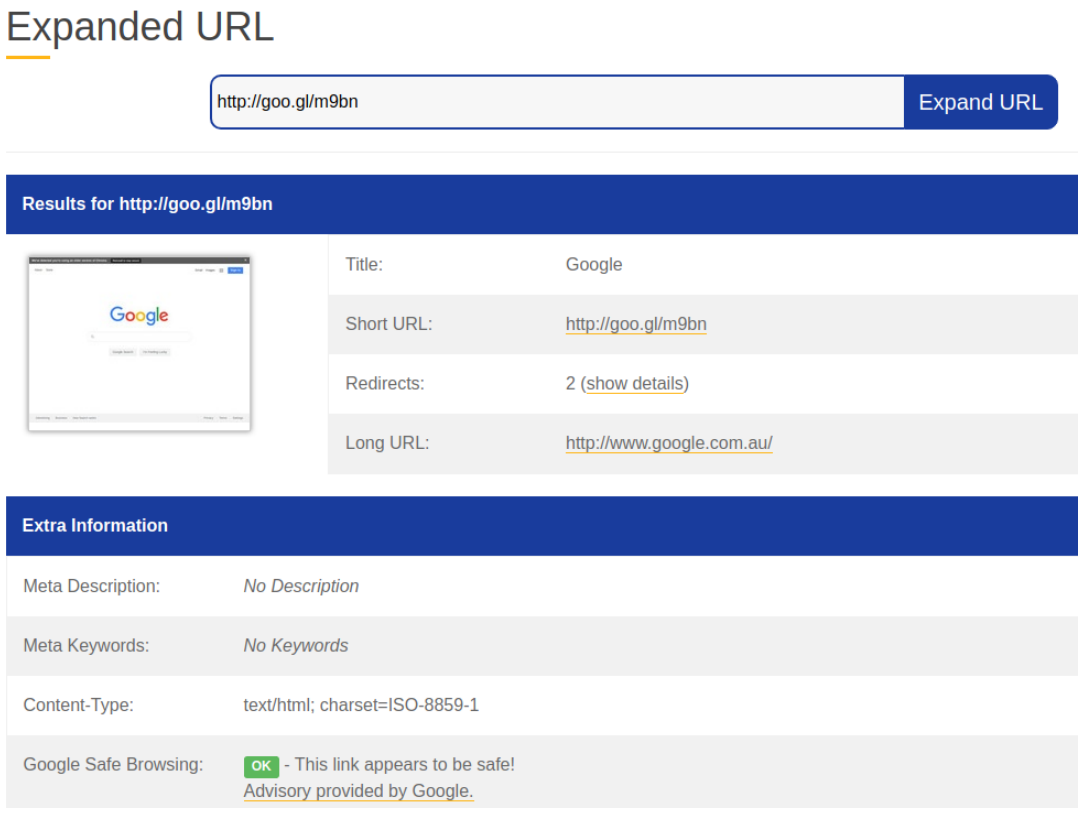
A LinkedIn egyfajta szakmai közösségi platfrom, ahol a szakmai fejlődés lehetőségét és az álláskerést helyezi előtérbe. Ezen a felületen szintén van lehetőség üzenetek küldésére, emiatt könnyen találhatunk olyan üzenetet, ami tartalmazhat kártékony kódot tartalmazó linket. Az új ajánlatok az előrelépés lehetősége az embereket felcsigázzák, ebben az esetben nyitottabbak lesznek egy ártatlannak tűnő ajánlattal kapcsolatban, ami miatt előfordulhat, hogy nem ellenőrzik a linket, ami az ígért leírást tartalmazza. A Social Engineering technikákat kihasználva a támadó könnyedén hozzáférhet a kiszemelt áldozat önéletrajzához, személyes adataihoz. Hogyan védjük meg a LinkedIn fiókunkat?

- A követések engedélyhez kötését aktiváljuk
- Szűkítsük azok körét akik küldhetnek Üzeneteket.
- Gondoskodjunk arról, hogy minden eszközünkön alkalmazzuk az elérhető legmagasabb védelmet.
- Mobilkészülékünk rendelkezzen csak számunkra könnyen, demások számára nehezen kitalálható képernyőzárral, vírusírtó alkalmazással, és zároljuk az alkalmazást.
- Bejelentkezéshez használjuk a hivatalos linket vagy alkalmazást.
- Számítógépünk legyen erős jelszóval védett és naprakész vírusírtó alkalmazással rendelkezzen.
- Ne mentsük a bejelentkezéshez használt jelszót a böngészőben.
- Minden eszközünk a lehető legfrissebb operációs rendszert használja.
- Egyedi megfelelően erős jelszót használjunk, amire korábban a jelszavak kezeléseénél kitértünk.
- Alkalmazzunk többfaktoros azonosítást, Authenticator alkalmazás, hardveres kulcs, vagy ezek kombinációit.

- Ha rövidített linket tartalmazó üzenetet kapunk, ne nyissuk meg őket.
- Harmadik féltől származó alkalmazásokat ne kapcsoljunk a LinkedIn fiókhoz.
- Linkedin profilunkat se kapcsoljuk össze más fiókokkal a korábban említett ok miatt.

Láthatjuk, hogy mind a négy esetben lehetőségünk van precízen szűrni, hogy milyen adatok lehetnek publikusak. Mindamellett mind a négy esetben látható, hogy üzeneteken keresztül küldött fájlok és linkek esetén nem találhatunk olyan lehetőséget, ami megszűri a tartalmat. Ebben az esetben szükség van kellő körültekintéssel kezelni a kapott linket vagy fájlokat.

- Csak olyan személyektől fogadjunk tartalmat, akit ismerünk, azonban ezt is szűrjük meg, előfordulhat, hogy a küldő fiókját kompromittálták
- Minden esetben ellenőrizzük a kapott linket. Az Expand URL kulcsszavakkal keresve találhatunk oylan szolgáltatást, amelyik megmutatja, hogy mi az eredeti link, így ennek tudatában eldönthettjük, hogy releváns-e a számunkra vagy sem. Erre egy példa: 14.16 ábrán látható.



14.16. ábra. Példa egy rövdített link felfedésére

14.4. Mobilkommunikáció és a telefonszám

Manapság már nagyon vigyázunk, hogy kinek adjunk meg telefonszámunkat, ezzel elkerülhetjük a zaklatosáokat és az egyéb kényelmetlen, időrabló telemarketinges hihetetlennek tűnő ajánlatokat, megkereséseket. Viszont érdemes tisztában lenni azzal is, hogy mint minden informatikai eszköznek, úgy a mobilkészülékeknek is vannak sérülékenységeik. Előfordult már olyan eset, amikor használhatatlanná váltak egyes készülékek, egy SMS-ben kapott bizonyos karaktersortól. Más sérülékenységek kihasználása esetén a támadók az áldozatnak egy SMS-ben küldött, megadott karaktersor által kiváltott események hatására átvehették az irányítást a készülék felett. Ezt a sérülékenységet SimJackernek [27] nevezték el. Ez a rosszindulatú alkalmazás a SIM kártya és a mobilkészülék sebezhetőségét kihasználva fejti ki hatását. Ehhez szükséges a mobilszolgáltató által elmulasztott biztonsági beállítás hiánya is. A jövőben is várható, hogy egyre több hibát fedeznek fel, de az esetek többségében csak a támadások végrehajtása után kerül napvilágra és kijavításra. Az, hogy nem tudunk egy hibáról, vagy nem gondoljuk, hogy a hiba létezik, attól még a hiba fennáll és előbb-utóbb felfedezik és kihasználják. Ajánlott figyelemmel kísérni, hogy a készülékünkre milyen szoftverforrásból telepítettünk alkalmazásokat. Egyébiránt ha a kétfaktoros azonosítás során az SMS a második faktor, az egy gyenge pont a folyamatban. Sajnos nem minden szolgáltatás esetén elterjedt, hogy SMS-en kívül más is használható legyen a kétfaktoros azonosításra. Emiatt javaslom, az olyan online szolgáltatók használatát, ahol virtuális SIM vásárolható, amivel a csak SMS-t támogató kétfaktoros azonosítás használható. Ezzel megoldható, hogy ne kelljen kiadni a saját telefonszámunkat. Ilyen szolgáltató például a Hushed [28]. Ideiglenes telefonszámok használatával csökkenthető a saját telefonszámunk és mobilkészülékünk kitettsége.

14.4.1. Mobilkészülékünk védelme

A készülék és a rajta futó operációs rendszer, valamint az alkalmazások biztonsága abban az esetben adhat magasabb védelmet, ha a felhasználói beállítások kitérnek a következően ajánlott pontokra. A teljesség igénye nélkül lentebb található egy lista, melyek alkalmazását a Texasi Egyetem [29] is javasolja.

- Semmiképp ne használjuk root vagy rendszergazda jogokkal.
- A készüléket titkosítsuk akár a gyártói előre telepített funkciókkal.
- Tartsuk naprakészen az operációs rendszert és az alkalmazásokat.
- Alkalmazzuk a SIM-kártya zárat.
- PIN kóddal, vagy biometrikus azonosítással kombinált Képernyőzár használata.
- Csak megbízható forrásból szerezzük be az alkalmazásokat.
- A nem használt alkalmazásokat távolítsuk el.

- Alkalmazások megfelelő jogosultság beállításával elkerüljük a kamera és mikrofon illetéktelen használatát.
- Antivirus alkalmazás használata.
- Ha nincs használatban, kapcsoljuk ki a Wifi Bluetooth és GPS funkciókat.
- Rendszeres időközönként készítsünk biztonsági mentéseket.

15. OSINT TECHNIKÁK FELHASZNÁLÁSA

OSINT vagyis Open Source Intelligence, jelentése nyílt forrású hírszerzés, számtalan szkript és eszköz segítségével a támadók nyílt és bárki számára elérhető információk között keresik meg a célpontjukról elérhető összes információt. A felderítést két kategóriába sorolhatjuk.

- Passzív: olyan módszerek használata, amellyel nem keletkezik nyoma a kutatásnak, ezek jellemzően különböző kereső algoritmusok és keresési tevékenységek. A célponnak nem lesz információja az elvégzett információgyűjtésről.
- Aktív: ebben az esetben a keresésről készül egy bejegyzés, a monitorozott rendszerben, ami lehet tűzfal, rendszernapló, vagy egyéb szolgáltatás. A naplóbejegyzés alapján. A célpont ilyenkor tudomást szerezhet a tevékenységről.

Ezek olyan nem titkosított információk, melyek felfedezése, azonosítása, feldolgozása szándékos és célirányos. A legtöbb esetben ezek az információk valamilyen figyelmetlenség következtében lettek nyilvánosak. Paráda István és Farkas Tibor [30] által bemutatott metódus szerint látható, hogy a felderítés és elemzés több szintből áll. Első lépésben a nyilvánosan elérhető adatok elmezése során kigyűjtött információkból és az elérhető hálózati információk elemzéséből kapott adatokból a támadók az áldozat számítógép hálózatának feltérképezésével gyenge, támadható felületek kihasználásával képesek lehetnek a hálózati forgalom lehallgatására, eszközök megfertőzésére. A felhasználó viselkedése, illetve a viselkedésére jellemző mintázatokból elemzések során megszerzett információk segítségével feltérképezhetőek akár épületek is. Az amerikai hadsereg emiatt megtiltotta katonáinak okosórák használatát. A Strava fitnessz alkalmazás által generált és nyilvánossá tett térképeken használóik által bejárt útvonalakat jeleníti meg. A tiltást egy incidens előzte meg, mely során amerikai katonák távolkeleti állomáshelyeiken is használt okosórák által gyűjtött adatokból az épületeken belül bejárt útvonal alapján a bázisok alaprajza kivehetővé váltak. Az esetet részletesebben Cyprian Aleksander Kozera [31] cikkében ismerteti.

OSINT alkalmazásokat és használatukhoz szükséges leírások megtalálhatóak az interneten, illetve CaaS vagyis Crime as a Service rendszerben bérelhető szolgáltatást is kínálnak a kiberbűnözők. Nyílt információként begyűjthetőek többek között a publikus IP címek, telefonszámok, e-mail címek, sociális kapcsolatok, megosztott fotók, képeken megjelölt címek és személyek információi, valamint minden olyan információ, ami szándékosan, vagy véletlenül vált nyíltan elérhetővé.

A közösségi oldalakon megosztott információk alapján a támadóknak lehetőségük van követni az célpontját, időrendi sorrendben megtalálhatóak a megosztott tartalmak Ezeket felhasználva Social Engineering segítségével a támadó az áldozat megtévesztésével

eléri az imerős felkérés visszaigazolását, követését, majd az Osintgram [32] alkalmazás segítségével begyűjthetik azokat a tartalmakat, melyet csak privát vagy ismerősi jogosultsággal lehet elérni. Ehhez csupán egy Google fiókra és egy Instagram fiókra van szükség. A Google Cloud Platform segítségével ingyenesen elérhető a futtatáshoz szükséges Linux szerver. A Phoneinfoga [33] alkalmazás segítségével a Google kereső által eddig beindexelt tartalmak között képesek vagyunk telefonszámhoz tartozó információkat keresni, keresők által beindexelt oldalakon, nyilvános közösségi média posztokban megkeresi az adott telefonszámot, ahol az áldozattal kapcsolatos információk, melyeket vagy ő osztott meg vagy róla osztottak meg. Ezen információk az áldozatról készített profilt részletgazdagabbá teszi. A megszerzett információk alapján további támadásokat hajthatnak végre.

OSINT eszközök gyűjteményét és használatukhoz szükséges leírásokat több oldal is jegyez, melyek közül kiemelném [34] oldalát.

A kibertámadások sikeres lebonyolításához elengedhetetlen a releváns adatok begyűjtése, rendszerezése és elemzése. A támadónak tisztában kell lennie a támadás célpontjára, informatikai rendszerére jellemző, valamint a végrehajtáshoz szükséges lépések precíz megtervezéséhez szükséges információkkal. OSINT technikák segítségével a számítógép hálózatokra jellemző sérülékenységek felderítése és elemzése szintén lehetséges, ebben az esetben, ha ezt kéretlenül teszik, már illegális tevékenységnek számít.

15.1. Elvégzett információgyűjtés bemutatása

Az információgyűjtés bemutatásához véletlenszerűen kiválasztottam egy személyt a Facebook közösségi oldalon, akit nem ismerek, soha nem találkozatam. Kizárólag passzív információszerzés segítségével, vagyis nem léptem kapcsolatba a célponttal a következő adatokat gyűjtöttem össze:

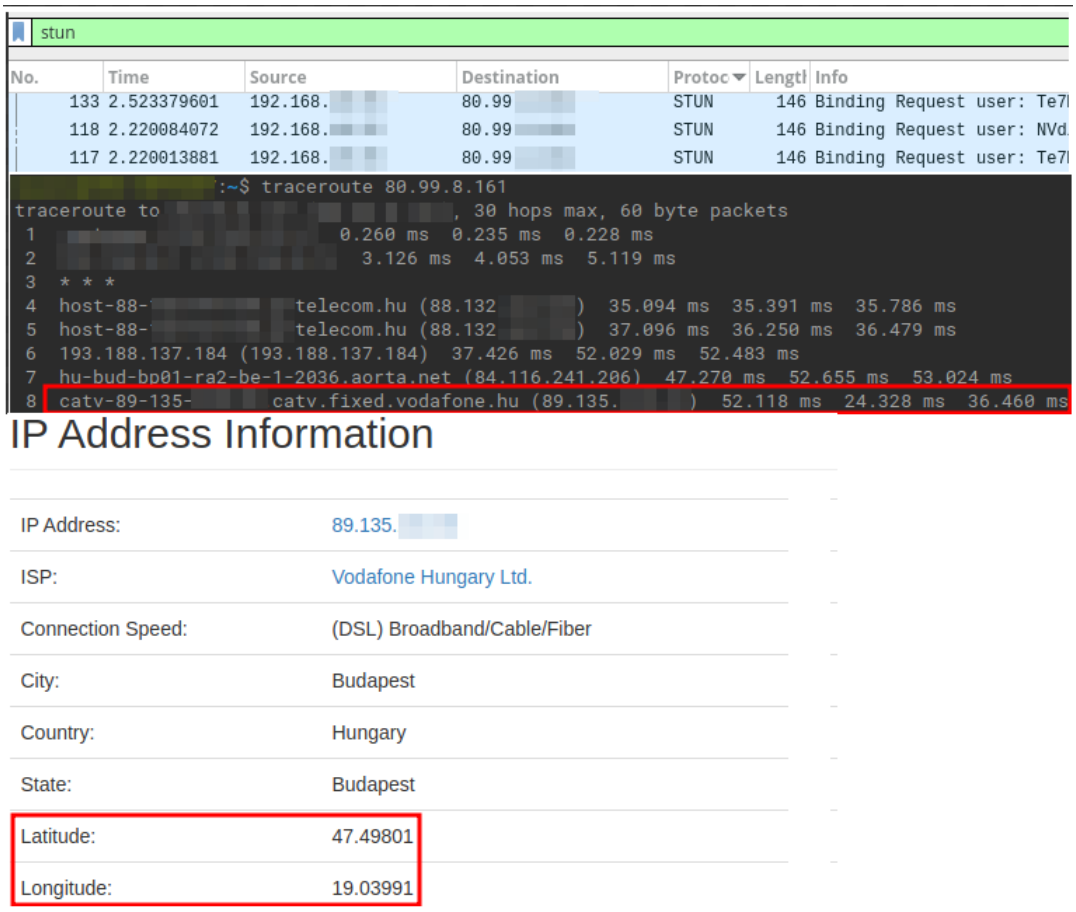
- Név, születési hely és idő. A Facebook profilban nyilvánosan megtalálható volt a születési hely, mint megjelölt életesemény. A születési időt a kereső segítségével találtam meg ahol ”Boldog születésnapot” kifejezések alapján adott találatok dátumából és tartalmából összerakható a pontos dátum. A jókívánságok között volt olyan, aki az életkort is feltűntette az üzenetében.
- Családi kapcsolatok felderítését a nyilvános képeken megjelölt személyek és hozzá fűződö szöveges tartalom alapján végeztem el. Ezeket az adatokat könnyedén sikerült begyűjteni, viszonylag gyorsan, percekben mérhető időbe telt.
- A lakcímet megtalálni már jóval több időt vett igénybe. Ehhez felhasználtam a Facebookon elérhető képek között szerepelő néhány képet, amin látható a ház, amiben lakik, valamint annak környezete. Ezeken kerestem beazonosítható pontokat, mint a ház alakja, más objektumok, ami a Google Maps-en segítségül szolgálhat a cím

beazonosításához. A keresés szűkítéséhez a Facebook bejelentkezések között megjelölt helyek között legtöbbször szereplő településen kutatva sikerült beazonosítani az épületet és annak környezetét. A 15.17 ábrán látható az épület kiemelve néhány jellegzetességet, valamint ugyanaz az épület a Google Maps-en

- Google Dorks vagyis a Google kereső és hozzá kapcsolható egyéb Google alkalmazások segítségével megtaláltam a telefonszámát, e-mail címét, személyazonosító igazolvány számát. Ehhez a Google keresőben használható kereső operátorokat felhasználva a Google által beindexelt oldalakon kerestem a telefonszám illetve e-mail cím kifejezésekre, amit egy nyilvánosan elérhető Facebook csoportban találtam meg. A személyi igazolvány számát egy dokumentumban találtam, amit a doc, docx, pdf, xls, xlsx típusú fájlokra vonatkozó keresés alapján találtam meg.
- A fentebb említett begyűjtött információk felhasználásval tovább kutatva munkahellyel, foglalkozással kapcsolatos információkat, kerestem. Nyilvános YoutTube csatornán megosztott videókban egy internetes portál használatát mutatta be. Ebben az általa használt eszköz operációs rendszerének típusát sikerült beazonosítanom, illetve ugyanezt az információt a mobileszközön futó operációs rendszerre vonatkozóan is sikerült kiderítenem.

15.17. ábra. Épület Google Maps-en és a letölttött képen

A megszerzett adatokat felhasználva több típusú támadás kivitelezése is felépíthető, melyek az illegális és büntetendő cselekmények közé tartoznak. Ahhoz, hogy a lehető legkeveseb szenzitív adat váljon nyilvánossá az előző fejezetekben tárgyalt javaslatok betartása segíséget nyújthat. Mindamellett további adatok megszerzésére is van lehetőség, melyekhez az aktív technikák felhasználásával szerezhetünk meg. Erre lehet példa egy internetes kommunikáció, mely során adatgyűjtő alkalmazást juttatunk a célpont számítógépére vagy mobilkészülékére. A kommunikáció során bevethetőek lehetnek még a korábban tárgyalt Social Engineering technikák, amivel a felhasználó befolyásolható. Vagy a kommunikáció során elemezhető az adatfolyam Wireshark segítségével, aminek segítségével kideríthető az IP cím és az internetszolgáltató is, valamint egy közelítő jellegű geolokáció. Ha a célpont nem használ VPN-t a lakcím beazonosítás esetén segítséget jelenthet ez az információ. 15.18



15.18. ábra. IP cím megszerzése kommunikációs adatfolyamból

16. ÖSSZEFOGLALÓ

A dolgozatomban felvetett probléma alapján a felhasználókat és adataikat fenyegető veszélyekre hívtam fel a figyelmet. A magatartásuk és viselkedésük következtében bekövetkező támadások felépítésének módját, valmaint a támadók lehetőségeit mutattam be. Emiatt emeltem ki a biztonságtudatos magatartás kialakításának fontosságát. Minden esetben olyan biztonságot növelő lehetőségeket javasoltam, melyek ugyan megszokást és odafigyelést igényelnek, de egyszerűek, könnyen kivitelezhetőek és a mindenapok során jól használhatóak. Ezek alkalmazása esetén az apró sikerélményeknek köszönhetően egyénfüggően növelhető a motiváció, illetve a korábban fennálló félelemérzet a biztonságot növelő technológiák iránt csökkenthető.

Az emberi tényezőkket követte az általuk használt eszközök és szolgáltatások használatával járó veszélyek bemutatása, árnyaltabb képet adva az esetleges veszélyekre. Mindamellett a felhasználó által végrehajtható biztonsági beállítások, illetve tudatos magatartása segítséget nyújthat a biztonság növelésére. Ezért fokozottan ajánlott a használt szolgáltatások és eszközök precíz biztonsági beállításainak elvégzése és időszakos felülvizsgálata. Helyenként összehasonlító és magyarázó infromációval kiegészítettem a dolgozatot, hogy megkönnyítse a választást a megfelelő biztonságot növelő eszközök kiválasztásában. Ahhoz, hogy tudjuk, hogy milyen aktuális veszélyek fenyegetnek. Javaslom a kiberbiztonsági hírek legalább felhasználói szintű követését. Ha tudjuk, hogy mikor mit frissítsünk, mert hibajavítás érkezett, hogy befoltozzon egy hibát, akkor saját magunk is elvégezhetjük azt. Amint elértük ezirányú kompetenciánk határait mindenképp kérjük szakember segítségét. Ahogy az otthoni hálózat mélyebb biztonsági beállítása esetén is javasolt. Az általam bemutatott funkciók alkalmazása szintén csökkenti a sikeres támadások esélyét. Ezzel hosszútávon időt, pénzt takaríthatunk meg és elkerülhetjük a felesleges bosszankodást. Majd a népszerűbb online szolgáltatások és közösségi média felületek biztonsági beállításait mutattam be, melyekkel csökkenthető a szenzitív adatok szivárgása. Ahhoz, hogy könnyen megértsük, hogy mennyire egyszerű személyes adatokhoz jutni a dolgozatban bemutattam egy példán kersztül egy általalm véletlenszerűen kiválasztott személy adatainak összegyűjtését és rendszerezését, melyeket passzív OSINT technikák felhasználásval hajtottam végre. A leírt példákon keresztül a védekezésre tettem javaslatokat, melyekkel csökkenthető annak az esélye, hogy az adatok illetéktelen kezekbe kerüljenek.

17. SUMMARY

In my thesis I described the rest of the reasons of data breach what can cause a user during staying online. People can be the weakest link in security chain, because their behaviors tells more about them they think. This information is useful for the attacker and increase the chance of a successfull attack. This is the reason why I started with the human firewall, how to build up and form the security awarness with easy memorable steps. This can increase the willingness to learn new methods to stay safe online. After we built up and hardened the human firewall the next step is the hardening of our devices and network. with the description of possible threats the reason of the hardening can be more acceptable then before. Backups, password database and other security enhancing features will defend as good as it can do all user data and related information. To be able to use these features and tools we have to learn new skills and it is highly recommended the progress to alwaysbe better in self defence-online. There are tons of tools out there with well defined user manuals what can be used by anybody who can find them to catch and steal user masterdata and information about any person who are sharing it online via social media or other services. With these OSINT tools information gathering can be easier then before. Because of this I made a description how I was able to gather a bunch of sensitive information about someone using passive OSINT techniques on the internet. Name, address, e-mail address, phone number, devices, and so on. These data can gives solid base to start a successfull attack against this person. Just to be on the safe side I provide solutions what can help avoid these kind of data breaches.

18. HIVATKOZÁSOK

[1] K. Anikó, „A bátorság – pszichológiai nézőpontból," *B Philosophy. Psychology*, vol. 76, no. I, pp. 1–5, 2011. utoljára megtekintve: 2021.04.21.

[2] K. Anikó, „Biztonság és magánélet. Az alkumodell megkérdőjelezése és meghaladása," *K Law / jog ¿ K Law (General) / jogtudomány általában*, vol. 103, no. I, pp. 13–36, 2017. utoljára megtekintve: 2021.07.15.

[3] L. Muha, „Az informatikai biztonság egy lehetséges rendszertana," *Q Science / természettudomány ¿ QA Mathematics / matematika ¿ QA75 Electronic computers. Computer science / számítástechnika, számítógéptudomány*, vol. 17, no. 4, pp. 137–156, 2008. utoljára megtekintve: 2021.01.09.

[4] O. E. Diána, „Social Engineering Az emberi erőforrás, mint az információbiztonság kritikus tényezője," 2008. utoljára megtekintve: 2021.02.11.

[5] „Nemzeti Kibervédelmi Intézet - Riasztások." (`https://nki.gov.hu/figyelmeztetesek/riasztas/`). utoljára megtekintve: 2022.03.17.

[6] M. W. Karen Renaud, Robert Otondo, „A biztonságtudatosítás pszichés gátjai: szubjektív veszély- és kontrollpercepció a digitális térben," *Nemzetbiztonsági szemle*, vol. 9, no. 4, pp. 241–260, 2019. utoljára megtekintve: 2021.02.15.

[7] C. V. G. M. R. Anett, *Általános pszichológia 3. - Nyelv, tudat, gondolkodás*. Budapest HU: Osiris Kiadó Kft., 2007. utoljára megtekintve: 2021.08.21.

[8] K. Héder, „A biztonságtudatosítás pszichés gátjai: szubjektív veszély- és kontrollpercepció a digitális térben," *Nemzetbiztonsági szemle*, vol. 9, no. 4, pp. 62–78, 2022. utoljára megtekintve: 2022.03.17.

[9] „HHS Cyber Security - Malware." (`https://www.hhs.gov/sites/default/files/unix-mac-linux-os-malware.pdf`). utoljára megtekintve: 2021.11.04.

[10] CVE, „Common Vulnerabilities and Exposures." (`https://cve.mitre.org/`). utoljára megtekintve: 2021.05.01.

[11] AV-TEST, „How to tell if your computer has a virus and what to do about it." (`https://www.av-test.org/en/antivirus/home-windows/`). utoljára megtekintve: 2022.03.08.

[12] NSA, „The best Windows antivirus software for home users." (`https://staysafeonline.org/blog/`

how-to-tell-if-your-computer-has-a-virus-what-to-do-about-it/). utoljára megtekintve: 2022.03.09.

[13] *Hack the Stack*. Elsevier, 2006. utoljára megtekintve: 2021.05.06.

[14] Lyrebirds, „Cable haunt vulnerability cve-2019-19494." (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19494). utoljára megtekintve: 2021.04.15.

[15] „Google Safe Browsing." (https://transparencyreport.google.com/safe-browsing/overview?unsafe=dataset:1;series:malware,phishing;start:1579219200000;end:1611791999999&lu=unsafe). utoljára megtekintve: 2021.12.04.

[16]

[17] „Yubikey 2FA Hardware Key." (https://www.yubico.com/products/). utoljára megtekintve: 2022.03.18.

[18] Techxplore, „How many passwords can you remember? get ready to remember more." (https://techxplore.com/news/2018-12-passwords-ready.html). utoljára megtekintve: 2022.03.02.

[19] „Best password managers in 2021." (https://cybernews.com/best-password-managers/)). utoljára megtekintve: 2021.12.12.

[20] „99firms - How Many Email Users Are There?." (https://99firms.com/blog/how-many-email-users-are-there/). utoljára megtekintve: 2022.06.14.

[21] „Scherlock project." (https://github.com/sherlock-project/sherlock). utoljára megtekintve: 2021.11.17.

[22] „Hunter - Email finder." (https://hunter.io/). utoljára megtekintve: 2022.01.17.

[23] Cybernews, „Secure email providers to protect your privacy in 2022." (https://cybernews.com/secure-email-providers/). utoljára megtekintve: 2022.03.01.

[24] E. URL, „Expand url." (https://www.expandurl.net/). utoljára megtekintve: 2022.03.01.

[25] I. Dobák and T. Tóth, „Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, social engineering)," *Belügyi Szemle*, vol. 69, pp. 195–212, Feb. 2021. utoljára megtekintve: 2021.11.07.

[26] „BBC News - Tony Abbott was hacked.” (https://www.bbc.com/news/world-australia-54193764). utoljára megtekintve: 2022.03.04.

[27] „The Hacker News - SimJacker.” (https://thehackernews.com/2019/09/simjacker-mobile-hacking.html). utoljára megtekintve: 2021.12.20.

[28] „Hushed - Temporary Second Phone Number.” (https://hushed.com/). utoljára megtekintve: 2021.12.04.

[29] „Handheld hardening checklists.” (https://security.utexas.edu/handheld-hardening-checklists). utoljára megtekintve: 2021.12.04.

[30] I. Parada and T. Farkas, „Felderítés és analízis a penetrációs tesztben – 1. információgyűjtési technikák,” *Hadmérnök*, vol. 15, no. 1, pp. 159–182, 2020. utoljára megtekintve: 2021.02.01.

[31] C. Kozera, „Fitness OSINT: Identifying and tracking military and security personnel with fitness applications for intelligence gathering purposes,” *Security and Defence Quarterly*, Dec. 2020. utoljára megtekintve: 2022.03.02.

[32] „Datalux, Osintgram.” (https://github.com/Datalux/Osintgram). utoljára megtekintve: 2021.10.018.

[33] „sundowndev, phoneinfoga.” (https://github.com/sundowndev/phoneinfoga). utoljára megtekintve: 2021.10.10.

[34] „A curated list of amazingly awesome osint.” (https://github.com/jivoi). utoljára megtekintve: 2021.12.04.

19. ÁBRAJEGYZÉK

20. TÁBLÁZATOK JEGYZÉKE