IT biztonság közérthetően

verzió 5.0

Neumann János Számítógéptudományi Társaság

dr. Erdősi Péter Máté, CISA
Solymos Ákos, CISM, CRISC, CDPSE

IT biztonság közérthetően

verzió: 5.0
2023 december

Kiadja a Neumann János Számítógéptudományi Társaság (NJSZT)

Szerzők:
dr. Erdősi Péter Máté CISA és Solymos Ákos CISM, CRISC, CDPSE

Szakmai lektor:
dr. Keszthelyi András

Nyelvi lektor:
Rákosi Szilvia

Kiadó: Neumann János Számítógéptudományi Társaság
1054 Budapest, Báthory u. 16.

Felelős kiadó:
Szalay Imre, ügyvezető igazgató NJSZT

ISBN: 978-615-5036-26-2

A könyv elkészítését támogatták:
QUADRON Kibervédelmi Szolgáltató Zrt.

Időérték Kft.

Crowe FST Audit Kft.

Tartalomjegyzék

Ábrajegyzék

1 Bevezetés

Az *IT biztonság közérthetően 5.0* című könyv online bemutatóján a szakértők hiánypótlónak nevezték a megjelentetett művet, merthogy a stílusa közérthető és olvasmányos, ugyanakkor a tartalma alapos. *Dr. Keszthelyi András*, a könyv szakmai lektora szerint: *„A szerzők jól eltalálták a tudományos ismeretterjesztési egyensúlyt a szakmai ismeretekkel rendelkezők és a nem szakember olvasók között."*

A most megjelent tankönyv az előző, 2019. évi változatot bővítette ki, aktualizálta, hiszen az azóta eltelt időszakban számtalan változásnak lehetettünk tanúi. Az is bebizonyosodott, hogy az életünk minden területét átható digitalizáció a biztonság kérdését is felhangosítja. Éppen ezért nagyon fontos szerepet kap az információbiztonság kérdése, amelyről e tankönyvben átfogóan, de ugyanakkor a lényegesebb részleteket kiemelve olvashatunk, tanulhatunk. Felkészülhetünk a munkánk, a magánéletünk során, és különösen figyelmet fordítva a gyermekeink védelmére, a minket érő digitális fenyegetettségek felismerésére és elhárítására.

A szerzők, *Dr. Erdősi Péter Máté* és *Solymos Ákos* a téma kiváló szakértői, már több évtizede foglalkoznak információ biztonsággal. De nemcsak elméleti síkon mélyültek el a kiberbiztonságban, hanem mindennapi gyakorlati tapasztalatokkal is rendelkeznek, és ezeket is megjelenítik a tankönyv jelenlegi, 5. kiadásában.

A *Neumann Társaság* nem most kezdett el foglalkozni az információbiztonság kérdésével. Ezt bizonyítja az is, hogy az ICDL (korábbi néven ECDL) modulok közé mintegy már egy évtizede beemeltük a Cyber Security nemzetközi ICDL modul követelményeit, vagyis magyarul az IT biztonság vizsgamodult. Ezzel egyidőben készült el a téma fontosságára való tekintettel az IT biztonság közérthetően tankönyv, amely egyébként mindazokat az ismereteket tartalmazza, amelyek egy sikeres ICDL IT biztonság vizsga letételéhez szükségesek.
Társadalmi felelősségvállalásunk okán, és támogatóinak köszönhetően a könyvet ismét ingyenesen tesszük elérhetővé bárki számára, a honlapunkról letölthető formában.

A kiberbiztonság mindannyiunk ügye. Mindenkinek jó szívvel ajánlom az IT biztonság közérthetően tankönyvet!

Szalay Imre
ügyvezető igazgató
Neumann János Számítógéptudományi Társaság

2 Biztonsági alapfogalmak

2.1 Biztonság

Az élet számos területén sokszor használjuk azt a fogalmat, hogy „**biztonság**”. De mit is értünk alatta? Mit jelent például a létbiztonság? Azt, hogy a mindennapi életünk alapjai a jelenben megvannak (nem éhezünk és van hol laknunk) és a jövőben sem várható ebben jelentősebb mértékű változás. Hasonló értelemben szoktuk használni a „közbiztonság” fogalmát is – ha a környezetünkben elvétve fordul elő bűncselekmény, akkor jónak érezzük a közbiztonságot, viszont, ha minden nap kirabolnának valakit az utcánkban, akkor előbb-utóbb elkezdenénk félni attól, hogy ez velünk is megtörténhet, és sürgősen szeretnénk a közbiztonságot javítani. Valahol mindkét esetben arról van szó, hogy a biztonság a szubjektum (azaz az egyén) számára egy kedvező állapot, amelynek megváltozását nem várja, de nem is tudja kizárni[1]. Idealizált, édenkerti esetben ez az állapot örökkön-örökké fennmaradhat. Azonban világunk nem ideális, ezért minden időpillanatban számos **veszély** fenyegeti a biztonságot. Annyira érezzük magunkat biztonságban, amennyire a körülöttünk lévő világ képes megelőzni és felismerni a fenyegetéseket, illetve javítani a bekövetkezett események káros hatásait. Ha elfogadjuk, hogy biztonság akkor van, ha a fenyegetettség minimális, akkor a biztonság a sérülékenységek hiányát vagy a fenyegetésekkel szembeni védelmet jelenti[2].

A biztonság a minőség és a megbízhatóság mellett a harmadik olyan követelmény, amelyet figyelembe kell venni a hosszútávú működés fenntartása szempontjából. Hétköznapi értelemben a biztonság veszélyektől mentes, zavartalan állapotot jelent[3]. Az informatikai rendszerek esetében a legfontosabb az adatok biztonságát megvalósítani. Három **adatbiztonsági követelmény** létezik:

- **bizalmasság:** valami, amit csak az arra jogosultak ismerhetnek meg, korlátozott a megismerésre jogosultak köre,
- **sértetlenség vagy integritás:** valami, ami az eredeti állapotának megfelel és teljes,
- **rendelkezésre állás:** a szükséges infrastruktúrák, valamint adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van.

[1] Vasvári György: Bankbiztonság. Infota, 2006.
[2] Ürmösi Károly: A biztonság, a biztonság fogalma. Hadtudományi Szemle, 2013
[3] Magyar Értelmező Kéziszótár, Akadémiai Kiadó (1978), 139. oldal

Ha egy szemléletes példával szeretnénk illusztrálni a fenti hármas követelményt, akkor erre talán a munkavállalók fizetési listája lenne a legjobb. Bizalmasság: a fizetési információk jellemzően érzékeny adatok, senki sem szeretné, ha az arra feljogosítottakon túl mások is látnák azt, hogy mennyi a fizetése. Sértetlenség vagy integritás: komoly probléma lenne, ha a fizetési adatokat valaki illetéktelenül módosítaná, valakinek csökkentené, valakinek pedig emelné a fizetését. Végül a rendelkezésre állás: ha valaki letörölné vagy egyéb módon elérhetetlenné tenné a bérlistát és a dolgozók nem kapnának fizetést, az komoly problémát okozna.

A fenti hármas követelmény biztosítása érdekében minden esetben számos védelmi intézkedést kell tennünk.

A tárgyban további fogalmakat is szoktak használni, amelyek értelmezése olykor nem egyértelmű [a]:

- **adatbiztonság:** a számítógépes rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése (nem foglalkozik az alkalmazások és a kisegítő berendezések – pl. szünetmentes áramforrás – biztonságával),
- **informatikai biztonság:** az információs rendszerekben tárolt adatok és a feldolgozáshoz használt hardveres és szoftveres erőforrások biztonságára vonatkozik – ha az „adat” fogalmát kiterjesztjük az „információ”-ra, akkor ez a definíció egyenértékű az információbiztonság fogalmával, egyébként szűkebb értelmű nála,
- **információbiztonság:** tények, utasítások, elképzelések emberi vagy gépi úton formalizált, továbbítási, feldolgozási vagy tárolási célú reprezentánsai bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése – amennyiben az informatikai biztonságnál az „adat” fogalmába beleértjük az emberi formalizálást is (beszéd, előadás, beszélgetés), akkor egyenértékű az informatikai biztonság fogalmával, egyébként bővebb nála,
- **adatvédelem:** személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége[4],
- **kiberbiztonság:**
    - a kibertér védelmének vagy megvédésének képessége a kibertámadásokkal szemben,

[4] https://www.naih.hu/adatvedelmi-szotar.html

- számítógépek, elektronikus kommunikációs rendszerek, elektronikus hírközlési szolgáltatások, vezetékes kommunikáció és elektronikus kommunikáció károsodásának megelőzése, védelme és helyreállítása, beleértve az ezekben található információkat is, azok elérhetőségének, integritásának, hitelességének, bizalmasságának és letagadhatatlanságának biztosítása érdekében.

Az ENISA 2015-ös „A Kiberbiztonság definíciója – különbségek és átfedések a szabványosításban”[5] című dokumentuma számos szervezet fogalmi magyarázatát tartalmazza a „kiberbiztonság” kifejezésre. Mi most a fenti fogalmakat mutattuk be, hogy érzékeltessük, hogy ez az egy szó mennyiféle mélységet és értelmezést kaphat az egyszerűtől a bonyolultig. A NIST SP 800-39 Managing Information Security Risk Organization, Mission, and Information System View dokumentumában a kiberbiztonság fogalma nagyon egyszerűen van megfogalmazva, ez lett az első definíciónk. Mi mégis inkább a Committee on National Security Systems CNSSI Glossary (CNSSI No. 4009[6]) dokumentumának „kiberbiztonság” fogalmát érezzük a legjobban érthetőnek, ezt adtuk meg második definícióként, mivel véleményünk szerint jobban levezethetőek a védelmi feladatok ebből a definícióból, mint az elsőből.

2.2 Kibertér

Miért jelentkezik ma már társadalmi szinten az információbiztonsági igény? Mert a mai társadalmi rendszerek – ideértve a gazdaságban, a kormányzatban, önkormányzatban és otthon működő rendszereket egyaránt – függenek az információtechnológiától, és ez a függés az egyes rendszerek összekapcsolódásával, a **kibertér** létrejöttével világméretűvé vált.

Magyarország is felismerte a kibertér fontosságát, ezért megjelent Magyarország Nemzeti Kiberbiztonsági Stratégiája is, az 1139/2013. (III. 21.) Kormányhatározat [1] formájában.

A stratégia a kibertér fogalmát így definiálja:

„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információ rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információrendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek

[5] Definition of Cybersecurity – Gaps and overlaps in standardisation v1.0 | December 2015
[6] Committee on National Security Systems (CNSS) Glossary

Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett."

Nem hagyható ki a kibertér fogalmából a „kutatási, felsőoktatási és közgyűjteményi hibridhálózat" és az arra épülő informatikai rendszerek, amelyek fejlesztője és üzemeltetője a NIIF (Nemzeti Információs Infrastruktúra Fejlesztési Program).

2.3 Nemzeti Kibervédelmi Intézet

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon a hatósági, biztonságirányítási, sérülékenység-vizsgálati és CERT (tanúsítási) feladatokat - alapvetően az állami és önkormányzati szervek vonatkozásában. Ezen komplex feladatkörének köszönhetően az Intézet az előbb említett szervezeteknél üzemelő elektronikus információs rendszerek teljes információbiztonsági életciklusára vonatkozóan rendelkezik feladatkörrel. Ezen túlmenően nyomon tudja követni és segíteni tudja azok alakulását, beleértve a tervezési szakaszt, a szabályozást, az ellenőrzést, valamint az incidenskezelést egyaránt.

Az NKI részét képező Kormányzati Eseménykezelő Központ az országon belüli koordinációs szervezeteként végzi az internetet támadási csatornaként felhasználó incidensek kezelését, illetve elhárításuk koordinálását; továbbá közzéteszi a felismert és publikált szoftver sérülékenységeket. Főbb feladatai fentieken kívül a biztonsági események kezelése, ügyeleti szolgálat, elemzés/értékelés, kibervédelmi gyakorlatok, képzések, tudatosítási programok és sérülékenység vizsgálatok végrehajtása.

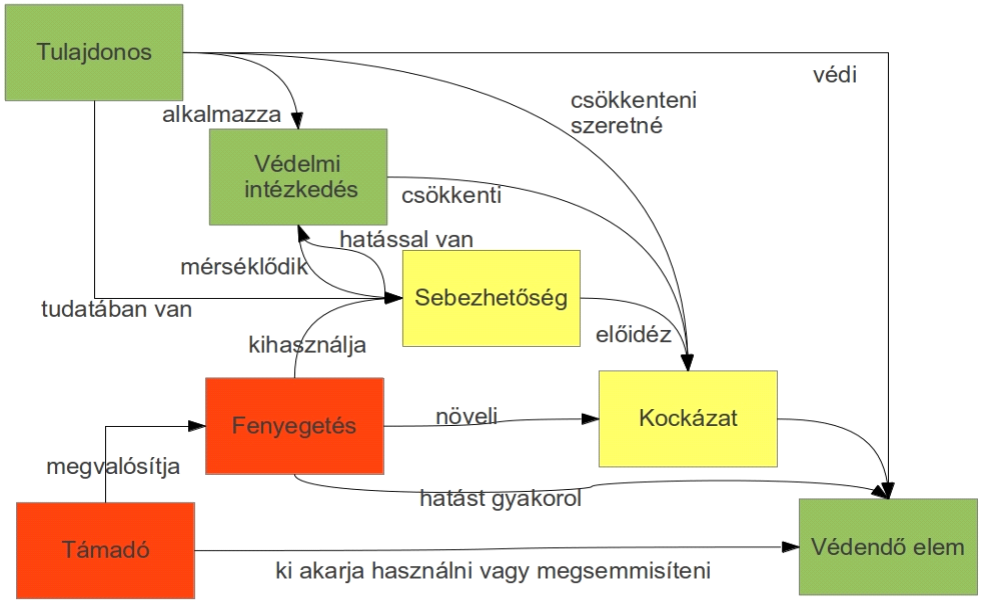
A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. Nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a teljes magyar kibertér biztonságának erősítéséhez.

További információ az Intézetről a https://nki.gov.hu/ [b] oldalon olvasható.

2.4 A biztonság koncepcionális megközelítése

A Common Criteria [7], melyet szoftverrendszerek biztonsági értékelésére dolgoztak ki – és amely ISO/IEC 15408 szabványként is ismert - a biztonság teljeskörű koncepcióját a 2.3 verziójában fogalmazta meg a rendszerek tulajdonságait is figyelembe véve. A koncepció

tartalmazza a támadót, a támadásokat, a védelmet megvalósító tulajdonost, a védelmi intézkedéseket és a védendő elemeket egyaránt. Nem tartalmazza azonban azokat a tényezőket, amelyek nem támadás miatt következnek be, és amelyek szintén biztonsági eseményhez és károkhoz vezethetnek. Például természeti katasztrófák, hardver meghibásodás, emberi hiba stb.



1. ábra: Biztonsági koncepció

Az ábrán szereplő fogalmak definícióit a következőkben adjuk meg [3] felhasználásával:

- **Védelmi intézkedés:** a fenyegetettség bekövetkezési valószínűségének csökkentésére, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési vagy technikai eszközökkel alkalmazott intézkedés. Például: tűzfalak, végpontvédelem, biztonsági szabályzatok bevezetése, felhasználók oktatása, beléptető rendszer, mentések stb.

- **Sebezhetőség:** A veszélyforrás képezte sikeres támadás bekövetkezése esetén a védendő elemek sérülésének lehetősége. Más szóval a védendő rendszer olyan tulajdonsága, amelyben rejlő hiba, hiányosság kihasználásával a támadó sikeres támadást hajthat végre az adatok, rendszerek, szolgáltatások vagy egyéb erőforrások ellen.

- **Támadás:** A támadás egy, az erőforrások bizalmassága, sértetlensége és/vagy rendelkezésre állása ellen irányuló, többnyire egy vagy több sebezhetőségből kiinduló, valamilyen fenyegetést megvalósító folyamat.
- **Fenyegetés:** A fenyegetés a támadás lehetősége, vagy a biztonság megsértésének lehetősége; amely a támadás tárgyát képező erőforrásra irányul.
- **Kockázat:** A kockázat annak a valószínűsége, hogy egy fenyegetés támadás útján kárkövetkezményeket okoz. Kárkövetkezmény lehet anyagi, jogi, reputációs, humán erőforrást stb. érintő. A kockázati érték meghatározásánál adott fenyegetettség bekövetkezési valószínűségét és az általa okozott kárkövetkezmény nagyságát szokták alapvetően figyelembe venni. Különböző módszertanok ettől eltérő számítási metódusokat is használnak.
- **Védendő elemek:** a szervezet vezetősége (menedzserei) által meghatározott küldetést/üzleti célt vagy társadalmi célt megvalósító erőforrások összessége, ideértve az informatikai feladatok végrehajtásához rendelt embereket, eszközöket (informatikai és egyéb), dokumentumokat, fizikai telephelyeket, folyamatokat és nem utolsó sorban az adatokat.

Az ábrából a fenti definíciókra támaszkodva a következő koncepcionális állítások olvashatók ki:

- A támadó rosszindulatú tevékenységeket akar végezni a védendő elemeken.
- A tulajdonos meg akarja védeni a védendő elemeit.
- A tulajdonos tisztában van a sebezhetőségekkel, ezért védelmi intézkedéseket alkalmaz.
- A védelmi intézkedések csökkentik a kockázatokat.
- A sebezhetőségek idézik elő a kockázatokat.
- A védelmi intézkedések hatnak a sebezhetőségekre, mérséklik azok hatását a védendő elemekre nézve, úgy, hogy vagy mérséklik a támadások kárkövetkezményeit, vagy csökkentik azok bekövetkezési valószínűségét.
- A támadó igyekszik megvalósítani a fenyegetés bekövetkezését, ami növeli a kockázatot.
- A fenyegetések a sebezhetőségeket használják ki.

A támadások működési mechanizmusa tehát az, hogy a támadó megkeresi a védeni kívánt informatikai rendszer sebezhetőségeit, amelyeken keresztül támadásokat próbál meg realizálni. A tulajdonos a kockázatokat védelmi intézkedésekkel csökkenti, melyek lefedik a sebezhetőségek által jelentett gyengeségeket. A biztonság innentől kezdve mérhető, mégpedig egyrészről a sikeres támadások számával, másrészről a kárkövetkezmények elhárításának és a védelemre fordított erőforrásoknak a számszerűsítésével. Ugyanakkor fontos kijelenteni, hogy 100%-os biztonság nem létezik. Amennyiben egy kockázatot teljesen meg szeretnénk szüntetni, akkor azt jellemzően a védendő erőforrás, rendszer vagy szolgáltatás megszüntetésével lehet elérni. Megjegyezzük, hogy a költségek exponenciálisan növekedhetnek, ahogy a biztonság szintje közeledik a 100%-hoz, így az erről hozott döntés alapvetően pénzügyi-üzleti döntés szokott lenni általában. A döntéshozók számára ki is dolgozták a biztonságra fordított befektetések megtérülésének kiszámítási módszertanát[7].

Maga a folyamat, amely a fent megismert koncepciót valósítja meg, az a kockázatkezelés. A kockázatkezelés során a szervezet felméri, milyen fenyegetések irányulnak a szervezet eszközei ellen, amelyek lehetnek rendszerek, adatok, telephelyek és maga a felhasználó is. Azt is megbecsülik, hogy ezek a fenyegetések mennyire valószínű, hogy bekövetkeznek, és ha bekövetkeznek, akkor milyen hatással járnak. Több hatás mentén is lehet mérni a kárkövetkezményeket, hogy minél pontosabb képet kapjon az értékelő, hogy milyen hatással lehet az adott fenyegetés a szervezetre. Az így kapott információ mutatja a kockázatokat, amelyek kapcsán négyféle koncepció mentén dönthet a szervezet azoknak a kezeléséről:

- Kockázatcsökkentő intézkedések foganatosítása, azaz olyan kontrollokat alkalmaz, amelyek csökkentik a bekövetkezés valószínűségét, esetleg a hatásait.
- Kockázat elkerülését is választhatja, ha például egy kockázatosnak ítélt tevékenységet nem követ, így a kockázat is megszűnik.
- Kockázat kapcsán áthárítást is választhat, azonban ebben az esetben nem a kockázatot, hanem annak hatását hárítja át. Tipikusan ide tartoznak a biztosítások.
- Kockázatot el is lehet fogadni, amennyiben a szervezet úgy dönt, hogy a kockázat hatása számára elfogadható szinten van, nincs szükség további intézkedésekre.

Nézzük ezt egy, a hétköznapi életből vett gyakorlati példán keresztül. Az a tervünk támad, hogy a családdal síelni megyünk. Autóval szándékozunk menni, és azt is tudjuk, hogy síelni nem igazán tudunk. A kockázat, amit értékelünk, egy esetleges lábtörés. Mit tehetünk, hogy a felmerülő kockázatokat csökkentsük? Van néhány lehetőség előttünk:

[7] Lásd az ENISA legújabb módszertanát: Introduction to Return on Security Investment.

- Elmegyünk oktatásra és felkészülünk a kihívásra. Ez egy kockázatcsökkentő intézkedés.
- Biztosítást kötünk. Amennyiben az oktatás ellenére is közelebbről megismerkedünk a hóval, a mentés költségeit a biztosítóra hárítjuk. (A kárt nem, mert mi leszünk a sérültek.)
- Elfogadjuk a kockázatot, és bízunk a szerencsénkben.
- Elkerüljük a kockázatot, inkább nyáron megyünk a tengerpartra.

3 Információrendszerek

Az információnak **életciklusa** van, ahogyan ahogyan azt a COBIT 5 először megfogalmazta [6], és a COBIT 2019 [c] is megőrizte[8]. Az életciklus arra fókuszál, hogy a működtetett folyamatok hogyan képesek azt az értéket előállítani, aminek az érdekében ezeket a folyamatokat létrehozták. Nagyon fontos megállapítás az, hogy a létrehozni kívánt értékek előállításhoz tudás szükséges, amihez a megfelelő információk nélkülözhetetlenek. Az információkat adatok feldolgozásával állítjuk elő, az **adat**ok pedig információs rendszerekben jönnek létre, tárolódnak és itt dolgozzák fel őket.

Az információs rendszerek **számítógépes architektúrákon** [d] működnek, ideértve mind a hardveres, mind a szoftveres környezetet. A szoftveres környezet a virtualizáció fejlődésével jelentős átalakuláson ment keresztül. Korábban a hardver és az alkalmazás nem volt nagyon távol egymástól, ma már több virtuális szint is létezhet az egyes számítógépes architektúrákban, anélkül, hogy ebből a felhasználó bármit is észrevenne.

Az egyes számítógépek összekapcsolási módja is megváltozott, a vezeték nélküli technológiák jelentős teret nyertek minden szektorban a hálózatok kialakítása terén a vezetékes átviteli technológiák mellett – ez a trend új fenyegetéseket is hozott be a mindennapjainkba.

3.1 Hardveres infrastruktúra

A számítógépes architektúrákat két alapvető részre szokás felbontani: hardverre és szoftverre. A **hardverek** adják a számítási műveletek fizikai hátterét a szükséges adat-beviteli és kimeneti egységekkel együtt. Ezeken a hardvereken pedig különböző szintű programokra lesz szükség a **szoftveres** adatfeldolgozási feladatok ellátására.

[8] COBIT 2019

Felépítésükben nem különböznek, de feladatuk különböző, ezért meg lehet különböztetni az adatok feldolgozására szolgáló **számítógép**eket, adatbázis-szervereket, adattárházakat a kommunikációra szolgáló hardverektől (jelismétlő, híd, útválasztó). A kliens-szerver architektúrában két oldal jelenik meg: a kiszolgáló architektúra és a kliens-oldal, ezeken a speciális körülményeket figyelembe vevő programok működtethetők.

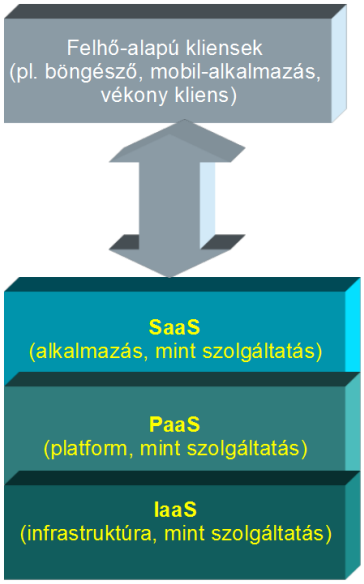
3.2 Alkalmazások, szolgáltatások

A hardveres egységek összeszerelésüket követően még nem képesek szofisztikált felhasználói utasításokat végrehajtani, ezeket teszik majd lehetővé a különböző programok, szoftverek, alkalmazások. Anélkül, hogy mély technikai részletekbe mennénk, megemlítjük, hogy a hardverek működtetéséhez az úgynevezett meghajtó- és vezérlőprogramok – driverek, valamint a firmware[9] programok – szolgálnak. A számítógép-architektúra teljes funkcionalitásának kihasználását az operációs rendszer teszi lehetővé, míg a felhasználók által igényelt egyes funkciókat önálló alkalmazásokkal valósítják meg.

Biztonsági szempontból azt érdemes tudni, hogy bármilyen alkalmazás fejlesztése esetén elengedhetetlen, hogy a funkcionális követelmények mellett a fejlesztés legkorábbi szakaszától a biztonsági (ún. nem funkcionális) követelmények is meg legyenek határozva. Ennek elmaradása és/vagy nem megfelelő teszteltsége okozza azokat a szoftveres sérülékenységeket, amelyek révén a támadók megpróbálják a különböző informatikai rendszereket megtámadni, feltörni, divatos kifejezéssel élve „meghekkelni”. De ezeket a sérülékenységeket használják ki az automatizált robotok is, amelyek sérülékeny weboldalak kezdőoldalait cserélik le (deface), illetve azon kártevők (vírusok, trójai programok), amelyek a felhasználókat is veszélyeztetik.

A kibertér és a virtualizáció fejlődésével megszületett az igény, hogy a felhasználók ne csak a saját gépeiken legyenek képesek szoftvereket futtatni, hanem legyen lehetőségük a különböző alkalmazásokat távolban, a **felhőben** futtatni és csak az adatokat mozgatni a helyi és a távoli számítógépek között. Ez a technika odáig fejlődött, hogy lehetőségünk van a böngészőnkön keresztül igénybe venni egy teljes virtualizált számítógépes felületet (Platform as a Service, PaaS) vagy egy szoftvert (Software as a Service, SaaS), illetve egy infrastruktúrát is (Infrastructure as a Service, IaaS) [e]. És sajnos kialakult az a szolgáltatási infrastruktúra, ahol a korábban komoly informatikai ismereteket igénylő számítógépes bűnözéshez kapcsolódó szolgáltatásokat (vírusterjesztés, szolgáltatás-megtagadásos támadások, spamküldés, informatikai rendszerek feltörése stb.) lehet elérni, gyakorlatilag bárki számára. Ez a Fraud as

a Service, Faas. Ezt a témát azonban jelen tankönyv nem tárgyalja részletesen, de jó, ha a felhasználó is tisztában van vele, hogy létezik.



2. ábra: Felhő alapú szolgáltatások

Néhány példa az egyes szolgáltatási típusokra:

- **SaaS**: e-mail felület, virtuális desktop, játékok, kommunikáció,
- **PaaS**: adatbázisok, fejlesztési környezetek, webszerverek,
- **IaaS**: virtuális gépek, szerverek, tárolók, terhelés-elosztók, hálózat.

A felhasználók számára mindez azt jelenti, hogy képesek többnyire telepítés nélkül, böngészőn keresztül akár egy irodai szoftvercsomag funkcionalitását kihasználni (pl. GoogleDocs), komplex kommunikációs (telefonálás, levelezés, azonnali üzenetküldés) szolgáltatásokat felhasználni (pl. Skype, Viber, Whatsapp, Gmail, Messenger, Signal) vagy közösségi oldalakon információkat, fájlokat megosztani és megkapni (pl. Facebook, Twitter, Instagram, TikTok stb.). A **fájl-megosztás** saját gépről is történhet és lehetőség van már nagyméretű fájlok megosztására is (Pl. Mammutmail, WeTransfer) valamint a fájljaink felhőben való tárolására is, (Pl. GoogleDrive, Dropbox, OneDrive). Ezen szolgáltatások használata előtt érdemes elolvasni az Általános Szerződési Feltételeket. Ebben van leírva, hogy a szolgáltató mit szolgáltat, miért vállal és miért nem vállal felelősséget, ki férhet hozzá adatainkhoz és így tovább. Fontos tudni továbbá, hogy az egyes szolgáltatók ingyenes és fizetős, illetve akár vállalati

felhasználásra szánt szolgáltatásai között jelentős különbségek lehetnek, biztonsági szempontból is.

Érdemes megismerkedni a CaaS – City as a Service fogalmával, hiszen pár éven belül tapasztalni fogjuk, hogy a mindennapi életünkben is meg fognak jelenni az okosvárosok szolgáltatásai. És rajtunk felhasználókon is múlik a biztonságuk. A CaaS számos innovatív információtechnológiai fejlesztést foglal magába, azért, hogy a városaink élhetőbbek, gazdaságosabbak legyenek. Ilyen szolgáltatások a teljesség igénye nélkül: a közösségi közlekedés optimalizálása, megosztott autó használat, közösségi terek menedzsmentje, kulturális értékek szélesebb körű elérése, köztéri információs rendszerek és nyilvános szolgáltatások adatgyűjtései és értékelése, várostervezési megfontolások és még sorolhatnánk. Ahhoz azonban, hogy ezen szolgáltatások valóban az emberek érdekeit szolgálják, a biztonsággal is kiemelt szinten kell foglalkozni.

3.2.1 Elektronikus ügyintézés

Magyarországon az egykapus ügyintézési felületet a https://magyarorszag.hu [g] portált biztosítja, ahol egy hiteles regisztrációt követően (ami bármelyik okmányirodában, kormányhivatali ügyfélszolgálati irodában, adóhatóság ügyfélszolgálatán, külképviseleten vagy elektronikusan indítható el 2016. január 1-jét követően kiállított érvényes e-személyazonosító igazolvány birtokában) számos ügy kezdeményezésére van már lehetőségünk teljesen elektronikus formában, több államigazgatási rendszerből tölthetünk le magunkkal, gépjárműveinkkel, vagy ingatlanjainkkal kapcsolatosan adatokat is (pl. NAV, OEP, JSZP, Földhivatal). 2017 óta az egészségügyi adataink is hozzáférhetőek elektronikusan, az orvosi recepteket is a felhőben kapjuk meg, és ezen adatok kezelése kapcsán is tájékozódhatunk az Egységes Egészségügyi Szolgáltatási Térben is (EESZT[10]). Figyelmet érdemel az ingatlanok tulajdoni lapjának online lekérdezhetősége is (Földhivatal Online[11]), itt minden bejegyzett adat hozzáférhető az ingatlannyilvántartásból.[12]

[10] https://www.eeszt.gov.hu/

[11] https://www.magyarorszag.hu/szuf_ugyleiras?id=5abe39f4-28b1-4862-8ec6-89e74c2f9a4d&_n=ingatlankereso_online_foldhivatali_szolgaltatas-_tulajdoni_lap_lekerdezes

[12] A kézirat lezárta után került sor a digitális állampolgárságról szóló törvénytervezet benyújtására, elfogadása pedig 2023 decemberében történik meg, ennélfogva ennek elemzése és ismertetése a könyv következő változatában következhet be. Vizsgálata azért is indokolt, mert ez a törvény az elektronikus ügyintézésről szóló törvényt teljes mértékben hatályon kívül helyezi.

3.3 Számítógép-hálózatok

A számítógép-hálózat egy olyan speciális rendszer, amely különböző informatikai, többnyire valamilyen telekommunikációs eszközök segítségével a számítógépek egymás közötti kommunikációját biztosítja. Manapság már ideértünk minden olyan eszközt, ami a hétköznapi értelemben vett számítógépeken túl valamilyen számítógép alapú működést biztosít. Gondolva itt az okoseszközökre (okostelefon, IP kamera, autó fedélzeti számítógép, okoshűtő, okoscipő, otthon-automatizálás vezérlők stb.), valamint Machine to Machine (M2M) technológiákra. Az M2M technológia olyan adatáramlást jelent, amely emberi közreműködés nélkül, gépek között zajlik.

A hálózatokat fel lehet ugyan osztani kiterjedésüket alapul véve számos típusra [2], azonban ez felhasználói szemmel nem releváns, a hálózatok fenntartásához szükséges erőforrások nem látszódnak végfelhasználó szinten, legfeljebb az üzemeltetés szempontjából lehet ez érdekes.

Nem fizikai távolság alapján különböztethető meg a többi hálózat típustól az egyre több szervezetnél és már magánszemélyek által is használt virtuális magánhálózat (VPN – Virtual Private Network). A virtuális magánhálózat egy számítógép-hálózat fölött virtuálisan kiépített másik hálózat. „Magán” jellegét az adja, hogy a VPN-en keresztülmenő adatok nem láthatók az eredeti hálózaton, mivel titkosított adatcsomagokba vannak becsomagolva. Ez biztosítja, hogy akár a világ másik feléről is biztonságos titkosított csatornán be lehessen jelentkezni egy vállalati hálózatba és ott használni lehessen a vállalat erőforrásait (fájlszerver, üzleti alkalmazások, levelezés stb.), miközben a felhasználó fizikailag távol van.

3.4 Fenyegetések, támadások

Az információ olyan érték, amely megléte vagy hiánya alapvetően befolyásolja minden folyamatunk elvégezhetőségét és eredményességét. Növelheti a hatékonyságot, ha jó, és teljes használhatatlanságot vagy kiesést okoz, ha rossz. Az informatikafüggés során vált világossá, hogy a minőségi információk megléte nélkülözhetetlen a mindennapi élethez. Világos, hogy relevánsabb információval több eredmény elérésére lehetünk képesek, míg helytelen információval egyetlen folyamat sem adhat helyes és maximálisan felhasználható végeredményt. Az információt informatikai biztonsági szempontból általában az adatfeldolgozás kimenetének tekintjük, és mint ilyen, valamely számítógépes adathordozón reprezentált. De nemcsak így fordulhat elő az információ, gondoljunk csak a beszédre, a telefonos közlésekre, valamint a papír alapon tárolt információkra is, amelyeket adott esetben szintén

védeni szükséges. Az információ olyan fontos és értékes elemmé vált, hogy be is épült az információtechnológiai **erőforrás**ok közé a hardver és a szoftver mellé minden keretrendszerben, szabványban. Védeni kell tehát a hardver és a szoftver mellett a fontosnak ítélt információkat is. Egyre inkább elterjedt nézet, hogy a legfontosabb erőforrás az adat. Hiszen sokszor nem megismételhető, vagy nagyon nehezen reprodukálható folyamatok, számítások alapján áll elő. Gondoljunk itt egyszerű példaként a saját családi fotóalbumunkra. Vagy arra, hogy a gyermekünk első feltápászkodásáról és első lépteiről szóló videófájl, ha nincs meg több példányban és megsérül, véletlenül letöröljük, vagy egy zsarolóvírus letitkosítja, akkor jó eséllyel soha többet nem láthatjuk viszont, mert nem megismételhető a forrásesemény. Ezzel szemben a hardver vagy a szoftver, bár pénzben kifejezve komoly értéket képviselnek, reprodukálhatók. Tudok venni egy új laptopot, újra meg tudom venni a programot rá. Az egyedi adatokról, legyenek azok dokumentumok, fotók, fájlok, hangfelvételek, már ez nem mondható el.

Ezeket az értékeket a támadók is felismerték, és támadásaikat két tényező köré csoportosították:

- **rombolás:** károkozás a megtámadottnak, a működési folyamataihoz szükséges erőforrások sérülésének előidézésével (beleértve az információt is)
- **haszonszerzés:** az erőforrások eltulajdonításával saját szakállukra megszerezni azt a hasznot, ami a más erőforrásai illegális felhasználásával elérhető (információ-lopás, zombi hálózat stb.). Ennek minősített esete a **személyazonosság-lopás**, amikor a haszon a támadóé, a büntetés a megtámadotté – hacsak nem tudja ártatlanságát bizonyítani. Az utóbbi években pedig első helyre lépett elő a **zsarolás**, amelyet a támadók zsarolóvírusok terítésével hajtanak végre. Az anyag részletesen tárgyalja majd ezt a témát.

Fenti két célt jellemzően rosszindulatú szoftverekkel és egyéb változatos támadási formákkal valósítják meg a támadók.

Fenti két nagy kategória mellé muszáj beiktatni egy „Egyéb” kategóriát is, mivel az információs rendszerek, a közösségi oldalak, alkalmazások már olyan önálló kategóriává nőtték ki magukat, amelyek nagy tömegeket érnek el közvetlenül, ezért kiválóan alkalmasak az egyének vagy csoportok tömeges befolyásolására. A hamis információk terjesztése ma már óriási mértéket ölt és akár népek, nemzetek elleni uszításra, vagy akár választások befolyásolására is bevetik őket a támadók. Éppen ezért meg kell említenünk itt a lélektani műveleteket is, amelyek lehetnek támadó vagy védelmi jellegűek. A támadó jellegű információs művelet esetében a cél az, hogy a speciális érdekekre vagy speciális fenyegetésekre választ adva

gyakoroljanak hatást az ellenérdekű félre akár békében, válságban vagy konfliktus idején, míg a védelmi jellegű művelet során a saját információ védelme a cél[13]. A hétköznapok során leginkább a társadalmi vírus koncepciója alapján terjedő álhírekkel találkozhatunk, amelyekkel képesek a támadók a társadalom jelentős részének a véleményét befolyásolni a saját céljuk érdekében. A hitelesség annyiban segít az álhírek megfelelő kezelésében, hogy ha a látszólagos információforrás mögött fel tudjuk fedni a tényleges forrást, akkor a tartalmat is az ennek megfelelő fenntartásokkal tudjuk ebben az esetben kezelni.

3.5 Rosszindulatú szoftverek

Rosszindulatú szoftvereknek nevezünk minden olyan programot, amely a tulajdonos előzetes engedélye nélkül valamilyen tevékenységet akar végezni a számítógépeken lévő vagy a hálózatra feltöltött adatokkal, a tulajdonos érdekei ellenére. A kifejezés angol változata (**malware**) a „malicious software" kifejezés rövidüléséből eredt. A rosszindulatú programkód tehát számítógépes rendszerekbe engedély nélküli beszivárgást, vagy a felhasználóknak kárt okozó, nem engedélyezett tevékenységet lehetővé tévő vagy megvalósító szoftver. Ezeket károkozási, befolyásolási, adatlopási célból vagy kifejezetten károkozási céllal készítik és küldik. A rosszindulatú programok elrejtésére a rendszerszinten tevékenykedő kártékony kódokat (**rootkit**) használják általában.

Az egyes rosszindulatú programokat az alábbiak szerint osztályozhatjuk:

- vírusok: olyan programok, amelyek magukat lemásolva önálló fájlként vagy más fájlokhoz kapcsolódva küldés vagy letöltés útján terjednek, így e-maileken keresztül is küldhetik őket csatolmányként, de önálló létezésre és működésre – a biológiai vírusokhoz hasonlóan – nem képesek. A. Az eszközök elindulásakor futó statikus programokkal (firmware) együtt betöltődhetnek vagy honlapokról töltődnek le automatikusan a felhasználó engedélye nélkül, és futásukkal károkat okozhatnak az informatikai eszközökön. A vírusok magukat lemásolva az e-mailes vagy közösségi kommunikáció segítségével is tudnak terjedni. Kiemelt alfajuk a zsarolóvírusok, amelyek letitkosítják a megfertőzött eszköz (munkaállomás, szerver, okostelefon stb.) fájljait és váltságdíj fizetése ellenében ígérik meg a titkosítás feloldásához szükséges kulcs átadását. Bővebben lásd: zsaroló programok.
- férgek: a számítógépes féreg olyan kártékony kódot tartalmazó program, amely hálózatba kötött számítógépeket támad meg, és a hálózaton önmagától terjed. A

[13] Bányász Péter, Dobos László, Palla Gergely, Pollner Péter: Lélektani műveletek a közösségi médiában. Hálózatok a közszolgálatban, 2019.

vírusok és a férgek között az az alapvető különbség, hogy a férgek önállóan képesek terjedni hálózati metódusokat alkalmazva – ehhez nincs szükségük gazdafájlokra (vagy rendszertöltő szektorokra). A férgek a névjegylista e-mail címein keresztül is terjedhetnek, illetve a hálózati alkalmazások biztonsági réseit használják ki.

- trójai programok: nevüket az ókori Trója ostrománál alkalmazott hadicsel eszközéről, a legendás falóról kapták, amely révén egy hasznosnak látszó letöltésben egy olyan program bújik meg, ami előbb-utóbb aktivizálódik incidenseket okozva (például hátsó kapukat nyit vagy rosszindulatú programokat indít el).
- hátsó kapuk: szoftverekbe épített olyan kiegészítések, amelyek bizonyos kiválasztott személyek részére hozzáférést engednek az egyes programokhoz, a számítógéphez, vagy az azokon kezelt adatokhoz. A hátsó kapuk egy részét a szoftverek fejlesztői tudatosan, szervizcélokkal építik be, míg kisebb részük programozási hiba következtében teszi lehetővé a hozzáférési szabályok kikerülését a jogosulatlan hozzáférést így megszerző támadóknak. Ezen kívül léteznek kifejezetten hátsó kapuk nyitásának céljával létrehozott támadóprogramok is, amelyeket általában vírusok, illetve kémszoftverek részeként terjesztenek a felhasználó tudta nélkül. Ezek támadási célú használata azért veszélyes, mert minden egyes esetben rosszindulatú programkódok telepítéséhez vezethet. A hátsó kapu a rendszerbiztonság megkerülésével működik, így az egyébként kialakított védelem itt nem fog érvényesülni.
- rendszerszinten rejtőző programok: olyan kártékony szoftverek, amelyeknek célja korlátlan, illetéktelen és rejtett hozzáférés megszerzése a számítógép erőforrásaihoz. Fontos tudni, hogy ezek a programok megkerülik a kialakított hozzáférés-védelmi rendszert, így az itt megszerzett hozzáférés a rendszer szintjén nem kontrollálható.
- szolgáltatás-megtagadási (Denial of Service, DoS vagy Distributed Denial of Services - DDoS) támadást indító programok: egy vagy több számítógépen futó program másodpercenként kérések sokaságát indítja a megadott cím felé úgy, hogy a küldött válaszokra nem kíváncsi, azt nem dolgozza fel. Így éri el azt, hogy a rendszert használó többi felhasználó a valódi kéréseire nem kap választ, a megtámadott számítógép túlterheltsége miatt. Ily módon, ha egy internetes áruházat ér például ilyen támadás, akkor ott nem lehet vásárolni, ergo tényleges bevételkiesés valósul meg.
- kémszoftverek: a felhasználó tudta és engedélye nélkül valamely adatot a támadónak továbbító rejtett programok. Elrejtőzhetnek bármilyen alkalmazás-csomag részeként, ahol futtatható programok vannak. A számítógépes programok mellett

megjelentek az okostelefonokra írt adatlopó programok is. A kémszoftverek akár a billentyűzet leütéseinket is naplózhatják például jelszavaink ellopása céljából, vagy a kamerán, vagy mikrofonon keresztül egyéb információkat lophatnak tőlünk – rólunk.

- zsaroló programok: a támadó olyan programot juttat be a felhasználó gépére vagy telefonjára vagy bármilyen számítógép alapú rendszerére, melyek a fertőzött eszközöket zárolják, vagy értékes állományokat titkosítanak, és ezáltal teszik azokat használhatatlanná. A program azt is állíthatja, hogy csak ellenszolgáltatás fejében oldja fel a zárolást. Nincs garancia arra, hogy fizetés után az áldozat visszakapja az adatait.
- kriptovaluta bányász programok: a támadó olyan programot telepít a felhasználó számítógépére, telefonjára vagy egyéb eszközére – egyre gyakoribb, hogy céges hálózatok nagy teljesítményű szervereire – amely a felhasználó tudta nélkül kriptovalutát bányászik gazdájának (aki nem a felhasználó). A kriptovaluta bányászat önmagában egy legális tevékenység, ha a „bányász" a saját tulajdonában lévő infrastruktúrán teszi ezt. Felhasználói szempontból a kriptovalutabányászat közvetlen kárt nem, de közvetettet okozhat, mivel jelentősen lelassítja a programot futtató eszközt, ezáltal a felhasználói élmény sérülhet és az eszköz jelentősen több energiát fogyaszt, mint normál működés közben. Céges környezetben már komolyabb problémát is okozhat a bányászat, mivel ilyen esetekben a szervereken futó üzleti folyamatokat támogató alkalmazások belassulhatnak, esetleg le is állhatnak, ami viszont már pénzben is kifejezhető kárt jelent.
- kéretlen levelek: A „spam" elnevezést egy amerikai cég (Hormel Foods) konzervhúskészítményének nevéből kölcsönözték (Spiced Pork and Ham), amely 1937 óta létezik. Az internet világában ez lett a szokásos kifejezés a tömeges e-mailek jelölésére, egy Monthy Pyton darab nyomán. A kéretlen levelek közös jellemzője, hogy valamely terméket vagy szolgáltatást reklámoz, mások informatikai erőforrásait jogosulatlanul és – többek között Magyarországon is – törvénytelenül felhasználva.
- kéretlen reklámszoftverek (adware): olyan ingyenesen letölthető és használható programok, melyek reklámokat jelenítenek meg a felhasználó gépén. Szokás őket PUP-nak is (Potential Unwanted Programs) hívni, mivel gyakran előfordul, hogy ezen programokon keresztül juttatnak el kártékony programokat a felhasználó gépére.
- zombi hálózati szoftverek: a botnet angol kifejezés, a „ro**bot**" szóból és „**net**work" szavak összevonásából származik. Az informatikai szakzsargonban ezzel egy olyan programot jelölnek, amely távirányítással vagy automatikusan dolgozik a megfertőzött gépen. Előfordulhat, hogy a felhasználó számítógépe része egy botnet-

hálózatnak és távirányítással dolgozik (dolgoztatják), anélkül, hogy a felhasználó tudna róla. Ehhez általában szükséges az online jelenlét. A zombi-hálózat szoftvere képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül. A zombi-hálózat szoftverét lehet adatlopásra, spamküldésre, vagy más számítógépek megtámadására is használni, hiszen a felhasználó gépére észrevétlenül feltelepül és ott bármilyen tevékenységet folytathat.

A rosszindulatú programok leggyakrabban az interneten keresztül kerülnek fel a megtámadott gépre, amihez csak annyi szükséges, hogy a gép az internetre legyen kötve. A támadások java részét a hálózaton keresztül követik el, ennek kivitelezési formája nagyobb biztonságot nyújt a támadó számára, és jobban lehetővé teszi a rejtve maradását. Emiatt sokkal ritkábban szoktak **fizikai támadó eszközöket** alkalmazni a támadók, mivel ehhez valamilyen személyes jelenlét szükséges, ami a lebukás kockázatát jelentősen megemeli. Otthoni eszközök elleni fizikai támadásnak meglehetősen alacsony a kockázata általánosságban véve, de ha a támadási cél értéke megnövekszik (például közszereplő vagy egy híresség otthoni eszközeiről van szó), akkor ez a támadási forma sem elhanyagolható. Sikeresen lehet használni az alábbi eszközöket is egy támadáshoz:

- **billentyűzet-leütéseket naplózó eszközök**: olyan kisméretű hardveres eszközök, melyeket a támadó a billentyűzet és a számítógép közé csatlakoztat be, és amely rendelkezik tárolókapacitással, amibe az eszköz az összes billentyűzet-leütést rögzíti. A támadó az eszköz tartalmának kiértékelésével juthat hozzá érzékeny információkhoz – tipikusan rendszeradminisztrátori jelszavakhoz vagy egyéb bejelentkezési adatokhoz.
- **rejtett kamerák**: olyan kisméretű adatrögzítő eszközök, melyek alkalmasak jó minőségű kép és hang rögzítésére. A kamerák működésüket tekintve lehetnek folyamatos vagy mozgásra/hangra aktivizálódók, vezetékes vagy rádiós jeleket továbbítók, illetve saját belső tápról vagy elektromos hálózatról működtethetők is. A támadó alkalmazhatja ezt a jelszavak vagy érzékeny információk eltulajdonítására, megfigyelés közben. Hátránya a személyes jelenlét, illetve a fizikai elhelyezés szükségessége. Egyes esetekben a támadók a számítógépek beépített vagy hozzákapcsolódó webkameráit képesek a felhasználó tudta nélkül bekapcsolni, rejtett kameraként használni és azokon keresztül adatokat ellopni a felhasználó környezetéből.

A modern kártevők már összetett funkcionalitást tartalmaznak, fenti listából akár többet is képesek szimultán végrehajtani.

3.6 Jellemző támadási formák és módszerek

A támadó szoftverek és fizikai eszközök áttekintése után felsoroljuk azokat a támadási formákat, melyek a felhasználó aktív vagy passzív közreműködésével jöhetnek létre – a teljesség igénye nélkül:

- Eltérítéses adathalászat (pharming): a támadó a felhasználó egy adott weboldal felé irányuló forgalmát átirányítja a saját weboldalára (vagy az általa birtokolt, feltört weboldalra) a felhasználó gépén egyes adatok módosításával, így a felhasználó gyanútlanul megadhatja a személyes adatait – például bejelentkezési adatok – azt gondolván, hogy a valódi oldalon van. A hamis weboldalak (ál weboldalak) egy az egyben lemásolják az igaziakat, a felhasználókat gyakran a sikertelennek jelzett bejelentkezési kísérletük után vissza is irányítják a támadók az érintett szervezet igazi weboldalára (nem feltétlenül a bejelentkezési oldalra), hogy a gyanút még jobban elterelјék a csalási kísérletről. Az különbözteti meg az adathalászattól, hogy itt a támadó az áldozata gépére, vagy WiFi routerére betörve módosítja annak beállításait. Ezt a támadási formát DNS mérgezésnek (poisoning) hívják.
- Egyklikkes támadások (Cross Site Request Forgery - CSRF): a támadók azt a bizalmi kapcsolatot használják ki, ami a felhasználó böngészője és a felhasználó által meglátogatott weboldal között fennáll. A támadónak a felhasználó környezetébe kell bejuttatnia a támadó kódot, amit a weboldal a felhasználó hiteles kérésének értelmez és megpróbál általában automatikusan végrehajtani. A támadás akkor sikeres, ha a támadó pontos üzenetet tud küldeni a weboldalnak és nincs olyan biztonsági szűrés bekapcsolva, mely a támadó által – ebben az esetben vakon – elküldött üzenetek hitelességét ellenőrizné.
- Csatolmányokba rejtett rosszindulatú programok letöltetése: nagyon gyakori támadási forma, hogy a támadó ráveszi a felhasználót egy érdekesnek látszó csatolmány letöltésére és megnyitására, amikor a csatolmányba rejtett rosszindulatú program aktivizálódik – esetleg a látszattevékenység fennmaradása mellett (pl. dokumentum/kép megjelenítés, program futása stb.). A legtöbb zsarolóvírus és kriptovaluta bányász program így jut az áldozatok gépére.
- Adathalászat (phishing): egy valódi weboldal támadók által lemásolt képének felhasználása (ál weboldal), amely kinézetében nem különbözik az eredetitől. A támadók arra használják, hogy bejelentkezési vagy személyes adatokat csaljanak ki a gyanútlan felhasználókból, miközben azt hiszik, hogy az eredeti weboldalon adják meg azokat. A fejlett ál weboldalak hamisított vagy akár valódi SSL-tanúsítvánnyal is

rendelkezhetnek. Az ál weboldalak meglátogatását hamis üzenetekbe rejtett linkekkel érik el (pl. adatváltoztatási kérés a rendszeradminisztrátortól e-mailben, vagy jelszóváltoztatási kérés a banktól egy biztonsági incidenst követően, számlatartozás jelzése egy szolgáltatótól stb.).

- Kifigyelés (shoulder surfing): közvetlen megfigyelési technikát jelent, a támadó leselkedik a felhasználó válla fölött vagy mellett, hogy információt szerezhessen. A kifigyelés zsúfolt helyeken hatékony, amikor a felhasználó begépeli a PIN-kódját egy POS terminálnál, vagy egy ATM-nél (ennek észlelésére vannak az ATM-eken kis tükrök), vagy például nyilvános helyeken – internetkávézóban vagy könyvtárban begépeli ügyfél-biztonsági kódját, jelszavát stb.
- Pszichológiai manipuláció - szélhámosság (social engineering): emberi hiszékenységen, befolyásolhatóságon vagy fenyegetésen alapuló támadási forma. A támadó a saját kilétéről megtéveszti a felhasználót, így érve azt el, hogy olyan információkat osszanak meg vele, amire egyébként nem lenne jogosult. Például a támadó rendészeti, kórházi dolgozónak vagy rendszeradminisztrátornak adja ki magát, de nem ritka a kezdő munkatárs szindróma is, ami a kezdők felé megnyilvánuló segítőkészséggel él vissza. Előfordul, hogy pszichológiai trükkökkel veszik rá az áldozatot az információ kiadására, vagy egy tevékenység végrehajtására. Ilyen, amikor a felhasználót valamilyen fiktív esemény közlésével (pl. unokáját baleset érte) vagy fenyegetéssel, például a főnőkére való hivatkozással és egy esetleges negatív következmény felvázolásával ráveszik a tevékenység elvégzésére. Itt a felvázolt esetekben a megtámadott fél motivációja az esetleges negatív következmény elkerülése, ami az egyént a cselekvésre készteti. Továbbá ez a módszer sokkal könnyebben kivitelezhető, mint találni egy még senki által sem ismert sérülékenységet a célrendszerben.
- Adatszivárgás: Manapság mind a magánszemélyeknél, mind a szervezeteknél rengeteg elektronikus információ és adat keletkezik napi szinten. A kommunikációs csatornák és adathordozók lehetőséget adnak ezen adatok és információk felhasználók általi kezelésére és mozgatására. Adatszivárgásnak hívjuk azon eseményeket, amikor bizalmasnak/titkosnak (de semmiképp sem nyilvánosnak) minősített adatok, az adatokhoz jogosultan hozzáférő felhasználó vétlen vagy szándékos tevékenysége következtében kikerülnek a szervezet védett kontrollkörnyezetéből és fentiek miatt ezen bizalmas adatokhoz, információkhoz jogosulatlan hozzáférés történhet a későbbiekben. Fontos a feltételes mód – történhet. Minthogy a szervezet kontrollkörnyezetéből kikerült az adat vagy az információ, a szervezetnek nincs már lehetősége azt

megvédeni, ergo úgy kell az ilyen adatokra tekinteni, mint potenciálisan kompromittálódott adatokra.

- Célzott támadás (APT - Advanced Persistent Threat): Az APT jellegű támadások jellemzője, hogy több, sokszor egymásra épülő támadási módszert is alkalmazva, lehetőleg minél észrevétlenebbül, akár hosszú ideig is rejtve, jellemzően nem ismert sérülékenységeket kihasználva támadják a célpontot, hogy ott kifejtsék tevékenységüket. Ez lehet akár adatlopás, informatikai rendszerek megrongálása vagy más illegális tevékenység. Ezen típusú támadások jellemzője a támadók magas szintű tudása és többnyire az erőforrások – itt akár pénz vagy eszközök biztosítása egy „szponzor" által, amelyek lehetnek üzleti vagy kormányzati szereplők is. A célpontokon kívül egyéb áldozatok is bekerülhetnek a szórásba, de a támadók célja, hogy az eredeti céljuk alapján kitűzött áldozatot kapják el. (Legismertebb támadás a STUXNET, amely az iráni atomprogram belassítását célozta, sikeresen.)
- Sérülékeny csomópontok keresése: pásztázó – általános fenyegetettséget jelentő – támadások eredményeként egy adott hálózaton belül azonosíthatóvá válik egy sérülékeny csomópont, amelynek kompromittálásával (rosszindulatú programkódok feltöltésével) a hálózat belülről válik támadhatóvá (pl. nyomok eltüntetése, félrevezetés, botnet kiépítése céljából).
- A kiberbűnözés szó a kibertéren keresztül, számítógép-használat közben elkövethető jogellenes bűncselekményekre utal. Ilyenek lesznek például az adathalászat és a bankkártya adatok (név, szám, lejárat, cvc) ellopása, online.
- E-mail alapú zsarolások: a támadó jellemzően angol vagy magyar nyelvű szöveges (a szöveget ritkán képként tartalmazó) elektronikus levélben megfenyegeti az áldozatot egy, az áldozat számára nem, vagy nehezen ellenőrizhető állítással. Például a támadó állítja, hogy megfertőzte az áldozat számítógépét, kémprogramot telepített rá és kifigyelte, sőt felvette a kamerán keresztül az áldozatot illegális („felnőtt") tartalmak nézése közben. Egyes esetekben az eszköz feltörését bizonyítandó, egy valóban az áldozathoz köthető jelszót is bemutat a támadó – amely azonban nem az áldozat eszközéről, hanem egy évekkel korábbi adatlopási incidensből származik (ezekről még lesz szó később.) A támadó megfenyegeti az áldozatot, hogy amennyiben nem fizeti meg az előírt összeget a támadó Bitcoin vagy más kriptovaluta számlájára, akkor közzé teszi a róla készült videót. A támadók újabban egyre gyakrabban alkalmazzák azt a fenyegetést is, hogy az áldozat feltört számítógépén gyermekpornót találtak –

amit akár ők maguk másoltak az áldozat számítógépére, és azzal zsarolják őt, hogy ha nem fizet, akkor ennek tényét nyilvánosságra hozzák és értesítik a hatóságokat is.

A **hackerek** olyan személyek, akik jól értenek az információtechnológiához, programozáshoz, és képesek arra, hogy behatoljanak informatikai rendszerekbe, hálózatokba. Azok a hackerek, akik rossz szándékkal, rombolás, adatok törlése, ellopása vagy módosítása, általában véve haszonszerzés miatt törnek be, azokat fekete kalapos (black hat) hackereknek hívjuk. Vannak olyan fehér kalapos (white hat) hackerek, akiket „etikus hackereknek" hívunk. Ők az ügyfelek megbízásából, az ügyfél felhatalmazásával, a feltárt hibákat dokumentálva törnek be a rendszerekbe és a tapasztalataikat jelentés formában átadják az ügyfélnek. Viszont ha egy hacker, ugyan jó szándékkal, de felhatalmazás nélkül keres hibát egy rendszerben, akkor ő nem minősül etikus hackernek. Fontos megjegyezni, hogy az informatikai rendszerek és adatok ellopása, jogosulatlan megismerése, vagy elérhetetlenné tétele (amit esetenként mind a fekete, mind a fehér kalapos hackerek végeznek) bűncselekmény és a törvény bünteti. Ezért a legnagyobb különbség a fekete és fehér kalapos hackerek között az, hogy a fehér kalapos hackereknek van írásos engedélyük, úgynevezett „támadási engedélyük/permission of attack" az ügyfelüktől, míg a fekete kalaposok ilyennel nem rendelkeznek.

Gyakran felmerül a kérdés, hogy a hackerek mit csinálnak az ellopott adatokkal? Az egyik legértékesebb adattípus a feltört rendszerekben a titkosított formában jelen lévő jelszavak. Ahhoz, hogy a jelszavak eladhatóak legyenek, azokat vissza kell fejteni olvasható formában. Ez a tevékenység a "**jelszótörés**". Megemlítjük, de mélyebben nem megyünk itt most abba bele, hogy a rendszerek tulajdonképpen nem a jelszavakat tárolják, hanem az azokból képzett rövid kivonatot (hash), így a támadó akkor is sikerrel járhat, ha nem pontosan a mi jelszavunkat találja ki, de talál egy olyan szöveget, aminek a kivonata megegyezik a mi eredeti jelszavunk kivonatával. A rendszer ebben az esetben is el fogja azt fogadni jelszóként.

- Jelszótörés: A jelszavak az elsődleges hitelesítési adatok. Ez az egyetlen „faktor", amit az azonosítón kívül tudni kell a rendszerbe való belépéséhez. Mivel azonban a jelszó ellopható, lefigyelhető, feltörhető, ezért kritikus rendszereknél már többfaktoros hitelesítést használnak. A jelszótörés [h] jelentése ennek megfelelően tehát a jelszó nyílt, szöveges verziójának megszerzése. Több módszer is ismeretes erre (nyers erő, szótár alapú, szivárványtáblázat stb.). A jelszótörésnek kettős szándéka lehet. Az egyik, hogy a támadó gyorsan megtalálja a jelszót az adott felhasználó fiókjához. A másik cél az lehet, hogy a támadó egy ellopott jelszóadatbázisból minél több jelszót visszafejtsen. Ez a tevékenység vagy nagy számítási kapacitást igényel, vagy nagyon

sokáig tart. Fentiek miatt szükséges, hogy az informatikai rendszerek üzemeltetői különösen odafigyeljenek a jelszavak – illetve azok kivonatainak a – rendszerben történő biztonságos kezelésére és védelmére, többek között a hibás bejelentkezések figyelésével és bizonyos számú próbálkozás utáni védelem (tiltás, felfüggesztés) életbe léptetésével, a jelszavak kivonatainak megfelelő tárolásával és a jelszóadatbázisok fokozott védelmével. Az egyik jó módszer a jelszókivonatok „sózása", amikor a jelszót a hozzá tartozó azonosítóval (amelyek egyediek a rendszerben) együtt kivonatolják, így minden egyes jelszókivonat teljesen egyedi lesz.

Természetesen lehetnek olyan fenyegetések az adatokra, amelyekről adott helyzetben nem tehet senki sem, így a „**vis maior**" kategóriába tartozik. Ilyen például az adatok esetében azok megsemmisülése egy tűzeset kapcsán. Fenyegetést jelentenek az adatokra az emberi tevékenységből adódó, nem szándékosan, hanem , gondatlanságból elkövetett hibák is.

Minden egyes támadási formában közös, hogy a felhasználók, tulajdonosok rovására történik, valamilyen kárt okoz, és emiatt a Büntető Törvénykönyv (Btk.) szerint ma már ezek számítógépes bűncselekményeknek számítanak.

A számítógépes bűnözés igen jól jövedelmező tevékenység. Elég csak a levélszemét küldéséből befolyó dollármilliárdokat megemlíteni, vagy az egyre emelkedő számú zsarolóvírus-aktivitást, amelyből a támadóknak akár közvetlen bevétele származhat. . Ezen kívül a Fraud as a Service (FaaS) megjelenésével bárki hozzá nem értő is tud olyan internetes bűncselekményeket elkövetni, amelyhez korábban komoly programozói, informatikai vagy hacker tudás kellett. Például botnet hálózat bérlése, zsarolóvírus terjesztő hálózat bérlése, saját zsarolóvírus kampány készítése, kiválasztott célpontok támadása elosztott szolgáltatás megtagadásos (DDoS) támadással és még sorolhatnánk. Mindezek mindenhol növelik egy esetleges információbiztonsági incidens bekövetkezési valószínűségét.

4 Fenyegetettségi és támadási trendek az elmúlt évekből

Számos internetbiztonsággal foglalkozó cég ad ki évről évre olyan dokumentumot, amely az internetbiztonsággal, támadási trendekkel, statisztikákkal és a jövőre vonatkozó fenyegetettségi előrejelzésekkel foglalkozik. Ezek a fenyegetettségi riportok bemutatják az addig tapasztalt és mért internetes fenyegetettségek statisztikáit, módszereit és a várható trendeket.

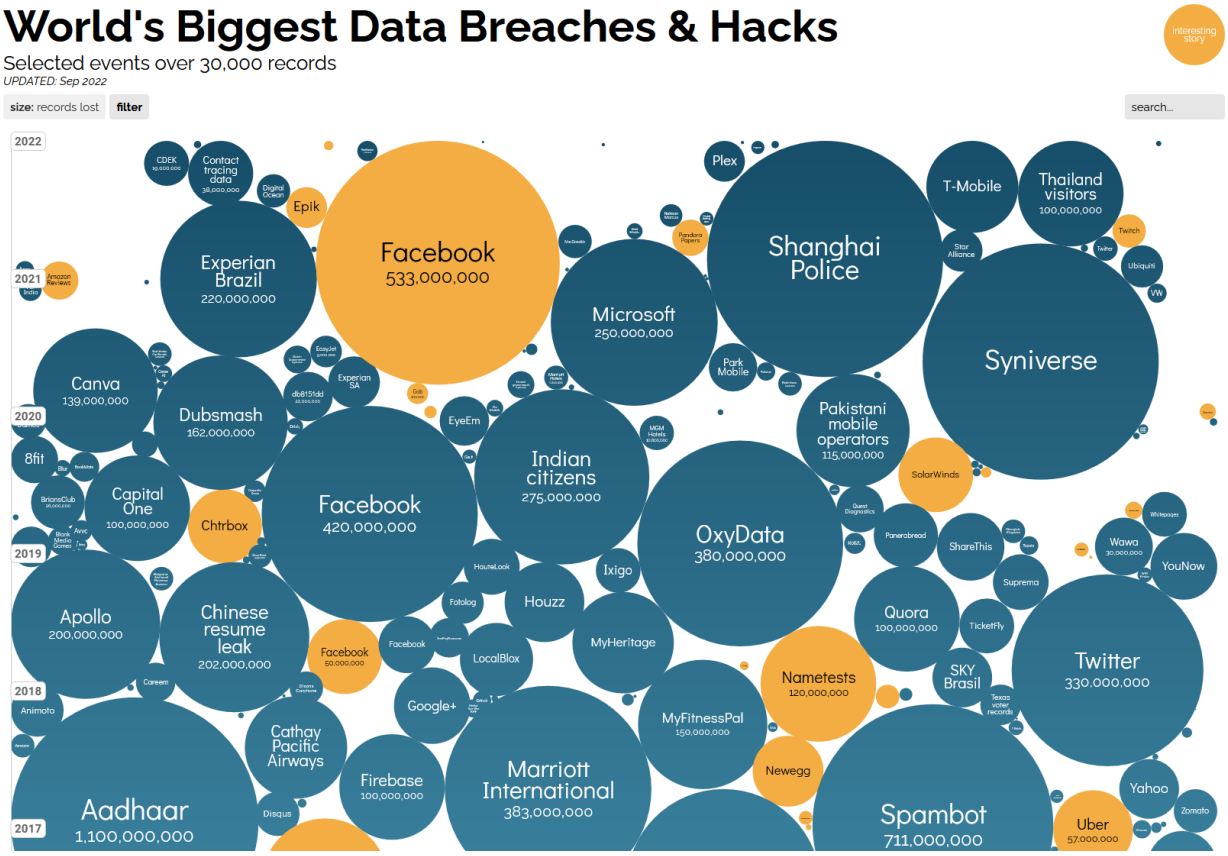
A trendek folyamatosan változnak és minden gyártó más termékpalettával, más fókusszal készíti el ezeket a fenyegetettségi riportokat.

Ezért a korábbi évek hagyományát megszakítva nem egy konkrét gyártó trend előrejelzéseit és statisztikáit ismertetjük, hanem megadjuk számos ilyen fenyegetettségi riport elérhetőségét és az olvasóra bízzuk, hogy melyik gyártó, vagy szervezet ilyen riportját ismeri meg.

- Sophos - https://www.sophos.com/en-us/content/security-threat-report
- Crowdstrike - https://www.crowdstrike.com/global-threat-report/
- Manidiant - https://www.mandiant.com/m-trends
- Checkpoint - https://resources.checkpoint.com/report/2023-check-point-cyber-security-report
- Kaspersky - https://securelist.com/smb-threat-report-2023/110097/
- Fortinet - https://www.fortinet.com/demand/gated/wp-threat-prediction-2023
- Forrester - https://www.cisco.com/c/en/us/products/security/top-cybersecurity-threats-2023.html
- ESET - https://www.eset.com/us/business/resource-center/reports/
- McAfee - https://www.mcafee.com/en-us/resources/cybersecurity-reports-and-guides.html
- ENISA - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Egyes gyártók és szervezetek szektorokra vagy akár technológiákra lebontva is adnak ki riportokat.

4.1 Személyes adatokat érintő incidensek



3. ábra: 30.000 rekordnál többet érintő adatbiztonsági incidensek infografikája[14]

A világban többszázmillió adatot érintő adatlopás történik, amelyben a könyvünk előző, 2019-es kiadásában megjelentetett adatokhoz képest sincs változás. . Ha ellátogatunk a fenti ábra weboldalára, akkor az egyes buborékokba kattintva további részleteket olvashatunk. Megnézhetjük, hogy milyen típusú adatok voltak érintve az adatlopásokban (személyes adatok, bankkártya számok, társadalombiztosítási azonosítók stb.), illetve részletes beszámolókat, híreket is böngészhetünk.

4.2 Kiberbűnözés, mint szolgáltatás

Az előző fejezethez is kapcsolódva az egyik legaggasztóbb trend az elmúlt években az, hogy a már a 2019-es könyvünkben is említett FaaS – Fraud as a Service, vagyis

[14] https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

az internetes csalások és támadások szolgáltatásként történő elérhetősége kiszélesedett. Már önálló ágakként működnek tovább és ez lehetőséget ad egyre több és egyre képzetlenebb „új belépőnek", akik kiberbűnözésből szeretnének anyagi haszonra szert tenni.

A Sophos biztonsági cég 2023-as Threat Reportja szerint „*Ahogyan az informatikai vállalatok is áttértek a "szolgáltatásként" nyújtott ajánlatokra, úgy a kiberbűnözés ökoszisztémája is ezt tette. A hozzáférési brókerek, a zsarolóprogramok, az információlopó- és rosszindulatú programok szabad elérése és egyéb, a kiberbűnözési műveletek és eszközök elérhetősége csökkentették a belépési korlátokat a leendő kiberbűnözők számára.*"

A SOPHOS az alábbi szolgáltatási kategóriákat ismerteti a riportjában:

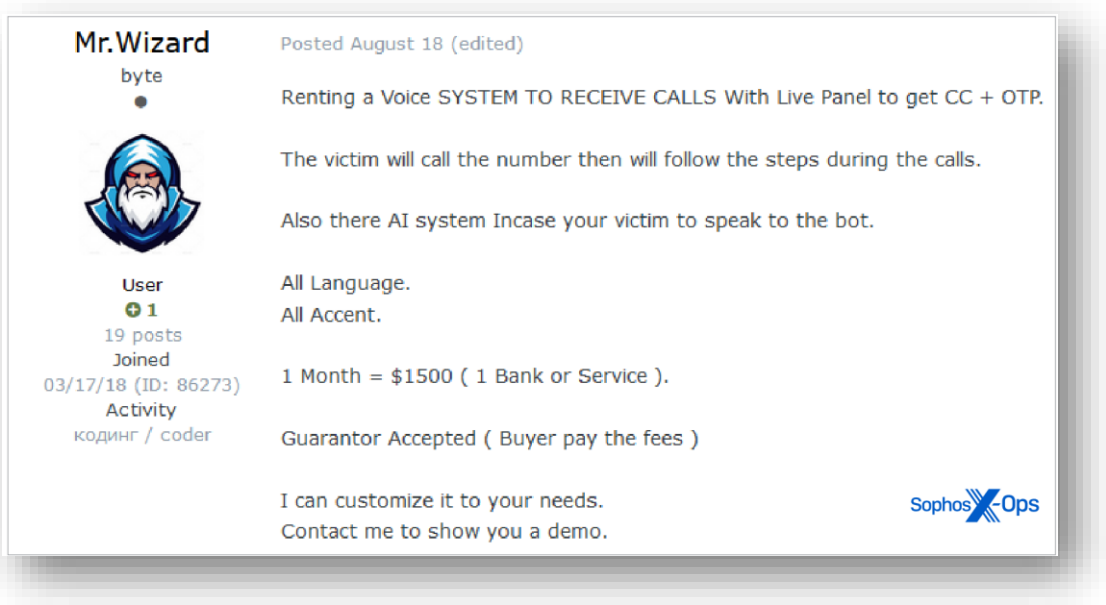
- Access as a Service: hozzáférés, mint szolgáltatás: A kompromittált számlákhoz és rendszerekhez való hozzáférést egyenként vagy nagy tételben értékesítik a kiberbűnözők.
- Malware distribution/spreading-as-a-service: rosszindulatú programok terjesztése szolgáltatásként.
- Phishing-as-a-service: adathalászat, mint szolgáltatás. Az adathalász kampányokhoz végponttól végpontig tartó szolgáltatást nyújtanak a kiberbűnözők, beleértve a klónozott oldalak és tárhelyeik elérhetőségét, a spamszűrők megkerülésére szolgáló, szerkesztett e-maileket és az eredmények nyomon követésére szolgáló adminisztrációs felületeket.
- OPSEC[15]-as-a-service (Szerkeszői megjegyzés: jelen esetben a kiberbűnözők infrastruktúrájának védelmére): a kiberbűnöző eladó felajánlja, hogy OPSEC-szolgáltatással segíti a vevőket, akár egyszeri beállítással, akár havi előfizetéses rendszerben, amelynek célja a Cobalt Strike[16] használata során a fertőzések elrejtése és a felderítés kockázatának minimalizálása.
- Crypting-as-a-service: a titkosítás, mint szolgáltatás, egy gyakori, számos fórumon eladásra kínált szolgáltatás. Célja a rosszindulatú programok titkosítása, hogy azok

[15] Az operatív biztonság (OPSEC) egy biztonsági és kockázatkezelési folyamat, amely megakadályozza, hogy érzékeny információk rossz kezekbe kerüljenek.

[16] A Cobalt Strike egy olyan biztonsági szoftver és tesztelési eszköz, amelyet eredetileg a "pentester" (vagyis etikus hackerek) és biztonsági szakértők használnak az IT rendszerek sebezhetőségeinek és biztonsági réseinek feltárására. Az eszköznek azonban vannak olyan verziói is, amelyeket rosszindulatú hackerek használhatnak a támadások végrehajtására.

elkerüljék a felismerést - különösen a Windows Defender és a SmartScreen és egyéb vírusirtó termékek által.

- Scamming-as-a-service: kriptovalutás és egyéb csalásokhoz kapcsolódó programok és szolgáltatások.
- Vishing-as-a-service: hangalapú adathalászat ("vishing") szolgáltatás, amelynek során a kiberbűnöző olyan szolgáltatást nyújt, ahol nem emberek, hanem emberi hangon beszélő mesterséges intelligencia chat robotok kommunikálnak az áldozatokkal.



4. ábra: A SOPHOS 2023-as Threat Reportjában szereplő kép a „vhishing as a service" szolgáltatásról

- Spamming-as-a-service: a „klasszikus" kéretlen üzenetküldési (SPAM) szolgáltatás, amely során a kiberbűnözők olyan infrastruktúrát biztosítanak egyedi díjért vagy előfizetéses formában, amelyben SMS-ben, e-mailben lehet nagy tömegű kéretlen üzenetet eljuttatni a felhasználóknak.
- Scanning-as-a-service: a szolgáltatás során a kiberbűnözők elérhetőséget biztosítanak számos legális kereskedelmi biztonsági sérülékenységkereső eszközhöz (Metasploit, Invikti, Burp Suite, Cobalt Strike, Brute Ratel stb.), amelyek segítségével a vevő a célpontok infrastruktúráját vizsgálhatja sérülékenységek keresésére – majd a talált sérülékenységek kihasználására.

Bár a SOPHOS riport nem említi, de már a 2019-es kiadásunkban is szerepelt a Túlterheléses támadások szolgáltatásként történő igénye vétele, amelyről könyvünk egy későbbi fejezete szól részletesen, képekkel illusztrálva.

Összefoglalva: a trend ijesztő, hiszen egyre többen férnek hozzá informatikai rendszerekhez és az internethez. A kiberbűnözőknek elég egyetlen gyenge pontot találni a rendszereinken vagy felhasználóinkon, míg a védelmi oldalnak folyamatosan, mindenre kiterjedően tudni kell biztosítani az adatok védelmét.

4.3 Mobileszközök fenyegetettségei

Ahogy terjednek a mobileszközök – főleg az okostelefonokra és táblagépekre gondolva itt – úgy emelkedik a rájuk írt kártevőprogramok száma is. Ráadásul növekszik azon támadások mennyisége is, amely a mobil eszközön tárolt adatok megszerzésére, vagy az eszköz fölötti irányítás átvételére irányul. Bár minden gyártó azt javasolja, hogy csak a hivatalos alkalmazás áruházból töltsünk le alkalmazásokat, természetesen lehetőség van ettől eltekinteni, bár ez jelentős kockázatokat hordoz magában. A hivatalos alkalmazás-áruházakban is előfordulnak kártevőt tartalmazó alkalmazások, dacára annak, hogy az üzemeltetők igyekeznek mindent megtenni, hogy csak „tiszta” appok legyenek a felhasználók számára elérhetőek.

Rendkívül fontos, hogy az okoseszközöket is lássuk el megfelelő védelemmel, tartozzon bármelyik operációs rendszer kategóriába (Android, iOS, Windows stb.).

Minden olyan neves gyártó, aki vírusvédelmi megoldásokat kínál, vagy valamelyik programcsomagja részeként, vagy önállóan, de kínál az okoseszközökre készített védelmi megoldásokat is. Általános szabály, hogy védelmi programokat is csak az adott platform hivatalos honlapjáról vagy applikáció boltjából töltsünk le (Google Play, Apple Store, Microsoft Store). Különösen ügyelni kell az okoseszközökön a számos ingyenes program által megjelenített reklámokra. Ezek gyakran ijesztgetik a felhasználókat azzal, hogy vírusos az eszközük, és ezért azonnal töltsék le a felkínált vírusirtót. Nagyon gyakran pontosan ezek az ál-vírusirtó programok hordozzák a tényleges fenyegetettséget.

Mobileszközökre is elérhetőek olyan teljeskörű védelmi megoldások, amelyek képesek már ellopott/elveszett eszköz nyomon követesére, szülői felügyeleti funkciókra és minden olyan egyéb tevékenységre, amit az asztali PC – munkaállomás környezetben megszokhattunk.

Ha egy rosszindulatú program megfertőzte az eszközünket, akkor előfordulhat, hogy a támadó vezérelni tudja a telefont távolról. Emelt díjas hívásokat indíthat, továbbküldheti a

beérkező sms-eket, bekapcsolhatja a kamerát és a mikrofont és gyakorlatilag mindent megtehet az eszközzel, amit csak szeretne.

A mobileszközök esetében azonban nem csak a vírusfertőzés jelent problémát. A mobileszközeinket és a rajtuk tárolt adatainkat az eszközök mérete és hordozhatósága is veszélyeknek teszi ki. Minden esetben tegyünk az eszközre képernyő zárolást, amelyet csak PIN kóddal, jelkóddal, vagy valamilyen biometrikus azonosítóval - jellemzően ujjlenyomattal oldhatunk fel. Így egy esetleges ellopás vagy elvesztés esetén nem fognak tudni a támadók az eszközünkbe belépni és ott jogosulatlan műveleteket végezni.

Az eszközeink fizikai védelme, az adatok védelme miatt is fontos. Lássuk el az eszközt, a telefont, a tabletet olyan tokkal, amely gátolja a fizikai behatások káros következményeit. Tessünk rájuk üvegfóliát, amely megvédi a kijelzőt a sérüléstől. Okostelefonok és tabletek esetében a kijelző különösen kritikus pontja az eszköznek, mert azon keresztül vezéreljük az eszközt. Ha sérül a kijelző – például mert élére ejtettük és összetört – akkor nem fogunk tudni utasításokat adni az eszköznek még akkor sem, ha számítógéphez csatlakoztatjuk és az eszköz maga működik. Ugyanis ilyenkor engedélyt kell adni, hogy a számítógép hozzáférjen az eszközhöz. De kijelző nélkül ez nem működik. Ilyenkor vagy kicseréltetjük a kijelzőt, vagy a teljes eszközt kicseréljük. Ilyenkor figyeljünk oda, hogy az adataink még az eszközön vannak és jó eséllyel el fognak veszni, hacsak nem volt mentésünk.

A másik fontos védelmi intézkedés az eszköz, vagy ha erre nincs lehetőség, akkor legalább a háttértárak titkosítása. Amennyiben például memóriakártyával van bővítve az eszközünk, egy ellopás vagy elvesztés esetén azt ki lehet venni az eszközből és más eszközben olvasható az adattartalma. Kivéve, hogyha titkosítottan tároltuk a rajta lévő adatokat. A háttértárak titkosítása egy opció, amelyet az eszköz biztonsági beállításai között találunk.

A titkosítás megvéd az illetéktelen adathozzáférésektől, de nem véd meg az adatok elveszésétől. Sőt, ha a titkosító alkalmazás vagy a titkosító algoritmus nem jól működik, vagy sérül a titkosító kulcs, akkor sajnos mi sem fogjuk tudni az adatokat visszafejteni és abba helyzetbe kerülünk, mintha biztonságosan töröltük volna az adatainkat. Ezért rendkívül fontos az adatok rendszeres mentése. Erről a mentésekről szóló fejezetben szólunk bővebben.

Ha mobileszközök fenyegetettségeiről beszélünk, akkor nem mehetünk el szó nélkül a mobilalkalmazások hozzáférési igényei mellett sem. A mobilalkalmazások is hozzáférést igényelnek a telefon/tablet erőforrásaihoz. Az alkalmazás célja és funkciója szerint ez a hozzáférés kiterjedhet akár a kamerára, mikrofonra, híváslistára, geolokációs adatokra és még sorolhatnánk. Az alkalmazás használata során a felhasználási feltételekben a fejlesztők

leírják, hogy az alkalmazáson keresztül milyen adatokat érnek el, és hogy mit tesznek ezekkel az adatokkal, kiknek adják át és milyen célból.

Érdemes ezeket figyelmesen elolvasni és ha egy alkalmazás túlzó jogosultságokat szeretne, vagy olyan adatokhoz szeretne hozzáférni, ami nem indokolt a funkcióját és célját tekintve, akkor keressünk másik, kisebb jogosultság igényű alkalmazást. Modernebb operációs rendszer verziókon már funkciónként adhatunk engedélyt az alkalmazásoknak az erőforrások elérésére. Az utóbbi évek tapasztalata, hogy rendkívül sok olyan adatbiztonsági incidens van, amely során a mobilalkalmazások feljogosítva – vagy engedély nélkül - felhasználói adatokat továbbítottak a fejlesztőknek, akik ezen adatokat értékesítették vagy kiadták harmadik feleknek a felhasználók tudta és belegyezése nélkül.

4.3.1 Esettanulmány a FluBot kártevőről

A FluBot egy olyan kártékony szoftver, amely mobiltelefonokat megfertőzve terjedt, és különféle rosszindulatú tevékenységeket hajtott végre. Először 2020 év végén és 2021 elején jelent meg Európában, különösen Spanyolországban és Németországban, de magyar bankok mobilalkamazásaira is veszélyes volt. A hamis SMS-ekben olyan linkek és mellékletek voltak találhatók. amelyekre, ha rákkattintott a felhasználó, akkor a kártevő program egy csomagküldő szolgáltató (DHL és FedEx) csomagkövető alkalmazásának álcázva magát települt rá a mobiltelefonokra.

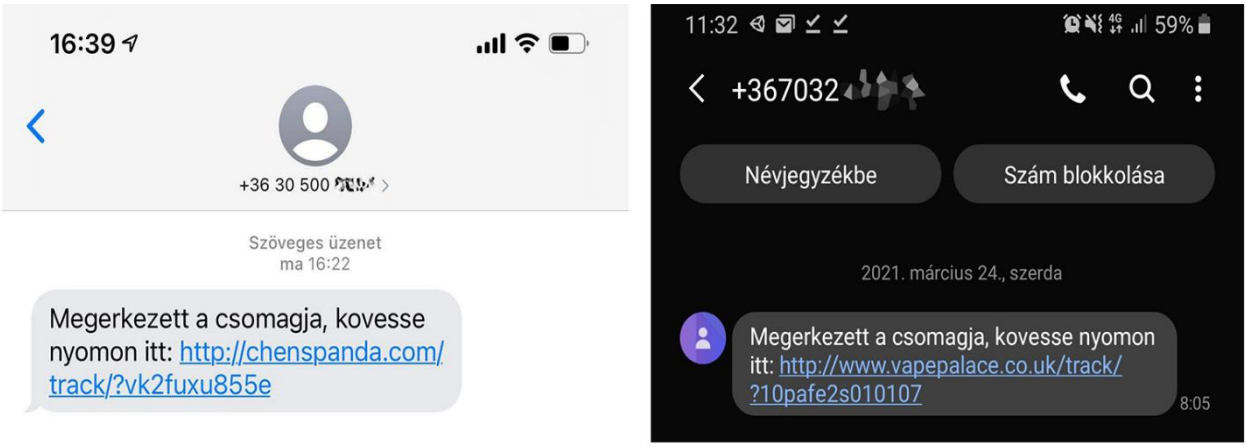
A FluBot, miután rátelepül a mobilra, képes számos káros tevékenységet végrehajtani, például SMS-eket küldeni az áldozat telefonjának kontaktlistájáról, amelyet előzetesen feltöltött a szoftver vezérlő C&C szerverére. Az SMS üzenetben rosszindulatú webhelyekre irányította a felhasználót, azért, hogy érzékeny adatokat, például banki adatokat szerezzenek meg a támadók.

A Nemzeti Kibervédelmi Intézet több figyelmeztetést is kiadott a kártevővel kapcsolatban, ebben a következőképpen foglalták össze a FluBot kértevő lényegét.

"*a fertőzésben érintett készülékek esetén a FluBot kártevő folyamatosan figyeli a készülékeken futtatott alkalmazásokat. Amennyiben a program pénzügyi vagy kriptovalutákhoz kapcsolódó alkalmazás indítását észleli, abban az esetben az eredeti alkalmazást „elfedi" (egy ún. overlay technikával), és az eredeti alkalmazás mellett, egy az eredetihez hasonló*

adathalász felületet nyit meg, amely képes a felhasználói (felhasználónév, jelszó) adatok kinyerésére és továbbítására."

Ezzel a módszerrel, valamint azzal, hogy a kártevő az SMS szolgáltatáshoz is hozzáfért és képes volt átirányítani a banki tranzakciók hitelesítő és jóváhagyó üzeneteit, képes volt észrevétlenül az áldozatok bankszámláihoz is hozzáférni, jelentős károkat okozva.



5. ábra: FluBot kártevőt terjesztő SMS üzenetek

6. ábra: FluBot kártevő csomagkövető alkalmazásnak álcázva

Az ilyen jellegű támadások elleni védekezéshez a felhasználóknak alapvetően néhány lépést kell követniük:

1. **Legyünk körültekintőek**: soha ne kattintsunk nem megbízható forrásból származó linkekre és ne nyissunk meg gyanús mellékleteket, különösen ismeretlen vagy nem várt e-mailekben, vagy SMS-ekben!

2. **Naprakész alkalmazások a telefonokon és számítógépeken:** az operációs rendszer és az alkalmazások rendszeres frissítése segít a biztonság javításában és a sebezhetőségek minimalizálásában.
3. **Telepítsünk megbízható biztonsági szoftvereket**: használjunk megbízható mobilbiztonsági alkalmazásokat, amelyek képesek az ilyen típusú fenyegetések felismerésére és eltávolítására!
4. **Legyünk tudatosak:** legyünk tisztában a kibertámadások módszereivel! Tanulmányozzuk rendszeresen, hogy hogyan működnek a phishing támadások, és hogyan lehetünk képesek felismerni azokat!

4.4 Kiberkonfliktusok hatásai

Az utóbbi években megszaporodtak a kiberkonfliktusok, mivel egyrészről az ellenséges felek beemelték az interneten történő károkozási eszközöket is a támadófegyvereik közé, másrészről az eszközök könnyebb elérhetősége és a várható eredmény jelentősége egyre több ilyen jellegű eseményt hozott létre a kibertérben[17]. Alapesetben nem feltétlenül az otthoni számítógépünk megtámadása a cél, azonban a dezinformálás, illetve a pásztázó támadások (nem kellően védett gépek keresése az interneten) következtében ezek kihatással lehetnek a hétköznapi életünkre is. Lehet, hogy nem mi voltunk a célpont, csak ha beleesünk a „szórásba", és ha a gépünk nem annyira védett, akkor a támadók – adott esetben többszázezer hacker – ennek megörülnek, és ki fogják használni a kínálkozó alkalmat akkor is, ha nem ez volt az eredeti céljuk.

A védekezésnél nem lehet eleget hangsúlyozni tehát a számítógépeink védelmének fontosságát (vírusirtó, személyi tűzfal, mentés), a hiteles információforrások elérése, és az információk hitelességének ellenőrzése mellett.

A kibertér védelmével az Európai Unió is emelt szinten foglalkozik. Mindezek hatására 2023. január 16-án kiadásra került az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2)[18]. Ennek célja a

[17] Dr. Krasznay Csaba: Kiberbiztonság a XXI. században. Katonai Nemzetbiztonsági Szolgálat, 2022.
[18] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022L2555&qid=1696685541293

kiberbiztonsági képességeknek (kiberreziliencia) az egész Unióban történő kiépítése, a kulcsfontosságú ágazatokban az alapvető szolgáltatások nyújtására használt hálózati és információs rendszerek fenyegetéseinek mérséklése, valamint az említett szolgáltatások folyamatosságának biztosítása az események során. Ennek hatására számos olyan szervezetnek, vállalkozásnak kell a jogszabályi megfelelőség biztosítása érdekében növelnie a kiberbiztonsági képességeit, amelyek eddig saját hatáskörben dönthettek az ilyen irányú képességeik kialakításáról. A védekezés tehát nem csak az egyén feladata és felelőssége, intézményi szinten is számos olyan intézkedés jelent meg a közelmúltban, amelyek a kiberreziliencia megteremtését és növelését társadalmi szinten képzeli el, minden szereplő közreműködésével.

4.5 Gyermekeket érintő fenyegetettségek

Napjainkra a gyerekek mindennapi életének szerves részévé váltak az informatikai eszközök és az internet is. Ahogy az első informatikai eszközök a kezükbe és látókörükbe kerülnek, saját maguk fedezik fel azok tulajdonságait és használatát. Saját barangolás útján ismerik meg az internetet is, és természetesen jelentős hatással van rájuk a korosztályuk, a nagyobb testvér és az úgynevezett influenszerek. Ők azok a fiatalok, akik saját bloggal vagy videócsatornával komoly tömegeket érnek el és szólítanak meg – ezáltal hatást gyakorolva a nézőközönségre – ritkábban olvasótáborra.

Ebből az ismerkedési fázisból nagyon sokszor hiányzik a szülő és a pedagógusok tevékenysége. Ez pedig komoly gátja a későbbi szülői, pedagógusi kontroll gyakorlásának. A szülőknek hatalmas erőfeszítést igényel(ne) lépést tartani a gyermekeik informatikai tudásával és az interneten elérhető tartalmak megismerésével. Ahogy a gyerekeket beszippantja az online tér, úgy tűnnek el a szülő elől a valós és virtuális világban egyaránt. Több negatív következmény mellett egy különösen figyelemre méltó következménye van annak, ha a szülő vagy pedagógus képzetlenebb az internet és az információtechnológia világában, mint a gyermekek. Ez pedig az, hogy a gyerekek nem fogják elfogadni a tanácsaikat, és még kevésbé fogják elfogadni a tiltást, vagy büntetést. Kutatások kimutatták, hogy mind a szülők, mind a gyermekek úgy gondolják, hogy a gyerekek értenek jobban manapság az internethez és az informatikai eszközökhöz – ez pedig egy nagyon veszélyes tendencia.

Ennyi bevezető után a szülőknek és pedagógusoknak érdemes az alábbi témaköröket áttekinteni és a gyermekeikkel és tanítványaikkal átbeszélni. Elkerülve jelen tankönyv

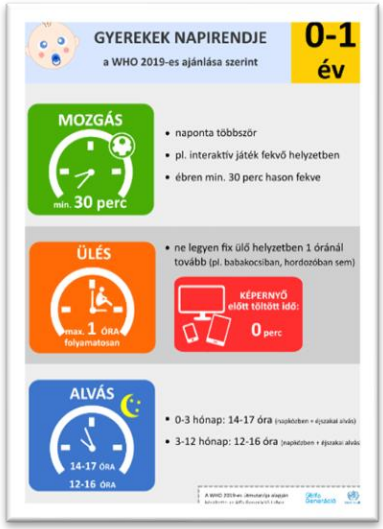
tartalmának ismétléseit, itt csak röviden fogjuk kiemelni az áttekintendő témákat, megadva, hogy a könyvben melyik fejezet foglalkozik részletesebben a témával.

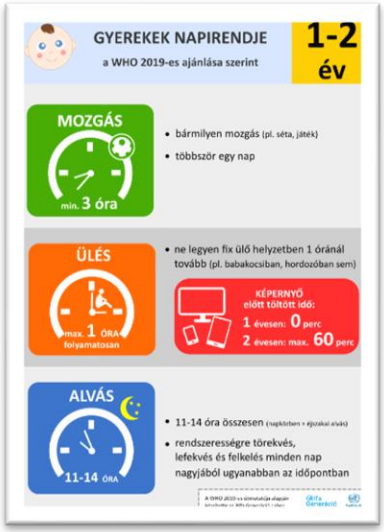
4.5.1 A kezdetek

Manapság egyre kisebb kortól kapnak a gyerekek a kezükbe informatikai eszközöket. Ennek egyik, még kutatás alatt álló következménye, hogy a képernyő nyújtotta vizuális ingerek annyira a bűvkörükbe vonják a gyermekeket, hogy nem mozognak eleget. És mozgás alatt most nem a sportolást értjük, hanem azokat az alapvető mozgásokat, amelyek elősegítik azon agyi kapcsolatok kialakítását, amik felelősek a nagy mozgásokért és a finommotorika kialakulásáért – később pedig az olvasás, írás és számolás megfelelő alkalmazásáért. Meredeken esik a gyerek olvasással töltött ideje, ami egyenes következménye a vizuális tartalmak térnyerésének. Ez azonban azzal jár, hogy a későbbiekben az írott tartalmak – iskolai feladatok értelmezése, a szövegértés nem fejlődik ki, ami majdnem minden további tanulásnak az alapja.

Fontos feladata lenne a szülőknek, hogy ne a tablet vagy az okostelefon legyen a digitális bébicsősz, mert később visszafordíthatatlan következményei lesznek. Igyekezzünk minél későbbi időpontban informatikai eszközt adni a gyerekek kezébe és korlátozzuk a képernyőidőt az ajánlott szintre.

A WHO ajánlása a gyerekek napirendjéről, ideértve a képernyő előtt töltött időt is.





Sajnálatos tapasztalat, hogy már óvodáskorban is a gyerekek egyre nagyobb tábora rendelkezik saját tablettel, számítógéppel vagy éppen okostelefonnal.

A későbbiek során pedig a közösségi informatikai eszközhasználat határozza meg azt az időpillanatot, amikor a gyereknek is el kell kezdenie informatikai eszközöket használni. Hiszen már általános iskola alsó tagozatában is megfigyelhető, hogy a gyerekek „nem hivatalos", önszerveződő, azonnali üzenetküldő szolgáltatásokon tartják a kapcsolatot és ha valaki ehhez nem tud kapcsolódni, mert nincs mondjuk saját okostelefonja, akkor kizáródik a közösségből, aminek szintén negatív hatásai lehetnek, már rövidtávon is. Felső osztályokban pedig már szinte alap, hogy az osztályoknak saját – remélhetőleg zárt – csoportjaik vannak, így a közösségi oldal és annak elérése egy nagyon fontos kommunikációs csatornává lépett elő. De vajon az oktatás lépést tart-e ezekkel a tendenciákkal? Tanulják-e a gyerekek használni az eszközöket, szolgáltatásokat? Ki tanítja meg nekik a veszélyek felismerését?

4.5.2 Szülői kontroll hiánya

Az előző pontban említett problémának másik oldala, hogy maguk a szülők sem értenek megfelelő szinten sem az általuk használt és a gyerekek által is hozzáférhető informatikai eszközökhöz, sem az azokon futó szolgáltatásokhoz. A gyerekek viszont rendkívül kreatívak, céltudatosak és ami fontos, sokkal több idejük van az eszközök és szolgáltatások megismerésére, mint a szüleiknek. Ez azonban azzal jár, hogy egyre kisebb korban érkezik el az a pont, ahol a szülő ráébred, hogy nem ért eléggé a digitális eszközhöz, az internethez és internetes szolgáltatásokhoz, és a gyerekek pedig rájönnek – vagy ezt kezdik tapasztalni, hogy jobban értenek hozzá, mint a szüleik. Megfordulnak a szerepek, sok esetben már a gyerekek tanítják a szüleiket, ők konfigurálják az otthoni informatikai eszközöket. És a tendencia itt nem áll meg, hiszen az internet korlátlan forrása a tudásnak és a tanulási lehetőségeknek. És a gyerekek megtalálják azokat a csatornákat, ami őket érdekli.

Szülőként nagyon fontos, hogy ne csak a gyermek fizikai életét ismerjük és támogassuk, hanem a digitális térben zajló életét is. Szülőként az alábbi tevékenységeket kell napról-napra, egyre magasabb szinten művelnünk, ha azt szeretnénk, hogy a gyermek digitális életébe is bele lássunk és annak is részesei legyünk. Sok szülőnek ez ijesztő lehet, hiszen jó esély van rá, hogy fordított tanulási szituációba kerülünk, amikor is a gyermek tud többet az adott témáról és nekünk kell tanulnunk tőle. De ez nem szégyen, fogjuk fel egy közös programnak! A következőkben összefoglaljuk, hogy mi mindent tehetünk szülőként:

1. **Kommunikáció:** a legfontosabb az, hogy nyitott és őszinte kommunikációt tartsunk fenn a gyermekünkkel a digitális életéről. Beszéljünk a gyermek online

tevékenységeiről, élményeiről és esetleges problémáiról, és biztosítsuk őt arról, hogy szülőként bármikor szívesen segítünk.

2. **Tanulás:** tanuljunk meg együtt használni néhány platformot, alkalmazást, hogy jobban megértsük, hogyan működnek.
3. **Korlátozások és szabályok:** határozzunk meg digitális időkereteket és szabályokat, például a képernyőidő korlátozását vagy az online tevékenységek monitorozását, vagy ami nagyon fontos, hiszen a gyerekek sokat játszanak a digitális térben is, a játékokból való kiszállás szabályát. Fontos, hogy az ilyen szabályokat együtt állapítsuk meg, legyen magyarázva a szabályok oka és értelme.
4. **Online biztonság:** beszéljünk a gyermekekkel az online biztonságról, és tanítsuk meg nekik a fontos alapelveket, például a biztonságos jelszavak és erős hitelesítés használatát, az adatvédelmet és a közösségi média etikettjét.
5. **Példamutatás:** legyünk jó példák és modellek a gyermekeink számára! Mutassuk meg nekik, hogyan lehet egészségesen és felelősen használni a digitális eszközöket.
6. **Tudatosság a tartalmakról**: beszéljünk a gyermekekkel az online tartalmakról és a média kritikai olvasásáról. Tanítsuk meg nekik, hogyan válogassanak és a különböző tartalmak között, és hogyan értékeljék azokat.
7. **Empátia és online viselkedés:** Az online viselkedés és az empátia fontos téma. Tanítsuk meg a gyermekeinknek, hogyan kell másokkal tisztelettudóan és empatikusan kommunikálni az online térben.
8. **Követés és monitorozás:** Nyomon követhetjük a gyermekek online tevékenységeit, az erre a célra az NMHH által is javasolt szülői felügyelet programok valamelyikében. Azonban fontos megtalálni az egyensúlyt a szabadság és a biztonság között.
9. **Támogatás és segítségnyújtás:** Ha a gyermekeink problémába ütköznek az online térben, legyünk ott, hogy segítsünk és támogassuk őket. Beszéljünk velük arról, hogyan kell kezelni a zaklatást, a közösségi média nyomást és egyéb kihívásokat.
10. **Minőségi idő együtt:** Keressünk időt arra, hogy közösen töltsünk el időt online és offline egyaránt. Az együtt töltött idő lehetőséget ad a beszélgetésekre és az együttműködésre és közös élményeket ad.

4.5.3 Közösségi oldalak

A világ legnagyobb közössége jelen pillanatban a Facebook. 2019-ben, jelen kötet előző kiadásának idején a Facebooknak napi szinten másfél milliárd aktív felhasználója volt. Most 2023 második negyedévében ez a szám már 2 milliárd felett jár[19].

Mégis az a tapasztalat, hogy a gyerekek már be sem regisztrálnak, a fiatalok pedig elhagyják a Facebook használatát. Bár 13 éves korhatárhoz kötött a használat, azok a gyerekek, aki mégis kipróbálják, rendre meghamisítják a születési dátumukat és jóval ezen kor elérése előtt elkezdik használni a szolgáltatást. Vannak gyerekek, akik hatéves koruktól aktívan használják azt. Teszik mindezt vagy szülői engedéllyel, vagy szülői nemtörődömséggel és/vagy tudatlansággal karöltve.

És hogy hová pártolnak át a gyerekek? Azon közösségi oldalakra, ahol nincsenek ott a szülők és ilyenekből egyre több van. Jelenleg az egyik legfeltörekvőbb közösségi szolgáltatás/alkalmazás a TikTok (korábban Musical.ly), ahol kezdetben rövid – jellemzően tizenöt másodperces vagy fél perces kis videókban lehetett valamilyen zenei vagy szöveges mini produkciókat bemutatni. 2021-ben a videók már 3 percesek is lehettek, most 2023-ban pedig már 10 perces videókat is megoszthatnak a felhasználók. Ez egyre több képernyő előtt töltött időt jelent. A videók lehetnek táncok, vicces hangalámondások vagy bármi. A probléma itt is az, hogy nincs valós felügyelet a regisztrációnál. A szabályok szerint itt is tizenhárom év lenne a korhatár, de gyakorlatilag bármilyen korú gyerek be tud regisztrálni és ezt kihasználják a bűnözők is. A TikTok a pedofilok kedvenc vadászterülete is, ráadásul egyre több a felnőtt jellegű tartalom is, amik szintén nem a gyermekek fejlődésben lévő személyiségének valók.

A közösségi oldalak egyéb veszélyeiről és a gyermekek által használt legnépszerűbb alkalmazásokról (amelyek között sok közösségi média alkalmazás is van) az 5.4.6 Bizalmassági eszközök közösségi oldalakon és a 4.5.7 A gyerekek által használt legnépszerűbb mobilalkalmazások fejezetekben szólunk részletesebben.

4.5.4 Fizikai biztonság

Az informatikai eszközök jellemzően sok pénzbe kerülnek, de pénztárcától függően mindenki megtalálja azt a verziót, amit a gyermekére rá mer bízni. Sajnos a gyerekek esetében az informatikai eszközök és kiemelten az okostelefonok egyfajta státusz szimbólumként működnek. Míg egy szülő el tudja fogadni, hogy adott funkcionalitást egy olcsóbb eszköz is tud

[19] https://www.statista.com/statistics/346167/facebook-global-dau/

biztosítani, egy gyermek esetében sokszor nem ez az elsődleges szempont, mivel, ha használt, régi, lassú okostelefonja van – ne adj' Isten – butatelefonja van, akkor ezért cikizhetik, sőt adott esetben ki is közösíthetik.

Ezért sajnos minden gyerek igyekszik jobb és jobb készülékeket beszerezni, vagy beszereztetni. Egyes eszközök ára a többszázezer forintot is elérheti, ezért potenciális célpontja lehet a bűnözőknek egy-egy ilyen eszköz megszerzése, ellopása. Ráadásul, ha az eszköz leesik, összetörik, megsérül, akkor a kár is értelemszerűen nagyobb. Szülőként törekedjünk arra, hogy az optimális megoldást biztosítsuk, helyezzük a hangsúlyt a szükséges és elégséges funkcionalitású és minőségű eszköz biztosítására. Így a gyermekünket sem tesszük ki fölösleges fenyegetéseknek.

A gyerekek informatikai eszközei esetén is ugyanúgy fontos lehet az adatok mentése. Csakhogy ezt a szülők sem szokták komolyan venni, és amikor már megtörtént a baj, egy elvesztés, egy zsarolóvírus, vagy egy szoftverhiba bekövetkezése esetén jut eszükbe, hogy de jó lett volna, ha van mentés.

Itt kell megemlítenünk, hogy a gyerekek körében egyre jellemzőbb a folyamatos eszközhasználat – ilyenkor gyakorlatilag felkeléstől lefekvésig maguknál hordozzák és használják az okostelefont. Utcán sétálva, tömegközlekedési eszközökön, autóban folyamatosan online vannak és különböző alkalmazásokat használnak, vagy zenét hallgatnak. Ebből fakadóan egyre több a baleset – amely közül végzetes, halálos kimenetelűek is voltak az utóbbi években. Bár nem csak a gyerekeket érinti, de állítólag az elmúlt években többen haltak meg a világban szelfi készítés közben (pl. lezuhantak szikláról), mint cápatámadásban.

4.5.5 Gyermekeket érintő internetes zaklatás – személyes adatokkal való visszaélés

Az internetes zaklatás (5.7.9 Internetes zaklatás) mind a korosztály, mind bűnözői oldalról az egyik legnagyobb fenyegetés, ami a gyermekeket érinti.

A TikTok alkalmazás az egyik legjellemzőbb példa erre, amellyel részletesen is foglalkozunk egy későbbi fejezetben. Az alkalmazás 2018-as statisztikái szerint havi százmillió aktív felhasználója volt és a felhasználók napi átlag ötvenkét percet használták az alkalmazást. Az egyik legnagyobb probléma itt is – ahogy a Facebook és szinte minden közösségi média alkalmazásnál – a felhasználói profilok és tartalmak láthatóságának rossz beállításai. Ha a szülő nem is tud erről, a gyerekeknek pedig senki nem magyarázta el, hogy a nyilvános profil és a nyilvános posztok azok tényleg mindenki által láthatók, kommentelhetők – sőt

beindexelik a keresők is – akkor ez a táptalaja a pedofil és egyéb beteges hajlamú – esetleg bűnöző felhasználóknak.

Fontos, hogy a gyermek fel legyen készítve az online térben történő kapcsolatteremtés lépéseire és veszélyeire. Tudjon arról, hogy az interneten rengetegen hamis profillal jelentkeznek be, és mások bőrébe bújva élik digitális életüket. Ezért alapvetően bizalmatlansággal kell fogadni minden olyan közeledést vagy kapcsolatépítést, ahol ismeretlenek keresik meg a gyermeket, sőt még néha az ismerősöket is érdemes leellenőrizni.

Az elmúlt években kialakultak azok a bűnözői csoportok, akik a gyermekek és fiatalok bizalmába férkőzve intim képeket csalnak ki tőlük, majd megzsarolják őket ezen képek nyilvánosságra hozásával. Rendkívül fontos, hogy felhívjuk a figyelmet a közösségi oldalakra feltöltött tartalmak láthatóságára, annak korlátozására – ahogy tesszük is ebben a könyvben.

4.5.6 A gyerekek életének és nyilvánosságának hatása a jövőre

Az, hogy ha egy gyermek élete a teljes nyilvánosság előtt zajlik, és születésétől kezdődően minden fontos életesemény a közösségi oldalakon dokumentálva van leírásokkal, videókkal, ismerősök és esetleg ismeretlenek általi kommentekkel az később komoly hatással lehet a gyermek személyiségfejlődésére, felnőtté válására és akár egész életére. „A tubusba a fogkrémet már nehéz visszanyomni” – ha egy gyerek életéről minden elérhető online és ez bekerült internetes keresők adatbázisába, lementhetik őket magánemberek, hozzáférhetnek cégek, és egyéb szervezetek (lásd Facebook és a Cambridge Analytica botrány), akkor a gyermek ez ellen később nagyon nehezen fog tudni fellépni, a következményeit meg viselnie kell.

Egyrészt születésekor és még évekig nem az ő döntése, hogy mi jelenik meg róla, másrészt sok kép és esemény a későbbiekben a felnőtt gyermek számára vállalhatatlan és jelentősen sérti a személyiségi jogait az, hogy ezek elérhetőek az interneten.

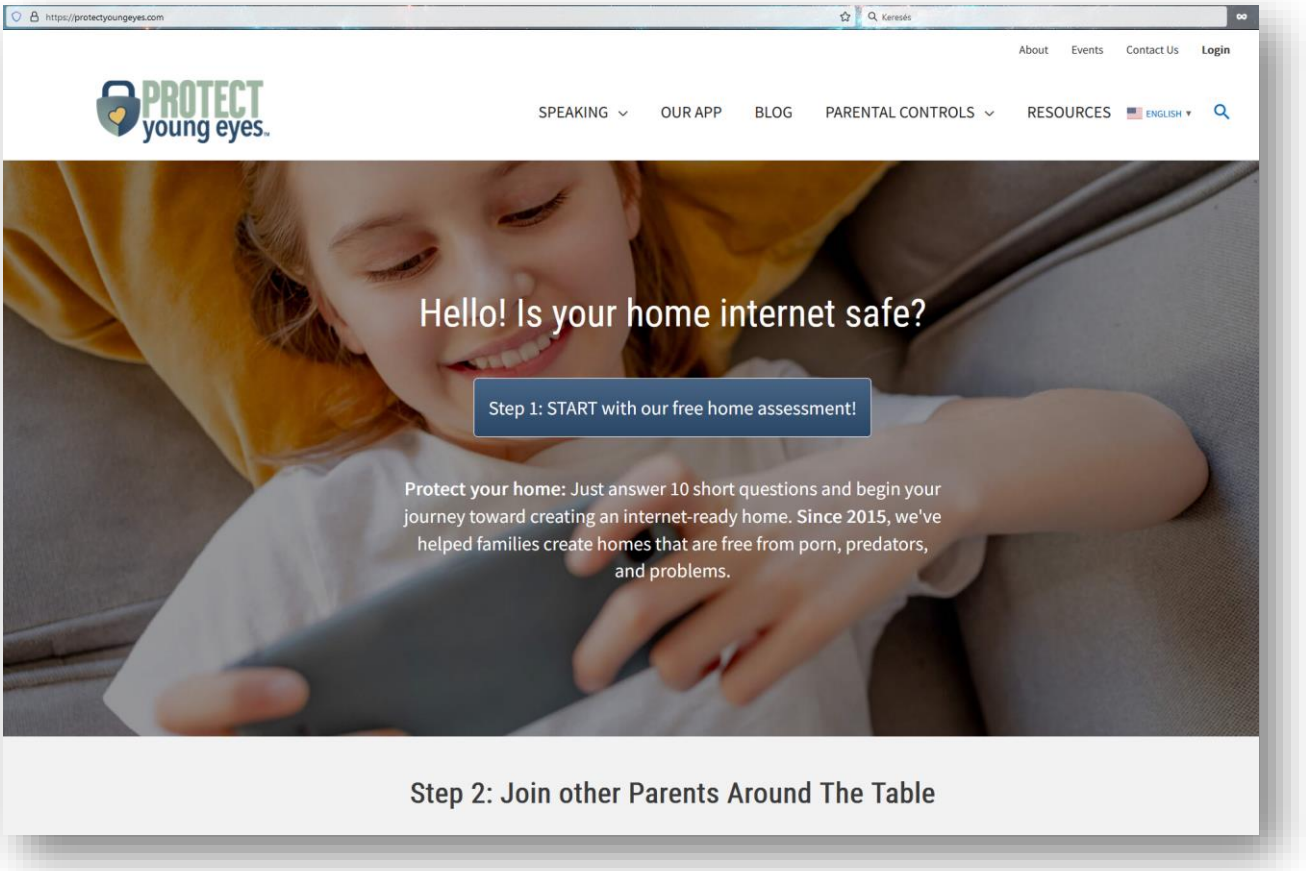
Minden szülőnek el kell gondolkodnia arról, hogyan tudja felelősségteljesen kielégíteni a szülői büszkeségből és közösségi – rokoni érdeklődésből fakadó azon igényeket, amelyek a gyermekei online megjelenését hozzák magukkal.

Az is egy fontos szempont, hogy ha a szülő rossz gyakorlatot követ – akkor előfordulhat, hogy a gyermek is ezt az utat fogja járni, akár a saját életeseményeivel, képeivel, videóival – ezek nyilvánossá tételével. Ez pedig, ha esetleg társadalmi normákat feszeget, vagy ízléstelen vagy sértő bárki gondolkodására vagy érzéseire nézve, akkor később visszaüthet egy álláskeresés vagy párkapcsolat építése során. Remélhetőleg nem fog eljönni az a korszak, amikor Kínához hasonlóan pontrendszerrel lesznek az emberek mérve és értékelve – ez

alapján pedig jutalmazva vagy büntetve, de az a fajta nyíltság, ami sokszor egyszerűen a tudatlanságból és nemtörődömségből fakad, kiváló táptalaja a hátrányos megkülönböztetésnek.

4.5.7 A gyerekek által használt legnépszerűbb mobilalkalmazások

Az alkalmazások száma több ezerre rúg, ezért meg sem kíséreljük, hogy akár egy mélyebb ismertetőt közöljünk ezekről. Szerencsére vannak olyan önkéntes kezdeményezések, amelyek tudnak időt és erőforrást biztosítani erre. Egyik ilyen honlap a „Protect Young Eyes[20]" nevet viseli.



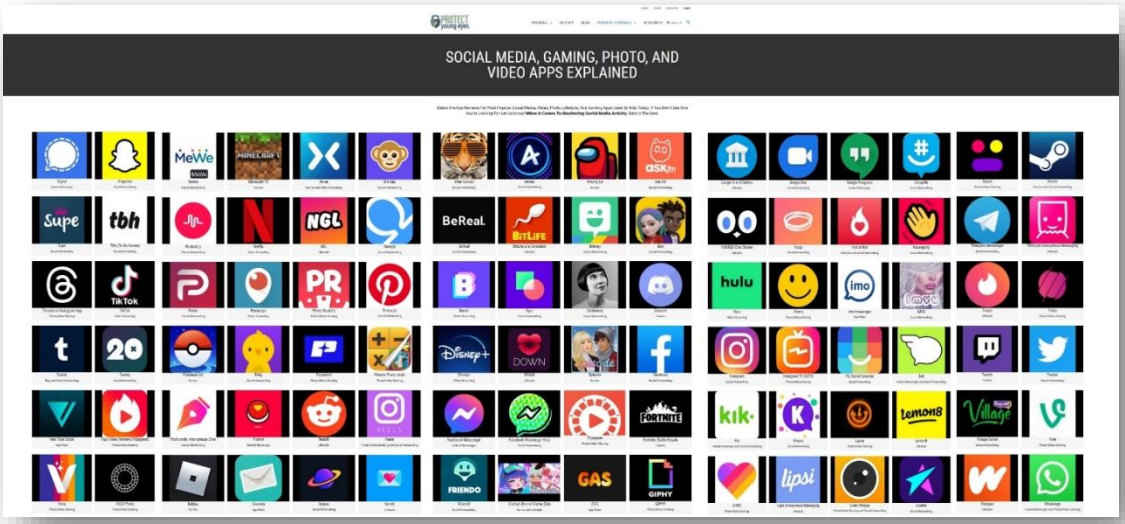
7. ábra: Protect Young Eyes weboldal

20 https://protectyoungeyes.com/

Az oldal egyik nagyon fontos funkciója, hogy a Parental Controls/Apps menüpont alatt elérhető rengeteg közösségi média, játék, fotó- és videó alkalmazás, amit a gyermekek és a fiatalok használnak napjainkban.

Az alkalmazások logójaira kattintva minden alkalmazásról megtudhatjuk az alábbi információkat:

- mi az adott alkalmazás – biztonságos-e,
- kategória,
- az alkalmazás áruház korosztályi besorolása,
- az alkalmazással kapcsolatos posztok,
- hogyan állítsuk be az alkalmazásban a „szülői felügyelet” opciót,
- fontosabb tulajdonságok és beállítások a gyermek védelmében,
- szülőként mit szükséges tudnunk az alkalmazásról,
- speciális információk, például TikTok esetében információ a „Kihívásokról”,
- Összefoglalásként: biztonságos-e a gyermeknek az adott alkalmazást használni?



8. ábra: A Protect Young Eyes - Parental Controls/Apps

5 A védelem kialakítása

Az előző fejezet megmutatta, hogy az adatainkat láthatóan számos veszély fenyegeti. Ezek között vannak olyanok, amelyek bekövetkezési valószínűségét valamilyen védelmi intézkedéssel, kontrollal csökkenthetjük, és vannak olyanok, amelyek bekövetkezését nem láthatjuk előre és nem is tehetünk semmit a megtörténése ellen (földrengés, hurrikán, céltudatos betörő). Mindkét típusú fenyegetés következményeként az adatok, valamint az adattároló és a feldolgozó eszközök is megsérülhetnek, ellophatják őket, vagy megsemmisülhetnek. Cél az, hogy ahol lehet, a fenyegetés megvalósulását megakadályozzuk, bekövetkezési valószínűségét csökkentsük. Ahol nem lehet vagy nem sikerült megakadályozni, ott pedig első lépésként felismerjük azt. Nagyon fontos célkitűzés lehet az is, hogy minden pillanatban legyünk képesek arra, hogy a bármilyen okból bekövetkezett információtechnológiai sérülés kárkövetkezményét gyorsan meg tudjuk szüntetni, vagy le tudjuk csökkenteni az elviselhető szintre. Ez csak akkor fog a gyakorlatban a kellő mértékben működni, ha megvannak az ehhez szükséges információk – például visszaállítási tervek - így nem érheti ezeket semmilyen katasztrofális esemény sem. Ezért a védelmet nagyon gondosan kell kiépíteni.

A **biztonság mértéké**ben jelentős különbségek mutatkoznak abból a szempontból, hogy milyen kifinomult és mennyire automatizálható támadások ellen védett a rendszerünk.

Támadási szint / Támadó	Automata (program)	Ember	Védelmi szint
Kifinomult	-	+	magas
Programozott	+/-	+	közepes
Programokat lefuttató	+	+	alacsony

Kifinomult támadást kizárólag az ember képes végrehajtani, mivel ehhez a támadási cél minden összegyűjthető fizikai és logikai tulajdonságát intuitíven felhasználhatja a támadó. Az egyes támadási formákat programokba öntve számos bonyolultabb támadási forma is létrehozható, de ebben az esetben a program működésre bírásához a legtöbb esetben szakismeret is szükséges. Ezzel ellentétben a programokat lefuttató támadásoknál, ahol a támadónak csak az elindítógombot kell megnyomnia, egy egyszerűen kivitelezhető támadás realizálható. Nyilvánvalóan mindhárom formához eltérő támadói tudásszint tartozik és némiképp eltérően is lehetséges védekezni ellenük. A védelemnek is növelnie kell a tudását az egyre hatékonyabb védelmi módszerek kialakításához, amiben nagyon fontos eszközök az automatizált támadások java része ellen védelmet nyújtó automatikus megoldások (tűzfal, vírusirtó, WiFi-beállítások stb.). Az internet veszélyeinek egy részét úgy tudjuk kiszűrni, hogy nem engedjük meg a bejövetelét. Ebben segítenek az egyes tartalomellenőrző szoftverek,

weboldalak elérését kategóriák alapján engedélyező vagy tiltó szoftverek, szülői felügyeleti szoftverek stb. A tartalomellenőrző szoftverek célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása, hogy csak olyan tartalmú oldalak jelenhessenek meg a számítógépünkön, amit szeretnénk, amit nem tartunk például károsnak a gyermekeink számára és aminek a megjelenítéséhez explicit módon – a beállítások révén hozzá is járulunk. Ha korlátozni szeretnénk az interneten eltölthető időt, erre a szülői felügyeleti szoftverek alkalmasak.

Emlékezzünk a 2.1 fejezetben megadott definícióra: *a biztonság egy olyan kedvező állapot, amelynek megváltozását nem várjuk, de nem is tudjuk kizárni*. Annak elismerésével, hogy nincsen tökéletes (100%-os) biztonság, tudatában kell lennünk a 20%-os és a 80%-os biztonság közötti különbségnek, ami leggyakrabban a biztonsági incidensek számában mérhető. Másképpen fogalmazva, magasabb szintű a biztonság, ha kevesebb a biztonsági incidens, kevesebbszer kerülünk bajba. A globális fenyegetettség állapotában nem bízhatunk abban, hogy védelem nélkül az informatikai rendszereink sokáig incidens nélkül maradnak. A biztonság tehát nem a „szükséges rossz”, hanem a folyamatok működőképességét biztosító eszköz.

Hogyan kell nekifogni a **biztonság megteremtéséhez**? Működőképes biztonságot teremteni az egyenszilárdság elvét figyelembe véve lehetséges, ami azt mondja ki, hogy úgy kell a védelmet kiépíteni, hogy minden eleme azonos erősségű legyen. Védelmi tekintetben ugyanis minden védelem olyan erős, amilyen erős a leggyengébb pontja. A támadó meg fogja keresni a védelem hiányosságait és a lehető legkevesebb ráfordítással a lehető legnagyobb eredményt akarja elérni, ez pedig a legtöbb esetben a leggyengébben védett elem támadásával lehetséges. A történelem folyamán kialakult az úgynevezett „mélységi védelem”. Ezt alkalmazták már a várak és erődítmények építésénél is (kívülről befelé haladva – vizesárok, dárdákkal, külső vár várfala katonákkal és bástyákkal, beljebb a belső várfal, legbelül a fellegvár.) Ezt a védelmi elvet az informatikai rendszerek védelme során is alkalmazzák az intézmények (most leegyszerűsítve a lényeget) – többrétegű tűzfal architektúra és biztonsági zónák, behatolásjelző és megelőző rendszerek, forgalomszűrő rendszerek és legbelül – a védendő adatok. Ha ehhez hozzávesszük a biztonsági követelményeket, máris világos, hogy mit kell tennünk a biztonság érdekében: az általunk használt informatikai erőforrások (adatok/információk, technológiák, alkalmazások) biztonságáról – vagyis ezek bizalmasságáról, sértetlenségéről és rendelkezésre állásáról – kell a megfelelő mértékben gondoskodni.

Szervezeti keretek között a védelem szabályait Informatikai vagy Információbiztonsági Szabályzatban (IBSZ) szokták rögzíteni, amely követendő magatartásmintákat, előírásokat tartalmaz minden számítógép-felhasználó számára. Az IBSZ helye középen van a biztonsági előírások hierarchiájában, mivel felette a stratégiai szintű Információbiztonsági Politika,

alatta pedig az operatív szintű eljárásrendek találhatók. A szabályzatok közé soroljuk még a katasztrófahelyzetben végrehajtható intézkedéseket tartalmazó Informatikai Katasztrófa-Elhárítási Terveket is. Ezek otthoni vetülete annak végiggondolása, hogy mit tehetünk az otthon tárolt adataink védelme érdekében a mindennapokban és extrém helyzetekben (pl. árvíz, lakástűz, fizikai vagy internetes betörés, adatvesztés megelőzése) is.

5.1 Felhasználók felelőssége az incidensek, biztonsági események során

A felhasználóknak kulcsszerepe van az információbiztonság fenntartásában, hiszen ők azok, akik nap, mint nap, ténylegesen hozzáférnek az adatokhoz, informatikai rendszerekhez. Ők azok, akik az adatokat előállítják, továbbítják, különböző informatikai eszközökön letárolják vagy adathordozókon hordozzák, majd az adatot megsemmisítik, ha ez szükséges. Fentiekből következően felhasználónak minősül mindenki, legyen vezető, üzemeltető, szakértő vagy külsős, aki hozzáfér a szervezet adataihoz. Otthoni környezetben ugyanez elmondható, hogy minden családtag, barát, rokon vagy ismerős, aki hozzáfér az otthoni informatikai rendszerekhez, az felhasználónak minősül.

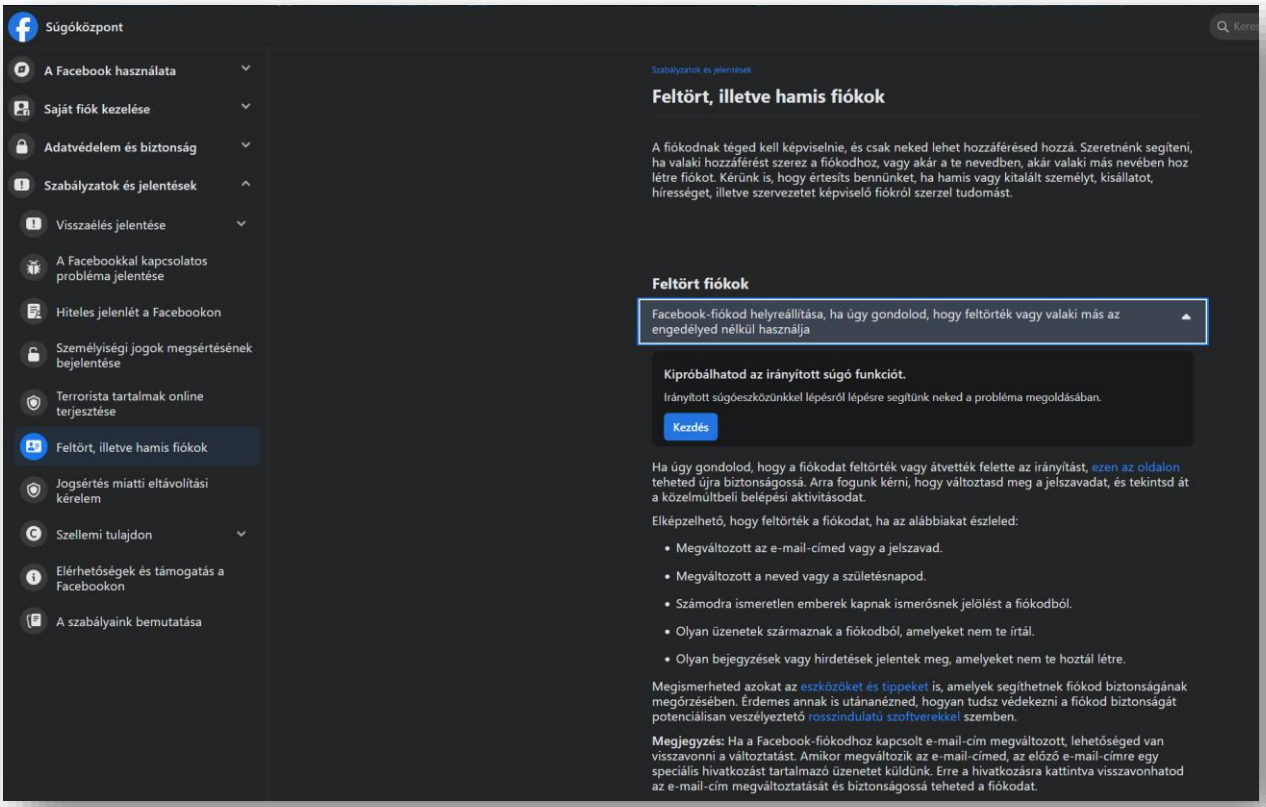
A legfontosabb, hogy a felhasználók tisztában legyenek a fenyegetettségekkel, a szabályokkal, valamint azon folyamattal, hogy mit kell tenniük, hogy megelőzzék az információbiztonsági (és egyéb biztonsági) incidenseket, vagy ha megelőzni nem is sikerült, időben felismerjék azokat és tudják, hogy milyen csatornán lehet jelenteni azt az illetések felé.

A végfelhasználók hatalmas értéket képviselnek az incidenskezelést végző csoport vagy szervezet számára az incidenskezelés folyamatában. Ugyanakkor hatalmas felelősséggel is bírnak. Kritikus szerepük van az incidenskezelési folyamatban azáltal, hogy ők, a végfelhasználók az elsők, akik általában valamilyen incidens jelével először találkoznak. Gondolhatunk itt egy alkalmazás nem megszokott működésére, egy gyanús csatolmány beérkezésére az e-mail postafiókba, egy gyanús telefonhívásra, egy elhagyott pendrive-ra, ami az irodában a folyosón hever, vagy egy gyanúsan sétálgató ismeretlenre az irodában. Létfontosságú a szervezet számára a felhasználók azon képessége, hogy időben felismerjék a fenyegetettségeket és a megfelelő kockázati attitűddel felmérjék a valós veszélyt és időben jelezzék azt az incidensmenedzsmenttel foglalkozó szervezet számára.

Mit tegyünk, ha feltörték vagy adathalászat útján ellopták a felhasználói fiókomat? Egyre gyakoribb, hogy átlagos felhasználók esnek áldozatul közösségimédia-platformokon adathalászatnak. Ezek a támadások azért különösen veszélyesek, mert az ismerősi, bizalmi hálón keresztül érkeznek sok esetben, kihasználva azt, hogy az ismerősöktől érkező üzenetek esetében kevésbé gyanakszunk.

Amennyiben ellopták tőlünk a közösségimédia-fiókunk bejelentkezési adatait, a támadó már belépett a fiókunkba és ott megváltoztatott kapcsolattartási és bejelentkezési adatokat, akkor az első és legfontosabb szabály, hogy maradjunk nyugodtak. Fontos, hogy ne regisztráljunk azonnal egy másik fiókot a korábbi kapcsolati és bejelentkezési adatainkkal, mert ezek jelentősen megnehezítik a fiók visszaszerzését, mivel az algoritmusok az újonnan létrehozott fiókunkat fogják megtalálni az ellopott helyett.

Minden platformon (Facebook, Instagram, TikTok stb.) történnek ilyen támadások, ezért az üzemeltetők már jól bejáratott kész folyamatokkal segítik az áldozatokat. Példaként a legnépszerűbb közösségimédia-platform, a Facebook vonatkozó oldalát mutatjuk meg:



9. ábra: Feltört Facebook fiók visszaállítása

Nagyon fontos, hogy minél több platformon használjuk a két- vagy többfaktoros hitelesítést. Ez meg tud védeni az adathalászat során ellopott hitelesítési adatokkal való visszaélések ellen!

5.2 A bizalmasság

Az üzleti életben értelemszerűen nagyon jelentős az üzleti titok védelme. Ennek az az oka, hogy a vállalatok nagyon odafigyelnek az ügyfeleikre és az ügyfeleik adataira, és meg akarják előzni az ügyfelek adataival való visszaélést, valamint az ügyfeleik adatainak ellopását, hiszen ennek bekövetkezése súlyos bevétel-kiesést és büntetést is okozhat számukra, ahogyan ezt több példa is bizonyította a közelmúltban. 2016. április 27-én lett elfogadva és 2018. május 25-től kötelezően alkalmazandó az Európai Unió Általános Adatvédelmi Rendelete (GDPR – General Data Protection Regulation), amely vonatkozik minden olyan cégre és szervezetre, amely az Európai Unió állampolgárainak személyes adatait kezeli. A korábbi szabályokhoz képest némileg szigorodtak az elvárások. Ami jelentősen változott, az a büntetési tétel, ha az adatokért felelős szervezet nem tartja be a szabályokat, vagy ha emiatt az adatokat érintő incidens következik be.

A 2019-es évben három rekord is született személyes adatok gondatlan kezelése miatt. Az egyik a Marriott szálloda láncot sújtotta 339 millió vendég személyes adatainak ellopása miatt – itt kifejezetten a GDPR előírásai miatt kell a hotel láncnak 100 millió GBP-t (kb. 35 milliárd forint) fizetnie. A másik gigabüntetés a Facebook-ot érintette, ott nem a GDPR-ra hivatkozva, hanem az Egyesült Államok saját rendelkezései miatt - egy milliós nagyságrendű személyes adatokat érintő korábbi incidens kapcsán (Cambridge Analytica botrány) kell 5 milliárd USD-t (kb. 1.650 milliárd forint – 1.650.000.000.000 forint) fizetnie.

Hogy 2019 a legek miatt bevonul a személyes adatok biztonságáról szóló történelemkönyvekbe az azért is valószínű, mert 2019 júliusában történt meg először (legalábbis ekkor került napvilágra), hogy egy egész nemzet – Bulgária – összes adófizetőjének személyes adatait ellopták – a Bolgár Állami Adóhivataltól[21]. Arra, hogy egy teljes nemzet szinte minden állampolgárának ellopják egyszerre az adatait, még nem volt példa.

2023-ban a Meta vette át a legnagyobb GDPR bírságra ítélt szervezet vezető szerepét[22], ugyanis 2023. májusában az Ír Adatvédelmi Bizottság (DPC) 1,2 milliárd eurós, „történelmi léptékű" bírságot szabott ki a Meta amerikai technológiai óriásra. Ezt a rekordot döntő bírságot azért szabták ki, mert az európai felhasználók személyes adatait megfelelő adatvédelmi mechanizmusok nélkül továbbították az Egyesült Államokba. A Meta ugyan várhatóan fellebbez majd, de ez a pénzbírság egyértelmű figyelmeztetés a vállalatok számára, hogy a

[21] https://www.bbc.com/news/technology-49015511
[22] https://dataprivacymanager.net/meta-hit-with-record-e1-2b-gdpr-fine/

GDPR követelményeit komolyan kell venni, és a be nem tartás súlyos pénzügyi következményekkel is járhat.

Az adatokhoz való jogosulatlan hozzáférést alapesetben az akadályozza meg, ha valamilyen azonosítási és hitelesítési módszert használunk (például azonosító+jelszó). A jogosulatlan adat-hozzáférés ellen ezen túlmenően a titkosítás is védelmet nyújt. A kettő között az a különbség, hogy az azonosítás+hitelesítés jellegű hozzáférésvédelemnél a támadónak a védelem esetleges megkerülésével mégis sikerülhet hozzáfernie a védendő adatokhoz. Például megszerezve a jelszó kivonatokat /hash/, közvetlenül ezekkel fordul a hitelesítést végző rendszer felé, így nincs is szüksége az eredeti jelszavakra – ez az úgynevezett „pass the hash" támadás, Míg titkosítás alkalmazásával hiába fér hozzá a titkosított adatokhoz, azokat akkor sem tudja elolvasni a titkosító kulcs ismerete nélkül, vagy a feltörés megvalósítása nélkül. A titkosított adatok előnye az, hogy kulcs nélkül nem lehet az adatokat elolvasni. A titkosításnak azonban korlátja is van. Mivel kulcsot kell használnunk a titkosításhoz és a feloldáshoz is, ezért a titkosító kulcs elvesztésével nem tudunk többé titkosítani, a feloldáshoz szükséges kulcs elvesztésével pedig az adat használhatatlanná válik.

Azt az információbiztonsági tulajdonságot, amelyik biztosítja a tárolt adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét, bizalmasságnak hívjuk. A jogosulatlan hozzáférés következményei lehetnek a sértetlenség (benne a hitelesség) és a rendelkezésre állás sérülése is, amennyiben a támadó átírja az egyes adatokat vagy törli azokat. Az adatok jogosulatlan módosítása elleni védelmet tehát a bizalmasság információbiztonsági jellemző biztosítja, a sértetlenség csupán detektálni képes ennek megváltozását, de nem tudja megakadályozni azt.

Bizalmasságról akkor beszélhetünk, ha az adataink egy részének megismerhetőségét korlátozzuk, és minden időpillanatban tudjuk, hogy ki van feljogosítva az egyes adatokhoz történő hozzáférésre. A bizalmasság megteremtését lehetséges saját és felhő környezetben is értelmezni. Amennyiben a saját gépeinken és egyre több esetben a felhő szolgáltatásokban tárolt adatokról van szó, lehetőségünk van hozzáférés-védelmet kialakítani (többször használható jelszó, erősebb esetekben valamilyen egyszer használatos jelszó (SMS kód, percenként változó token kód vagy tanúsítvány). Ez annyira védi az adatainkat, amennyire a védelmet nem lehet megkerülni. Vagyis ez a védelem nem sokat ér akkor, ha a támadó meg tudja kerülni a hozzáférés-védelmünket (például rendszerszinten tevékenykedő kártékony kód használatával szerez hozzáférést minden helyi adatunkhoz anélkül, hogy bármilyen jelszó ismeretére szüksége lenne).

Ettől erősebb védelmet biztosítanak a különböző titkosító programok, melyeket használhatunk lemezpartíciók, USB-lemezek, adatbázisok, fájlok, tömörített állományok és kimenő üzenetek titkosítására is. Ekkor a megfelelő kulcs nélkül nem lehetséges elolvasni a titkosított adatokat még akkor sem, ha a támadó megszerezné a titkosított fájlokat. Ez a védelem persze nagymértékben függ az alkalmazott kriptográfiai algoritmustól és a kulcs hosszúságától. Önmagában nem elegendő a titkosítás megléte, az is szükséges, hogy megfelelően legyen az adat titkosítva. Ehhez nélkülözhetetlen, hogy ismerjük az egyes algoritmusok tulajdonságait olyan szinten, hogy meg tudjuk állapítani az alkalmazott paraméterek megfelelőségét. Felhasználói szinten már egy alapszintű titkosítás is megfelelő védelmet nyújthat, mivel a védett adatok értéke várhatóan nem áll arányban azzal az erőforrás szükséglettel, ami az adatok ellopásához és feltöréséhez szükségesek. Konkrétan egy hacker nem fogja célzottan az idejét pazarolni arra, hogy az otthoni titkosítással védett családi költségvetést tartalmazó excel táblát vagy fotóalbumot feltörje. Vagy ha el is lopja egy tolvaj a hordozható adattárolónkat (pendrive, mobil merevlemez), sok esetben nem lesz elegendő tudása és motivációja ahhoz, hogy a rajta lévő titkosított word fájlokat feltörje – amelyek például a szakdolgozatunk anyagait tartalmazzák. Az adataink bizalmassága így megmaradhat az adathordozó eltulajdonítását követően is.

5.2.1 Bizalmasság az operációs rendszerben

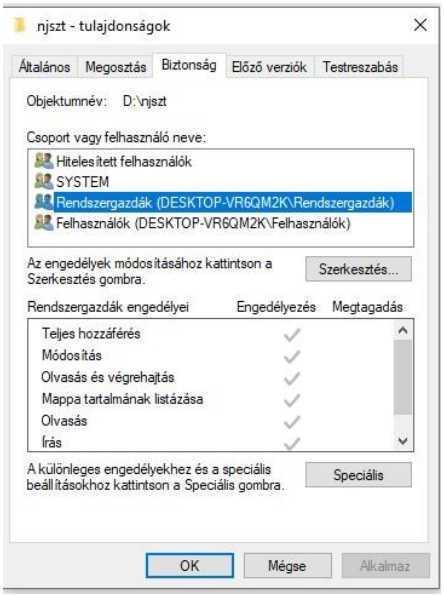
Az operációs rendszerek biztonsága, felhasználói szemszögből nézve, tipikusan fájlok biztonságát jelenti. A fájlok biztonságáról több aspektusból lehet beszélni, a hozzájuk kapcsolódó műveletek révén. Ezek az olvasás, írás, törlés, módosítás. Fontos kérdés, hogy ki rendelkezik ezekkel a **fájl-jogosultságok**kal?

Az olvasást megakadályozza a titkosító program általi **fájl-titkosítás** – amikor esetleg ugyan megnyithatjuk a fájlt, de értelmezni nem tudjuk - vagy a szövegszerkesztőben való megnyitás jelszóhoz való kötése is, amikor a jelszó ismerete nélkül itt sem tudjuk megnyitni (**feloldani a titkosítást**) a fájlt. Jelszavas védelmet beállíthatunk irodai programcsomagok által készített dokumentumokhoz (szöveg, táblázat, prezentáció stb.) vagy tömörített fájlokhoz egyaránt (zip, rar stb. [i]). A biztonságkritikus fájlokhoz (pl. digitális aláíráshoz használható kulcs) a rendszer nem is engedi meg a jelszó nélküli hozzáférést alapértelmezésben.

A fájlt akkor tudjuk kiírni egy háttértárolóra, ha ahhoz van jogosultságunk, egyébként a létrehozni kívánt fájl a memóriából nem megy tovább és onnan a program bezárásakor (ha jól van a program memória kezelése megírva) törlődik. Egy fájlba beleírni (módosítani) akkor lehetséges, ha az a fájl módosításra – írásra – hozzá van rendelve a felhasználóhoz,

egyébként nem fogja tudni a felhasználó a módosításokat elmenteni. Fontos megismételni itt azt is, hogy van-e olyan eleme egy fájlnak, amit a rosszindulatú támadás során fel lehet arra használni, hogy a tulajdonos tudta nélkül írjanak bele a fájlba vagy a rendszerbe – ilyenek lehetnek például a makrók [j].

Otthoni számítógép használat esetén javasolt minden családtagnak saját felhasználói fiókot létrehozni általános jogosultsági szinttel. Az adminisztrátori fiókot pedig csak akkor használni, ha feltétlenül szükséges. Ezzel lehetővé válik, hogy az operációs rendszerünkben korlátozzuk az egymás adataihoz való hozzáférést, és egy esetleges támadás során a támadó nem rögtön a teljes rendszeradminisztrátori jogosultsággal kezdhet el tevékenykedni a gépünkön.



10. ábra: Hozzáférések megadása Windows operációs rendszerben

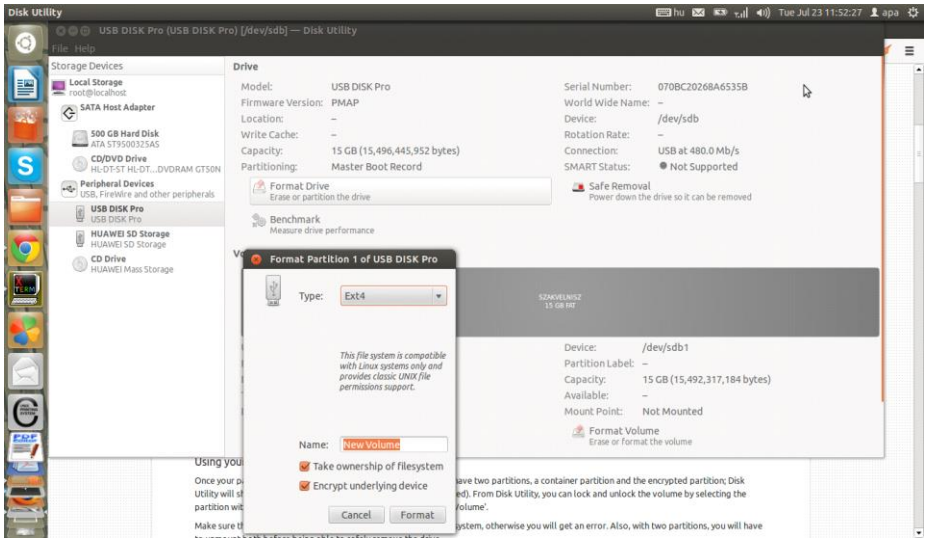
5.2.2 Merevlemezek és USB-lemezek titkosítása

Az adataink mindazok számára alapértelmezett esetben hozzáférhetők, akik a tárolására szolgáló lemezek (belső, külső, felhő, USB) birtokában vannak. Leggyakrabban a jogos tulajdonosa van birtokon belül, de a támadók sokszor sikeresen tudják ezeket a tárolókat – illetve a rajtuk tárolt adatokat távolról – eltulajdonítani. Voltak, vannak és lesznek hordozható számítógép-lopások és távolról betörni kívánó tolvajok is. Emiatt is szükséges, hogy védjük adatainkat.

Az adatok bizalmasságának legáltalánosabb védelmére a titkosítást használják. Lehetséges titkosítani mind a számítógépek merevlemezét, mind pedig egy külsőleg csatlakoztatható

USB-eszközt is, illetve egyedileg fájlokat vagy könyvtárakat. Egy lényeges különbség létezik rendszerindításra alkalmas és nem alkalmas lemezek titkosítása között, mégpedig az, hogy a rendszerindításra alkalmas lemeznek kell, hogy legyen egy nem titkosított része is, ahonnan a rendszer addig betölthető, amivel már a titkosított partíciót el tudjuk érni. Rendszerindításra nem felkészített lemez teljes mértékben titkosítható.

A titkosítás előnye az, hogy nem kell annyira aggódnunk innentől kezdve az adatok miatt, ha esetleg az eszközt el is lopnák, amennyiben a jelszót megfelelően erősre választottuk, az alkalmazott megfelelően erős kriptográfiai titkosítás visszafejtése jellemzően meghaladja a támadók erőforrás-lehetőségeit. Természetesen itt is vigyáznunk kell a jelszó rendelkezésre állásának megmaradására, mert enélkül a titkosított adatok előlünk is el lesznek rejtve mindörökre.

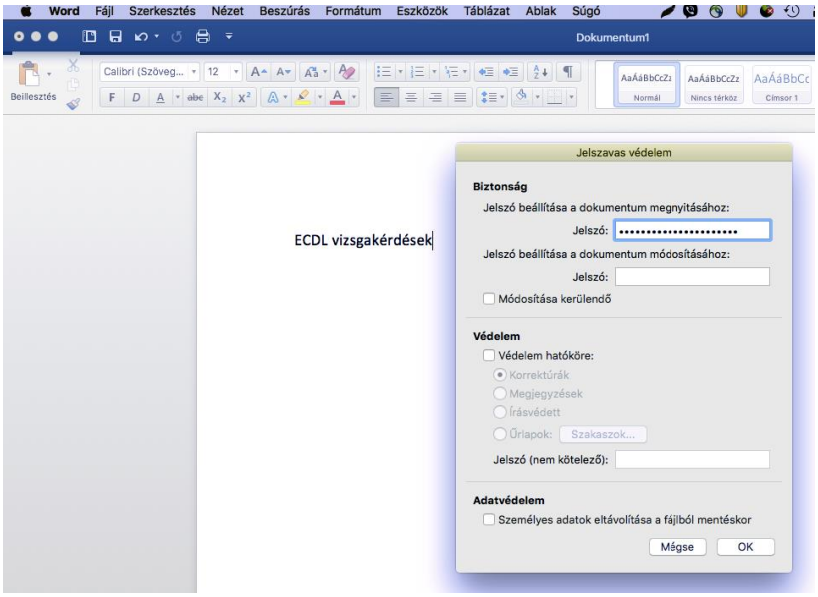


11. ábra: USB-lemez titkosítása Linuxon

5.2.3 Titkosítás irodai programcsomagokban

A szövegszerkesztők, táblázatkezelők, irodai programcsomagokban használható programok beépített funkciókat tartalmaznak a szöveg jelszavas védelmének megteremtéséhez, más szóval a **dokumentumtitkosítás**hoz. Amennyiben használjuk ezt a funkciót, a szövegszerkesztő bekér tőlünk egy – megfelelően biztonságos – jelszót, aminek segítségével a teljes dokumentumot titkosítja, így azt a jelszót nem ismerő számára teljesen olvashatatlanná teszi. Vigyázat, amennyiben a jelszót elfelejtjük, nem biztos, hogy létezik olyan módszer, ami vissza tudja állítani az eredeti tartalmat! A nem megfelelő titkosítás tehát az adataink

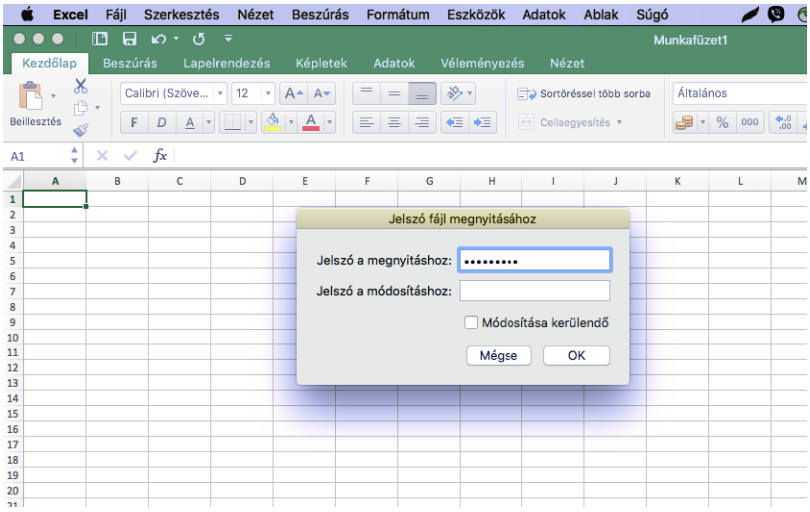
számunkra való hozzáférhetetlenségét is eredményezheti, amivel túllőhetünk az eredeti titkosítási célkitűzésen.



12. ábra: Megnyitási jelszó beállítása Mac Microsoft Word 2019 szövegszerkesztőben

Mac Microsoft Word 2019 programban az Eszközök / Dokumentumvédelem menüpontra történő kattintással jelenik meg a jelszót bekérő ablak.

Fontos megismételni, hogy a titkosítási algoritmus lehet nagyon erős, de ez nem védi meg a dokumentumokat az illetéktelen olvasástól akkor, ha a jelszó rövid, vagy könnyen kitalálható.



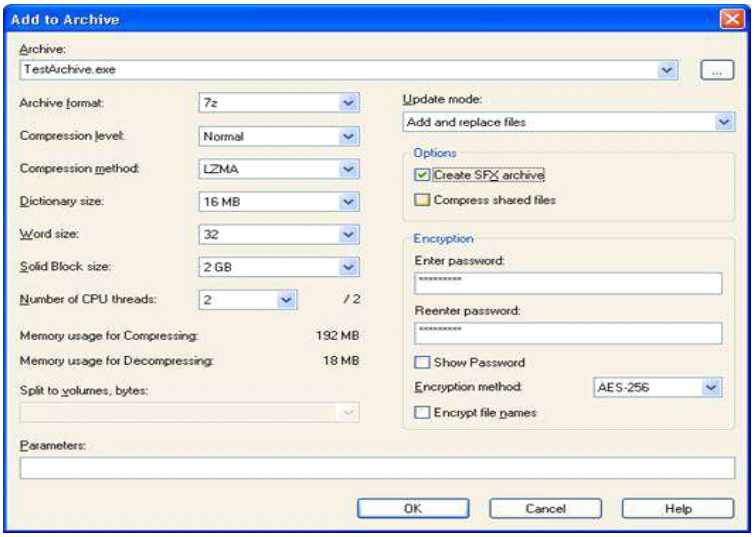
13. ábra: Megnyitási jelszó beállítása Mac Microsoft Excel 2016 szövegszerkesztőben

A képen látható Mac Microsoft Excel 2019 verzióban a File menü / Jelszavak menüpontra történő kattintással jelenik meg a jelszót bekérő ablak.

Nem lehet elégszer elismételni, hogy a biztonság kulcsa ezekben az esetekben is a jelszó megfelelő megválasztása, hiszen egy gyenge jelszóval a védelem pillanatok alatt feltörhető.

5.2.4 Bizalmasság tömörített állományoknál

A tömörítőprogramok legtöbbje fel van arra készítve, hogy a tömörített állományokat olyan titkosítással védjék, mely a felhasználó által megadott jelszó/jelmondat alapján végzi el a fájl kriptográfiai titkosítását. A titkosítást az archívum létrehozásakor kell kiválasztani és a jelszót beállítani a **fájltömörítés**hez, az alábbi kép jobboldalán találhatunk ehhez segítséget.



14. ábra: Jelszó beállítása archív állomány létrehozásakor

A megfelelő jelszó kiválasztása itt sem árt, mivel egy jelszótörő programmal rendelkező támadónak egy 10-számjegyből álló, vagy egy egyszerű (pl. csak az angol ábécé kisbetűiből álló) jelszó megfejtéséhez kb. 30 másodpercre van szüksége, egy közepesen erős számítógépen.

5.3 Hálózat és bizalmasság

A nyílt internetes kommunikáció során nemcsak a jogosultak láthatnak bele az adatokba. Adatok alatt egyrészről a hálózaton továbbított adatfolyamot, másrészről a hálózaton elérhető eszközökön tárolt adatokat – összefoglaló néven a **hálózati adat**okat értjük. A támadók a hozzáférés-védelmi rendszerek és a protokollok gyengeségeit, a ki nem javított

programhibákat, valamint a felhasználók jóhiszeműségét kihasználva számtalan esetben képesek megszerezni jogosulatlanul az adatainkat és többször sikeresen vissza is élnek vele. Ma már sajnos számos támadás ismert, ami a kommunikációs hiányosságokra, és a felhasználók megtévesztésére alapozza sikerét. Fontos az adathalászat fogalmával megismerkedni, és tudni, hogy a támadók sokszor felhasználják létező cégek, személyek neveit is a bizalom felkeltése érdekében. Ennek során alkalmanként és ideiglenesen hamis weboldalakat is felhasználhatnak, amelyek a megtévesztésig hasonlítanak az eredetihez. A hamis weboldalak segítségével a támadók kicsalhatják az eredeti honlapon megadni kívánt azonosítási és egyéb adatokat (ügyfélszám, felhasználói név, jelszó, egyéb személyes adatok, akár bankkártya adatok is). A hazai bankok mindegyike biztonsági tanácsokat és ajánlásokat fogalmaz meg a felhasználók számára, a biztonság érdekében. A szabályok kikényszerítését otthoni felhasználók esetében egyrészt tűzfal programok (personal firewall) végzik, másrészt választhat a felhasználó olyan komplex internet védelmi csomagot is, amely tartalmaz beépített tűzfalat, behatolás detektálót, spam és vírusszűrőt, szülői felügyelet programot, illetve akár az internetbankolás során védő böngésző modulokat is. Akár külön-külön, akár csomagban veszi meg a felhasználó, a lényeg, hogy otthoni környezetben is legyenek védettek az eszközök. Ugyanez vonatkozik természetesen az okostelefonokra is, mint funkcionalitásban ma már a személyi számítógépekkel vetekedő eszközök.

A hálózatokon belül megkülönböztetünk védett és nem védett hálózatokat. A védett hálózatok tulajdonsága, hogy valamilyen korlátozást alkalmaz a hozzáféréshez, és csak az arra feljogosítottaknak engedi meg a hálózati kommunikáció során a rendszerekhez való hozzáférést és az adatok olvasását és küldését.

A csatlakoztatható védett vezetékes hálózatot az első, a védett vezeték nélküli hálózatot pedig a második ikon jelöli.

15. ábra: Védett hálózati csatlakozások megjelenítése

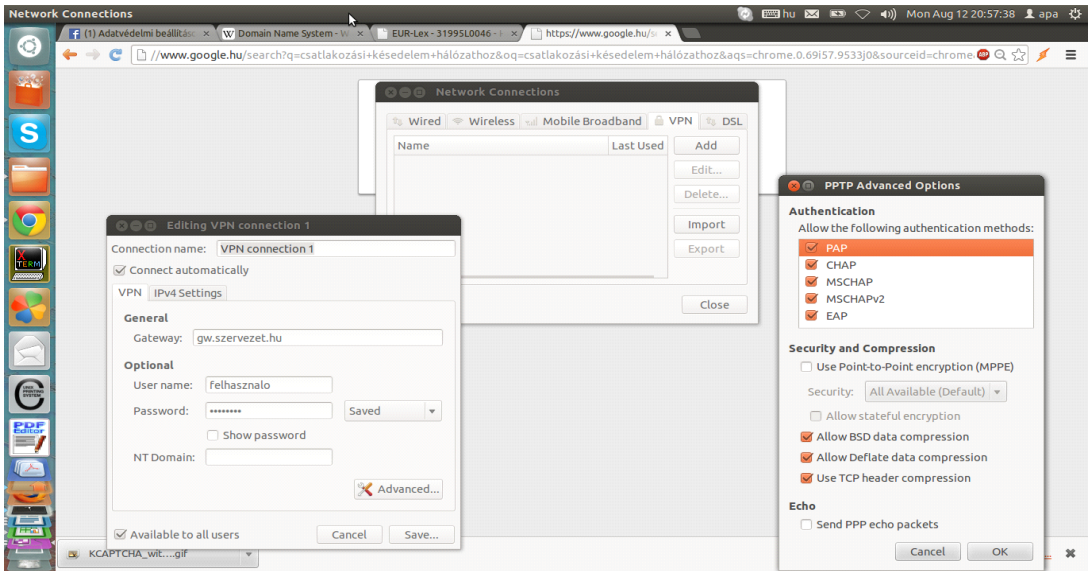
A hálózatra való csatlakozásnak a leggyakoribb biztonsági kihatása egyszerűen szólva az, hogy megfertőződhet a számítógép és okostelefon, de akár okoseszköz is rosszindulatú szoftverekkel. A hálózatra történő csatlakozás biztonsági vonatkozása ennél fogva a személyes és privát adatok védelme köré csoportosul, hiszen a netre kötött gépeken tárolt adatokhoz a külső támadó egy sikeres támadás során távolról hozzáférhet, akár korlátozás nélkül is, illetőleg tetszés szerint használhatja a számítógépet és annak erőforrásait.

Gyakran felhasználják bejegyzett cégek neveit a személyes biztonsági adatok megszerzéséhez az eltérítéses adathalászat során. A támadó módosítja áldozata számítógépén például az internetes bankjának a címét, így az áldozat azt hiszi, hogy annak adta meg az adatait, akit lát, mert nem gondol támadásra.

5.3.1 Hozzáférés-védelem, jelszavak, hitelesítés

A támadások legtöbbjét hálózaton keresztül követik el abból az egyszerű okból kifolyólag, hogy egy internetre kötött számítógépet, okoseszközt és okostelefont az egész internet közössége láthatja, míg egy számítógép esetén, a számítógépet tartalmazó helyiségbe, otthoni gépek esetén a lakásunkba fizikailag belépők száma igen erősen korlátozott. Míg korábban a hálózatok logikai védelme (tűzfal, tartalomszűrő, adatszivárgás-elleni védelem) sokkal nagyobb jelentőségű volt, mint a fizikai védelem, manapság a hordozható eszközök korában az eszközök fizikai védelmére is komoly figyelmet kell fordítani. Egy telefont könnyű elveszíteni, könnyen kikaphatják az ember kezéből egy forgalmas helyen. A hordozható eszközök, laptopok túlnyomó többségét autókból lopják ki. Ezért a legrövidebb ideig sem szabad autóban őrizetlenül hordozható eszközt hagyni, még zárt helyen, például csomagtartóban sem. A városok forgalmas helyein (áruházak, plázák, parkok, iskolák) kifigyelik a tolvajok, hogy ki pakol laptopnak tűnő táskát a csomagtartóba, és vagy ott helyben, vagy a következő parkolásnál ellopják azt. Mire a tulajdonos visszatér, az eszköznek hűlt helye lesz. Sokszor a tulajdonos még azt sem tudja, hogy honnan lophatták el az eszközt. Ilyen esetekre jótanács az, hogy legyen titkosított a háttértár, az eszköz legyen védve jelszóval, a telefonon is legyen képernyőzár, a SIM kártyán pedig PIN kód. Nem utolsósorban ne tároljunk nem mentett adatokat a hordozható eszközeinken, hiszen telefont tudunk venni másikat, de például a gyermekünk első lépéseit megörökítő videót soha többé nem vehetjük fel újra.

A VPN (Virtual Private Network – Virtuális Magánhálózat, melyekről a 3.3 Számítógép-hálózatok fejezetben szóltunk korábban) kialakításához is kell egy olyan szoftver, amely a két végpontot titkosított csatornán összeköti és ahol azonosítás és hitelesítés történik, meggyőződve arról, hogy valóban a jogosult személy jelentkezik be. Ezt mutatja a következő ábra.



16. ábra: Bejelentkezés VPN hálózatba

Általában minden hálózatnál van valaki, aki kiosztja és visszavonja a fájl- és eszköz-hozzáféréseket – ha egynél több személynek kell hozzáférést adni a saját zárt hálózatunkhoz, ezáltal megvalósítottunk egy **hálózati adminisztrátor**i szerepkört, aki a hálózaton belüli hitelesítés, feljogosítás és számonkérés kezelésére van feljogosítva, és feladata fenntartani a szükséges adathozzáférést a hálózaton. Otthoni környezetben ez jellemzően az otthoni vezeték nélküli hálózatunkhoz való hozzáférést jelenti. Célszerű első lépésként megváltoztatni az alapértelmezett adminisztrátori (admin) jelszót, majd beállítani hozzáférési jelszót (WiFi jelszót), mivel a rádiójelek nem állnak meg a falnál és nem feltétlenül jó, ha a szomszéd a mi vezeték nélküli hálózatunkon keresztül internetezik.

A hálózat biztonságát számos veszély fenyegeti. Tudatában kell lenni annak, hogy a nem védett vezeték nélküli hálózat használata lehetővé teszi az adataink megismerését a forgalmat lehallgatók számára, vagy az adatok szivárogtatásánál ezt a jogosultak követik el, akár a tudtuk nélkül is. A jelszavas védelem kialakításánál nagyon fontos, hogy a jelszó megfelelően biztonságos legyen. A jó jelszókezelés szabályait ajánlott betartani, mint a jelszavak másokkal való nem megosztása, időszakos megváltoztatása, megfelelő jelszó-hossz, megfelelő jelszó-karakterek – betűk, számok és speciális karakterek – együttes használata, valamint, hogy a jelszavakat ne írjuk fel füzetbe, excel fájlokba, cetlikre és ne használjuk ugyanazt a jelszót több helyen.

A jelszavak használatakor három típusú jelszót különbözetünk meg:

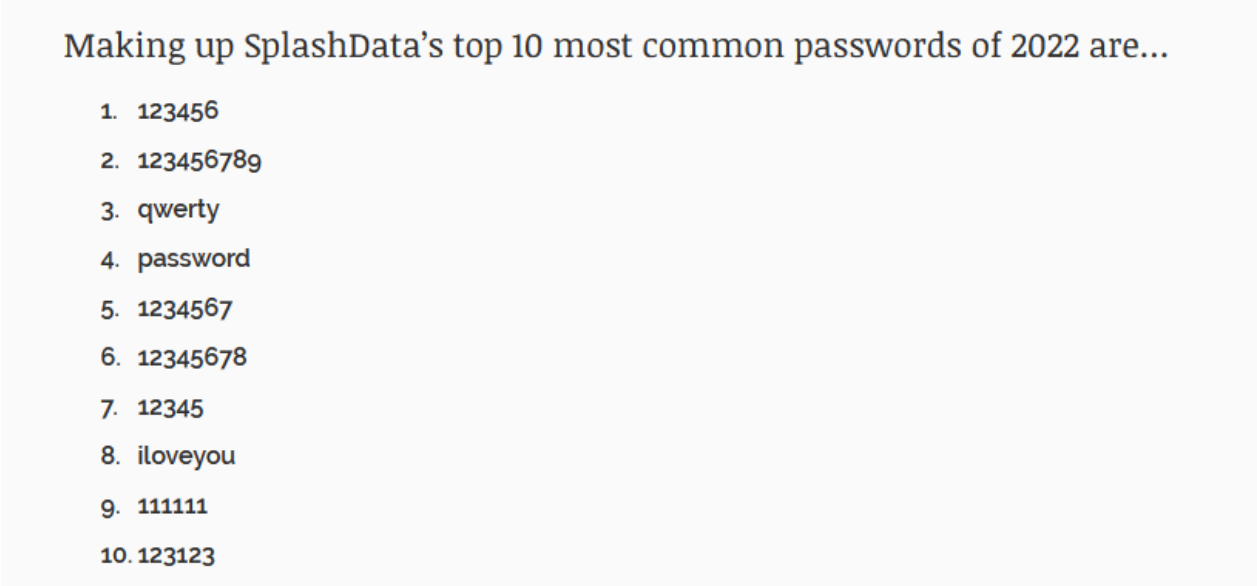
- többször használatos jelszó: egyszer megaduk adott rendszerben, majd a következő jelszóváltoztatásig ezt a jelszót használjuk,
- egyszer használatos jelszó (OTP – One Time Password): ezt a jelszót vagy a felhasználó saját maga generálja és a generálás után csupán egyetlen egyszer használhatja fel – jellemzően egy token, hardveres eszköz szükséges hozzá, vagy azon rendszer állítja elő, ahová belépni szándékozunk és valamilyen csatornán eljuttatja hozzánk – ennek legékesebb példája a bankok internetbankolás során alkalmazott belépési SMS jelszava, illetve tranzakció hitelesítő SMS jelszava,
- biometriai jelszó: az ember valamely fiziológiai jellemzője (pl. ujjlenyomat, hang, retina, tenyérlenyomat stb.).

A rossz jelszavak nem nyújtanak biztonságot, hiszen a potenciális támadót nem tudják megállítani, legfeljebb egy-két pillanattal tudják késleltetni a támadás bekövetkezését, mert a rossz jelszavak feltörését vagy kitalálását másodpercek alatt el lehet végezni. A jelszóhasználati rossz szokások bemutatására számos elemzés készült itthon és a nagyvilágban is.

Mit is jelent a megfelelően erős, megfelelően biztonságos jelszó? A jelszóerőssége három dologtól függ alapvetően. A jelszó kódolását végző algoritmustól (erre általában a felhasználónak nem sok ráhatása van), a jelszó hosszától (ez már függhet a felhasználótól, bár egyes helyeken meghatározzák, hogy milyen hosszú (például 8-15 karakterig terjedő) jelszót választhatunk és végül a jelszó bonyolultságától. Az általános ajánlás a jelszóválasztással kapcsolatban az, hogy ne legyen könnyen kitalálható, a felhasználóra utaló (pl. születési év, lakcím, házikedvenc neve stb.), illetve ne legyen a jelen dokumentumban is bemutatott legjellemzőbben használt jelszavak között (például 123456 – ez a jelszó továbbra is a legrosszabb jelszavak listájának éllovasa). De hogy milyen is legyen? Legyen legalább 8-15 karakter hosszú, tartalmazzon kis és nagybetűket, számokat és egyéb karaktereket. Ha nincs a hossz korlátozva, akkor érdemes több jelszót egymás mögé fűzni, illetve léteznek olyan jelszószéf alkalmazások is, amelyek képesek előre megadott feltételek mentén jelszavakat generálni számunkra – ezekről később még lesz szó. Még egy fontos dolog, hogy a jelszavainkat ne tároljuk nyílt szöveges állományként (pl. egy excel táblában, vagy papírra leírva a gépünk mellett.) Ha lehetséges ugyanazt a jelszót ne használjuk egynél több alkalmazásban.

2019 januárjában többmillió, magyar felhasználók által használt azonosító és jelszó is kikerült az internetre, ezekből egyelőre még nem készült nyilvánosan elérhető statisztika. Ezért most egy angol nyelvterületre vonatkozó „legrosszabb 25 jelszó” statisztikát mutatunk be a 2018-as évről. Ez az elemzés is a felhasználók által használt, többször használatos jelszavakra vonatkozik, de a korábbi események megmutatták, hogy a jelszóképzés terén nincs

olyan nagy különbség a világ számítástechnikai felhasználói között, ezért például a „jelszo” jelszó igen gyakori lehet Magyarországon is. Amennyiben a lenti táblázatban szerepel a jelszavunk, vagy nagyon hasonlít rá, akkor sürgősen változtassuk meg, figyelembe véve az előző bekezdésben szereplő tanácsokat.


Making up SplashData's top 10 most common passwords of 2022 are...

1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. iloveyou
9. 111111
10. 123123

17. ábra: 10 leggyakrabban használt jelszó 2022-ben (forrás: SplashData) angol nyelvterületen

Korábban a biometriai védelem viszonylag ritka volt otthoni felhasználásban, azonban a modern okostelefonok esetében elérhető már az ujjlenyomat és arcfelismerés technológiája is, valamint számos laptopgyártó integrálta az ujjlenyomat felismerést az eszközeibe. És természetesen a kritikus biztonságú helyszíneken alapértelmezett a használatuk. Ilyen védelmi technika az ujjlenyomat, kézgeometria, tenyérlenyomat beolvasása, hangazonosítás vagy retina-szkenner a hozzáférés-védelemben.

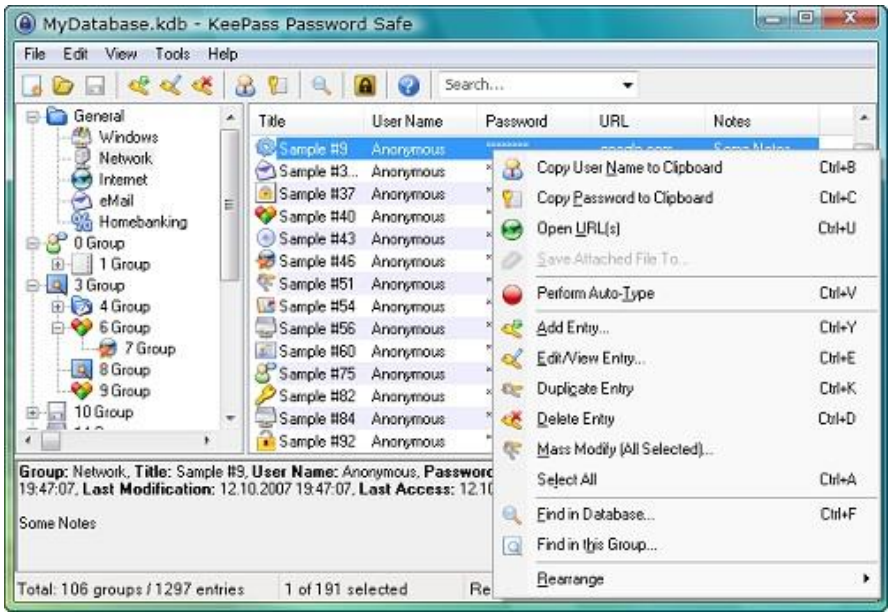
Az eszközök fizikai biztonságának növelésére használható módszer például hordozható számítógépek esetén a biztonsági kábelek (pl. Kensington lock) alkalmazása, hogy a támadó ne tudja egyszerűen ellopni az eszközöket, fizikailag legyen meggátolva benne.

A fizikai védelem témakörébe tartozik valamelyest a webkamerák védelme is. A számítógépekhez kapcsolt vagy beépített webkamerákat egy külső támadó a saját irányítása alá tudja vonni bizonyos támadásokkal – még akkor is, ha nem világít a webkamera működését jelző LED, így erősen javasoljuk a webkamerák „megvakítását” használaton kívül (pl. egy ragasztócsíkkal való leragasztását vagy egy papírdarabbal való lefedését, vagy a kifejezetten erre a célra szolgáló, felragasztható és eltolható ablakkal rendelkező kameratakarók használatát).

5.3.1.1 Jelszószéf

A jelszószéfek olyan alkalmazások, amelyek egy titkosított adatállományban eltárolják a felhasználók által alkalmazott jelszavakat és a hozzájuk kapcsolódó egyéb információkat (kapcsolódó weboldal, vagy alkalmazás, felhasználónév, jelszólejárat, megjegyzés). A jelszószéf alkalmazásánál két dologra kell figyelni. Az első, hogy a széfet nyitó mesterjelszó (Master Password) kellően biztonságos legyen és ne felejtsük el. Mert ebben az esetben mi sem fogunk hozzáférni a jelszavainkhoz. A másik fontos dolog, hogy legyen a titkosított adatokat tároló fájlról mentésünk. Mert ha a fájl megsérül, vagy törlődik – vagy neadjisten egy zsarolóvírus letitkosítja, akkor szintén nem fogunk tudni hozzáférni.

Az egyik legnépszerűbb, nyílt forráskódú és ingyenes ilyen alkalmazás a KeePass alkalmazás. Erős titkosítással védi a beleírt adatokat, képes előre megadott szempontok szerint jelszavakat generálni nekünk, illetve logikus tárolási struktúrát ad és nem utolsósorban tartalmaz egy jelszóerősség mérőt is, amely útmutató lehet a felhasználónak. Egy rendkívül hasznos tulajdonsága, hogy ha az alkalmazásból másoljuk ki az adott jelszót (Copy Password to Clipboard), akkor az pár másodpercen belül törlődik a vágólapról, meggátolva más alkalmazás hozzáférését.



18. ábra: KeePass Jelszószéf

Munkahelyi környezetben érdemes megérdeklődni az információvédelemmel kapcsolatos területtől, hogy mi a céges szabály az ilyen jelszószéfek alkalmazásával kapcsolatban, mert ha nincs valamilyen központi menedzsment, akkor pont az ellenkezőjét is elérhetjük az

eredeti célnak és akár üzletmenetfolytonossági incidenst is okozhatunk, ha senki nem fér hozzá egy fájlhoz vagy alkalmazáshoz, csak azért, mert egy ilyen széfben tároltuk a jelszavakat. Otthoni használatra mindenképpen javasolható.

5.3.1.2 Kétfaktoros hitelesítés

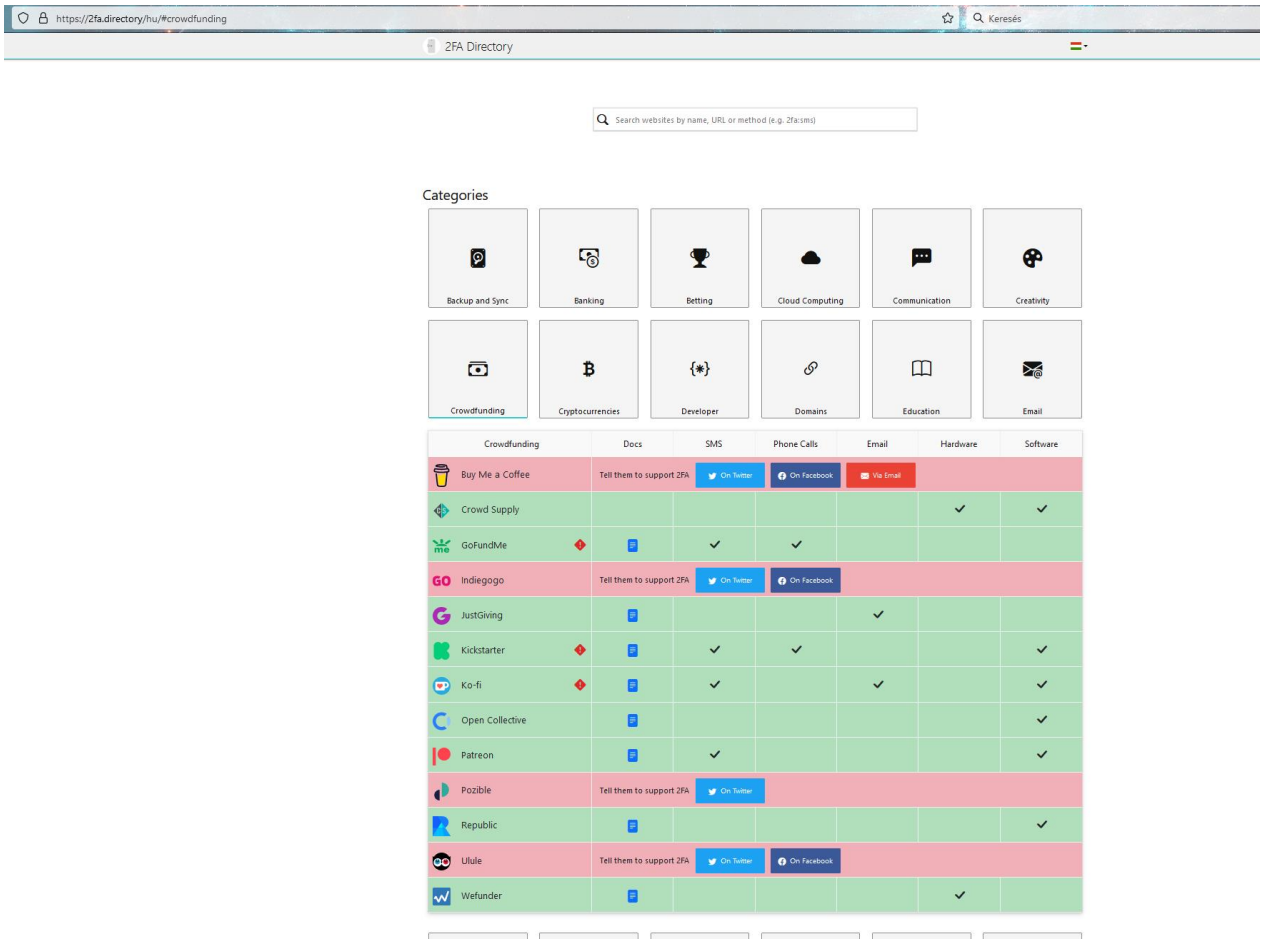
A világban rendkívül sok olyan biztonsági incidens történt az elmúlt években – és félő még történni fog a jövőben is – amely során felhasználói adatokat, ezen belül például jelszavakat is elloptak a támadók. Amennyiben kétfaktoros hitelesítés van beállítva a belépésnél, akkor a támadók nem tudnak – vagy jóval nehezebben tudnak – visszaélni az adatokkal ezen szolgáltatásoknál.

A kétfaktoros hitelesítés egy olyan biztonsági funkció, amely az adott szolgáltatáshoz tartozó jelszóval együtt védi a felhasználói fiókunkat. Ha beállításra került a kétfaktoros hitelesítés, a rendszer a bejelentkezési kísérlet megerősítéséhez egy külön bejelentkezési kód megadását kéri minden alkalommal, amikor be szeretnénk lépni a szolgáltatásba. Ezt a kódot több különböző módon megkaphatjuk, például SMS-ben, e-mailben, vagy külön hardveres vagy szoftveres véletlenszám-generátor által előállítva. Szerencsére a kétfaktoros hitelesítés egyre elterjedtebb, és már a SZÜF portál (magyarorszag.hu) bejelentkezés során is választható opció, aminek beállítására csak bátorítani tudunk minden ügyfélkapus felhasználót.

A 2FA Directory[23] egy olyan oldal, ahol szolgáltatás típusonként megnézhetjük, hogy melyik szolgáltatás milyen kétfaktoros hitelesítési lehetőségeket biztosít, illetve, hogy elérhető-e dokumentáció a témában. Ilyen kétfaktoros hitelesítési lehetőségek:

- SMS
- Telefonhívás
- E-mail
- Hardver token (véletlenszám generátor)
- Szoftver token (véletlenszám generátor)

[23] https://2fa.directory/hu



19. ábra: Two Factor Auth (2FA) kétfaktorú hitelesítés szolgáltatások[24]

5.3.2 WiFi eszköz biztonsági beállításai

Az otthoni hálózatok kiépítésében is teret nyertek a vezeték nélküli technológiák, mivel kényelmesek, nem kell az egész házat, lakást bekábelezni és egyszerű telepíteni őket. A biztonságukról azonban alapértelmezésben nem gondoskodnak, sőt, a gyári beállítások minden támadó számára ismertek, amivel nem okoz nekik gondot bármelyik nem megfelelően védett otthoni hálózatot ugródeszkaként felhasználni a további támadásaikhoz. Az otthoni vezeték nélküli eszközök alapértelmezésben a saját típusukat adják meg hálózati névnek. Amennyiben ezt nem változtatjuk meg, egy támadó könnyen utánakereshet az eszközünk alapértelmezett beállításainak, megnövelve egy sikeres támadás valószínűségét.

A vezeték nélküli hálózatok hozzáférés-védelmét titkosítással oldják meg, ezt több szinten megtehető. Erre szolgál például a vezetékes kapcsolódással megegyező bizalmasságú

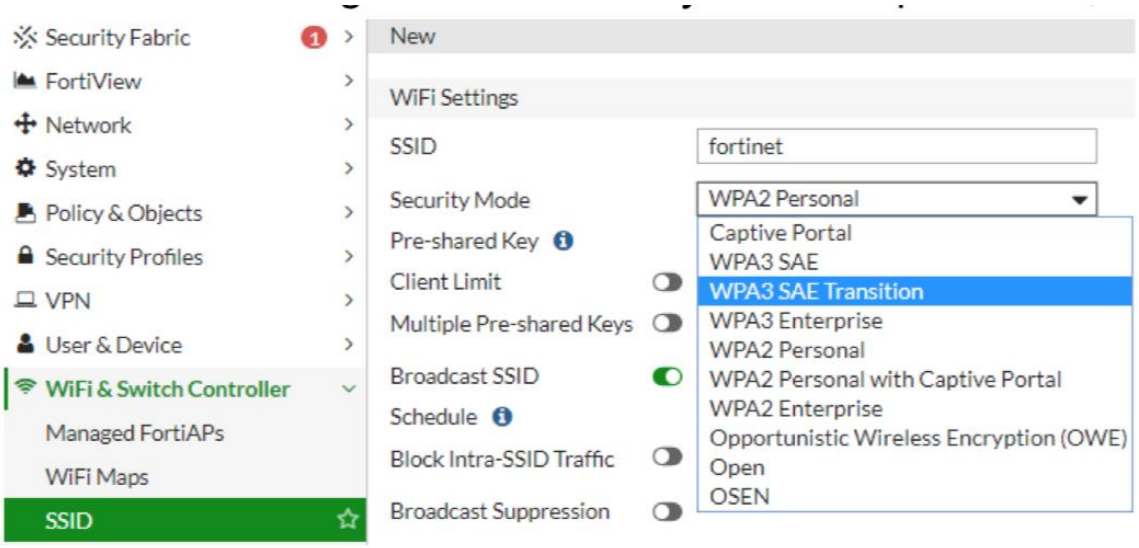
[24] https://2fa.directory

hálózat (WEP – Wired Equivalent Privacy – már nem tekinthető biztonságosnak), a WiFi védett hozzáférés (WPA – WiFi Protected Access – ebből is a WPA2 és a WPA3 szabványok, amelyek jelenleg a legfejlettebb biztonságosnak elfogadott módszerek) és ez személyre szabott -módban az előre kiosztott forgalomtitkosító kulcson alapuló védelem (PSK – Pre-Shared Key) – ez utóbbiak alkalmazása erősen javasolt a maximális, 63 karakteres jelszóval együtt.

A Wi-Fi Protected Access (WPA, WPA2 és WPA3) a vezeték nélküli rendszereknek egy, a WEP-nél biztonságosabb protokollja. A létrehozása azért volt indokolt, mert a kutatók több fontos hiányosságot és hibát találtak az előző rendszerben (WEP), illetve a WPA3 javította a WPA2 biztonsági tulajdonságait is. A WPA tartalmazza az IEEE 802.11i szabvány főbb szabályait, és egy átmeneti megoldásnak szánták, amíg a 802.11i szabványt véglegesítik.

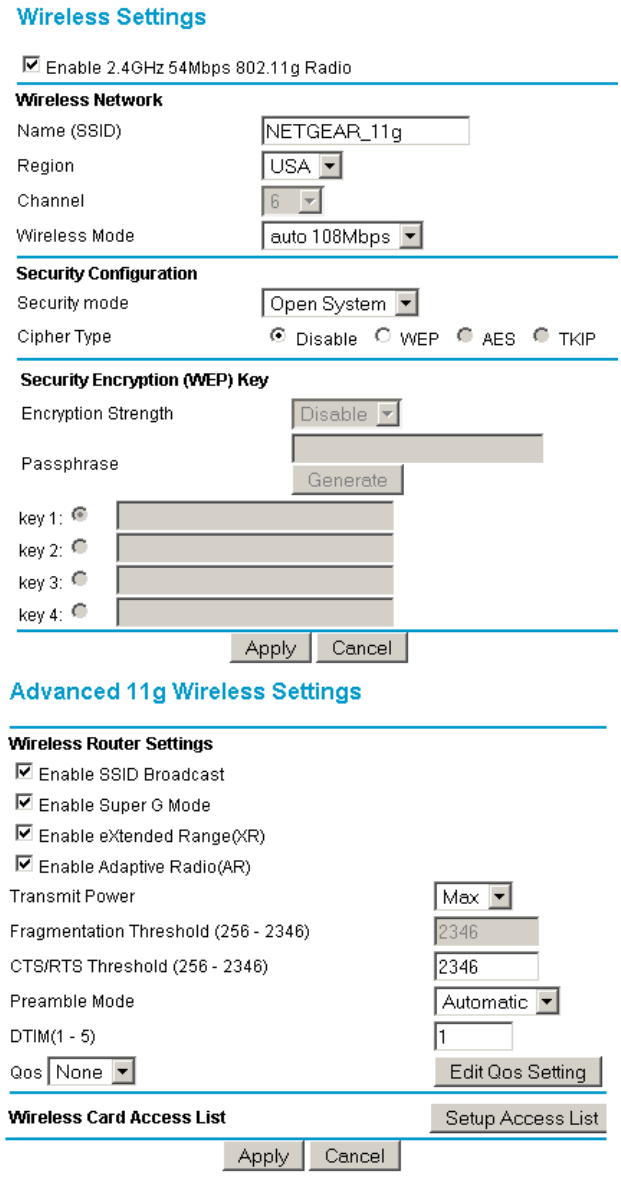
A WPA3 protokoll megnehezíti a bejelentkezési jelszó idegenek általi lehallgatását, mivel a jelszót nem nyílt szövegként, hanem egy jelszó alapú hitelesítési és titkosító kulcs létrehozási protokollt (SAE) alkalmazva juttatja el a hálózati eszköznek, ami így nehezebbé teszi a támadó feladatát, mert sokkal tovább kell a forgalmat analizálni egy sikeres támadáshoz. A másik védelmi módszer a hitelesítést követő adatforgalom titkosításához használt ideiglenes titkosító kulcsok kompromittálódása esetében nyújt a kompromittálódott adatforgalom előtti és utáni adatok számára védelmet, mivel ezek titkosításához véletlenszerűen választja meg a kulcsokat, így a teljes forgalom lehallgatásához mindegyik kulcsnak ismertté kellene válnia a támadó számára, mivel egy-egy elcsípett kulccsal nem tud mit kezdeni.

A „Personal” (WPA2-PSK) módban, amit a WPA3 funkcionalitással rendelkező hálózati eszközök elterjedéséig valószínűleg a legtöbben választanak otthon és hivatali környezetben, a megadandó jelszónak hosszabbnak kell lennie, mint a jellegzetes 6-8 karakter, amit az átlagfelhasználók általában még elfogadhatónak tartanak.



20. ábra: Vezetéknélküli hálózat titkosítás beállítás – WPA3 lehetőséggel

A védelemért sokat tehetünk az otthoni vezeték nélküli eszköz helyes biztonsági beállításaival és a hozzáférés korlátozásával [u]. Két alapvető védelmi szint van, egyrészről az eszközbe való bejelentkezési név és jelszó megfelelősége (gyári beállítások felülírása, hálózati név (SSID) megváltoztatás), másrészről a forgalom hozzáférhetetlenné tétele az arra nem jogosultak számára (WiFi jelszó).



21. ábra: Példa nyílt WiFi rendszer beállításaira

A hálózathoz való hozzáférést korlátozhatjuk a hálózati csatoló egyedi címe szerint is, ennek következtében idegen eszköz nem tud rácsatlakozni a hálózatunkra, másrészről a saját gépünk is csak akkor tud kommunikálni az eszközön keresztül, ha előtte hozzáadtuk a jogosult eszközök listájához.

22. ábra: MAC szűrés beállítása WiFi eszközön

Annyiszor ismételhetjük, ahány eszköz címének a befogadására képes a WiFi útválasztónk. Ne felejtsük el az eszközök MAC-címét kitörölni, amennyiben azok kapcsolódása már nem engedélyezett. A MAC cím (MAC-address) hat párból álló kombinációja a 0-9 számjegyeknek és az a-f betűknek, tehát ha ilyen látunk, akkor biztosak lehetünk abban, hogy egy hálózatra köthető eszköz második szintű csatolójának a címét tartalmazza ez a furcsa – de a számítógépes hálózatoknál teljesen megszokott – jelsorozat. Fontos tudni, hogy a MAC cím hamisítható [v], azaz egy képzett támadó a saját gépéről azt állíthatja a WiFi eszközüknek, hogy az nem is egy idegen eszköz, hanem a miénk. Otthoni hálózatok esetén ez a mélységi védelem egy eleme lehet, de ne bízzuk a hálózatunk védelmét erre az egy biztonsági elemre.

Bár nem triviális, de muszáj megemlíteni az eszközök saját szoftverének biztonságát (ideértve az IoT – Internet of Things – Dolgok Internete – internetre csatlakoztatott okoseszközöket [IP kamerák, okosTV-k, okoshűtők, egyéb okoseszközök]), illetve ezek szoftvereinek sérülékenységeit is. Minden célhardver, így a WiFi routerek is tartalmaznak egy úgynevezett firmware programot, amely magát az eszközt működteti. Ezek is ember által, gyakran évekkel korábban írt programok, amelyeknek idővel kiderülnek sebezhetőségeik. Rendkívül fontos, hogy az otthoni hálózati eszközeinken is a legfrissebb, ismert biztonsági hibákat nem tartalmazó firmware fusson. A gyártó oldaláról le lehet tölteni a legfrissebb firmware verziót és a router adminisztrációs felületén lehetőség van ennek frissítésére is. Ellenkező esetben áldozatául eshetünk egy támadásnak még akkor is, ha erős titkosításunk van, megváltoztattuk az admin jelszót és úgy gondoljuk, hogy mindent megtettünk a biztonságunk érdekében.

5.3.3 Bluetooth, IrDA

Két, arra alkalmas informatikai eszköz összekapcsolására van még lehetőség bluetooth és infravörös (IrDA) kapcsolat kialakításával, illetve fizikai kábellel történő összekapcsolással is. A bluetooth és infravörös kapcsolatok azért érdekesek biztonság szempontjából, mert ezeknek is vannak olyan sérülékenységeik, amelyeken keresztül – például egy állandóan bekapcsolt bluetooth kapcsolat esetén - a fizikai támadó át tudja venni az eszköz irányítását vagy bele tud ékelődni két bluetooth kapcsolatot használó eszköz közötti kommunikációba.

Érdemes a bluetooth és IrDA kapcsolatokat csak arra az időre aktiválni, amikor használni szeretnénk ezeket, és lehetőleg nem zsúfolt környezetben. Ezzel nem csak a biztonságunkat erősítjük, de mobil eszköz esetén az akkumulátort is kíméljük. Megjegyezzük, hogy már csak néhány specifikus alkalmazásban vagy régebbi eszközökön lehet találni IrDA portokat. A modern laptopok és eszközök általában már nem rendelkeznek ezzel a technológiával, mivel azok a vezeték nélküli kapcsolódásokra és más gyorsabb adatátviteli lehetőségekre támaszkodnak.

5.3.4 E-mail

Nagyon gyakori kommunikációs forma az internetes kommunikáció során az egész világon az elektronikus levelezés használata. Az amerikai Radicati piackutató cég riportja szerint a naponta küldött üzleti és felhasználói e-mailek száma 2022-ben elérte a 333 milliárdot (2018-ben ez 281 milliárd volt). Bár manapság kezdik átvenni ez e-mailezés funkcióját az azonnali üzenetküldési szolgáltatások (Facebook Messenger, Viber, Whatsapp, WeChat, Signal stb.). Az egyszerű e-mail szolgáltatások és programok nyílt szövegként küldik a leveleket a hálózaton keresztül.

Mivel egy e-mail keresztülhalad számos informatikai rendszeren, míg a címzettjéhez el nem ér, ezeknek a leveleknek a bizalmassági szintje megegyezik egy postai levelezőlapéval. Kivéve, ha a két levelezőszerver között TLS titkosított kapcsolat van kialakítva. Erről azonban jellemzően a felhasználóknak nincs tudomása, habár a levél fejlécében lehet találni erre utaló információkat. Ezért javasoljuk az e-mail kommunikációra alapesetben úgy tekinteni, hogy bárki, aki hozzáfér, az olvashatja is azt. Ezért azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet, csupán az elektronikus levél titkosítása biztosíthatja. Ide kívánkozik még az e-mail aláírás, mint fogalom. Az e-mail aláírás (nem tévesztendő össze a levelek digitális aláírásával) egy olyan előre megírt szöveg, melyet minden egyes kimenő e-mail végére a levelező programunk automatikusan be tud illeszteni. Tipikusan ilyen az elköszönő szöveg, pl. „üdv, Péter”.

E-mail vonatkozásában a legnagyobb kitettséget a csatolmányként küldött rosszindulatú programkódok megnyitása jelenti. Ezek tipikusan vagy neves cégek nevében hamisított levelekben érkeznek, olyan témában, amire a felhasználó ráharap és a kíváncsiság miatt megnyitja a levelet és a csatolmányt. Például fizetési felszólítások, számlák, biztonsági figyelmeztetések, hogy valaki be akart lépni a netbankba, de nagyon gyakori, amikor futárcégek csomagértesítő levelének van álcázva a fertőzést okozó fájl. Ki ne lenne kíváncsi arra, hogy ki és milyen csomagot küldött neki? Ezért kell nagyon óvatosnak lenni ismeretlen feladótól érkező levelekkel, illetve gyanakodni, ha csomag érkezéséről értesítenek, holott nem is vártunk semmit, vagy ha éppen várunk valamit, de nem attól a futárcégtől, aki éppen kézbesíteni szeretne nekünk „valamit”. Nagyon gyakori támadás az, amikor egy word vagy excel dokumentumba makró-vírust rejtenek el, ami a dokumentum megnyitásakor aktivizálódik. **Makró**nak (macro) nevezünk egy olyan rövidítést, amely valamilyen programnyelvi rész, utasítássorozat, vagy felhasználói műveletsorozat helyettesítéseként szerepel. Tekintettel arra, hogy a makrókat a felhasználó is készítheti, semmi akadálya nincsen egy rosszindulatú támadó által készített makró-vírust tartalmazó szöveges dokumentum létrejöttének. Szerencsére a mai vírusvédelmi rendszerek már odafigyelnek a makrókra is.

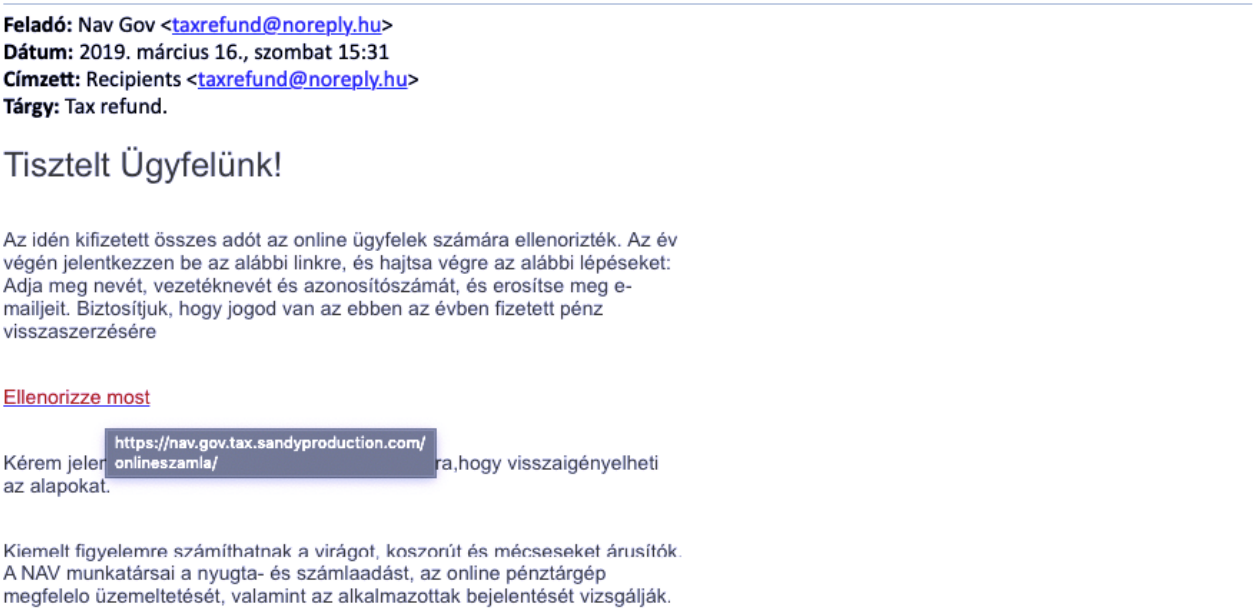
Egy-egy fájl megnyitását olykor azért kell elkerülni, mert felmerülhet a gyanú, hogy nem azt tartalmazza, amire mi gondolunk – és így jó nyitánya lehet egy sikeres támadásnak, más szóval a csalárd elektronikus levelek általában rosszindulatú programkódot vagy vírust tartalmazhatnak. A zsarolóvírusok egyik jellemző támadási formája a makrózott office dokumentumokban történő elrejtőzés. Ez azért is válhat kritikussá, mert terjed a különböző mesterséges intelligenciák által előállított Visual Basic Script (.vbs) előállítása egy-egy office dokumentumcsomaghoz tartozó feladat automatizálására (például egy adott témában prezentáció előállítása automatikusan). Ehhez azonban az kell, hogy tartósan engedélyezve legyen a makrók futtathatósága, zöld utat adva akár a zsarolóvírust tartalmazó fájloknak[25].

Egyre gyakoribb, hogy a levél önmaga nem tartalmaz vírust vagy kártékony kódot (ezért a vírusszűrésen sem akad fent) hanem a csatolmányra – vagy a levélben lévő hivatkozásra kattintás után kezd el letöltődni a kártevő. Ha naprakész a vírusvédelmi rendszerünk, akkor jó eséllyel meg tudja akadályozni a kártevő letöltődését.

Az adathalászatoknak is még a mai napig leggyakoribb csatornája az elektronikus levél. Az adathalászat során az eredeti, azonosítást kérő weboldalhoz megszólalásig hasonlító oldalra csalják az áldozatot, ahol az megadja az azonosító adatait és esetleg még egyéb adatokat is, amivel aztán a csalók később megpróbálnak visszaélni. Ide tartozik a banki adatokat

[25] További információ erről itt található.

bekérő hamisított elektronikus levelek témaköre is. Kaphatunk egy e-mailt és SMS-t is látszólag a bankunktól, amelyik arra kér, hogy látogassunk el az ott megadott linken a bank „speciális” honlapjára és adjuk meg a kért – leggyakrabban érzékeny – információkat. Ezzel kapcsolatosan megjegyzendő, hogy sem a banki, sem egy internetes szolgáltató ügyintézője sosem kérheti el a jelszavunkat telefonon, e-mailben vagy interneten keresztül, azt kizárólag a szolgáltató vagy bank hitelesített weboldalán kell használni. Minden más jellegű kérést, kérdést a jelszavakra (esetleg bankkártya adatokra) vonatkozóan kétkedve és bizalmatlanul javasolt kezelnünk, és az elutasítás után mérlegelhetjük az incidens jelzését is a bank vagy szolgáltató felé. Ez utóbbi azért fontos, mert az ügyfelek tömeges visszajelzései alapján az érintett szervezet egyrészről intézkedést tud tenni az incidens megállítására, másrészről az elkövetők elleni nyomozást is elindíthatja – ami sosem a mi feladatunk, ne is próbálkozzunk vele, mert esetleg a Btk. szerinti tiltott tevékenységekbe futhatunk bele.



Feladó: Nav Gov <taxrefund@noreply.hu>
Dátum: 2019. március 16., szombat 15:31
Címzett: Recipients <taxrefund@noreply.hu>
Tárgy: Tax refund.

Tisztelt Ügyfelünk!

Az idén kifizetett összes adót az online ügyfelek számára ellenorizték. Az év végén jelentkezzen be az alábbi linkre, és hajtsa végre az alábbi lépéseket: Adja meg nevét, vezetéknevét és azonosítószámát, és erosítse meg e-mailjeit. Biztosítjuk, hogy jogod van az ebben az évben fizetett pénz visszaszerzésére

Ellenorizze most

https://nav.gov.tax.sandyproduction.com/onlineszamla/

Kérem jeler ra,hogy visszaigényelheti az alapokat.

Kiemelt figyelemre számíthatnak a virágot, koszorút és mécseseket árusítók. A NAV munkatársai a nyugta- és számlaadást, az online pénztárgép megfelelo üzemeltetését, valamint az alkalmazottak bejelentését vizsgálják.

23. ábra: Adathalász levél példa

Fenti példában azt fontos kiemelnünk, hogy jól látszódik, hogy a csalók nem írtak ki hivatkozást, hanem csak egy szöveg mögé rejtett hivatkozást használtak, ahol, ha rávisszük az egerünket az emailekben található hivatkozásra (**de nem kattintunk!**), akkor pár másodperc múlva megjelenik a tényleges hivatkozás. Ha ez nem egyezik pontosan, vagy nagyon eltérő weboldalnak tűnik, akkor semmiképpen se kattintsunk rá. Fent például árulkodó, hogy a

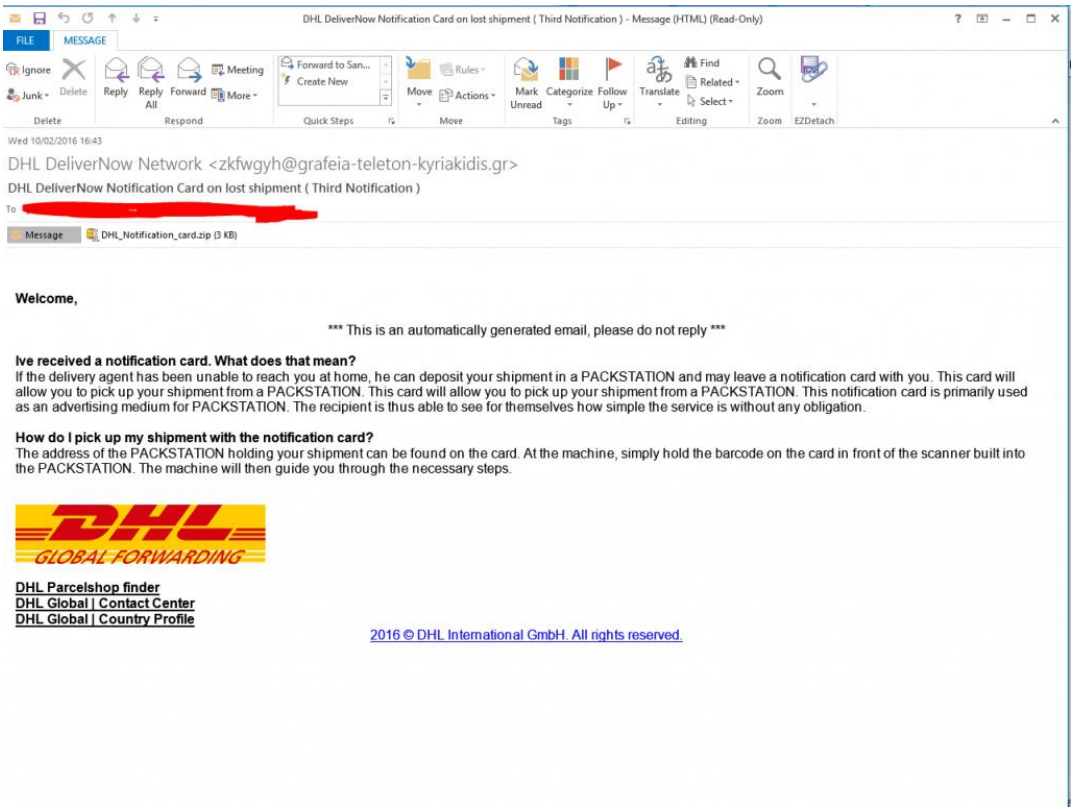
„nav.gov.hu” domain helyett a „nav.gov.tax.sandyproduction.com” a tényleges domainnév. Ami nyilvánvalóan nem az adóhivatal oldala.

Kiemelten szeretnénk felhívni a figyelmet a zsarolóvírusokra, mivel ezek a kártevők jellemző módon e-mailben érkeznek meg a felhasználókhoz. Ezért felismerésük az első lépés a megfelelő védekezéshez.

A zsarolóvírusok lefutásához, aktiválódásához felhasználói interakció szükséges. Az e-mailben jellemzően nem maga a vírus érkezik, hanem egy olyan csatolmány, amire a kíváncsi felhasználó rákattint, ezzel elindítva egy olyan programocskát, amely letölti az internetről a tényleges kártevőt, amely, miután letöltődött, elkezdi áldatlan tevékenységét. Éppen ezért életbevágó, hogy felismerjük az ilyen leveleket.

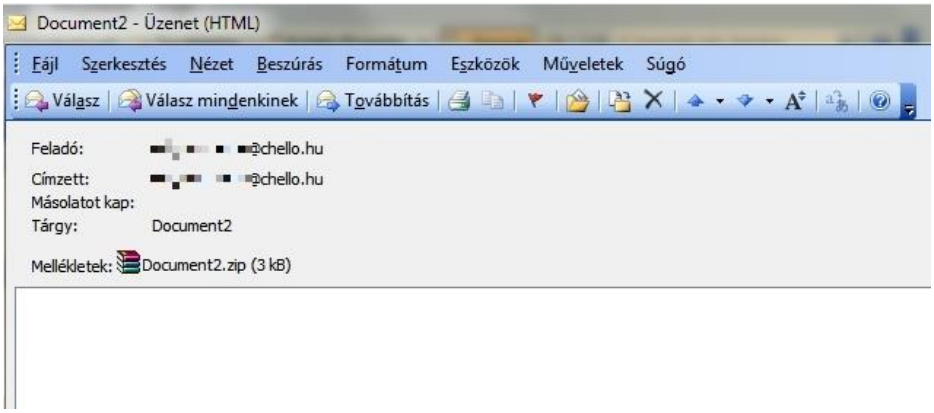
A kártevőterjesztés egyik fontos feltétele az, hogy a felhasználónak kell jellemzően elindítani a fertőzés első lépését. Nagyon fontos, hogy a támadók szeretnék, ha a felhasználó rákattintana a csatolmányra – vagy a levélben lévő hivatkozásra (linkre), ezért olyan tárgyat és szöveget írnak, ami megüti a felhasználó ingerküszöbét. Például kit ne érdekelne, hogy milyen számlája (bill/invoice) érkezett, ráadásul egy külföldi cégtől? Ezt próbálják kihasználni a támadók, a legtöbb kártevőt terjesztő levél a befizetetlen számlákkal riogatja a felhasználókat (hiszen mindenkinek lehetnek éppen még nem befizetett számlái). A második legjellemzőbb, hogy egy kézbesíthetetlen levélként érkezik (látszólag) vissza egy levél. Tipikus reakció, hogy ha sikertelenül kézbesített levél érkezik, akkor meg szeretnénk nézni, hogy ez melyik levelünk lehetett, kinek küldtük, mit küldtünk a csatolmányban? Ha bedőlünk vagy figyelmetlenek vagyunk és kattintunk, akkor könnyen megvan a baj. Harmadik helyen vannak a csomagküldő szolgáltatók értesítő leveleinek álcázott csaló levelek. Ki ne lenne kíváncsi, hogy milyen csomagja érkezett? A felhasználónak rá kell kattintania a csatolmányra, vagy hivatkozásra, hogy a csomagküldés részleteit megismerje. Nagyon ravasz. A tanulság, hogy ha nem várunk csomagot, akkor ne kattintsunk ilyen levélre. Igaz ez azon nyereményértesítésekre is, ahol többmilliós nyereménnyel kecsegtetnek, mert valaki, vagy valami kisorsolta a felhasználó e-mail címét. Ha nem játszottunk nem is nyerhetünk! Ha nincs milliomos afrikai bankár nagybácsink, akkor nem is örökölhetünk tőle mesés vagyont. Negyedik helyen a különböző jogszabályok megsértése miatti értesítések vannak, ami szintén olyan téma, hogy mindenki kíváncsi, hogy épp miért szeretnék megbüntetni. Az ötödik helyen az olyan üres levelek vannak, amelyekhez látszólag egy szkennelt dokumentum van csatolva, mintha egy rosszul konfigurált multifunkcionális gép küldte volna. Mivel nincs információ a szkennelt dokumentumról, a kíváncsi felhasználó könnyen rákattint és már meg is fertőződött.

Lenti példában a DHL nevében egy görög temetkezési vállalat címéről/címét behamisítva küldte a csaló az üzenetét, nyilvánvalóan hamis a levél.



24. ábra: Zsarolóvírust tartalmazó e-mail hamisított feladóval

A következő példában a címzett volt feladóként is behamisítva, és semmilyen szöveg vagy magyarázat nem volt a levélben, a felhasználó kíváncsiságára bízva a döntést a csatolmány megnyitásáról.



25. ábra: Zsarolóvírust tartalmazó levél, a címzett a behamisított feladó

5.3.5 Azonnali üzenetküldés

A valós idejű szöveges kommunikáció két vagy több személy között az azonnali üzenetküldés. Sok közösségi program része (Snapchat, Facebook, Skype, Viber, Whatsapp), de külön is használhatók az Instant Messaging (IM), azonnali üzenetküldési szolgáltatások a közösségi alkalmazások során. Megjegyezzük, hogy egyre több IM program része a titkosított üzenetküldés, amelyet, ha nem alapértelmezett, akkor vagy a beállításokban, vagy külön funkcióként érünk el.

Természetesen itt is léteznek sebezhetőségek, amelyek miatt az adataink és gépünk továbbra sincsenek biztonságban. Ezeket a használat során ismerni ajánlott a biztonság megteremtése és fenntartása érdekében. Ilyen veszélyek például a rosszindulatú szoftverek, hátsó kapu hozzáférés, nem kellően korlátozott fájl-hozzáférés. A védelem itt elsősorban bizalmasságot biztosító módszerekkel valósítható meg, mint titkosítás (ami már jellemző a legnépszerűbb üzenetküldőkre), fontos információk titokban tartása, fájl-megosztás korlátozása és természetesen figyelni illik a program integritására, vagyis észlelhetővé kell tenni azt, ha valaki a tudtunk nélkül átírná az azonnali üzenetküldő szoftverét, ami a gépünkön fut (erre szolgál a kódaláírás, amit a digitális aláírásoknál tárgyalunk).

5.3.6 Tűzfalak

A tűzfalak olyan hardveres vagy szoftveres eszközök, melyek egy előre definiált szabályrendszer alapján intézkednek egy hálózat határán a beérkező és kimenő adatelemek engedélyezéséről vagy tiltásáról. Más szóval a tűzfalak az általunk meghatározott hozzáférési szabályokat kényszerítik ki, tartatják be a kommunikáció során. Tűzfalak tekintetében számos különböző szintű és tudású tűzfal létezik. Felhasználói oldalról a legfontosabb a személyi tűzfal.

Személyi tűzfal (personal firewall): a saját számítógépen működő olyan szoftver, mely az egyes alkalmazások futtatását és hálózati kommunikációikat engedélyezi vagy tiltja, sok esetben öntanuló rendszerben. A személyi tűzfal minden esetben egy futó szoftver a számítógépünkön. A személyi tűzfal vagy az operációs rendszer része, vagy magunk telepíthetjük azt fel a számítógépünkre – például egy biztonsági programcsomag részeként.

A tűzfal feladata, hogy védje a hálózatot a **betörés**ektől, más szóval akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről az előre definiált hozzáférés-védelem kikényszerítésével. A korlátozást szabályok segítségével végzi, mely megmondja a hálózati forgalomról, hogy engedélyezett-e vagy tiltott, emiatt a tűzfal egy szabály-alapú rendszer. Szükség esetén létre lehet hozni további szabályokat a bejövő/kimenő hálózati forgalom

kezelésére – erre például egy új játékprogram telepítésekor is szükség lehet, amikor az addig bezárt portokat a játék használatához ki kell nyitnunk, vagyis engedélyeznünk kell.

A tűzfalak jóságát vagy nem megfelelőségét az adja, hogy mennyire képesek kiszűrni a nem kívánt forgalmat és mennyire képesek átengedni a várt forgalmat a hálózat minden szintjén. Ehhez képesnek kell lenni szabályokat megfogalmazni számukra, amihez számos segítség, fórum, útmutató található az interneten, de némi kísérletezgetés után saját kútfőből is elsajátítható egy biztonságos környezet megteremtése.

5.4 Adatvédelmi megfontolások, GDPR

Személyes adataink biztonságáról akkor beszélhetünk, ha minden adatunk (legyen a személyiségünkre vagy szokásainkra jellemző) biztonságban van az illetéktelen és jogosulatlan felhasználással, birtoklással szemben, vagyis az **adatvédelem** megvalósul. Sokszor kötelező megadni különböző okokból a személyes adatainkat egyes szervezetek számára, máskor önként adjuk meg az adatainkat, megosztjuk fényképeinket, gondolatainkat a közösségi oldalakon, esetenként arra való tekintet nélkül, hogy ki láthatja, ki kezelheti ezeket és ki nem. Mindez természetesen veszélyeket is rejthet magában. Fontos különbséget tennünk adatvédelem és adat- vagy információbiztonság között. Míg az adatvédelem elsősorban a vonatkozó jogszabályokban használt fogalom, és elsősorban a személyes adatok megfelelő, jogszabály által előírt kezelését értjük alatta, addig az adat- vagy információbiztonság azon biztonsági kontrollok összességét és elfogadott kockázati szinten való működését jelenti, amelyben az adatok és információk bizalmassága, sértetlensége és rendelkezésre állása biztosított.

A levéltitok védelmét már az 1949. évi XX. törvény is alapelvként rögzítette[26], mely jogszabály 1989-ben módosult és a személyes adatok védelmét tisztán és világosan előírta[27]. Ezt az előírást Magyarország Alaptörvénye is megőrizte[28] és 2011-ben kiegészítette az adatvédelem hatósági ellenőrzésével. Törvényi szinten az első részletes szabályozás 1992-ben jött létre[29], mely már rendelkezett – igaz, elég röviden – az adatbiztonságról (10. §), ezek a szabályok

[26] 1949. évi XX. törvény 57. § A Magyar Népköztársaság biztosítja a polgárok személyi szabadságát és sérthetetlenségét., a levéltitok és a magánlakás tiszteletbentartását.

[27] 1989. évi XXI. törvény 34. § alapján módosult az 1949 évi XX. törvény: „... 59. § (1) A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog."

[28] Magyarország Alaptörvénye VI. cikk
(2) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekû adatok megismeréséhez és terjesztéséhez.
(3) A személyes adatok védelméhez és a közérdekû adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenõrzi.

[29] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

2011-ben újabb részletekkel gazdagodtak[30], például kártérítési kötelezettség az adatbiztonság megsértésekor, illetve az adatvédelmi audit intézményének bevezetése is ekkor történt. Az EU irányelv által támogatott nemzeti szinten történő adatvédelmet az Európai Unió egységesen kötelezővé tette az adatvédelmi rendelet 2016-os elfogadásával és 2018-as bevezetésével.

5.4.1 GDPR

Az Európai Unió korán felismerte a személyes adatok kezelésének fontosságát, és az uniós egységes szabályrendszer előnyeit ezért 1995-ben létrehozta az Európai Parlament és a Tanács 95/46/EK irányelvét (Európai Adatvédelmi Irányelv) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Ezt követte 2018. május 25-től az Európai Parlament és a Tanács (EU) 2016/679 rendelete (elfogadva 2016. április 27.) „A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)" [k]. Fenti dokumentumra az angol rövidítéssel GDPR (General Data Protection Regulation) szoktak hivatkozni, még Magyarországon is.

A GDPR kimondja: „A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog." A GDPR ezen felül - részben összhangban a hatályos magyar szabályozással – rendelkezik a személyes adatok kezeléséről, feldolgozásáról, valamint meghatározza az egyes adatkezelésben résztvevők jogait és kötelességeit. Jelen anyagnak nem célja a GDPR részletes kifejtése, annyit azonban mindenkinek érdemes tudnia, létezik ez a rendelet és érdemes utánanéznie, hogy mint magánszemély milyen jogok illetik meg. Ha pedig valamilyen szervezetnek a felelős vezetője a kedves olvasó, akkor azért érdemes utánanéznie, mert az előírások és a büntetési tételek az európai szabályok bevezetésével sokkal szigorúbbá váltak.

Meg kell különböztetni az adatkezelőket az adatfeldolgozóktól. Az adatkezelők olyan személyek, akik vagy a saját maguk által meghatározott célból vagy jogszabály által felhatalmazva kezelik a személyes adatokat[31]. Az adatfeldolgozó feladatát az adatkezelő határozza meg[32], az adatkezelő megbízásából dolgozza fel a személyes adatokat, ebből adódóan az ügyfelekkel általában nincs is közvetlen kapcsolatban. Az adatkezelő vagy jogszabályi felhatalmazás,

[30] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
[31] GDPR 4. cikk 7.
[32] GDPR 4. cikk 8.

vagy az adattulajdonos felhatalmazása alapján továbbíthatja a személyes adatokat, de harmadik országba csak akkor lehetséges ezt megtenni, ha az adatkezelő garanciákat kap a személyes adatok GDPR által előírt módon történő kezelésére.

Sokszor felmerülő kérdés, hogy kell-e alkalmazni a GDPR rendelkezéseit a közösségi portálokon történő kommunikáció során. A rendelet úgy fogalmaz, hogy ha az adatkezelés semmilyen üzleti célt nem szolgál, akkor nem kell alkalmazni magáncélú csevegésnél az előírásokat, de a közösségi portál üzemeltetőjére – aki az eszközöket biztosítja a közösségi kommunikációhoz – már vonatkoznak ezek a szabályok. A részletes szabályokról javasoljuk tájékozódni a Nemzeti Adatvédelmi és Információszabadság honlapján.[33]

A GDPR létrejöttének célja volt az is, hogy az EU állampolgárainak a személyes adatainak kezelését a cégek és szervezetek komolyabban vegyék. Az adatlopások és egyéb biztonsági incidensek számának növekedése, valamint az évről évre növekvő fenyegetettségek ezt indokolttá teszik. Ezen fenyegetettségek többek között azok, amikor haszonszerzési célból csalással, számítógépes rendszerekhez való hozzáféréssel szereznek – jellemzően pénzügyi – adatokat rólunk, hiszen a feketepiacon a számlaadatoknak értéke van, nem is kicsi. Ennél azonban sokkal értékesebb célpontok lehetnek sok esetben az egészségügyi állapotunkra vonatkozó személyes adatok. Mivel a számlaadatok változnak, egy ellopott bankkártyát le lehet tiltani, egy jelszót meg lehet változtatni, addig az egészségügyi személyes adataink (betegségeink, kórtörténet, állandó gyógyszereink stb.) viszonylag állandónak tekinthetőek, emiatt mind a célzottan támadóknak, mind pedig a célzottabb reklámok küldőinek vagy esetlegesen a zsarolóknak sokkal nagyobb értéket tudnak képviselni.

Az adatok biztonságának kialakítására a GDPR rendelet a 32. cikkében az alábbiakat írja elő az adatkezelő és az adatfeldolgozó számára – a tudomány és technológia aktuális állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembe vétele mellett:

- az adatkezelőknek és adatfeldolgozóknak megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk annak érdekében, hogy a megfelelő szintű adatbiztonságot garantálni tudják, ideértve az alábbiakat is:
    - a személyes adatok álnevesítése és titkosítása,
    - a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritás, rendelkezésre állás és ellenálló képesség,

[33] http://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html

- fizikai vagy műszaki incidens esetén az arra való képesség, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani,
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárás kialakítása.

A képzett támadók sokféle módon szerezhetik be a szükséges információkat, például telefonhívásokkal (kikérdezés), adathalászattal (phishing), eltérítéses adathalászattal (pharming), kifigyeléssel (shoulder surfing), vagy személyesen, megtévesztéssel (szélhámosság – social engineering). A szélhámosság módszerei változatosak, nagyon gyakori például az, hogy a szélhámosok valamilyen ürügy révén (pl. üzleti tárgyalás) bejutnak a helyszínre és ott szétnéznek további adatok után kutatva. Ugyanilyen gyakran történik az meg, hogy a szélhámos **információbúvárkodás**t végez, azaz minden fellelhető információt begyűjt későbbi elemzés céljára, akárhol is találja meg azt – nem elfelejtve a szemeteskosarat és a szemeteskukákat sem.

A személyazonosság-lopásnak számos következménye is lehet, lehetnek személyes, pénzügyi, üzleti, jogszabályi következményei is, de mindenképpen kellemetlenséget okozhat. Közvetlen következménye a szélhámosságnak, hogy a személyes adataink és a számítógépes rendszereink mások által hozzáférhetővé váltak, és nagyon valószínű, hogy a begyűjtött adatokat csalásra fogják felhasználni.

A személyazonosság-lopásról jó tudni, hogy leginkább azt jelenti, hogy felveszik más személyazonosságát haszonszerzés céljából. Sűrűn előfordul a kikérdezés, amely során személyes információkat gyűjtenek be megtévesztéssel, vagyis miközben az áldozat például azt hiszi, hogy egy hivatalos közvélemény-kutatóval beszél, a valóságban egy álcázott támadó teszi fel neki a kérdéseket. Fontos, hogy vigyázzunk mások személyes adataira is. Ha elhagyott iratot, bankkártyát találunk, akkor annak képét, fotóját ne osszuk meg a közösségi oldalakon, hanem vigyük be a rendőrségre – ha személyazonosító irat, és a tulaj jelentette, akkor akár körözhetik is. Ha bankkártya, akkor pedig adjuk le az érintett bank valamelyik fiókjában, ahol be tudják a tulajt azonosítani és tudják értesíteni. A bankkártya adatokról bővebben lesz még szó, itt csak annyit jegyeznék meg, hogy az interneten már az alap kártyaadatokkal is lehet sokszor fizetni, így egy közösségi oldalon történő kártyafotó megosztással több kárt tudunk okozni, mint hasznot.

Ritkán ugyan, de előfordulhat a személyazonosító igazolványunkban vagy útlevelünkben lévő mikrochip klónozása, mint támadási forma. Ekkor az történik, hogy a támadó az

őrizetlenül hagyott igazolványunk digitális adatait lemásolja egy másik chipre, és ezt – vagy ennek módosított változatát – valós igazolványként feltüntetve próbálja meg a digitális térben felhasználni (ahol a kártya vizuális kinézetét nem ellenőrzik). A mikrochip és adatainak ellenőrzését nem megfelelően implementáló helyeken ez eredményes is lehet, azonban ahol a mikrochip másolását (cloning detection) és az eredetiségét (genuine chip) is ellenőrzik, ott ez már nem lehet sikeres támadási forma.

A személyes adatok védelmének legfontosabb oka tehát a személyazonosság-lopás megakadályozása és a csalások megelőzése. Sokat tehetünk ez ellen, ha a böngészés közben néhány egyszerű szabályt betartunk, illetve az igen gyakori kommunikációs felületté előlépett közösségi oldalakon elvégzünk néhány beállítást és figyelembe veszünk néhány szabályt is.

5.4.2 Védelem böngészés közben

Egy webböngészővel egyszerűen meg lehet az egyik internet oldalról egy másikat látogatni, mert a böngésző értelmezni tudja az oldalak közötti váltásra, letöltésre, és megjelenítésre vonatkozó utasításokat. Ezek a HTML (HyperText Markup Language) nyelvben vannak definiálva, amely a WWW (World Wide Web) szabványos nyelvének tekinthető. A HTML formátumú linkek (kereszthivatkozások) segítségével a dokumentumok kapcsolati hálót alkotnak az interneten.

A böngészőprogramok ma már alapesetben is számos funkciót nyújtanak, de kiegészítőkkel további feladatok végrehajtására is alkalmazhatók. Azonban éppen a funkciók sokasága idéz elő komplex konfigurációs lehetőségeket és potenciális biztonsági problémákat. Minél komplikáltabb a böngésző (minél több kiegészítőt tartalmaz), annál több hibalehetőség adódik. Az ilyen programozási hibákat nevezzük bugnak[34]. A bugok úgy általában minden szoftvert érintenek, mivel nincsenek tökéletes, hibátlanul megírt programok, appok, alkalmazások. A gyártók megpróbálják a bugokat állandóan javítani, és kínálnak javító „foltokat”, más néven javítócsomagokat is (patch), amelyeket fel lehet (és erősen ajánlott is) telepíteni, hogy az adott hibát a felhasználó a saját böngészőjében javíthassa. Ehhez nem kell a böngészőt teljesen letörölni, majd újra visszatelepíteni. Az ilyen „javító programokat” néha patch helyett update-nek, vagy bugfix-nek is nevezik. A fentiek tükrében mindig érdemes használni az automatikus frissítéseket, vagy ha a szoftver erre nem ad lehetőséget, úgy mindig a legfrissebb szoftververziót telepíteni és használni. A szoftverfrissítések telepítésének az a

[34] Érdekességképpen megjegyezzük, hogy az első feljegyzett számítógépes „bug” egy élő lepke volt, amelyik 1947 szeptemberében berepült egy számítógépbe, és ott hardverhibát okozott.

leglényegesebb oka, hogy ezzel lehetőséget kapunk kijavítani egy program hibáját vagy biztonsági kockázatát.

Már 2009 környékén látszott, hogy a böngésző lesz az új operációs rendszer, és a böngészőkiegészítők lesznek az új alkalmazások. Ahogy egyre több és több időt töltöttek az emberek a böngészőben – háttérbe szorítva a vastag kliens alkalmazásokat, úgy egyre több dologra lehetett használni ezeket a böngészőkiegészítőket. Természetesen erre a lehetőségre a rosszindulatú programok (malware) írói is felfigyeltek, hiszen könnyen és egyszerűen lehet nagyon értékes adatokhoz hozzájutni egy rosszindulatú böngészőkiegészítő segítségével. Balázs Zoltán (a CUJO LLC. cég Sérülékenységi Kutatólaborjának vezetője) 2011-ben kezdte el vizsgálni, mi mindenre használhatja egy rosszindulatú fejlesztő a böngészőkiegészítő-technológiát. Ezzel egyidőben a Google kiadta a Native Client technológiát, aminek segítségével weblapok vagy böngészőkiegészítők tudtak natív kódot hatékonyan futtatni a böngészőben. Így született egy kolléga/barát segítségével a Zombie Browser kiegészítő jelszótörő modulja. A lényege, hogy a gyanútlan felhasználók, akik egy ilyen funkcionalitással rendelkező kiegészítőt telepítenek, a számítógépes processzorkapacitásukat átadják a kiegészítő fejlesztőjének, aki elosztott jelszótörésre tudja használni az akár többszázezer számítógépet. Ezt a teszt-példakódot végül az antivírus-gyártók is elkezdték használni felkészülésként, ha valaki ezzel a technológiával szeretne visszaélni.

Ezenkívül, mivel a böngészők a weboldalak HTML nyelven megírt kódját értelmezik és jelenítik meg, ezért a forráskódba beszúrt olyan parancsokat vagy miniprogramokat is értelmezik és lefuttatják, amelyekről a felhasználónak nincs is tudomása, mivel magában a weboldal megjelenítésében ez nem okoz – közvetlenül látható – változást. Ha egy hacker feltör egy weboldalt, és ki akarja használni a weboldal népszerűségét arra, hogy gyanútlan felhasználókat fertőzzön meg, akkor az oldal forráskódjába beszúr egy olyan kis miniprogramot (scriptet), ami a weboldalon nem látszódik, de a böngésző értelmezi, és egy másik oldalról elkezd vírust telepíteni a felhasználó gépére. Ha a támadónak sikerül egy hirdetéssel vagy egyéb aktivitással nagyobb számú látogatót az oldalra csalni – akik emiatt nagyobb arányban fognak megfertőződni, akkor ezt a támadást itatóhely „watering hole” néven szokták emlegetni (a sivatagban az itatóhoz, víznyerő helyhez nagy tömegben érkező vadállatokra és az itt rájuk támadó ragadozókra utaló hasonlóság miatt). Ez a támadás addig folyhat, amíg valaki nem szól az oldal gazdájának erről, vagy a böngészők feketelistára nem teszik az oldalt, és jelzik a felhasználónak, hogy az oldal rosszindulatú programot terjeszt. Az ilyen fertőzés ellen a legjobb módszer a naprakész vírusirtó program, amely már letöltés előtt, vagy közben megfogja a kártevőt, és figyelmezteti a felhasználót. Sajnos ilyen fertőzési próbálkozással bármilyen weboldalon összefuthatunk, egy papírbolt weboldalától az iskolai

weboldalakon át egy magánszemély privát oldaláig bezárólag. Nem kell, hogy illegális vagy felnőtt tartalmakat megosztó oldalakra látogassunk.

Az internethasználat biztonsága alapvető fontosságú digitális értékeink védelméhez. Nagyon fontos tudatában lenni annak, hogy bizonyos online tevékenységeket (vásárlás, pénzügyi tranzakciók, internetes bankolás, internetes számlafizetés) csak biztonságos weboldalakon szabad végrehajtani. Meg kell tanulni azt is, hogy hogyan ismerhetjük fel a biztonságos weboldalakat jelölő elemeket, mint például a https-előtag és a zár-szimbólum. Az internetes vásárláskor, tranzakciók generálásakor számos esetben űrlapokat kell kitöltenünk, ahol lehetőség van a megfelelő engedélyezési, tiltási, automatikus kitöltési, automatikus mentési beállítások kiválasztására.

A magánélet védelme érdekében fontos – főleg nyilvános helyeken elhelyezett gépek közös használata esetében (pl. internet-kávézó), hogy megtanuljuk, hogyan kell személyes adatainkat törölni a böngészőből, különös tekintettel a böngészési előzményekre, könyvjelzőkre, ideiglenesen tárolt internet fájlokra, az elmentett jelszavakra, sütikre, és az automatikusan kitöltött űrlap-adatokra. Ez akkor is fontos, amikor ilyen helyeken a webalapú levelezőfiókunkat használjuk. Illetve alapszabályként érdemes alkalmazni, hogy nyilvános interneten (nyílt hozzáférési pontokon) sose indítsunk érzékeny tranzakciókat, azokkal várjunk, amíg biztonságos hálózaton leszünk (pl. VPN, internet bank, bankkártyás vásárlás stb.)[35].

5.4.3 A látogatott oldalak biztonsága

A WWW tulajdonképpen elkülönített dokumentumokat fog össze hálózatban. Linkek (kereszthivatkozások) segítségével fogalomról fogalomra, dokumentumról dokumentumra, weboldalról weboldalra lehet ugrani. A WWW világszerte felkínálja a legkülönbözőbb jellegű információkat, szövegeket, képeket, grafikákat, hangokat, videókat, az emberiség csaknem összes digitalizált tudása elérhető a weboldalakon keresztül. És ez – nap mint nap – többszázezer oldallal, egyes kutatások szerint 200.000-250.000 új oldallal is bővül[36]. A nyomtatott sajtó (kiadók), nyomtatott publikációk, egyetemek, magánszemélyek, múzeumok, nemzeti és nemzetközi szervezetek, egyesületek, vállalatok stb. is kínálnak számtalan információt.

26. ábra: Uniform Resource Locator - URL

[35] Lásd a Biztonságos internetes fizetés fejezetet is.
[36] https://siteefy.com/how-many-websites-are-there/

Minden weboldalnak van egy neve, az úgynevezett URL (Uniform Resource Locator), amit böngészővel lehet elérni, azaz a böngésző címsávjába kell beírni. A névhez egy IP-címnek is kell tartoznia, ami alapján a hálózati kapcsolat létrejöhet. Az URL áll egy protokoll-megnevezésből (ha titkosítatlan a kapcsolat akkor „http://", ha titkosított – secure – akkor „http**s**://" – mint a képen is), egy domainnévből (njszt.hu vagy www.njszt.hu) és egy oldalnévből (index.html), amely azonban nem minden esetben jelenik meg.

A nevek és címek összerendelését segíti a **DNS**, Domain Name System, magyarul a domainnév-rendszer [l]. A DNS rendszer a domaineket (tartományokat) kezelő, a világon több ezer szerverre elosztott hierarchikus adatbázis-rendszer. Ezek a domainek vagy tartományok úgynevezett zónákra vannak felosztva, ezekért egymástól független adminisztrátorok a felelősek. A nevek rendezése a múltban nagyon szigorúan kötődött a **DNS-végződés**hez, így például egy „valami.university.edu" névből azonnal lehetett tudni, hogy ez a szerver az Amerikai Egyesült Államokban van és egy oktatási intézmény áll mögötte. Hasonlóan a fenti példa „.hu" végződése egyértelműsítette, hogy egy magyarországi (Hungary) domaint takarhat csupán. Az egyes tartományokat (pl. .hu) felosztották zónákra (pl. ecdl.hu), ahol minden egyes IP-címet a zóna-felelős menedzsel, és rendeli hozzá a megfelelő tartományokhoz. A zónába a tartományon keresztül vezet az út, tehát a rendszer lelke a legfelső szintű tartományvezérlő szerverek összessége. Aki ide nincs bejegyezve – közvetlenül vagy egy zónán keresztül, azt nem lehetséges névvel megtalálni (pl. www.ecdl.hu), csak közvetlenül az IP-címén szólítható meg (pl. IPv4 esetében 193.225.14.73 vagy IPv6 esetében 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Ez nyilván sokkal kényelmetlenebb megoldás.

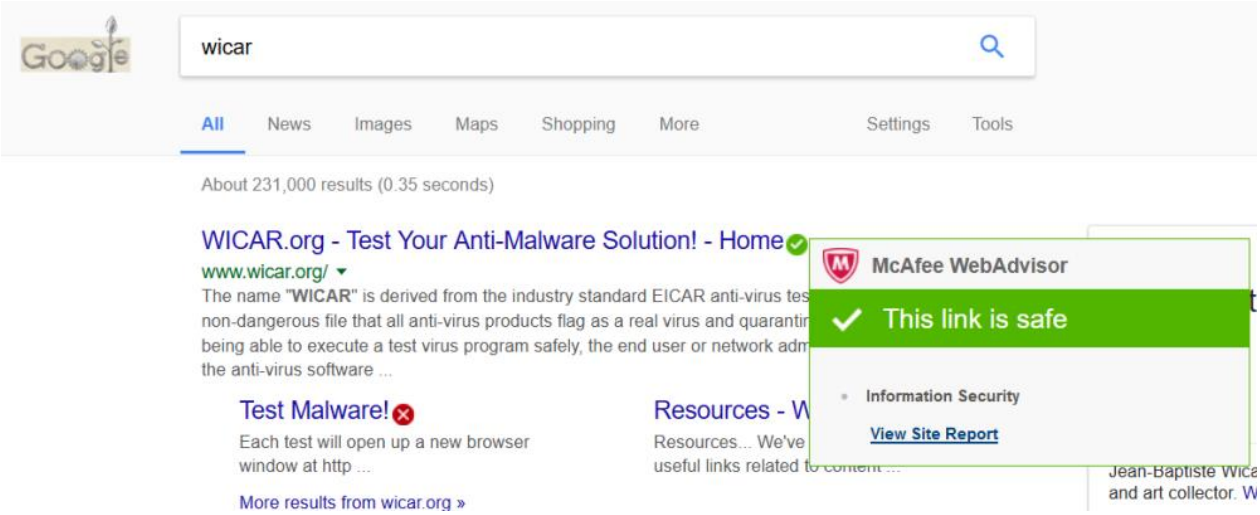
A TLD – Top Level Domains, azaz a felsőszintű tartományok végződéseinek köre évről évre bővül. 2015 februárjától lehet az „.onion" végű tartományokra is SSL-tanúsítványt kiadni, 2019-ben pedig megjelentek olyan domain végződések is, mint a „.monster", „.baby", „.OOO", illetve „.realestate", „.insurance" vagy „.shopping".

Ezen újfajta domainvégződések kiválóan alkalmasak arra, hogy adathalászathoz használják őket a csalók. Hiszen általában a felhasználók, ha a domainnevet ismerősnek találják, akkor már nem fordítanak figyelmet a domainvégződésre, ami adott esetben egy teljesen más – csaló, adathalász oldalt is takarhat. Például, ha a nem létező Balatonszöszmösz település weboldala a „balatonszoszmosz.hu", akkor el tudnánk-e dönteni, hogy a „balatonszoszmosz.business" oldalon szereplő teljesen ugyanolyan weboldal bejelentkezési oldal hamis-e vagy igazi?

A World Wide Web-en a Hypertext Markup Language (HTML) dokumentumnyelvet használják. Ennek alkalmazásával lehet kereszthivatkozásokat (linkeket) készíteni más

dokumentumokhoz, valamint tetszés szerinti nagyszámú képet, filmet, vagy hangot mellékelni. A HTML-adatokat többnyire a HTTP (Hypertext Transfer Protocol) kommunikációs protokoll segítségével közvetítik.

A támadók jellemzően az internet kevésbé ellenőrzött részein bújnak meg, **álweboldal**akat készítenek (amelyek a megszólalásig hasonlítanak az eredetire, de mögöttük már a támadó áll), illegális tartalmakat árulnak, vagy rosszindulatú programokat, szkripteket (parancssori programok), linkeket szeretnének letölteni vagy letöltetni a felhasználó gépére, és egyébként is, szeretnének a mások számítógépei és adatai felett tulajdonosi jogköröket gyakorolni, jogosulatlanul. A káros tartalmaknak azonban vannak olyan jellemzőik, amelyeket a védelmi programok képesek többé-kevésbé beazonosítani, és a felhasználót erre figyelmeztetni. Az egyik ilyen védelmi szolgáltatás a McAfee cég „WebAdvisor"-ja vagy a Norton „Safe Search" funkciója. Mindkét szolgáltatás a weboldalakat minősíti, és a minősítés alapján tanácsokkal látja el a felhasználót az oldallal kapcsolatosan.



27. ábra: McAfee WebAdvisor – a megbízható weboldalakért

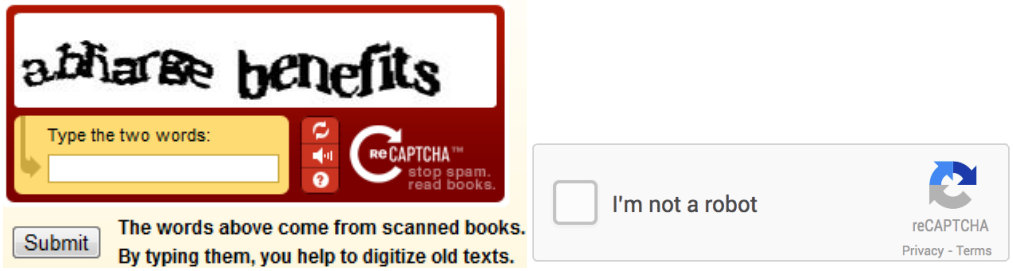
Például egy online pénzügyi tranzakció elvégzésekor, vagy személyes adataink megadásakor, azonosító és jelszó megadásakor a weboldal biztonságának biztosításához ragaszkodni kell. Ennek leggyakoribb eszköze a biztonságos böngészés, a "https" (secure http) protokoll használata. Ma már a keresőoldalak is "https" csatornán keresztül érhetőek el, ugyanakkor számos keresési eredmény (weboldal) még mindig "http", azaz nem titkosított csatornán tekinthető meg. Ezzel szemben szinte minden online bank, online webáruház ma már csak a biztonságos weboldalt jelző "https" előtaggal érhető el. A biztonságos webhasználatot számos más funkció is támogatja. Például nagy segítség a felhasználónak, ha a böngésző

automatikusan ellenőrzi a weboldal tanúsítványának megbízhatóságát és az ellenőrzés eredményét színkóddal jelzi (zöld pipa jelzi azt, ha a böngésző mindent rendben talált, sárga szín jelzi, ha nincs minden rendben, és piros szín esetében pedig erősen javasolt a weboldal meglátogatásától tartózkodni). A biztonságot erősíti az is, ha az internetbank pár perc üresjárat után megszakítja a kapcsolódást (időtúllépés), ez megnehezíti egy esetleges lehallgató dolgát is.

28. ábra: Biztonságos weboldal jele, a lakat ikon

A **biztonságos weboldal** jele a lakat-ikon (a színe, megjelenítése böngészőnként változik), egy lezárt lakat jelzi azt (a „https"-en kívül), hogy itt most titkosított forgalomról van szó a webszerver és a felhasználó számítógépén futó böngésző között[37].

Szintén az automatizált támadások elleni védelemre szolgál a „**captcha**" [m]. Ez a mozaikszó a „**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part" hosszú kifejezésből ered, ami gyakorlatilag annyit tesz, hogy hogyan tudja megkülönböztetni egy számítógép a hozzá forduló embert egy másik (esetleg támadó szándékú) programtól („Nem vagyok robot."). Leggyakrabban egy olyan módon eltorzított szöveg felismerését jelenti, mely meghaladja egy számítógépes program képességeit, de nem okoz gondot az embernek.



29. ábra: Captchák

Ezen kívül léteznek más típusú captcha-k, például amelyeken képeket kell megjelölni bizonyos szempont szerint. Például "válaszd ki azokat a képeket, amelyeken közlekedési táblák/autók/épületek/stb. vannak".

[37] A titkosított csatorna szükséges, de nem elégséges feltétele a biztonságos kommunikációnak, ugyanilyen fontos arról meggyőződni, hogy akivel kommunikálunk, az valóban az, akinek látszik, és nem egy hamis weboldallal létesítettünk titkosított kapcsolatot.

5.4.4 Aktív tartalmak és a biztonság

A legtöbb böngésző alapbeállításként lehetővé teszi olyan funkciók végrehajtását, amelyek a látogatott oldalakon elrejtve vannak jelen, vagy interaktív, esetleg animált tartalmat jelenítenek meg. Az ilyen rejtett programrészeket „szkripteknek", az interaktív/animált tartalmakat pedig „aktív tartalmaknak" nevezzük. A legismertebbek a sütik (cookie), Java-appletek, ActiveX Control-ok, JavaScript, Visual Basic Script és a Flash.

- Sütik: a sütik (cookie) a korábbi felhasználói történések, a böngészési állapotok megőrzését és reprodukálhatóságát biztosítják a webes böngészés során. A sütik által rögzíteni kívánt információkat a webszerver határozza meg. A sütiket mind a webszerver, mind a böngésző eltárolja. Ennek eredményeként egy későbbi bejelentkezést követően a felhasználó ott tudja folytatni például a webáruházi kosarának feltöltését, ahol abbahagyta. A sütik megkönnyítik a böngészést, de felvetnek néhány biztonsági problémát is. Egyrészről a sütik révén a webszerver gazdája rögzítheti tevékenységeinket az adott webszerveren. A sütik tetszőleges adatokat képesek elraktározni, ideértve a látogatott weboldalak címeit, azokat a kulcsszavakat, amelyekre kereséseket indítottunk és képesek eltárolni a különböző weboldalakon történő bejelentkezéseink adatait is a jelszavainkkal együtt. Ebből következik, hogy ha egy támadó hozzáfér a gépünkhöz és ki tudja olvasni a böngészőnk által eltárolt sütikből az adott weboldalhoz tartozó jelszavainkat – amennyiben azokat nem, vagy gyengén titkosítva tartalmazza a süti, akkor azokat máris fel tudja használni.
- Java appletek: a Java egy univerzális programozási nyelv, amit a Sun Microsystems eredetileg házi készülékek irányítására fejlesztett ki, azonban nagyon hamar elterjedt programozási nyelvvé vált az alkalmazások minden területén. Minthogy a Java független a hardvertől és az operációs rendszertől, nagy népszerűségnek örvendett, és a fejlesztők mindig hozzáigazították a mindenkori új igényekhez. Ma már az Oracle fejleszti tovább. A Java programok azon különleges fajtáját Java appleteknek nevezzük, melyeket a weboldalakba be lehet illeszteni, ami a weboldal meglátogatásakor letöltődik a felhasználó gépére. Java alapú megvalósítást használhatnak például a képgalériák, online játékok stb.
- ActiveX: a Microsoft az ActiveX-et a Java konkurenciájaként fejlesztette ki, ebben a funkciókat szorosan a Windows operációs rendszerekhez igazították, így más operációs rendszerek ezeket a lehetőségeket nem is tudják használni. Az olyan ActiveX elemeket, amelyek aktív tartalmakként beilleszthetők a weboldalakba, ActiveX

vezérlőknek (ActiveX Control) nevezzük. Fontos tudni, hogy az ActiveX program a bejelentkezett felhasználó gépén teljes jogosultsággal működik, minden korlátozás nélkül.

- Javascript: a JavaScriptet a Netscape fejlesztette ki aktív tartalomként való alkalmazásra a weboldalakon. A JavaScript a Jáván alapuló script nyelv, olyan programozási nyelv, amely a felhasználónál szövegformában van jelen, és külön e célra alkalmazott értelmezőprogram (interpretáló) által lehet alkalmazni. Alkalmazható például űrlapok kitöltésének ellenőrzésére, látogatottság számlálásra vagy képek cseréjére (ha ráviszem az egér mutatóját egy képre, akkor egy másik jelenik meg). Fontos veszélye, hogy lehetővé teszi ActiveX Control-ok aktivizálását, amelyeket már egyszer a számítógépre telepítettünk, és ezáltal ugyanolyan jogokkal bírnak, mint a helyi telepítésű program.
- VBScript: a VBScript ugyancsak a Microsoft által kifejlesztett programozási nyelv, amely a Visual Basic programozási nyelvre támaszkodik és szorosan kapcsolódik a Windows operációs rendszerekhez. VBScripttel is ki lehet egészíteni a weboldalakat aktív elemekkel. Mindenesetre az Internet Explorer az egyetlen böngésző, amely kiegészítők nélkül képes a VBScriptet a weboldalakon működtetni. Szintén képes ActiveX vezérlésére.
- Flash: 1996-ban vezette be a Macromedia (jelenleg az Adobe) a flash-technológiát, ami nagyon gyorsan teret hódított. Egy időben rendkívül sok weboldalon volt flash alapú tartalom, mára azonban ez a technológia egyre kevésbé népszerű, elterjedtsége jelentősen csökkent. A Flash alapvetően egy grafikai szerkesztő, amely animációt és interaktivitást is lehetővé tesz. Ezzel együtt a felhasználók gépein a flash lejátszását lehetővé tévő Flash Player továbbra is elérhető, ha azt nem törölték le közben. Amennyiben még az Adobe Flash Player fut a gépen, a támadók a lejátszóprogramok biztonsági réseit is kihasználhatják, hogy az áldozat gépére valamilyen káros programot telepítsenek, vagy az áldozat gépéről információkat szerezzenek. Az Adobe 2020. december 31-i dátummal megszüntette a Flash támogatását, egyúttal erősen ajánlja, hogy a Flash Player alkalmazásokat távolítsák el a felhasználók az eszközeikről.

Fordítsunk kiemelt figyelmet az aktív tartalmakat megjelenítő programjaink frissítésére az automatikus frissítés beállításával a számítógépeinken és okoseszközeinken is, mivel időről időre ismertté válnak olyan sérülékenységek, amelyek ezekre a programokra vonatkoznak. Mivel ezek a programok gyakorlatilag milliónyi felhasználó gépén futnak, potenciális célpontjai az internetes támadásoknak, vírusoknak. Ha sérülékeny verziót használunk – például

egy régi Adobe Flash Playert, akkor ennek sérülékenységeit kihasználva egy támadó kémprogramot vagy egyéb kártékony kódot telepíthet a számítógépre. Telepítéseken kívül egyszeri beavatkozásokat is végre lehet hajtani aktív tartalmakkal egy weboldal látogatása során, amelyek kétségkívül károsan hathatnak a felhasználó adataira. Hálózatbiztonsági szempontból ezért csak azt tudjuk tanácsolni, hogy az aktív tartalmakat elvből kapcsoljuk ki, vagy korlátozzuk (például Firefox böngészőben a „NoScript plugin" beállításával). Ennek hatására a felhasználó ugyan veszíteni fog valamit a kényelemből, tudniillik sok weboldal úgy van elkészítve, hogy csak akkor lehet őket rendesen megjeleníteni, ha az aktív tartalmak engedélyezve vannak, ellenben a biztonsági szint növelve lett ezáltal, ami mindenképpen a nyereség oldalon fog megjelenni a jövőben.

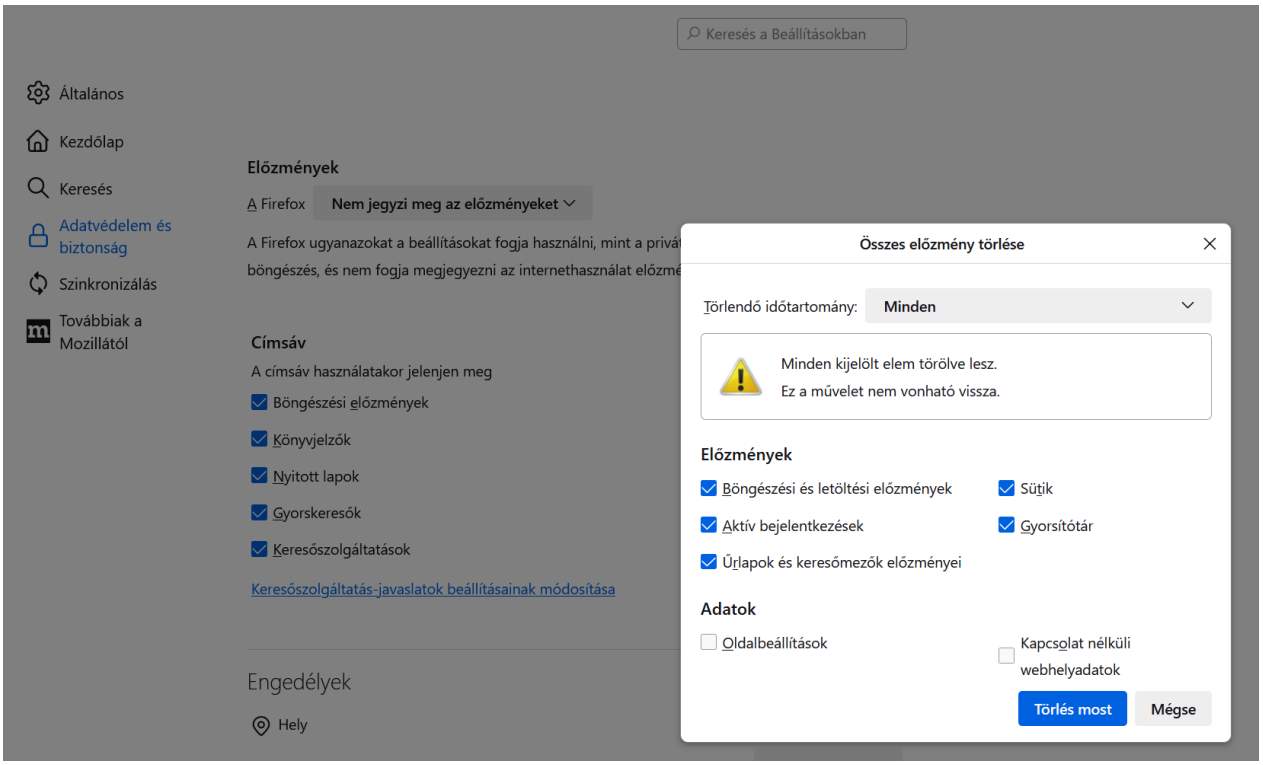
5.4.5 A böngészőben tárolt adatok biztonsága

Böngészés során – akár tudunk róla, akár nem – számos adat és szokás naplózódik a meglátogatott oldalak kapcsán.

- előzmények: a meglátogatott oldalak listája időrendi sorrendben,
- űrlapadatok: a böngészés során kitöltött űrlapok elmentett adatai (ideértve egy bejelentkezési ablak felhasználói név megadásának dobozkáját is), különösen akkor, ha az automatikus kiegészítés funkciót engedélyeztük,
- sütik: a látogatott oldalakkal kapcsolatos olyan személyes információk, melyek a webszerveren és a saját gépünkön is eltárolódnak a böngészési adatok dinamikus kezelése, későbbi felhasználhatósága érdekében,
- jelszavak: a bejelentkezések megismétlését megkönnyíti, ha a jelszó beírását követően elfogadjuk a böngésző azon javaslatát, hogy elmenti az éppen most beírt jelszót – de ez egyben kockázatot is képez, ha ennek tárolása nem megfelelően történik.

Az **automatikus kiegészítés** funkció használatával az űrlapok kitöltése egyszerűbbé és gyorsabbá válik, hiszen nem kell minden egyes esetben begépelnünk a teljes szöveget, mert a böngésző az előzetesen eltárolt adatokból az első pár karakter leütése után automatikusan felkínálja az oda illeszkedőket, legyen az bejelentkezési név, bankszámlaszám vagy e-mail cím. Az automatikus kiegészítés használata tehát jelentősen felgyorsíthatja egy-egy ismétlődő adatbevitelt is tartalmazó online űrlap kitöltését. De fontos arra is odafigyelni, hogy a böngésző által ez az adat törölhető is egyben, hiszen a tárolása veszélyeket is rejt magában. Ezeket az adatokat időnként javasolt a magánszféra védelme érdekében törölni,

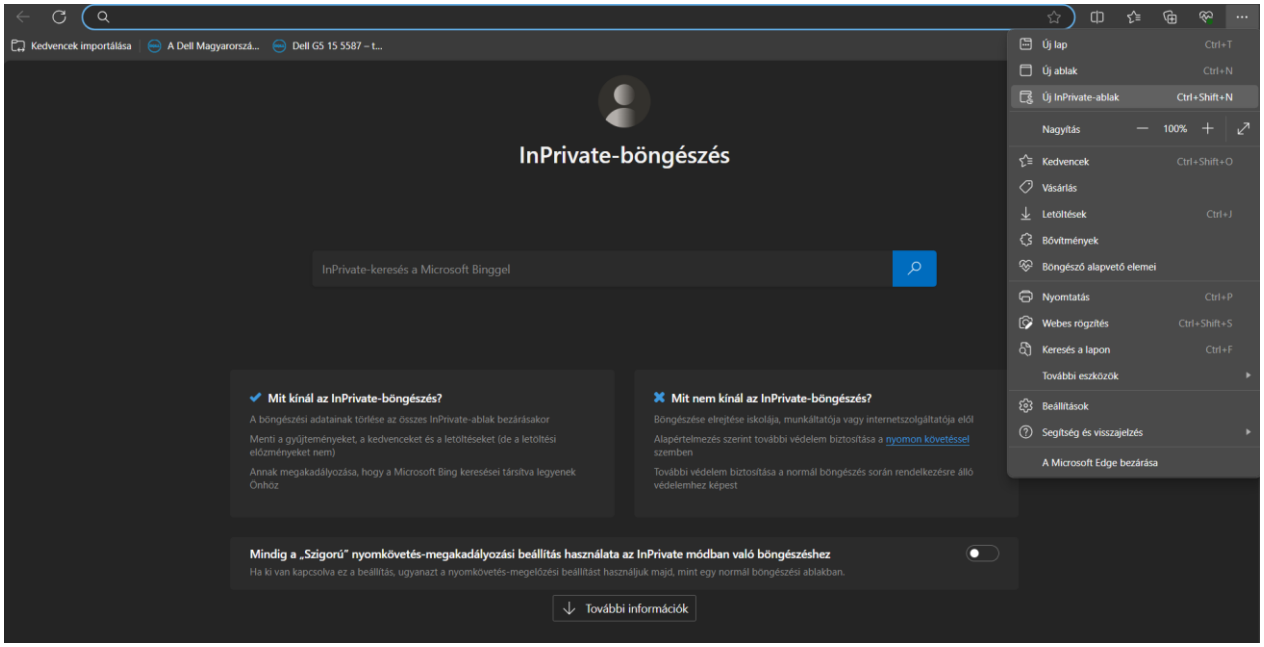
különösen akkor, ha nem a saját számítógépünkön internetezünk, hanem például egy internet-kávézóban levő gépen, közösen használt felhasználói név alatt.



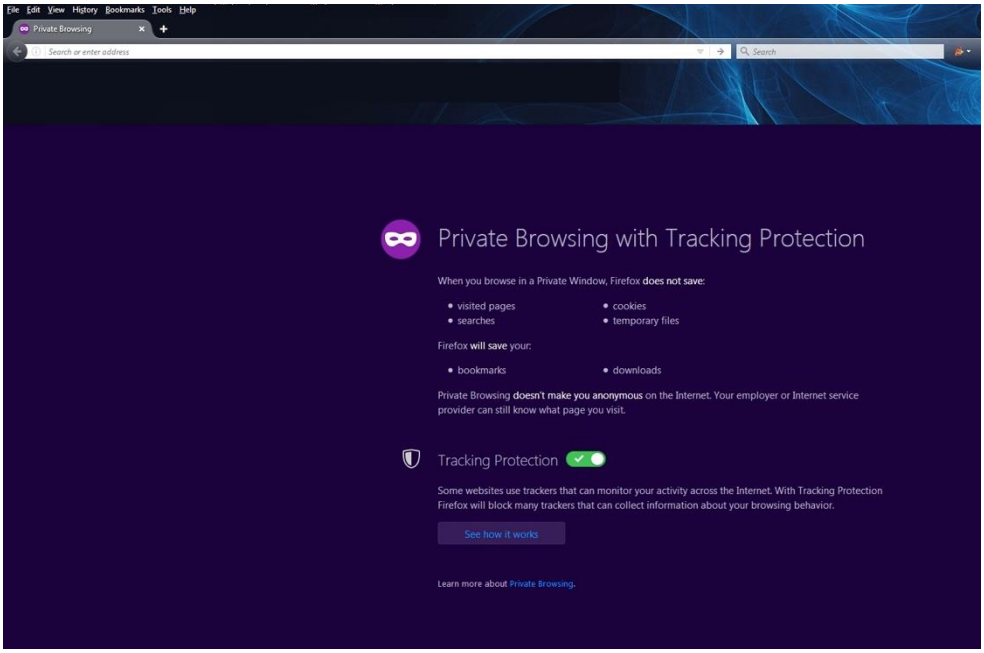
30. ábra: Böngészési adatok törlése Firefoxban

A böngészőben eltárolt személyes adatok törlését időről-időre javasolt elvégezni – amennyiben a tárolt jelszavak mindegyikére emlékezünk vagy más helyen (pl. jelszógenerátor programban) is megvannak. Különösen fontos a böngészési adatok törlése nyilvános internetes állomásokon vagy több személy által használt közös felhasználói fiókok esetében, de az otthoni gépünkön sem árthat.

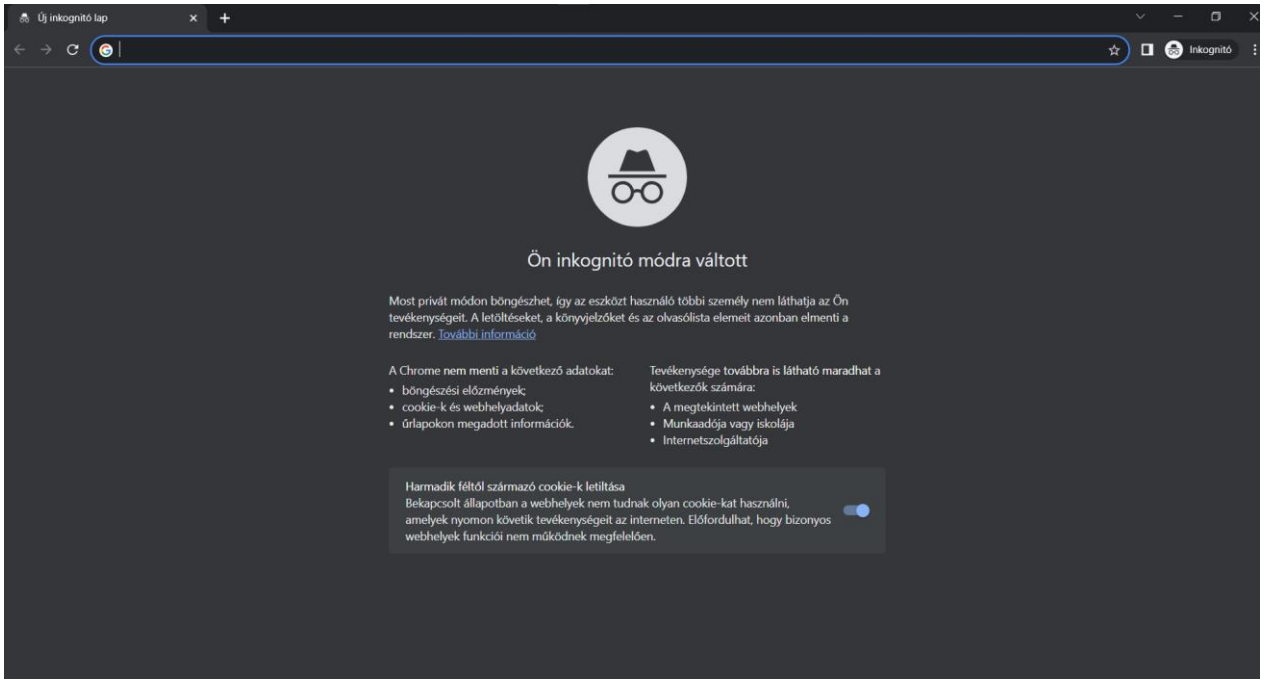
Az összes népszerű böngészőben megtalálható már olyan üzemmódú böngésző ablak, amelyet használva, a böngészett weboldalak adatai (sütik, url-ek, látogatott oldalak, kitöltött form-ok adatai, jelszavak stb.) nem tárolódnak el. Ezeket böngészőnként máshogy hívják. Az alábbi képeken az Microsoft EDGE (InPrivate böngészés), a Firefox (Private browsing) és a Chrome (Inkognitó mód) biztonságos böngészési ablakait láthatjuk.



31. ábra: Inprivate böngésző üzemmód Microsoft EDGE



32. ábra: Privát böngészés Firefox böngészőben



33. ábra: Inkognitó üzemmód Chrome böngészőben

5.4.6 Bizalmassági eszközök közösségi oldalakon

A közösségi oldalak terjedésével nagyon sok információ, személyes adat kikerülhet a nyilvános – bárki által elérhető – hálózatra, a nem megfelelő beállítások vagy az automatikus alapértelmezett beállítások következtében. Fontos megérteni, hogy bizalmas információkat közösségi oldalon miért nem szabad közzétenni, és hogyan kell azoknak a védelmi beállításait megvalósítani, valamint folyamatosan kontrollálni.

A közösségi oldalakon történő kontrollált és végiggondolt megjelenés azért is fontos, hogy a lehetséges veszélyeket képesek legyünk elkerülni, úgymint internetes zaklatás (cyber bullying), szexuális kizsákmányolás (grooming), félrevezető/veszélyes információk, hamis személyazonosságok, csalárd linkek vagy üzenetek használatából, elfogadásából adódó károk.

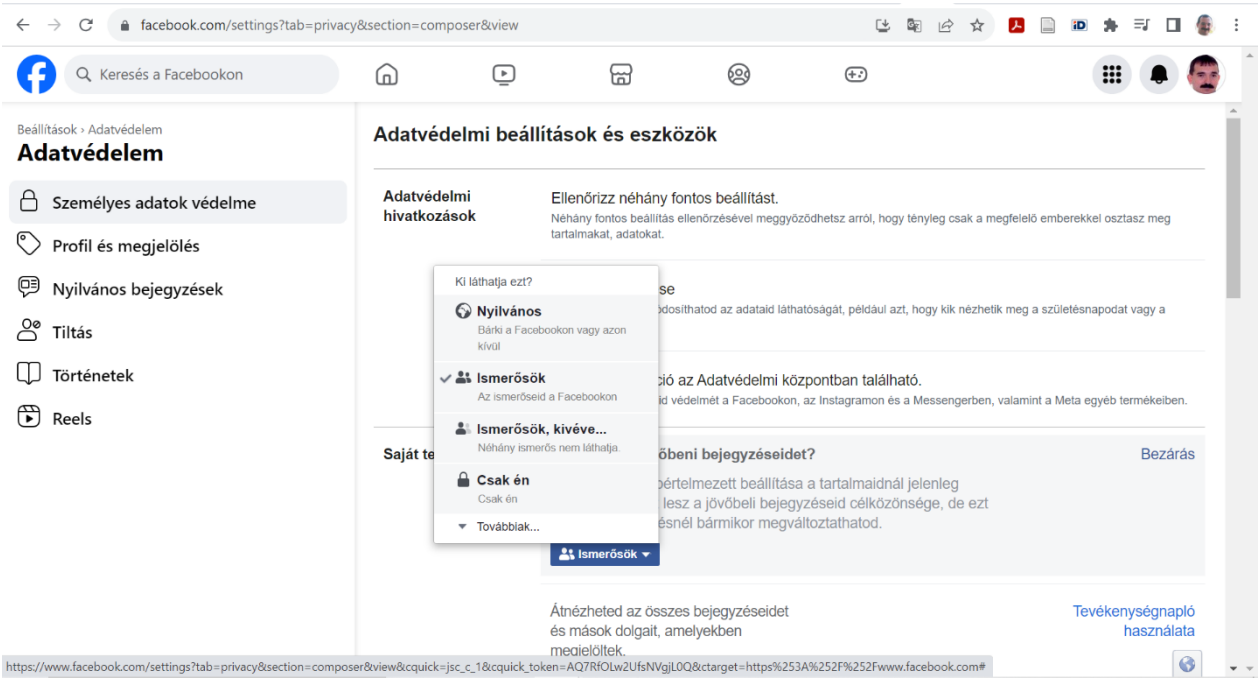
Nagyon könnyen a bizalmunkba férkőzhetnek a támadók akkor, ha olyan bensőséges adatokat adunk meg a közösségi hálózatokon, mint például a becenevünk, de fizikai közelségbe is kerülhetünk velük, ha a nyaralási dátumunkat a lakcímünkkel együtt hozzuk nyilvánosságra. Tekintettel arra, hogy a virtuális támadók potenciális száma jóval nagyobb, mint a valós térben várható támadók száma, a kockázat ennek megfelelően számítható.

Ilyen veszélyt kevésbé rejt a zenei érdeklődés és a kedvenc televízió műsor megadása, mivel ezek egyrészről több helyről hozzáférhető adatok, másrészről többek által megismerhető adatok, mint a becenév. Egy szexuális bűnöző számára megkönnyítheti a szexuális kizsákmányolás előkészítését minden apró információ, amit megadunk a közösségi oldalakon, ez egy ismert és nagyon veszélyes fenyegetés itt.

Az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk az, hogy a személyes adatokat bárki megnézheti, a keresőprogramok beindexelik és akár vadidegenek számára is megjelenítik, mint keresési találatok. A közösségi média használatakor nemcsak azok olvashatják adatainkat, akik barátságosan viseltetnek irányunkban, hanem azok is, akiknek esetleg valamelyik megnyilvánulásunk nem tetszik, és ezt **internetes zaklatás**ban fejezik ki.

Ezt elkerülni – illetve a kockázatait csökkenteni – három módszerrel lehet:

- barátaink megválasztásánál óvatosan járunk el vagy a kellemetlen barátot töröljük, és
- az adatvédelmi beállításokat olyan szigorúan szabjuk meg, amennyire csak tudjuk, hogy a barátainkon kívül más lehetőleg ne olvashassa bejegyzéseinket és ne nézegethesse a feltöltött képeinket, továbbá
- figyeljünk arra, hogy ki léphet velünk kapcsolatba – ha nem szükséges, a közvetlen kapcsolatfelvételt ne engedélyezzük senki ismeretlennek, csak annak, akit már valaki az ismerősi körünkben – valamilyen módon – hitelesített saját ismerőseként.



34. ábra: Adatvédelmi beállítások közösségi oldalon

Az előző ábrán az adatvédelmi beállításokat és azok közül a láthatóság beállítására vonatkozó lehetőségeket mutattuk be. A közösségi oldalak számos beállítási lehetőséget kínálnak a felhasználók számára, amelyekkel javasolt élni. Az alábbi témakörök köré csoportosulnak a beállítások – például – az egyik legkedveltebb közösségi oldalon, a Facebookon:

- Ki láthatja a dolgaimat?
- Ki láthatja az ismerőseim listáját?
- Ki léphet velem kapcsolatba?
- Ki találhat rám?

A Facebookon ezen kívül számos egyéb módon is növelhetjük a biztonságunkat.

Az egyik ilyen megoldás a kétfaktoros hitelesítés használata a bejelentkezéshez. A Facebook eddig is használta ezt abban az esetben, ha szokatlan bejelentkezést észlelt. Ilyen esetben a jelszó megadásán túl egy bejelentkezési kódot is küldött, amelyet szintén be kellett gépelni, így igazolva, hogy mi vagyunk a fiók jogos használója.

A kétfaktoros hitelesítést beállíthatjuk állandó funkcióként is, ilyenkor vagy SMS-ben, vagy valamilyen más, biztonsági hitelesítő alkalmazás (Pl. Google Authenticator vagy Duo Mobile) segítségével fogunk tudni bejelentkezni. Ekkor a Facebook biztonsági kódot fog kérni

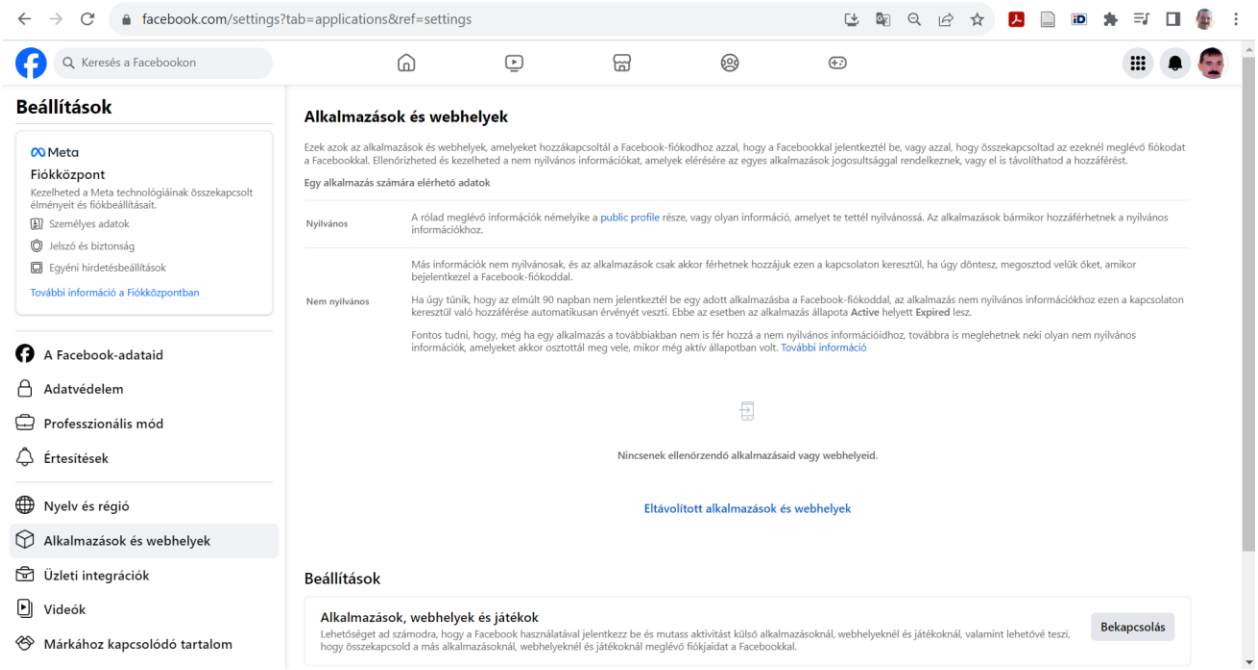
minden olyan esetben, amikor még ismeretlen készülékről vagy böngészőből kezdeményezett bejelentkezési kísérletet észlelt.

Érdemes megfontolnunk, hogy engedjük-e és ha igen milyen kontroll mellett, hogy mások is írjanak az idővonalunkra, vagy mások megjelölhessenek minket képeken.

A Facebookon számos olyan problémával szembesülhetünk, ami a Facebook-os alkalmazások használatából, pontosabban az alkalmazások túlzott jogosultságaiból fakad.

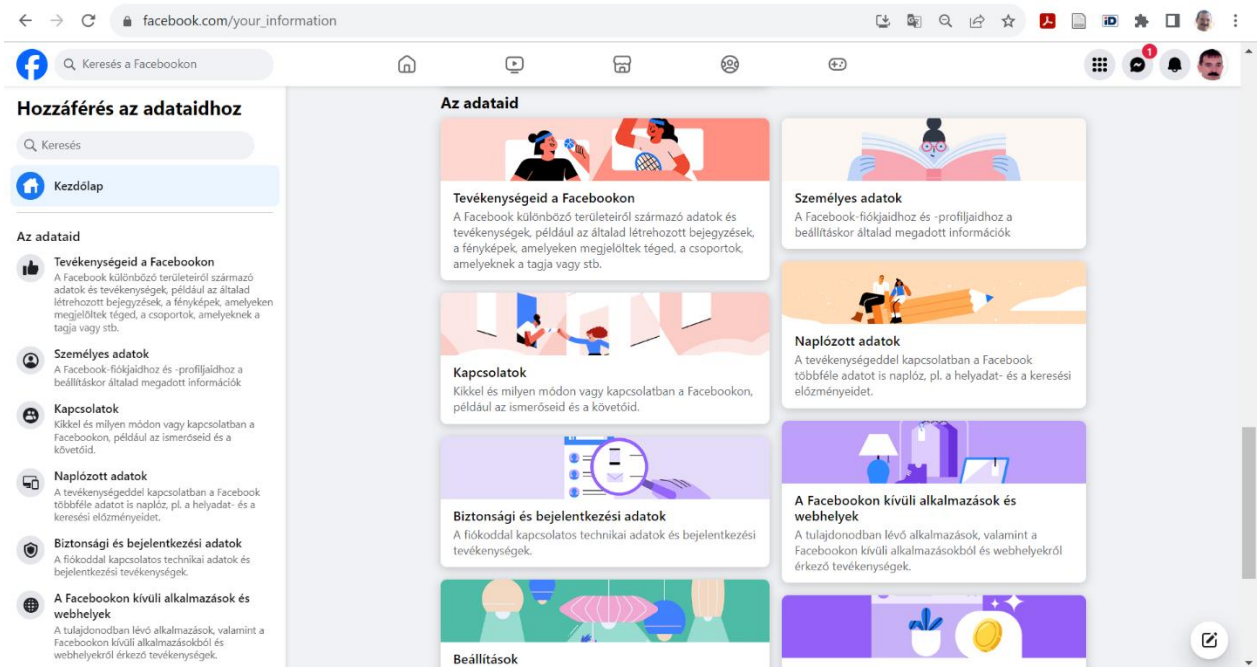
A Facebookon megtalálható alkalmazások is különböző dolgokhoz hozzá akarnak férni, például nyilvános profilunk, személyes adataink, ismerőseink, fotóink, bejelentkezett helyeink stb. Ezen kívül olyan jogosultságokkal is bírhatnak, mint például az üzenetküldés ismerőseinknek, vagy üzenetfalra írás (kvázi posztolás a felhasználó nevében). Ezek nagyon veszélyes jogosultságok, hiszen ilyenkor a felhasználó átadja a jogot az alkalmazásnak – és az alkalmazás írójának, hogy az ő nevében posztoljon, vagy írjon üzenetet. Sok esetben, ha sikerül egy ilyen jogosultságokkal bíró alkalmazást megfertőzni vírussal, akkor az pillanatok alatt terjedni kezd a Facebookon, hiszen a felhasználó azt látja, hogy milyen nagyon érdekeset írt az ismerősöm, rákattint és már ő is megfertőződött és így tovább – láncreakció-szerűen.

Amennyiben használunk facebookos alkalmazásokat időnként vizsgáljuk felül, hogy tényleg használjuk-e őket és ha nem, akkor töröljük, ha pedig igen, akkor nézzük végig, hogy mihez akar az alkalmazás hozzáférni és amit problémásnak gondolunk, azt tiltsuk le.



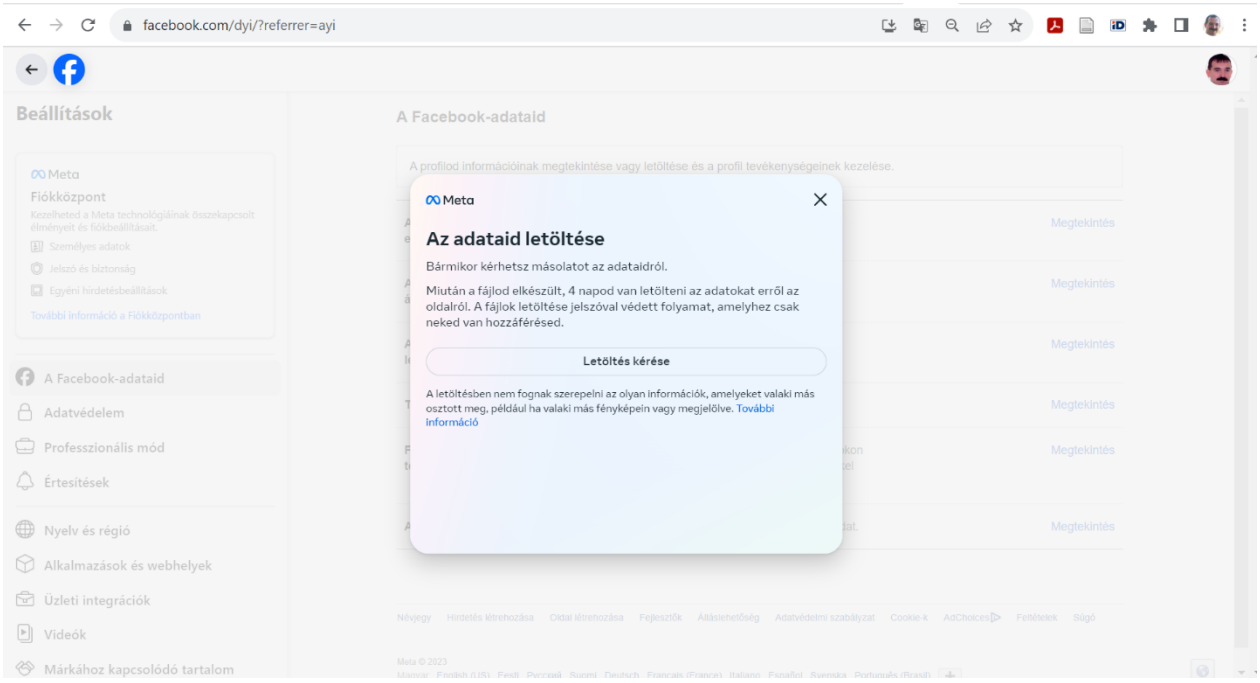
35. ábra: Facebook alkalmazások jogosultságainak beállítási helye

Ha tudni szeretnénk, hogy milyen adatokat és tartalmakat tárol rólunk a Facebook, akkor van lehetőségünk a tárolt adatok kategóriánkénti kijelölésére (a képernyőkép nem teljes, mivel a kategóriák több oldalon keresztül folytatódnak) és letöltésére a Beállítások menüben („A Facebook-adataid” menüpontban).



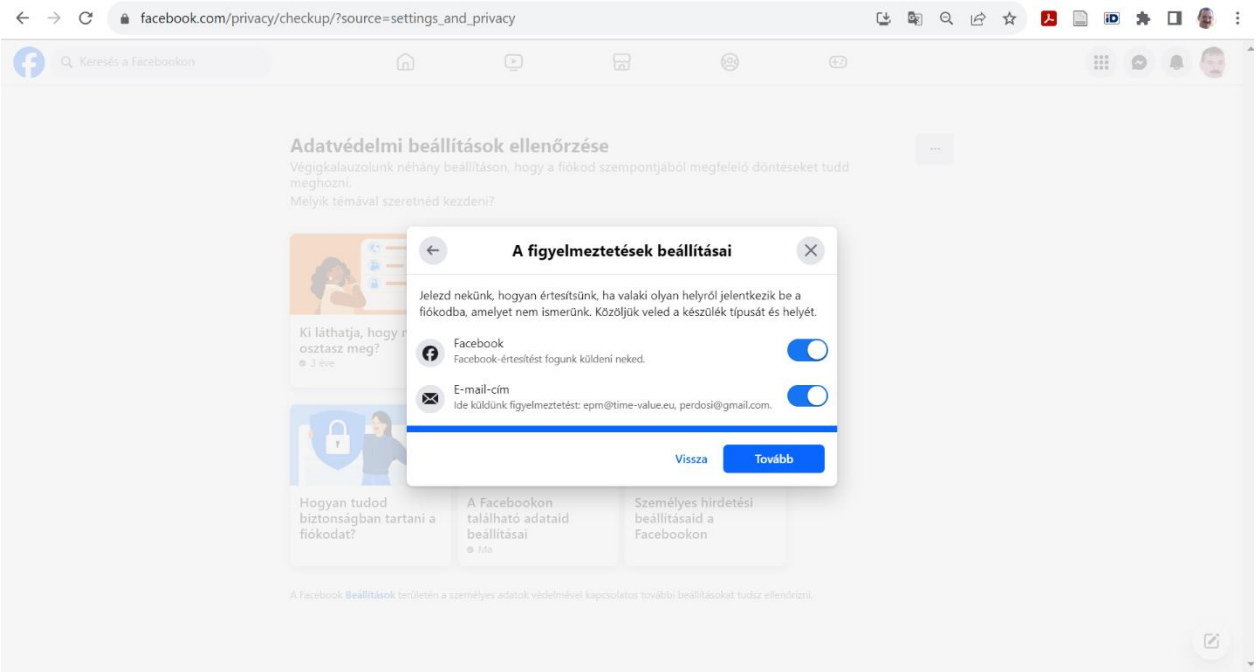
36. ábra: Facebook által rólunk tárolt adatok másolatának letöltése

Természetesen lehetőségünk van a tárolt adatokról másolat kérésére és letöltésére is. A sok képet és videót tartalmazó profiloknál azonban ez a letöltés nagyméretű fájlokat is eredményezhet, és időbe telik, míg a rendszer összegyűjti az összes adatot.



37. ábra: Facebook által rólunk tárolt adatok másolatának letöltése

A Facebook lehetőséget ad arra, hogy ellenőrizzük azt, hogy milyen eszközökről és milyen helyszínekről vagyunk bejelentkezve a fiókunkba – illetve ezt visszamenőlegesen is láthatjuk (A Tevékenységnapló menü Biztonsági és bejelentkezési adatok pontjában. Amennyiben azt tapasztaljuk, hogy olyan eszközről van aktív bejelentkezés, ami nem hozzánk tartozik, az adott eszközt el tudjuk távolítani a megbízható eszközök listájából.



38. ábra: Facebook bejelentkezések ellenőrzése

Bár a Tevékenységnapló rögzíti, hogy mi minden történt a fiókunkban, ami utalhat illegális tevékenységre, azt fontos tudni, hogy innen ki lehet törölni a bejegyzéseket – vissza lehet vonni a kedveléseket. Amennyiben itt nem általunk végzett tevékenység nyomait észleljük, akkor az előzőekben leírt bejelentkezési eseményeket érdemes átnézni, illetve – amennyiben nem többfaktoros bejelentkezést használunk – érdemes jelszót is változtatni.

5.4.6.1 Nyereményjátékok és kattintásvadászat vagy lájkvadászat

A legnépszerűbb közösségi oldalon rendszeresen megjelennek olyan oldalak, amelyek valamilyen nyereményt sorsolnak ki, és mindössze annyit kérnek a felhasználóktól, hogy lájkolják az oldalt (vagy más oldalakat, lásd a képen), osszák meg és írják oda, hogy például milyen színű autót szeretnének, ha ők nyernek.

Rengetegen gondolják úgy, hogy ez a minimális erőfeszítés megéri, hiszen megadják maguknak az esélyt, hogy nyerjenek. Valójában egész más van a háttérben. Ez a tevékenység egy nagyon egyszerű és jól jövedelmező csalási forma. Az alábbiakban leírjuk a működését.

Manapság egy jól felépített és kelendő termék vagy szolgáltatás marketing kampánya sokmillió forintba kerül és a kampány egyik célja, hogy egy termék vagy szolgáltatás Facebook oldalán minél több rajongó legyen, akiket így könnyen el lehet érni és meg lehet szólítani reklámokkal.

39. ábra: Lájkvadászat hamis nyereményjátékkal

A csalók arra jöttek rá, hogy az emberek rendkívül naívak és az ingyen nyereményért bármire képesek.

A csalók létrehoznak egy Facebook oldalt, ami lehet bármilyen néven, igazából nincs jelentősége. Meghirdetnek rajta egy nyereményjátékot, ahol faházat, utazást, drága autót, bútort, ékszert, telefont, bármilyen értékes dolgot lehet nyerni. Megfigyelhető, hogy a nyereményjáték szövegezése általában helyesírási, központozási hibákat tartalmaz, ami egy magára valamit adó cég esetében nem elfogadható, ez is egy gyanús jel lehet.

A nyereményjátékban való részvétel feltétele az oldal vagy más oldalak lájkolása és megosztása. Ezzel a módszerrel napok, rosszabb esetben hetek alatt elérik, hogy a frissen létrehozott termék vagy szolgáltatásoldal többtízezer, akár százezer követővel rendelkezzen. Természetesen a nyereményjáték nem igaz, valójában nincs sorsolás és nyertes sem. A százezres követői táborral rendelkező facebook oldalt ezután a csalók eladják. Az új tulajdonos pedig átírja a nevet, lecseréli a logot és a borítóképet és máris százezres potenciális ügyfélbázist ér el, miközben nem költött milliókat marketingkampányra.

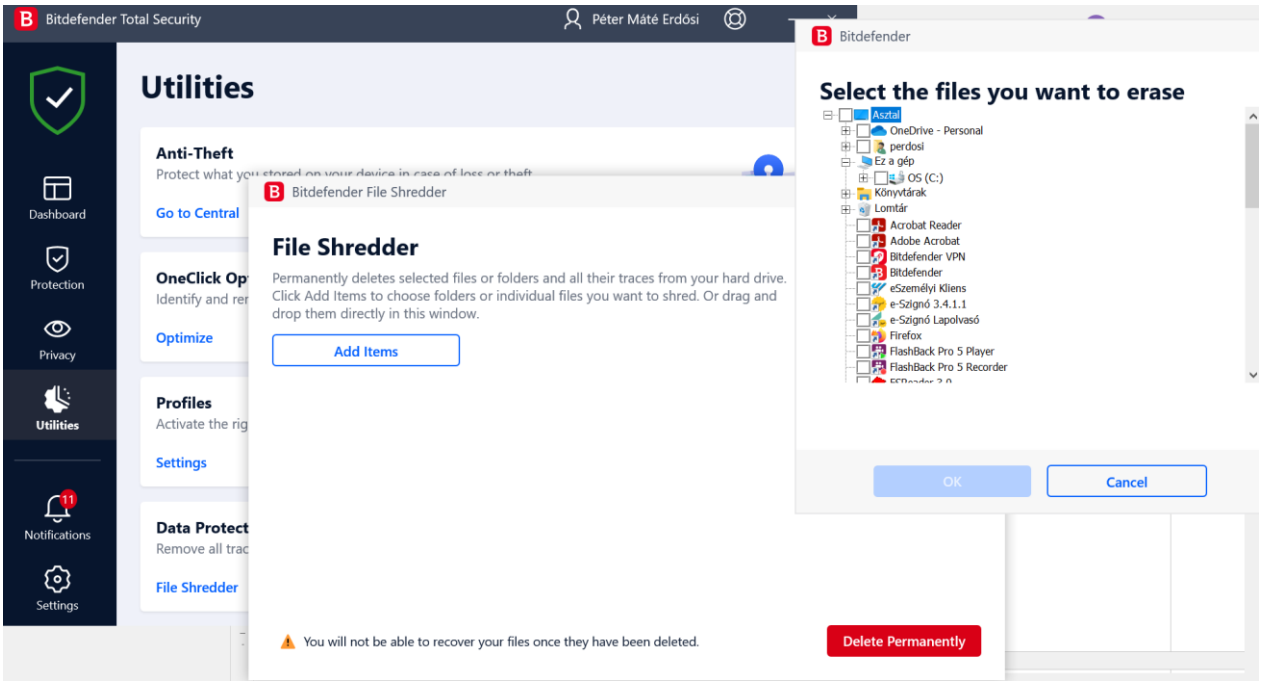
Az embereknek meg kell érteniük, hogy milliós nyereményjátékokat jellemzően nagy cégek hirdetnek, komoly feltételekkel, a saját honlapjukon is és egyéb médiafelületeken is hirdetve azt. Az ilyen Facebookon terjedő nyereményjátokok jelentős része átverés, és csak a csalók nyerhetnek rajta.

5.4.7 Az adatok végleges törlése

Az adatok visszaállíthatatlan törlésére, vagyis a **fizikai adatmegsemmisítés**re azért van szükség, hogy az adatok többé már ne legyenek visszaállíthatók, és nyugodtak lehessünk afelől, hogy a logikailag törölt adatainkban a támadók már nem kotorászhatnak értékes információk után. Erre azért van szükség, mert a számítógépes eszközökön tárolt adatokat nem törli visszaállíthatatlanul az adatok Lomtárba mozgatása (soft delete), csupán az elérésüket, kilistázásukat szünteti meg a könyvtárban. A visszaállíthatatlan törlésre egy jó módszer az adatokat tartalmazó adathordozó (CD, DVD, pendrive, memóriakártyák) **bedarálás**a, szétroncsolása fizikailag (hard delete). Ugyanígy az adatok végleges törlését eredményezi a merevlemezek **elektromágneses törlés**e (degaussing) – ami erős mágneses mező gerjesztésével tünteti el a mágnesezett adathordozókról az adatokat, gyakorlatilag felülmágnesezi azokat – ez főleg nagyvállalati környezetben érhető tetten, otthoni felhasználók esetében a merevlemez fizikai roncsolása, átfúrása, szétszerelése és roncsolása javasolt inkább. Megfelelő lehet még a **szoftveres adatmegsemmisítő eszközök** használata is, de csak akkor, ha a célszoftverek [n] többszörös felülírás alkalmazásával teszik véglegesen olvashatatlanná a korábbi adatokat.

Fontos, hogy ma már szinte minden informatikai eszköznek van saját beépített, vagy bővíthető háttértára, amely adatokat tárol el a felhasználás során. A telefonok is rendelkeznek saját memóriával és bővíthetjük őket külső memóriakártyákkal, de ugyanez van a fényképezőgépekkel, okostelevíziókkal is. Fentiek miatt fokozottan oda kell figyelni arra, hogy ezen eszközök leselejtezése vagy eladása esetén meggyőződjünk arról, hogy nem maradt a háttértárakon értékes adat. Erre jó módszer lehet fent említett adatmegsemmisítő szoftver használata majd a gyári beállítások visszaállítása.

A következő ábra a BitDefender szoftvernek mutatja be azt a képességét, hogy bármely kiválasztott fájlt képes véglegesen elérhetetlenné tenni, azaz végérvényesen törölni a merevlemezről.



40. ábra: Végleges adattörlés szoftveresen

5.5 A sértetlenségről

Az egyes fájlok, üzenetek tárolásánál vagy olvasásánál sokszor felmerülhet az a kérdés, hogy „vajon ezt tényleg az írta, akié az e-mailben látott e-mail cím?”. Máskor a tartalmak kérdőjeleződhetnek meg: „vajon tényleg ezt a szöveget küldte a Jóska?” Annak az eldöntésére, hogy az üzenet a küldés vagy tárolás során megváltozott-e, hitelességi eljárásokat lehetséges alkalmazni, melyek két kulcsfontosságú eleme a digitális aláírás és benne a kivonat.

5.5.1 Digitális aláírás

A digitális aláírás egy olyan titkosított kód, amely a titkosítást végző entitás, és a titkosított tartalom azonosságának ellenőrizhetőségét társítja ahhoz az adathoz, amelyen az aláírás létrejött, más szóval hitelesíti. A **hitelesítés** ugyanis az állított azonosság megerősítése, így a **hitelesség** az eredet és a küldő meg nem változását, illetve ennek bizonyítottságát jelenti. A digitális aláírás szabatosabban megfogalmazva egy aszimmetrikus kriptográfiai algoritmuson alapuló matematikai transzformáció, amelynek előállítási eszköze a **digitális aláírás séma** (amely tartalmaz minden algoritmust, amely szükséges az aláírás létrejöttéhez), és amely az üzenet hitelességének (eredetének és sértetlenségének) biztosítására szolgál. A digitális aláírás készítéséhez használatos aláírás-létrehozó adat (titkos kulcs) párja az aláírás-

ellenőrző kulcs (nyilvános kulcs) lesz. Ha egy digitális aláírást sikeresen ellenőriztünk a nyilvános kulccsal, akkor biztosak lehetünk abban, hogy az aláírást az ehhez a kulcshoz tartozó titkos kulccsal készítették, és az készítette, akinek ez a kulcs a birtokában volt. Hogy ez a bizonyosság egyenlő lehessen a kézi aláíráshoz kapcsolt bizonyossággal, jogszabály által erre felhatalmazott megbízható harmadik felek (minősített bizalmi szolgáltatók) készítik elő és adják át a felhasználóknak a minősített aláírások létrehozására alkalmas kulcsokat, és a nyilvános kulcsot a szolgáltatók digitális tanúsítványba foglalják az aláíró személy azonosítása és hitelesítése után. A digitális tanúsítvány ennél fogva igazolja, hogy az üzenet küldője valóban az, akinek állítja magát[38]. A digitális tanúsítványok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat is, mint például név, város, cím, személyes azonosító adat, beosztás, szervezeti egység stb. A tanúsítványok leggyakoribb alakjai az X509v3 szerinti és a PGP tanúsítványok. Az X509v3 megjelölés a nemzetközi telekommunikációs intézet által kibocsátott X.509 szabvány harmadik verziójára utal, míg a PGP a Philip R. Zimmermann által 1991-ben készített Pretty Good Privacy [o] titkosításra és hitelesítésre készített programcsomag részeként létrejött digitális tanúsítványokat jelöli.

A **digitális tanúsítvány**ok különböző célokra szolgálhatnak. Vannak aláíró, titkosító, hitelesítő, személyes, szervezeti, kódaláíró és SSL-tanúsítványok is. Mindegyik tanúsítvány felépítése ugyanolyan, a különbségek az egyes adattartalmakban és a használati célokban rejlenek. Például az **SSL-tanúsítvány** – amelynek a neve a Secure Socket Layer rövidítéséből ered – arra használatos, hogy valaki az eszközeinek birtoklását hitelesítse általuk és **biztonságos kapcsolódás**t lehessen megvalósítani ennek segítségével a védett weboldallal (lásd korábban a lakat és a „https”). A kapcsolat azért lesz biztonságos, mert titkosított, így az illetéktelen lehallgatás ellen védett.

Az aláíró tanúsítványok digitális aláírási célra szolgálnak. A tanúsítványok tartalmazzák az aláírás-ellenőrző adatot, amelyhez tartozó aláírás-létrehozó adattal készül a digitális aláírás.

A digitális aláírás elkészítésének és fogadó oldali ellenőrzésének lépései:

- az aláírandó adatokból elkészül annak fix (általában 160–512 bit) hosszúságú kivonata,
- a kivonatot az aláíró algoritmus és a titkos kulcs segítségével rejtjelezi az alkalmazás, és ez lesz a digitális aláírás,

[38] Emiatt ha rossz kezekbe kerül az aláírás-létrehozó adat, a digitális aláírás esetében nem az írásszakértő fogja tudni kimondani, hogy az aláírást nem a valódi tulajdonos készítette, hanem a kibocsátót kell értesíteni arról, hogy többé már nem a tulajdonosé az aláírás, ezt a státuszt a kibocsátó ezt követően jelzi a nyilvánosság felé. Amíg viszont ez a bejelentés nem következik be, az aláírások a tényleges tulajdonosra fognak mutatni.

- az aláírás kezdeti ellenőrzése automatikusan megtörténik,
- a digitális aláírás az adatokhoz csatolva eljut a fogadóhoz.

A digitális aláírás abban különbözik a nyilvános kulcsú titkosítástól, hogy itt a titkos kulccsal történik az üzenet aláírása, a nyilvános kulccsal pedig az aláírás ellenőrzése – titkosításnál pontosan fordítva. Az aláírás elkészítése a következő lépésekben leírtak alapján történik. Az aláíró a nyílt szövegből egy kivonat- vagy lenyomatkészítő egyirányú függvénnyel (hash function) elkészíti az üzenet kivonatát. Ezt a lenyomatot kódolja a magánkulcsával, így elkészítve a digitális aláírást. Az aláíró elküldi az eredeti kódolatlan üzenetet és az üzenetből készített kódolt lenyomatot.

Az aláírás ellenőrzését az aláírás létrehozása után a megfelelő információk birtokában utólag is el lehet végezni.

Emlékeztetve arra, hogy az aláírás készítésének utolsó lépéseként a küldő a digitális aláírást az adatokhoz csatolva eljuttatja azt a fogadóhoz, a fogadó az alábbi módon, utólagosan így ellenőrzi az aláírást:

- a fogadó az adatokból elkészít egy új kivonatot,
- a digitális aláírásból a nyilvános kulcs segítségével visszaállítja az eredeti kivonatot,
- a fogadó az új kivonatot és az eredeti kivonatot összehasonlítja, és ha egyezik, akkor az aláírás rendben van, ha nem egyezik, akkor pedig az aláírás elfogadását – alapesetben – megtagadja.

A digitális aláírás sikeres ellenőrzéséből az alábbiak következnek:

- az aláírt adatok ugyanazok, amit a küldő elküldött, menet közben nem változtak,
- az adatok aláírását a nyilvános kulcshoz tartozó titkos kulccsal végezték, és
- amennyiben a nyilvános kulcshoz létezik tanúsítvány, és tanúsítványban szereplő névhez tartozó személyt megbízható módon kapcsolták, akkor az a fizikai személy is ismert, aki aláírta az adatokat.

A digitális aláírás ellenőrzésének sikertelensége esetén az alábbiak lehetnek – a teljesség igénye nélkül – az okok:

- az adatok a küldés során megváltoztak,
- az ellenőrzéskor más kulcsot vagy algoritmust használtak,
- a tanúsítványt nem tette a fogadó még megbízhatóvá a saját rendszerében,

- a tanúsítvány lejárt,
- a nyilvános kulcshoz tartozó tanúsítvány hibás.

Az ellenőrzés sikertelensége okán kapott hibaüzenet behatárolhatja a hiba pontos okát, ami segít az aláírás ellenőrzésének sikeres megvalósításában. A megfontolt és körültekintő eljárás indokolt, mivel az érvénytelen aláírás elfogadásából adódó minden következmény az elfogadót terheli.

Hol alkalmazzák ezt a technológiát elsősorban? A programozók a fejlesztett kódokat alá szokták írni ma már digitálisan, hogy a támadók addig se tudják észrevétlen módosítani ezeket a tartalmakat, amíg eljutnak a felhasználók gépeire (kódaláírás). A telepítések előtt érdemes elolvasni azt az üzenetet, mely megmutatja a telepítendő szoftver íróját is. Másrészről a teljesen elektronikus ügyintézés nem képzelhető el másként, csak digitális aláírással, hiszen így tud meggyőződni az ügyintéző a beküldött nyomtatvány aláírójának személyazonosságáról anélkül, hogy az ügyfél személyesen is megjelenne előtte, továbbá így lehet biztosítani az ügyintézés során rögzített adatok hosszú távú hitelességét is a legegyszerűbben. Ilyen ügyintézési terület ma Magyarországon például a cégeljárás. Nemzeti és nemzetek feletti közösségek más területeken is használják már ezt a technológiát, érdemes kiemelni ezek közül az észt választási rendszert, ahol évek óta egyre növekvő mértékben választják a szavazópolgárok ezt a technológiát akaratuk kinyilvánításához[39], azonban globális alkalmazása egyelőre nem megoldott [p].

5.5.2 Kivonatok (hash-ek)

A digitális aláírások készítésénél felmerült az a probléma, hogy elviekben a digitálisan aláírandó fájlok mérete nem korlátos, illetve jelentős eltéréseket is mutathat (pár bájttól pár/sok terrabájtig is akár), így a hatékony aláíráskészítéshez szükségessé vált egy olyan eljárás közbeiktatása, mely az aláírandó adat méretétől függetlenítette az aláírási algoritmust – így őrizve meg annak hatékonyságát és alkalmazhatóságát. Ez az eljárás tetszőleges bináris adathoz egy fix hosszúságú bitsorozatot rendel egyedileg hozzá, amit az adat lenyomatának, kivonatának vagy - az angol szót átvéve - hash-énak nevezünk.

A digitális aláírásoknál felhasználható, "jó" kivonatoló, azaz hash algoritmusok az alábbi matematikai tulajdonságokkal rendelkeznek – emiatt lesznek alkalmasak a hosszú távú, biztonságos használatra:

[39] https://www.id.ee/en/article/e-voting-and-e-elections/

- Egyirányúság (pre-image resistance): ha egy adott üzenet hash értékét ismerjük csupán, akkor ebből gyakorlatilag lehetetlen legyen az üzenetet visszafejteni. Ha ez a tulajdonsága nem lenne, az aláírásokhoz utólag is lehetne üzenetet készíteni. Ez esetben nem lehetne az üzenet megváltozását felderíteni.
- Lavina-hatás (2nd pre-image resistance): adott kivonathoz és üzenethez gyakorlatilag lehetetlen olyan, az eredeti üzenettől különböző másik üzenetet találni, amelyeknek a kivonata megegyezne. Más szóval, ha bármely két üzenetet tekintünk – de például, ha veszünk egy szó kivételével teljesen azonos két üzenetet, a kivonat értékeinek (jelentős mértékben) különbözőnek kell lenniük. Az aláírásoknál ez a tulajdonság ott lesz fontos, hogy ne lehessen ugyanazt az aláírást felhasználni egy teljesen más (például a támadó által készített) üzenethez.
- Ütközés-mentesség (collision resistance): gyakorlatilag lehetetlen két olyan üzenetet találni a lehetséges üzenetek halmazában, melyeknek a kivonata megegyezik. Ez a tulajdonság fogja megvédeni az aláírást az előre megválasztott üzenetek típusú támadásoktól – amikor a támadó az előre elküldött üzenetet íratja alá, de az általa másodikként megtalált üzenetre cserélné ki az aláírt üzenetet. Erre az üzenetek halmaza és a lehetséges hash értékek halmaza méretének lényeges (sok-sok nagyságrendnyi) különbözősége ad lehetőséget.

5.6 A rendelkezésre állás megteremtése

A rendelkezésre állás megteremtése a gyakorlatban négy dolog biztosítását jelenti – hálózati környezetben:

- áramellátás a hardver számára,
- adatok és szoftverek az alkalmazások számára,
- hálózati sávszélesség biztosítása az elérhetőség érdekében, és
- végpontvédelem a működésbiztonság megőrzése számára.

Az áramellátást szünetmentes tápegységek [q] alkalmazásával tudjuk biztosítani – léteznek otthoni és ipari méretű eszközök is, egyszerűen beszerezhetők és telepíthetők. Időnként – az akkumulátorok elhasználódása miatt – cserére szorulnak, egyébként más többletfeladatot nem jelentenek és rövid távon hatékonyan védik a számítástechnikai eszközöket az áramellátás meghibásodásaitól.

A hálózati sávszélességben három tényező játszik szerepet:

- mekkora sávszélességre fizettünk elő a szolgáltatónál,
- mennyi a valós felhasználási igényünk, és
- mennyire van védve a hálózat a szolgáltatás-megtagadásos támadások ellen (DoS, Denial of Service)

A **DoS-támadás**ok kivitelezésekor a támadók valódinak látszó kérésekkel, de hibás, vagy módosított adatcsomagokkal bombázzák egy időben a szervert. De nem foglalkoznak a válaszokkal, mert a cél a folyamatos kérésekkel a szervert annyira leterhelni, hogy más felhasználók kérésének feldolgozására a szervernek ne maradjon kapacitása, így az lelassul a külső szemlélő számára, vagy megszűnik válaszolni. A leterhelés hatványozottan sikerülhet, ha hibás az adatcsomag és a szerver oldalnak több idő feldolgozni vagy mondjuk egy-egy hibás feldolgozásnál végtelen ciklusba kerül. Otthoni felhasználóknak jó hír, hogy az erre irányuló védelem megteremtése a szolgáltató feladata és nem is jellemző, hogy felhasználói gépeket támadjanak így. Sokkal gyakoribb, hogy nagyobb internetes szolgáltatásokat (közösségi oldalak, webáruházak, kormányzati szolgáltatások vagy egyéb egyedi célpontok) próbálnak meg elérhetetlenné tenni valamilyen politikai vagy egyéb érdekből, illetve zsarolási szándékkal.

A DoS támadásoknak van egy erősebb változata a DDoS (Distributed Denial of Service). Ezt a típusú támadást egy időben egyszerre több ezer, százezer, vagy millió gépről is indíthatja a támadó (akár megfertőzött okoseszközökről is). Felmerül a kérdés, hogy ki rendelkezik egyszerre mondjuk egymillió számítógép felett irányítási joggal? Ma már egyre több olyan bűnszervezet létezik, akik az otthoni felhasználók millióinak számítógépét és okoseszközeit megfertőzik trójai programokkal, amelyekkel át tudják venni felettük az irányítást a felhasználó tudta nélkül. Az ilyen módon összekapcsolt számítógépek hálózatát botnetnek (roBOT és NETwork szavakból alkotva) hívjuk. Az ilyen botneteket a támadók sokszor bérbe adják az internet sötét oldalán, a bérlők pedig arra használják ezeket a gépeket, amire akarják. DDoS támadás, SPAM küldés, jelszótörés és még számos illegális tevékenység felsorolható lenne itt. A rossz hír, hogy ilyen botneteket nem csak számítógépekből, hanem okoseszközökből (telefonok, okosTV-k, IP kamerák, okosotthon vezérlő számítógépek) is építenek már a támadók. Ennek ellenére az okoseszközök védelmével a felhasználók és a gyártók még nem kielégítően foglalkoznak, pedig fontos lenne.

DoS és DDoS támadások eredményeként a megtámadott internetes szolgáltatás nem lesz elérhető. Ha valakinek az üzleti működése múlik egy honlapon, akkor érdemes felkészülni egy ilyen támadásra. Hiszen, ha nem elérhető a webáruház például, akkor nincs bevétel.

Az alábbiakban egy olyan felületet látunk, ahol egy DDoS támadáshoz lehet bérelni felhasználók megfertőzött számítógépeit, kiiktatva például az internetes konkurenciát. Fontos tudni, hogy az ilyen szolgáltatások használata is törvénybe ütközik!

41. ábra: DDoS támadás megrendelő felület 1. rész

42. ábra: DDoS támadás megrendelő felület 2. rész

43. ábra: DDoS támadás megrendelő felület 3. rész

Ha egy szolgáltatás nem elérhető, vagy egy hacker feltörte a szolgáltatásunkat és adatokat törölt, akkor felvetődik az a kérdés, hogy hogyan lehetséges a szükséges információkat, programokat, alkalmazásokat úgy lementeni, hogy szükség esetén a lehető legrövidebb időn belül vissza lehessen őket tölteni, és újra a rendelkezésünkre álljanak. A digitális világ fejlődésével egyre több adat már csak elektronikusan készül és tárolódik, akár otthon, akár a munkahelyen vagyunk. A leggyakoribb hiba, amit el szoktak követni az, ha az adatnak csak egyetlen egy példánya keletkezik és nem készítenek róla másolatokat, **mentés**eket. A hardver meghibásodása (merevelemez olvasófej, mágneslemez felülete, mágnesezettség), vagy az eszköz (telefon, laptop) elveszése, ellopása következtében ezek az adatok megsérülhetnek, megsemmisülhetnek. Számos esetben a részleges vagy teljes visszaállításukra sem lesz lehetőségünk.

5.6.1 Fájlok biztonsági mentése

Az adataink a számítógépben fájlokban tárolódnak, emiatt az egyes fájlok rendelkezésre állásának biztosítása ezeknek a fájloknak a mentését, és a visszatöltési képesség biztosítását jelenti.

Az adatvesztés ellen az adatok megőrzése, a mentések létezése nyújthat egyedül védelmet, tekintettel arra, hogy az újbóli előállításuk sok esetben problémába ütközik. A mentések tervezésénél az alábbiakat kell megfontolás tárgyává tennünk:

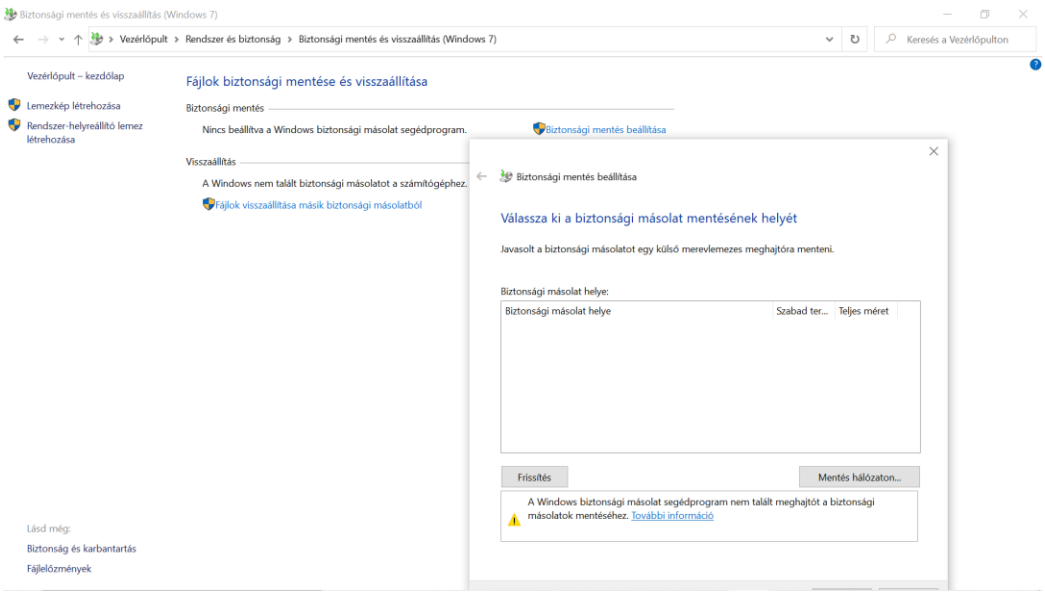
- Mekkora adatmennyiséget kell mentenünk?

- Milyen gyakran változnak meg a mentendő adatok? Milyen gyakran kell elmenteni őket ahhoz, hogy lehetőleg ne legyen súlyos adatvesztés?
- Hány példányban kell a mentést elvégezni?
- Mikor kell a mentést elvégezni, más szóval mikorra lehetséges ütemezni a mentést ahhoz, hogy ne zavarjon senkit sem?
- Meddig kell megőrizni a mentéseket?
- Hol tároljuk a mentéseket?
- Hogyan kell a mentéseket biztonságosan megsemmisíteni?

A Windows rendszerben a mentést a beépített automatikus biztonsági mentési eszköz, a Windows Backup [r] biztosítja a legegyszerűbb módon. A Windows backup a teljes rendszert lementi olyan formában, hogy egy visszaállítás után a működés ettől a ponttól fog újraindulni. Tekintettel arra, hogy ez a módszer a teljes rendszert, szoftvereket, adatokat, konfigurációkat is lementi, ezért nagy helyigénnyel rendelkezhet – emiatt sűrű használata nem célszerű ritkán megváltozó adatok esetében.

A teljes rendszer mentése helyett hatékonyabb megoldás az egyes fájlok, vagy könyvtárak mentése, amit különböző segédprogramok támogatnak. Ilyen eszköz például az Ubuntu Linuxra fejlesztett Time Vault [s] alkalmazás is, ami sokkal barátságosabb, mint rendszerparancsokat használni (rsync vagy xcopy) . Az egyes könyvtárak vagy fájlok kijelölése után a pillanatfelvétel egy gombnyomásra elkészíthető. A fájlok elnevezése hatással lehet olykor a mentés sikerességére, mivel a nagyon **bonyolult fájlnevek** (ékezetes betűk, különleges karakterek, mély könyvtárstruktúra) mentésére nem minden program van felkészülve. Kevésbé hatékony megoldás lehet a fájlok manuális másolása, például egy külső merevlemezre, vagy egy nem állandó jelleggel felcsatlakoztatott felhő alapú tárhelyre – de a semminél még ez is jobb megoldás.

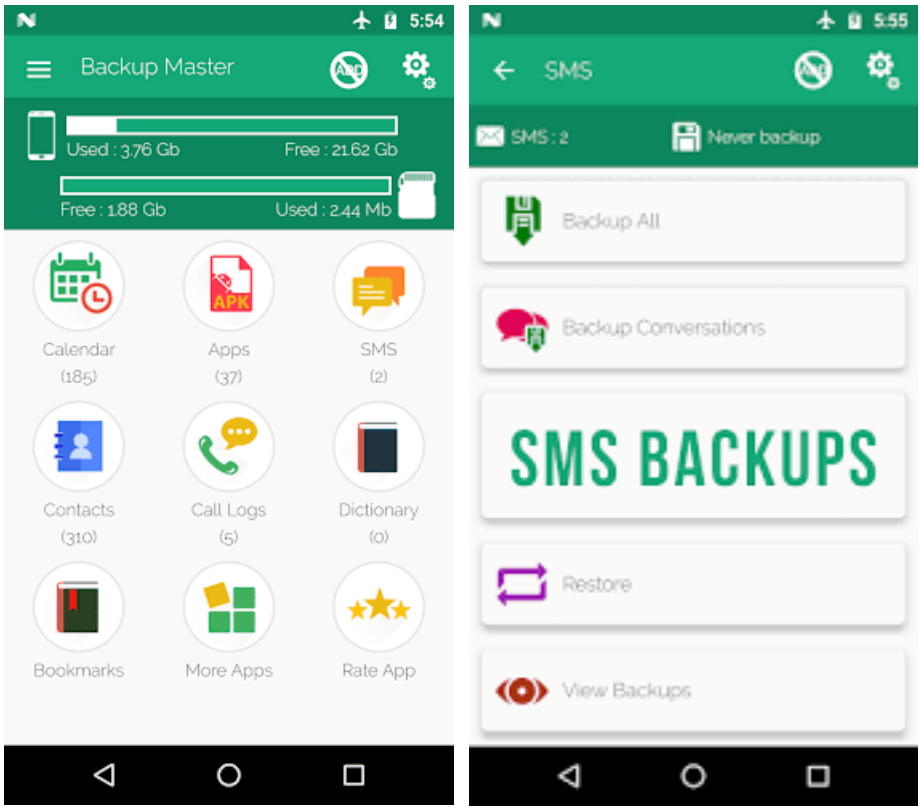
Fontos, hogy a mentési adathordozók ne legyenek állandóan a számítógéphez csatlakoztatva (vagy ha felhő alapú, akkor állandóan felcsatolva), mivel egy vírustámadás során a mentésünk is érintett lehet, és akkor nem sok értelme volt az egésznek. A másik ok, amiért nem szabad a mentéseknek fizikailag a mentett gép mellett lenni az az, hogy ha esetleg a gépet ellopják, vagy leég, vagy egyéb fizikai behatás miatt tönkremegy, akkor a mellette tárolt mentésünk is ugyanezt a kárt fogja elszenvedni. Érdemes időnként a fizikai mentés egy-egy példányát más helyszínre szállítani és ott tárolni. A cégek erre a célra vagy egy földrajzilag távoli és jól védett telephelyüket vagy bankok széfjeit szokták használni.



44. ábra: Windows Backup

A visszatöltés is egyszerűen elvégezhető egy kattintással, de javasolt a mentéseket másik lemezre vagy fizikailag védett médiára végezni – amit biztonságos háttér-adattárolónak nevezünk, hogy ne az eredetivel együtt sérüljenek meg.

Az okostelefonok használata során nagyon sokan elfeledkeznek arról, hogy ezeken az eszközökön is rengeteg fontos adatot tárolunk. Telefonszámok és egyéb kontakt adatok, SMS-ek, fényképek, feljegyzések, kimutatások, videók. Gondoskodni kell az okostelefonok adatainak mentéséről is. Erre szintén vannak célszoftverek, különböző funkcionalitással.



45. ábra: Okostelefonok fontos adatainak mentése

46. ábra: Adatok mentése Windows környezetben (Aomei backup)

A mentések gyakoriságát úgy válasszuk meg, hogy egyrészről ne jelentsen többletterhet, másrészről az utolsó mentés és a hiba bekövetkezése közötti időben keletkezett adatok pótlására is legyen reális lehetőség – vagy a hiányuknak ne legyen különösebb következménye. A mentések példányszámának kialakítása során vegyük figyelembe, hogy több mentés nagyobb biztonságot jelent ugyan, de többletfeladatot ró ránk a selejtezésük, és a bizalmasság terén is lépnünk kell (pl. mentések titkosítása) azért, hogy a mentett adataink bizalmassága is megmaradjon, hasonlóan az eredeti adatok bizalmasságához (az egyenszilárdság miatt).

Azt is vegyük figyelembe, hogy a technika változik. Ha a gyermekeink fotóit, a szakdolgozatunkat egy floppy lemezre mentettük le évekkel ezelőtt, azt bizony már nem fogjuk tudni elolvasni, mert nem lesz hozzá eszközünk. Sok számítógép már nem rendelkezik CD olvasóval sem. Az erre mentett adatokhoz nem fogunk tudni hozzáférni, ha nem rendelkezünk külső olvasóval. Illetve vannak olyan technológiák, amelyeknek van „szavatossági ideje”. A lejárati időtartam után a rajta tárolt adat már nem garantált, hogy elérhető lesz.

5.6.2 Védelem az áramellátás hibái ellen

A szünetmentes áramellátó berendezések használata számítástechnikai és ipari környezetben, vagyis otthon és a munkahelyen ma már elengedhetetlenné vált. Nem szívesen vállaljuk fel ugyanis egy áramszünet, illetve a feszültségingadozással járó zavarok hátrányos, költséges következményeit. Az **elektromos hálózat**ról üzemeltetett eszközök működése függ a hálózat működésétől, más szóval attól, hogy van-e áram. Az otthoni eszközök java része kizárólag az elektromos hálózatról működik, amelynek kiesése, meghibásodása esetén az eszközök károsodásokat szenvedhetnek. Az ilyen károk megelőzhetők és elkerülhetők akkumulátoros háttérrel rendelkező szünetmentes áramforrások alkalmazásával. A szünetmentes áramforrások ára és fenntartási költsége általában jóval kisebb, mint az a károsszeg, amelyet az áramszünetek és a hálózati áramellátás ingadozásai, túlfeszültségei okozhatnak.

Azt is érdemes figyelembe venni, hogy túlfeszültség keletkezhet egy villámcsapás okán is, és ennek a bekövetkezési valószínűsége elég magas. Egy esetleges közeli villámcsapás képes az eszközeinket tönkre tenni, pusztán azért, mert az elektromos hálózatba vannak kötve. Amennyiben a ház, ahol lakunk, nem rendelkezik villámhárító megoldással, ezzel a problémával is számolnunk kell. A védendő elektronikus eszközeinket érdemes olyan hálózati hosszabbítóba csatlakoztatni, amely rendelkezik túlfeszültség elleni védelemmel. Ezek drágábbak, mint egy normál hosszabbító, ugyanakkor szintén jóval olcsóbbak, mint egy nagyértékű eszközt kicserélni. Fontos azt is tudni, hogy egy villámcsapásból eredő feszültségimpulzus

az adatkábelen keresztül is érkezhet és ez is tönkreteheti az eszközt. Vihar és villámlás idején célszerű minden csatlakozót kihúzni az eszközökből.

A hordozható számítógépek akkumulátorai valameddig védelmet nyújtanak az áramkimaradás és az esetleges ingadozások ellen, de az asztali gépeknek nincs ilyen védelmük, így egy áramellátási incidenst működési zavar, meghibásodás is követhet. Ha a hálózati eszközöket nem védjük szünetmentes tápegységgel, akkor bár a számítógépünk működni fog, de nem érjük el az internetet a szokásos módon. Az otthoni védelemre példa az alábbi kis teljesítményű és méretű szünetmentes áramellátást biztosító egység.

47. ábra: Szünetmentes otthoni áramellátó eszköz

5.7 Komplex megközelítést igénylő fenyegetettségek és védelmi megoldások

5.7.1 Végpontvédelem és vírusvédelem

A számítástechnika és az internet kezdetekor is az első komoly, minden felhasználót érintő probléma a vírusok megjelenése volt, amit kezdetben unatkozó programozók készítettek szórakozásból, majd egy komoly evolúción keresztül eljutottak odáig, hogy ma már kiberfegyverekként emlegetik őket és az internetes bűnözés egyik fő bevételi forrását jelentik. Felhasználói oldalról ezért az egyik legfontosabb komplex védelmi intézkedés a saját számítógépünk, okostelefonunk védelme. Míg korábban egy szimpla vírusvédelmi program is elegendő volt, addig ma már az összetett támadások ellen hasonlóan komplex, többféle fenyegetéstől is megóvó végpontvédelemre van szükség.

5.7.1.1 Vírusvédelem

A vírusirtó szoftverek alkalmazása a legismertebb és legjellemzőbben elterjedt védekezési módszer, hatékonyan véd a **fertőzések** ellen. Az okostelefonok esetében a felhasználók jelentős része még nem gondolja úgy, hogy a számítógépéhez hasonló szintű védelemről kell gondoskodnia, pedig nagyon indokolt lenne. Szinte minden vírusvédelemmel foglalkozó szoftvergyártónak van kifejezetten okostelefonokra készített vírusvédelmi program verziója. Ezek közül vannak ingyenesek, fizetősek is. A lényeg, hogy legyen védelem az eszközünkön!

Vírusvédelmi programokat, hasonlóan más alkalmazásokhoz, az adott platform alkalmazás áruházából tudunk letölteni, illetve megvásárolni. A fizetős vírusirtókra is igaz a bővebb funkcionalitás, a gyártói támogatás biztosítása.

Fontos, hogy a telefonunkon használt ingyenes programok esetén a reklámok között felbukkanhatnak a telefonunk fertőzöttségével riogató és magukat vírusvédelmi programnak álcázó kártevők letöltésére ösztönző felugró ablakok, figyelmeztetések. Ne dőljünk be ezeknek, mivel ezek a programok maguk a kártevők! Összefoglalva, legyen egy saját, valamilyen neves gyártó által készített vírusirtó program a telefonunkon, amiben megbízunk!

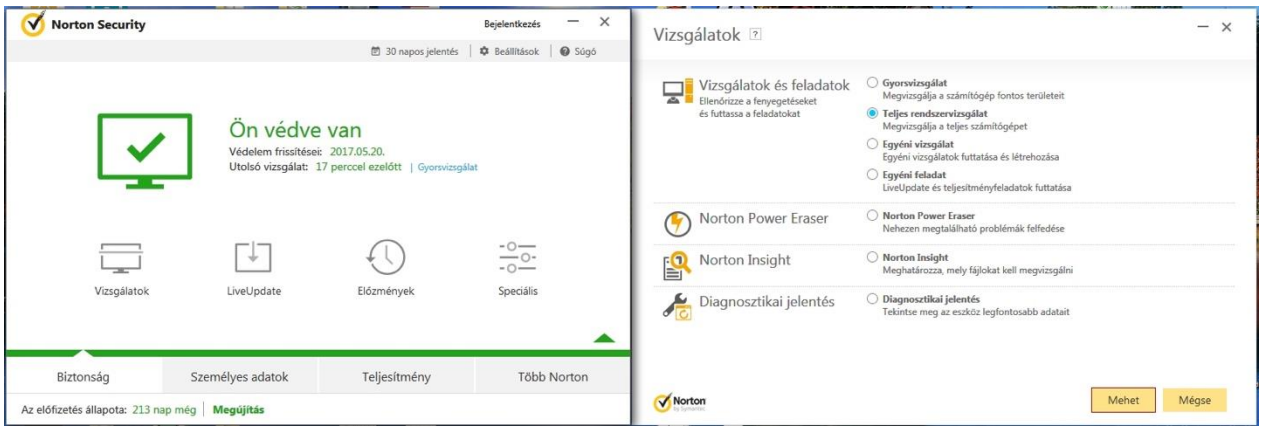
Míg régebben a fertőzés szó alatt számítógépes vírusok esetében egy speciális rosszindulatú program operációs rendszerbeli fájlokhoz való hozzákapcsolódását értettük, addig manapság már a felhasználói fájlokban is megjelentek, gondoljunk itt a különböző Office dokumentumokban található macro vírusokra. A vírusirtó programok több lehetőséget ajánlanak fel a fertőzött fájlok kezelésére, a megjelöléstől a karanténba helyezésen át a végleges törlésig terjednek a fertőzésmentesítés eszközei.

A **karantén** általában a vírusirtó program által létesített zárt tárolóterületet jelöl, amelyben a rendszer nem engedélyezi a programok aktív tevékenységét, futását. A karanténban lévő fájlok visszaállíthatók, ha ez éppen szükségessé válik, de ezt csak nagyon indokolt esetben javasolt megtenni. A karanténba zárás legfontosabb indoka ugyanis az, hogy ezeket a programokat el kell a működési környezettől különíteni, mert nem lehet őket fertőzés-mentesíteni, így nem tudjuk megszabadítani a gépet a károkozóktól, mert valamiért a vírusirtó program erre nem képes.

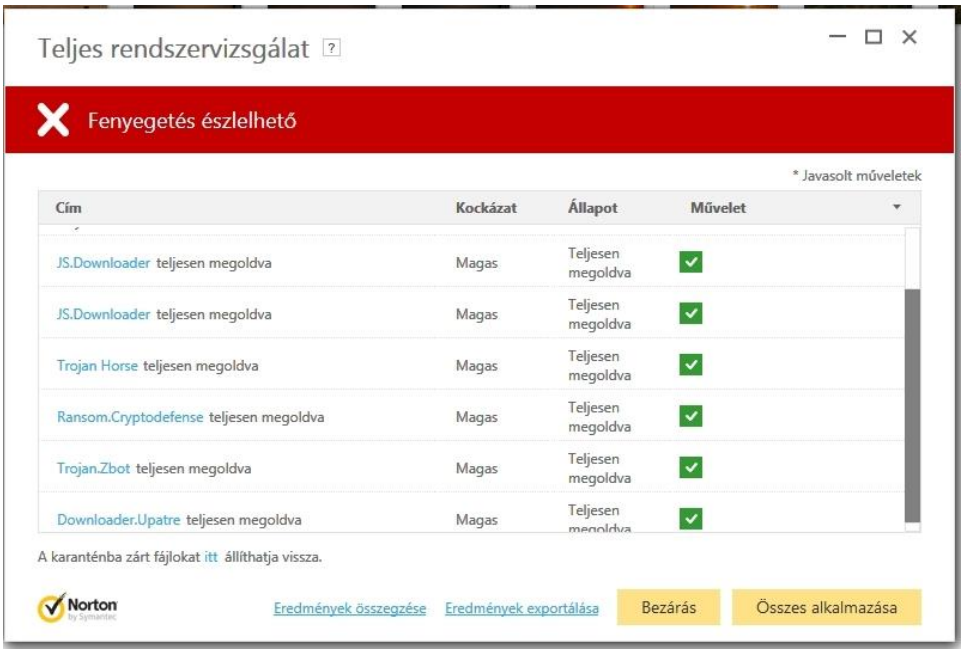
Minden vírusirtónak van egy állandóan működő része, ami az aktuális forgalmat szűri és különböző módszerekkel történő vizsgálatokat követően nem engedi a felhasználót hozzáférni a gyanús, vagy potenciálisan fertőzött fájlokhoz. Illetve különböző mélységű ütemezett kereséseket is végre tudnak hajtani, leginkább üresjárati időpontokban. Ezeket a felismeréseket egyrészt a vírusdefiníciós fájlban tárolt mintákkal való összehasonlítás teszi lehetővé, másrészt egyre elterjedtebb a reputáció alapú vizsgálat, amikor a vizsgált fájl tulajdonságai alapján ellenőrzi a program, hogy valahol máshol a világban ugyanerre a fájlra volt-e már riasztás vagy egyéb negatív tapasztalat. Azért, hogy a legújabb vírusok ellen is védettek legyünk, rendszeres időközönként javasolt a vírusdefiníciós fájlokat letölteni és frissíteni a víruskereső motor verzióját is. Jellemzően ezek a funkciók már automatikusan, naponta akár többször is elindulnak.

Célszerű legalább heti rendszerességgel úgynevezett „Teljes rendszervizsgálatot” végrehajtani. Ilyenkor a vírusirtó program a számítógépen/okostelefonon lévő összes fájlt (beleértve

a számítógéphez csatlakoztatott külső tárhelyeket is) átvizsgálja kártevők után kutatva. A heti rendszerességnek az ad indokoltságot, hogy egyre elterjedtebbek az úgynevezett nulladik napi sérülékenységeket kihasználó kártevők. A támadók az alkalmazott eszközeikből fakadóan olyan gyorsan tudják mutálni és kiküldeni, terjeszteni a kártevőket (pl. spam levelekben), hogy a legfrissebb vírusminta adatbázissal rendelkező program sem fogja felismerni ezeket, mert túl kicsi az az időablak, amíg a vírus elkészül, kiküldik millió számban, majd eljut a vírusvédelmi gyártókhoz, akik feldolgozzák, majd kiadják az újabb mintákat és azok elkerülnek a felhasználók vírusvédelmi szoftvereibe. Ezért lehetnek olyan levelek, fájlok, amelyek átjutottak a szűrésen és csak később két három nap, vagy akár egy hét múlva talál rájuk a teljes keresés.



48. ábra: Teljes rendszervizsgálat Norton Security programmal



49. ábra: Teljes rendszervizsgálat eredménye, ha vírusos a vizsgált számítógép

A vírusirtó szoftvereknek – mint minden védelmi intézkedésnek – vannak előnyei és hátrányai is. Előnye a vírusirtóknak, hogy felismerik a vírusokat a számítógépen, illetve megvizsgálják a számítógépet, hogy nem fertőződött-e meg. A vírusirtó szoftverek nagyon erős korlátja az, hogy a tényleges védettség fenntartásához naprakészen kell tartani a vírusdefiníciós fájlokat, ami rendszeres internet-kapcsolatot és frissítési tevékenységeket igényel. Elavult vírusdefinícióval hamis biztonságtudat alakulhat ki, ami szintén egy kockázati lehetőség.

5.7.1.2 Végpontvédelem

A végpontvédelem annyival nyújt többet az egyszerű vírusvédelemnél, hogy a komplex végpontvédelmi megoldások tartalmaznak személyi tűzfalat, behatolás-detektálást, spam védelmet, szülői felügyeleti lehetőségeket és végül, de nem utolsósorban, beépülve a böngészőkbe a böngészés során érkező fenyegetettségektől védenek (védelem adathalászat ellen, weboldalak biztonsági értékelése). Minden neves gyártónak van ilyen csomagja, általában „Internet Security csomag” név alatt érhetők el.

Bár korábban volt már szó az okostelefonok védelméről, itt is szeretnénk kiemelni ennek az eszköztípusnak a fokozott védelmét. Az okostelefonok is ugyanúgy számítógépek, mint nagyobb társaik, épp ezért ugyanúgy fenyegetettek, mint az asztali munkaállomások vagy laptopok. Okostelefonokra is elérhetőek végpontvédelmi megoldások – fizetősek és ingyenesek egyaránt. Rengeteg olyan kártevő program van – és számuk rohamosan nő, amelyeket

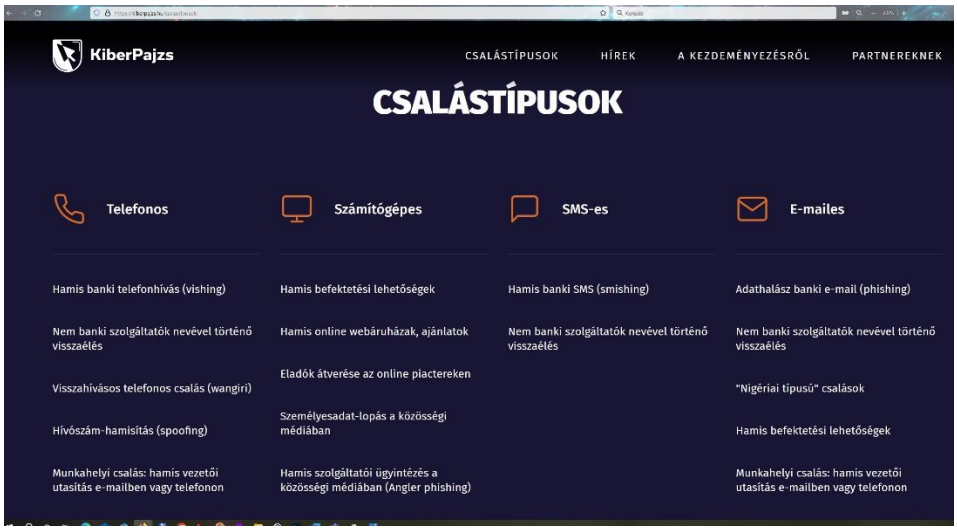
a legelterjedtebb okostelefon platformra az Androidra írtak meg. Természetesen nem kivétel ezalól a Windows és az iOS platform sem. Az okostelefonok szinte éjjel-nappal online vannak, elérik az internetet – és ezzel együtt ezek az eszközök is elérhetők az internet felől. Ugyanúgy meg tudnak fertőződni, mint a PC-k, ugyanúgy le tudja titkosítani a tartalmukat egy zsarolóvírus és ugyanúgy botnet hálózat részei lehetnek, ha a támadóknak sikerül az okostelefont megfertőzni. Figyelni kell ugyanakkor az ingyenes programok reklámjaiban felbukkanó és azonnal fertőzéssel riogató hamis vírusvédelmi programokra is. Lehetőleg valamilyen neves gyártó alkalmazását töltsük le a hivatalos forrásokból (Google Play, AppStore,) és használjuk rendszeresen ugyanúgy, mint a hordozható vagy asztali számítógépeinken (frissítések, online ellenőrzés, rendszeres teljes keresés).

Fontos információ, hogy 2017-ben megszűnt a Windows Mobile operációs rendszer fejlesztése és 2022-ben a támogatási tevékenység is megszűnt. Ebből is fakad, hogy ebben a könyvben nem foglalkozunk külön ezzel a platformmal.

5.7.2 Biztonságos internetbankolás

Manapság egyre elterjedtebb az internetes bankszámlakezelés. A bankok mindent megtesznek azért, hogy az e-banki szolgáltatásaik megfelelően védettek legyenek és védelmet nyújtsanak az ügyfelek adatai számára is. Egyrészt ez saját üzleti érdekük, másrészt a Magyar Nemzeti Bank (MNB) is szigorúan ellenőrzi a bankok információtechnológiai szempontból is biztonságos működését. Alapvetően a pénzügyek intézését az adott bank weboldalán keresztül elérhető internetbanki oldalon keresztül és mobilalkalmazásokon keresztül végezhetjük.

Szeretnénk az olvasók figyelmébe ajánlani a Kiberpajzs kommunikációs kampányt (https://www.kiberpajzs.hu). A Kiberpajzs olyan hiánypótló, tudatosító kezdeményezés, amely az utóbbi időszak megnövekedett internetes pénzügyi csalásaira és átveréseire hívja fel az állampolgárok figyelmét.



50. ábra: Kiberpajzs kommunikációs és ismeretterjesztési kampány

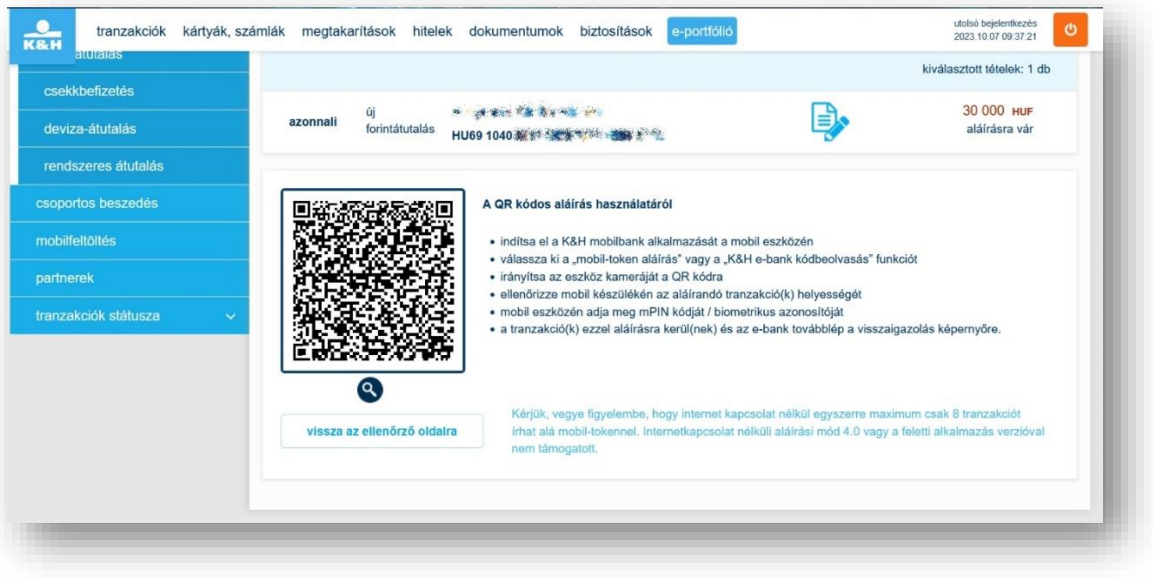
Az MNB mellett a Magyar Bankszövetség (mint a hazai bankok érdekképviseleti szerve), az Országos Rendőrfőkapitányság, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, a Nemzeti Média- és Hírközlési Hatóság, az Igazságügyi Minisztérium, a Szabályozott Tevékenységek Felügyeleti Hatósága, a Magyar Államkincstár és a Gazdaságfejlesztési Minisztérium is csatlakozott az ismeretterjesztési kampányhoz.

5.7.2.1 Számítógép/laptop - weboldal

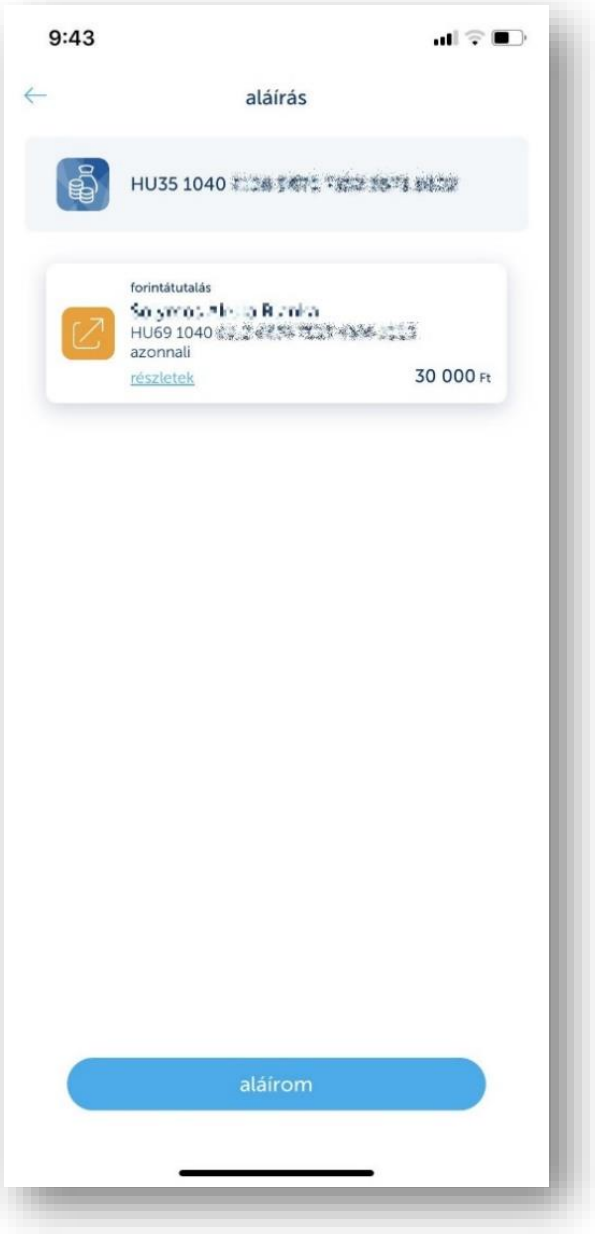
Az internetes bankolás weboldalon keresztül a felhasználói oldalról megvizsgálva két kritikus pontot hordoz. Az egyik a belépés, a másik a különböző pénzügyi műveletek végrehajtása.

Míg korábban ez egy választható opció volt, addig mára már az internetbanki belépésre minden hazai bank megerősített, úgynevezett kétfaktoros bejelentkezést követel meg. Ilyen lehet az SMS-ben érkező egyszer használatos jelszó, a bank által adott hardveres véletlenszám-generátor (token), a chipkártyás beléptetés vagy a QR kódon keresztül a banki mobilalkalmazásban megadott azonosító kód, illetve a mobilbanki alkalmazáson keresztüli hitelesítés. Ahhoz, hogy az ügyfeleket ne érje kár, ne lehessen a pénzüket jogosulatlanul ellopnia egy támadónak, a bankok a különböző tranzakciókat már kötelező jelleggel, csak valamilyen többfaktoros módszerrel megerősítve fogadják be. Egy példa erre, hogy az internetbanki felületen jóváhagyott tranzakció aláírása során a bank egy egyedi QR kódot jelenít meg, amelyet a számlához rendelt mobilbanki alkalmazással be kell olvastatni, ekkor a mobilbankban a telefonon megjelennek a tranzakció részletei. Ha ezek ellenőrzést követően rendben vannak, akkor az úgynevezett mPIN megadásával validálhatjuk a tranzakciót. Ez a folyamat

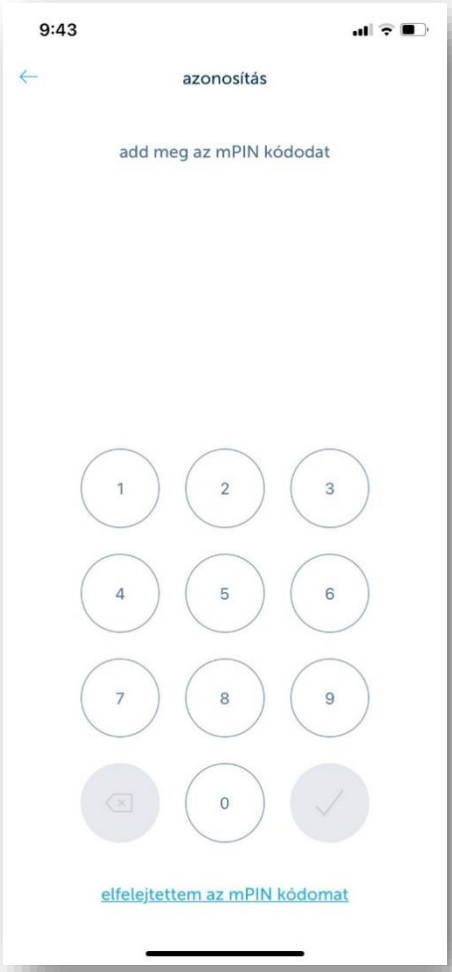
bankonként eltérhet, nem célunk az összes módszert itt megmutatni. Az azonban fontos, hogy a korábbi azonosító jelszó, vagy SMS-ben küldött kód már a múlté.



51. ábra: Tranzakció megerősítés QR kódos aláírás használatával



52. ábra: QR kód beolvasás után a jóváhagyandó tranzakció részletei



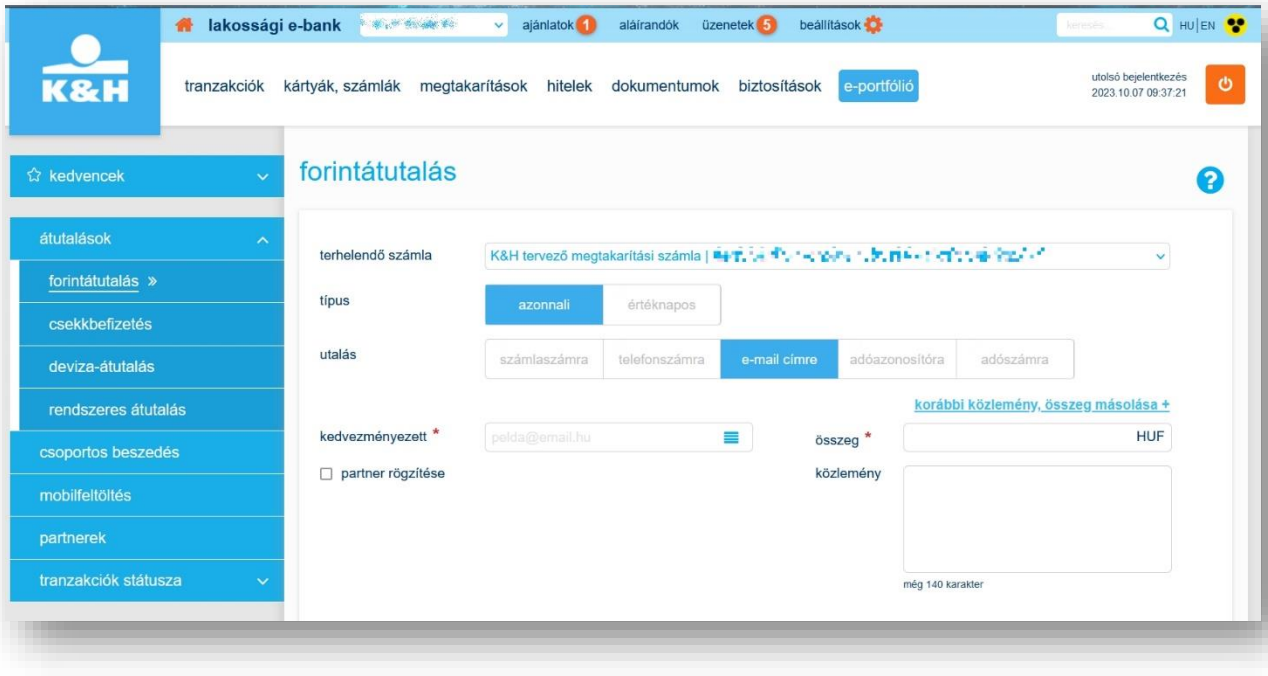
53. ábra: mPIN megadása – tranzakció jóváhagyás

Annak érdekében, hogy a felhasználó internetes bankoláshoz szükséges adatait ne lehessen ellopni és az ügyfelek felkészültek legyenek az ilyen típusú támadások ellen, minden bank különböző tudatosítási kampányokat folytat a weboldalán és különböző média felületeken.

A PSD2 bevezetése után lehetősége van a felhasználóknak arra, hogy ne csak számlaszámra tudjanak utalást kezdeményezni, hanem telefonszámra, e-mail címre, adóazonosítóra, illetve adószámra is, amennyiben ezek valamelyikét az utalás fogadó oldali fele a bankjánál beregisztrálta. Annak, hogy nem csak számlaszámra lehet utalni az az előnye, hogy egyrészt nem kell megjegyezni a 3x8 számsorozatot, hanem a sokkal könnyebben és gyakrabban használt adatokat lehet célszámla azonosítóként használni, aminek a megváltoztatása sokkal valószínűbben feltűnik egy adathalász levélben, mint egy bankszámlaszám módosítása.

Ráadásul sok esetben – például egyes közüzemi szolgáltatók esetében sokkal biztonságosabb, mint a bankkártyás fizetés egy olyan oldalon, ami esetleg hamis banki oldal.

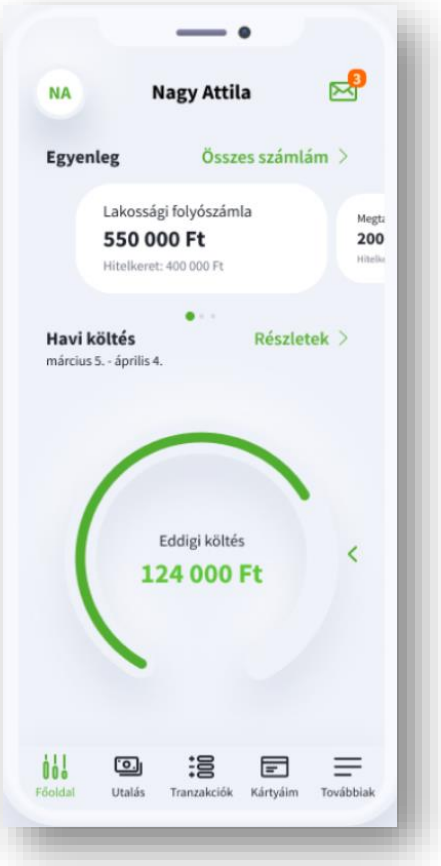
Természetesen az utalás végsősoron a bankszámlaszámra fog történni, hiszen ezek az azonosítónak használt adatok (e-mail cím, telefonszám stb.) össze vannak rendelve a fogadó oldali bankszámla számával.



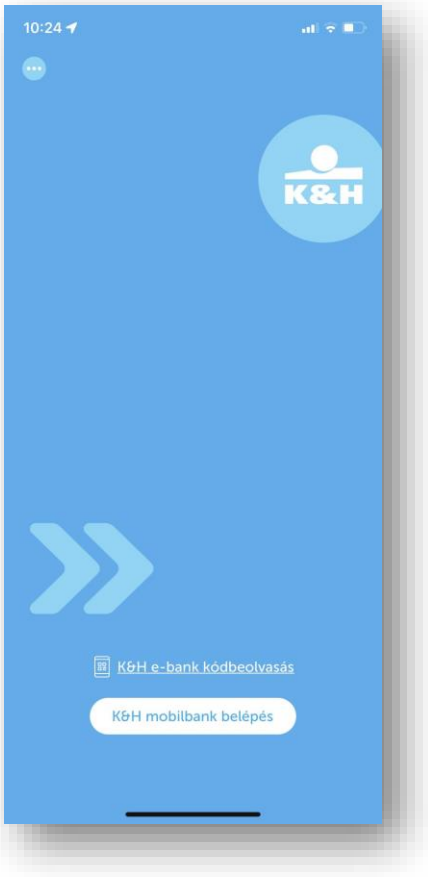
54. ábra: Utalás egyéb számlaazonosítóként használt adatokra (telefonszám, e-mail cím stb.)

5.7.2.2 Mobilbankolás

Szinte minden bank elkészítette a saját internetbanki szolgáltatásai elérésére a mobiltelefonra letölthető banki alkalmazását. Ebben az esetben ugyanazokat a funkciókat érjük el, mint a weboldalról elkérhető internetbankban. A különbség annyi, hogy a mobilbank a mobiltelefonunkra letöltött alkalmazás, és így a bankolás biztonsága innentől kezdve a mobiltelefonunk védelmétől – és a saját biztonságtudatosságunktól függ.



55. ábra: OTP mobilbank



56. ábra: K&H mobilbank

Mobilbanki alkalmazások esetén is először be kell lépni az alkalmazásba (Pin kód, ePIN, mPIN, ujjlenyomat (TouchID), mobile-token – sokféle lehetőség van és sokféle néven hívják a bankok a bejelentkezéshez szükséges hitelesítő adatokat), majd az adott funkció kiválasztása után – például egy utalás, vagy kártyalimit módosítás esetén a tranzakciót is meg kell külön erősíteni fenti módszer valamelyikével.

A mobilbank biztonsága itt már függ egyrészt a telefon hozzáférés védelmétől, vagyis, hogy használunk-e a telefon feloldásához valamilyen jelkódot, PIN kódot vagy biometrikus megoldást (arcfelismerés, ujjlenyomat stb.) vagy sem. Amennyiben nem, akkor egy tolvaj, vagy aki az elveszett telefonunkat megtalálja, közvetlenül próbálkozhat a mobilbankunkba történő belépéssel.

Ezen kívül fontos, hogy már évekkel korábban megjelentek azok a kártevők, amelyek kifejezetten a mobilbankok feltörésére és a felhasználók pénzének ellopására specializálódtak.

Egyelőre úgy tűnik ez a piac még kicsi a bűnözőknek, mivel olyan kártevőről egyelőre nem tudunk, ami magyar mobilbankokat támadna, azonban azt is fontos látni, hogy a nagyobb ügyfélbázissal rendelkező bankok mobilbankjai már 2014 óta célpontjai a támadóknak.

Az egyik ilyen híres kártevő a FluBot volt, amely csomagkövető alkalmazásnak álcázva magát, SMS-ben küldött linkről letöltve települt az áldozatok mobiltelefonjára és többek között magyar bankok felhasználóinak mobilbanki adatait lopta el.

A normál használat esetén is, de mobilbank használata esetén kifejezetten javasoljuk, hogy használjunk mobilvégpontvédelmi programot, amely jelentősen lecsökkenti a kockázatát a telefonunk megfertőződésének ezzel együtt pedig az adataink és pénzünk ellopásának.

Fontos, hogy a jelszavakhoz hasonlóan a mobilbankhoz kapcsolódó kódjainkat se írjuk fel nyílt szövegként se a telefon jegyzetébe, se telefonszámként vagy egyéb módon, hiszen, ha valaki böngészheti a telefonunk tartalmát, akkor ezeket is könnyen meg fogja találni.

A felhasználók érdekeit védve, a banki alkalmazások ellenőrizhetik, hogy a telefonunk fel van-e törve általunk. (A felhasználó a saját telefonját is feltörheti, amely során a gyártó biztonsági szolgáltatásait is megkerüli. Néhányan úgy gondolják, ez jó ötlet, mert így a gyártó „felesleges korlátozásait” oldják fel és hozzájutnak a készülék szabadabb használatához. Ezt az eljárást hívják rootolásnak vagy jailbreakelésnek.) A feltört telefonokon nem szokták engedélyezni ezeket a rendszereket, hiszen a környezet biztonsági szintje nem felel meg a bank előírásainak.

5.7.3 Biztonságos bankkártya használat – internetes fizetés

5.7.3.1 Kártyahasználat

A bankkártya egy olyan készpénzfizetést helyettesítő eszköz, melyet a bank ad(hat) a nála számlát vezető ügyfeleinek. Szinte mindegyik bankszámlához kapcsolódhat valamilyen típusú bankkártya. Használatával lehetőség van vásárolni és ATM-ekben készpénzt felvenni.

Fontos, hogy a bankkártyán fizikailag leolvasható adatok (általában 16 jegyű kártyaszám, lejárat, név, kibocsátó bank, hátul pedig a háromjegyű ellenőrző kód (CVC/CVV2)) a mágnescsíkon és a chipben is el vannak tárolva. Egy dolog nincs eltárolva, az a PIN kód.

Ha egy fizikailag is létező boltban fizetünk a kártyánkkal, vagy pénzt veszünk fel az ATM-ből, akkor fizikailag jelen kell lennie a kártyánknak és jellemzően tudni kell a kártyához tartozó PIN kódot. Éppen ezért nem szabad a PIN kódot felírni és a pénztárcánkban a kártya mellett

tárolni, még kevésbé szabad a kártyára ráírni. A PIN kód begépelésénél ügyeljünk arra, hogy ne lássák illetéktelenek a beírt kódot. Amennyiben lehetőségünk van megválasztani PIN kódunkat, akkor lehetőleg bonyolítsuk meg, ne a legegyszerűbb 1111 vagy 1234, illetve az ehhez hasonló kódokat válasszuk.

ATM készpénzfelételnél mindig győződjünk meg arról, hogy a kártyabeadó nyílásra nem helyeztek-e rá egy kártyamásoló eszközt. Ezt a kártyabeadó nyílás (csőr) finom megmozgatásával tudjuk ellenőrizni. Ha bármi gyanúsat tapasztalunk, például nem villog a csőr, vagy ragasztónyomokat látunk a szélén, akkor ne használjuk a kártyánkat, hanem azonnal értesítsük a bankot vagy az ATM üzemeltetőjét az automatán található telefonszámon.

57. ábra: Kártyamásoló eszköz ATM-en

Hasonlóan ellenőrizzük le a PIN billentyűzetet. Ott, ahol kártyamásolás van, a PIN kódot is el szeretnék lopni a támadók. Erre vagy rejtett kamerát használnak, vagy a PIN billentyűzetre rátesznek egy másik billentyűzetet, amelyen, ha az áldozat megadja a kódját, így az máris a támadók birtokába kerül.

Internetes fizetéshez nem szükséges a kártya fizikai jelenléte, elegendő, ha a kártyán szereplő adatokat ismerjük. Éppen ezért fontos, hogy amikor fizikailag fizetünk a kártyával, ne engedjük, hogy elvigyék, ne tévesszük szem elől, mert ez idő alatt lefotózhatják a kártyát és máris megvannak az adatok. A modern NFC technológiával ellátott kártyák esetében nem kell kiadni a kártyát a kezünkből, elég, ha odaérintjük a terminálhoz.

Az érintéses fizetés is elterjedt, hiszen már a bankunk nagy valószínűséggel olyan kártyát ad az ügyfelei számára, amely fel van készítve erre a technikára is. (PayWave, PayPass) Ennél a technológiánál közel kell tartani a POS terminálhoz a kártyát a fizetés során, Az adatok a

kártyáról csak közvetlen közelről olvashatóak le, távolról nem működik a leolvasás. Amennyiben 15.000 Ft alatt fizetünk vele, nem kér PIN-t, de a harmadik PIN nélküli fizetés után a negyedik már sok esetben kérni fogja azt.

Amennyiben félünk attól, hogy a kártyaadatainkat valaki észrevétlenül megpróbálja leolvasni – például tömegközlekedési eszközön vagy egyéb nyilvános helyen, akkor helyezzük őket olyan tokba, amely gátolja a rádióhullámok terjedését, ezáltal védve a kártyát és a pénzünket.

58. ábra: Rádióhullámokat blokkoló bankkártyatartó

5.7.3.2 Biztonságos internetes fizetés

A világban egyre elterjedtebb az online vásárlás, a COVID időszak bezártsága miatt pedig az elmúlt három évben folyamatosan emelkedő tendenciát tapasztalhattunk, amire a támadók is reagáltak. A különböző webáruházakban megvásárolt termékek esetében választhatjuk az utánvétes fizetést, de a leggyakrabban valamilyen elektronikus fizetési megoldást használnak az ügyfelek. Az elektronikus fizetési eljárások mögött jellemzően egy elektronikus bankszámla áll, amihez egy vagy több bankkártya is kapcsolódhat.

Érdemes olyan megbízható webáruházakat használni, ahol nem a webáruház kezeli a kártyánk adatait, hanem átirányít a bank fizetési oldalára, ott megtörténik a kártyás fizetés, majd a kereskedő megkapja az értesítést a fizetésről, mi pedig megkapjuk az árut vagy szolgáltatást.

Több bank kínál kifejezetten internetes fizetésekhez úgynevezett virtuális kártyát. Ez a megoldás azért jó, mert a kártya fizikailag vagy nem létezik, vagy ha igen, akkor sincs rajta sem

mágnescsík, sem chip, tehát készpénzfelvételre vagy POS terminálos fizetésre nem alkalmas. Csak a kártyaadatok érdekesek. A virtuális kártya általában vagy a főszámlánkhoz kapcsolódik, vagy saját alszámlával rendelkezik. Amikor használni szeretnénk a kártyát, akkor előzetesen fel kell a kártyalimiteket (összeg és használati darabszám) emelni (Telebank, Internetbank), amelyek vagy közvetlenül a vásárlás után vagy időzáras limitnél 24 vagy 48 óra után visszaállnak az alaplimitre – jellemzően 1 Ft-ra. Így, ha el is lopják a kártyaadatainkat valamelyik kereskedő számítógépes rendszeréből, nem férnek hozzá a számlán tartott összegünkhöz. Ott, ahol alszámlához kapcsolódik a kártya, ott annyit költhetünk (és annyit lophatnak el tőlünk), amennyi pénzt előzetesen az alszámlára utaltunk, vagy ott tartunk.

59. ábra: VISA Virtual kártya internetes fizetéshez

Korábban a legjellemzőbb internetes fizetési módszer a PayPal volt, amely egy virtuális számla, amely mögé szintén valamilyen bankkártyát kell megadni. Ha nagyon biztonságos tranzakciót akarunk használni, akkor megadhatunk virtuális kártyát a regisztrációhoz, majd utalhatunk valamennyi összeget a PayPal számlánkra, ennek terhére tudunk majd vásárolni az interneten. Mindeközben a fizikai kártyánk és a bankszámlán tartott pénzünk nincs veszélyben.

A PayPal mellett számos más internetes fizetési platform létezik, amelyek különböző mértékben osztoznak a piacon. Ezek között vannak globálisan elterjedtek, valamint olyanok, amelyek inkább egy adott régióban vagy országban dominálnak. Az alábbiakban néhány közismert internetes fizetési platformot és a piaci részesedésüket mutatjuk be:

1. **PayPal**: A PayPal a világ egyik legismertebb és legelterjedtebb online fizetési platformja. Globálisan elérhető, és lehetővé teszi a felhasználók számára online vásárlások fizetését, pénzküldést és pénz fogadást.
2. **Google Pay és Apple Pay**: Ezek a fizetési megoldások a Google és az Apple által kifejlesztett mobilfizetési platformok, és lehetővé teszik az Android és iOS eszközökkel történő online fizetéseket. Világszerte elérhetők, és számos üzlet és alkalmazás támogatja őket.

Fentieken kívül még a Square (ma már Block néven fut), az AliPay a WeChat Pay és a Stripe is világszinten elterjedt fizetési platformok, de Magyarországon kevésbé ismertek.

Az online fizetések biztonságosabbá tétele érdekében az Európai Parlament és a Tanács 2015/2366 számú, belső piaci pénzforgalmi szolgáltatásokról szóló irányelve (PSD2 – Payment Service Directive 2) már 2018., majd azt követő évben számos újítást vezetett be, többek között:

- a bankkártya tiltása díjmentessé vált,
- a bankkártya visszaélés esetén a bejelentés időpontjáig végrehajtott, a bankkártya tulajdonosa által jóvá nem hagyott fizetési műveletek esetében a bankkártya fedezetét biztosító számla számlatulajdonos ügyfelek kárviselése a korábbi 45 000 forintról 15 000 forintra csökkent,
- a hitelkártya zárlati díj eltörlésre került,
    - erős ügyfélhitelesítés bevezetése (SCA – Strong Customer Authentication), ez nem csak a kártyákra, hanem minden online fizetés esetén,
    - az azonosítási lépésekből az alábbiak közül legalább kettőnek meg kell történnie:

        1. biometrikus azonosítás, ujjlenyomat, arcfelismerés.

        2. a kártyahasználó által birtokolt eszköz alapján – mobiltelefon, kártya, valamilyen véletlenkód generáló eszköz (token)

        3. felhasználó által ismert - jelszó PIN kód, egyedi jelszó.

Az online kártyás fizetéseknél viszont nehezebb a két faktort teljesíteni, mert a szabályozás a kártyaadatok ismeretét nem tekinti egy faktornak, ugyanis ezeket ellophatják az ügyfelektől, és ha ezt elfogadnák, akkor lényegében véve semmi sem változna a korábbi szabályokhoz képest.

A PSD2 ezen kívül érint még számos kártyás szolgáltatást is. Olyan helyeken, ahol a szolgáltató eltárolta a kártyaadatainkat és úgynevezett egyklikkes kártyás fizetést tudtunk használni, ott az újonnan regisztrált kártyák esetében - minden tranzakciónál újra kell hitelesíteni magunkat. Ugyanakkor az előfizetéses jellegű kártyás fizetéseknél, ahol például havi rendszerességgel terhelik a kártyánkat, ott elég az első alkalommal a hitelesítést elvégezni.

Ezt a gyakorlatban úgy kell elképzelni, hogy ott, ahol eddig a kártyaadataink megadásával le tudtuk bonyolítani az internetes vásárlást, most egy sms-ben érkező kóddal, egy külön, a kártya kibocsátóbankja által használt mobiltelefonra érkező kóddal, vagy egyéb módon meg kell erősíteni a tranzakciót, EU-s kereskedők esetében. EU-n kívüli internetes kereskedők

esetén előfordulhat, hogy a hagyományos módon tudjuk használni a kártyát. Ilyen esetekben legyünk különösen óvatosak és általában is javasoljuk, hogy legyen beállítva minden kártyás tranzakcióhoz SMS-ben történő értesítés mind a sikeres, mind a sikertelen tranzakciókra. Az online vásárlási limit korlátozása is megakadályozhatja a korlátlan pénzleszívást a számlánkról.

Nagyon fontos, hogy akár fizikai (CP – card present), akár internetes fizetésre (CNP – card not present) használjuk a bankkártyánkat, igényeljük a bankunktól a kártyaőr SMS szolgáltatást, amely azért jó, mert azonnal értesülünk arról, ha mi sikeresen vagy sikertelenül fizettünk, illetve, ha valamilyen módon kompromittálódott a kártyánk és más szeretne a kártyaadatainkkal visszaélve fizetni. Ebben az esetben azonnal meg tudjuk tenni a szükséges lépéseket. A telefonunkban legyen eltárolva a bankunk kártya ügyfélszolgálatának telefonszáma az azonnali kártyatiltáshoz.

Már megjelentek azok a szolgáltatók, akik nem bankként, ám mégis nyújtanak bankkártyás szolgáltatást az ügyfeleik részére. Ilyenkor az ügyfél ugyanúgy kap egy plasztik kártyát, amelyre tölthet pénzt, és utána vásárolhat vele. Ezek a megoldások is képesek virtuális kártyát generálni akár 1-1 vásárláshoz is, amely „kártya” csak az adott vásárlás kapcsán él. További előnyük lehet, hogy a költéseink kapcsán kimutatásokat és költési szokás elemzéseket is adnak, amelyek segíthetnek a felelős pénzköltés elsajátításában is.

5.7.4 Elektronikus pénz és elektronikus pénztárcák

Az internet világában az elektronikus fizetések lebonyolításához olyan módszereket kellett találni, melyek a készpénzes vagy hagyományos banki átutalásos tranzakciók internetes alternatívájaként – jellemzően a kis összegű (1 eurocent és 25 euro közötti összegekre) – funkcionálhattak. Az elektronikus pénz formáját tekintve digitális adat, ami nem jelentett újdonságot a banki számlavezető rendszerek bevezetését és a hagyományos papíralapú főkönyvek elektronikussá válását követően. Az elektronikus pénznek két fajtája jött létre, az egyik a kártyapénz (pl. HelloPay kártyák) a másik a hálózati pénz (pl. PayPal) [x]. A kártyapénz esetében a pénzt a kártyán lévő mikrochip tárolja – esetenként csak korlátozott ideig, míg a hálózati pénzen egy szerveren működő alkalmazás tartja nyilván az elkölthető egyenleget. Közös a két esetben az, hogy a pénz elköltése kizárólag a feltöltést követően valósulhat meg, ami viszont lehet előzetes (kártyapénz) vagy utólagos (hálózati pénz) egyaránt.

Az elektronikus pénz kibocsátása Európában pénzügyi szolgáltatásnak minősül – de nem számít betétgyűjtésnek, és csak az erre feljogosított szervezetek végezhetik. A jogszabály az elektronikus pénz definícióját az alábbiakban határozta meg:

„az elektronikus pénz kibocsátójával szembeni követelés által megtestesített, elektronikusan tárolt - ideértve a mágneses tárolást is - összeg, amelyet pénzeszköz átvétele ellenében bocsátanak ki a pénzforgalmi szolgáltatás nyújtásáról szóló törvényben meghatározott fizetési műveletek teljesítése céljából, és amelyet az elektronikus pénz kibocsátóján kívül más természetes és jogi személy, jogi személyiség nélküli gazdasági társaság és egyéni vállalkozó is elfogad, ide nem értve az olyan specifikus készpénz-helyettesítő fizetési eszközökön alapuló szolgáltatásokat, amelyek csak korlátozott módon (zárt körben vagy szűkkörűen) használható eszközön tárolják az adataikat, vagy az elektronikus hírközlő hálózat üzemeltetője vagy az elektronikus hírközlési szolgáltatás nyújtója általi fizetési műveletre használt értéket."[40]

Az elektronikus pénz lényeges tulajdonsága tehát, hogy egyrészről fedezetet (feltöltést) igényel, másrészről széles körben elfogadják, mint fizetőeszköz. Például a PayPal felhasználóinak a száma 2010-ben 84,3 millió volt, mely 2018-ra 237 millióra, 2019-re 286 millióra duzzadt, 2022 év végén pedig 435 millió volt. (www.statista.com) [y].

A PayPal olyan hitelintézeti szolgáltatást nyújt, mely lehetővé teszi regisztrációt követően azt, hogy a felhasználók a bejelentkezést követően pénzügyi tranzakciókat hajthassanak végre – jellemzően kisértékű vásárlásokat vagy pénzküldéseket, illetve pénzküldemények fogadását – minden más eszköz használata nélkül. A hálózati elektronikus pénz természetesen bármikor visszaváltható a felhasználó bankszámlájára vagy bankkártyájára. Érdekesség, hogy ha egy tranzakcióhoz nincs elegendő fedezet a felhasználó PayPal számláján, akkor lehetősége van automatikus fedezetfeltöltésre a saját bankszámlájáról [z]. Fontos még tudni, hogy az elektronikus pénz a készpénzzel egyenértékű fizetőeszköz, így az európai törvények értelmében kamatszerzésre nem használható az elektronikus pénzre vonatkozó európai irányelv 12. cikke szerint[41].

A bankkártyás tranzakciók emelt szintű biztonsága érdekében fejlesztették ki a 3D-Secure hitelesítési módszert, mely egy biztonsági protokoll, amely fokozott biztonságot és megbízható hitelesítést nyújt az internetes vásárlásnál a bankkártyák vagy hitelkártyák használatakor. Ezt a különböző kártyatársaságok más-más névvel illették, például „MasterCard SecureCode", „Verified by Visa", „J/Secure" a Japan Credit Bureau esetében, illetve American Express kártyák esetén „Safekey". A 3D-Secure speciális biztonsági kódját a kártyakibocsátó banknak kell meghatároznia és eljuttatnia az ügyfelekhez, hogy a bank engedélyezze az online

[40] 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról, 6. § (1) 16.

[41] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2009/110/EK IRÁNYELVE (2009. szeptember 16.) az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről, a 2005/60/EK és a 2006/48/EK irányelv módosításáról, valamint a 2000/46/EK irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg)

tranzakciót. A kártyakibocsátó bankok különböző módszerekkel állítják elő és kézbesítik ezeket a kódokat az ügyfelek számára, melyek igazolni tudják, hogy az internetes regisztrációhoz vagy tranzakcióhoz használni kívánt bankkártyának valóban az adott felhasználó a jogos tulajdonosa. Az EU-ban 2015. augusztus 1. óta minden fizetési szolgáltató számára elvárás a 3D-Secure rendszer támogatása és betartatása.

A mobiltárca egy olyan elektronikus pénztárca, mely a SIM-kártyán elhelyezett speciális chip segítségével tárolja a felhasználó bankkártyájának az adatait és képes azt szolgáltatni elektronikus fizetési tranzakciókhoz mobilalkalmazások vagy NFC leolvasók számára. A chiphez csak az arra felhatalmazott alkalmazások képesek hozzáférni a fizetési tranzakció elindításakor. A biztonság növelése érdekében be lehet állítani egy négyjegyű PIN kódot, amely beírása nélkül nem lehetséges a mobiltárcás fizetés. A biztonságot tovább növelheti a képernyőzár aktiválása is a mobilalkalmazások esetében. Érdekesség, hogy a Vodafone Pay akkor is használható, ha a telefon ki van kapcsolva, vagy lemerült a telefon akkumulátora, mivel fizetéskor a SIM-kártya tartja a kapcsolatot a bankkártya terminállal passzív módon. A magas mobilpenetráció maga után vonta a mobilfizetések előretörését Kínában is, ahol ma már többen fizetnek mobiltelefonnal, mint bankkártyával. A mobilpénztárca használatának van egy adatvédelmi szempontból előnyösnek nevezhető tulajdonsága, nevezetesen a tranzakciónál a vevő adatai helyett a mobiltárca üzemeltetője jelenik meg, így a pénzügyi tranzakciókból nem lehetséges az egyes vásárló szokásait profilírozni, megismerni.

2019 nyarán indult el az ApplePay, amely már az iWatch eszközön keresztül is lehetővé teszi a fizetést. Új generációs órák esetén a már telefonnak sem kell a közelünkben lennie. Ezzel egy további kényelmi funkció jelent meg, amely ugyanakkor egy potenciális támadási felületet is nyit. Immár az óráinkra is figyelmet kell fordítanunk, mint potenciális adatvesztésre lehetőséget adó eszközre.

5.7.5 Fintech vállalkozások

A hagyományos pénzügyi szolgáltatások mellett újak is megjelentek ezen a piacon, az úgynevezett Fintech szereplők, például a a Revolut vagy a Wise.

A Fintech vállalkozások olyan technológiai megoldásokat alkalmaznak a pénzügyi szolgáltatások nyújtásához, amelyek gyakran megszüntetik a hagyományos bankok és pénzintézetek által kínált hosszadalmas és költséges folyamatokat. Mind a Revolut, mind a Wise digitális alapú pénzügyi szolgáltatásokat kínál, és az innovatív technológiákat használja fel a nemzetközi pénzátutalások és a devizaátváltás terén.

A Revolut és a Wise olyan új kockázatokat hoztak a pénzügyi szolgáltatások terén, amelyekre a hagyományos bankoknál kevésbé vagy egyáltalán nem volt példa. Ezek közé tartoznak:

- Kriptovaluta kockázata: mind a Revolut, mind a Wise lehetővé teszi a kriptovaluták vásárlását és tárolását az alkalmazásban. Ez új kockázatokat hoz a felhasználókra nézve, mivel a kriptovaluták volatilisek, és az áruk gyorsan változhat. A kriptovalutákhoz kapcsolódó biztonsági és szabályozási kockázatok is fennállnak.
- Adatvédelmi kérdések: a digitális pénzügyi szolgáltatók számára rendkívül fontos az ügyfelek személyes és pénzügyi adatainak védelme. Az online működés és az adatok digitális tárolása újabb veszélyforrásokat jelent az adatvédelmi szempontból. Az adatainkkal való visszaélés vagy az adatlopás kockázata is nőhet. Az elmúlt években mind a Revolut, mind a Wise elszenvedett olyan kibertámadást, amely során adatokat és konkrétan pénzt is elloptak az érintett szolgáltatók rendszereiből.
- Szabályozási kockázatok: a Revolut és a Wise gyakran működnek határokon átnyúlóan, és számos országban nyújtanak szolgáltatásokat. A különböző országok pénzügyi szabályozásai eltérhetnek, és ezeknek a vállalkozásoknak meg kell felelniük a különböző jogi követelményeknek és szabályozási rendszereknek. Ez szabályozási kockázatot jelenthet, és hatással lehet az ügyfelek szolgáltatásokhoz való hozzáférésére.
- Ügyfélszolgálat elérhetőség: a digitális pénzügyi szolgáltatók gyakran korlátozzák az élő ügyfélszolgálati támogatást, vagy csak online kommunikációs csatornákat kínálnak. Ez kihívásokat jelenthet az ügyfelek számára, ha problémák merülnek fel vagy segítségre van szükségük.

Amikor a digitális pénzügyi szolgáltatókat használjuk, a kockázatokat is figyelembe kell venni, ugyanúgy, mint minden más egyéb esetben is.

5.7.6 Csaló webáruházak

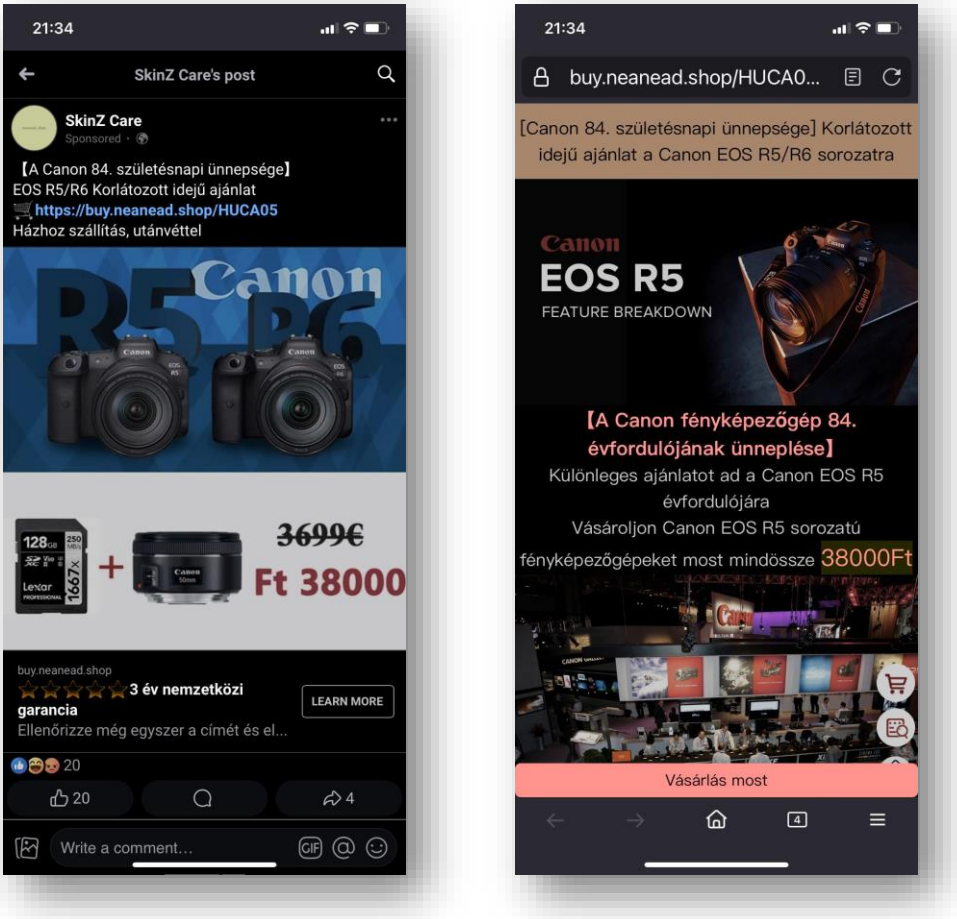
Ahogy növekszik az internetes vásárlások darabszáma és értéke, úgy jellennek meg azok a csaló webáruházak is, amelyek az óvatlan vagy éppen hiszékeny felhasználókat kívánják megkárosítani.

Ha hamis webáruházban vásárolunk, akkor nem csak a kártyával kifizetett összegnek mondhatunk búcsút, hanem az oldalon megadott személyes adatokkal is visszaélhetnek. A megadott kártyaadatokkal a csalók a tulajdonos hozzájárulása nélküli tranzakciókat kezdeményeznek és/vagy eladják a megszerzett adatokat az interetes feketepiacok valamelyikén. Fontos megkülönböztetni a csaló webáruházakat és a hamis termékeket forgalmazó

webáruházakat. Míg utóbbinál van szállítás, csak éppen egy bóvli árut vagy egy márkás áru helyett egy hamisítványt kapunk, addig az előzőnél a kifizetett áru sohasem érkezik meg és még az adatainkat is ellopják.

Az alábbiakban felsoroljuk, hogy miről ismerhetjük fel a csaló webáruházakat:

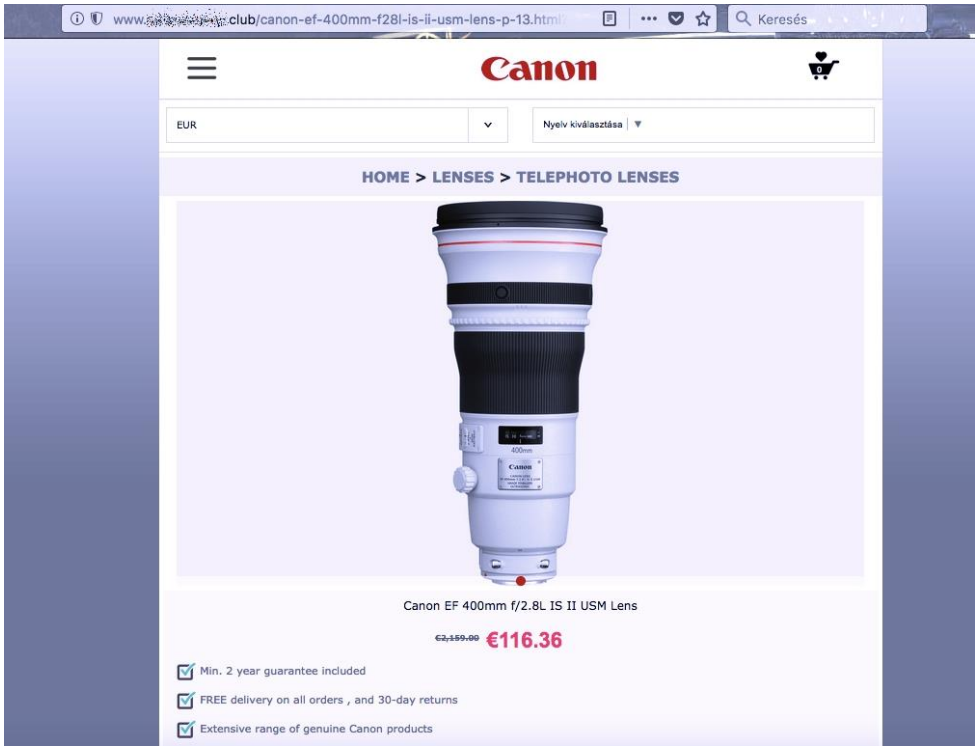
- Az első és legfontosabb: az ár túl szép, hogy igaz legyen. – Ez a valóságban azt jelenti, hogy milliós fényképezőgépek és objektívek, többszázezer forintos drónok vagy quadok kerülnek egyes oldalakon pár tízezer forintba, míg neves ruha és cipő márkák darabjai párezer forintért megtalálhatóak. Mindezt tetézik a csalók a világon bárhova történő ingyenes házhoz szállítással.



60. ábra: Facebookon megjelenő csaló webáruház reklám (a CANON EOS R5 átlagos fogyasztói ára kb. 1,8 millió forint)

- Nagyon egyszerű weboldal dizájn - A csalók nem fektetnek sok energiát a webáruház kinézetébe, hiszen a bomba ár úgyis elviszi a figyelmet - és sajnos az áldozatok pénzét is.
- Gyanúsan túl nagy választék - Legyen szó ruházati vagy műszaki cikkekről, minden márka minden terméke megtalálható az oldalon. Ez irreális, hiszen az elektronikus kereskedelemnek is megvannak a maga méretgazdaságossági szempontjai.
- A visszafizetésiszabályok hiánya, vagy tisztázatlansága - A csaló weboldalak jellemzően másoktól lopják az ilyen szövegeket, vagy annyira általánosak, irreálisak, hogy nem sokra megyünk velük.
- Hamis, vagy nem létező kapcsolati információk - Létező eset, hogy egy hamis webáruház oldalán egy repülőtér teherportájának a címe volt telephelyként megadva, sőt, előfordult, hogy egy létező személy – egy hasonló termékeket forgalmazó másik cég alapítója volt megadva kontaktnak. Érdemes a címnek utánanézni a Google Maps-en, a kontakt névnek és cégnek pedig általában az interneten.
- Csak lelkendező és pozitív kommentek és értékelések - Közösségi oldalakon terjedő hamis áruházaknál érdemes kritikus szemmel nézni a visszajelzéseket. Jellemzően hamis profilokról érkeznek lelkendező kommentek, mindenki elégedett, az összes terméket csodálják és magasztalják – ilyen esetben legyünk résen, mert ez nem életszerű.
- Hamis weboldal cím - A hamis webáruházak vagy egy eredeti termék weboldalhoz hasonló nevet regisztrálnak, kiegészítve valamilyen szóval - például „sales” -, vagy egy-két betű eltéréssel regisztrálják a nevet, amivel könnyen átejthető egy tájékozatlan vásárló. Például a www.michaelkors.com egy eredeti weboldal, de két „r”-rel www.michaelkorrs.com címről már egy hamis, vélhetően vírusos alkalmazás letöltését ajánló oldalra kerülünk. Erősen javasolt, hogy erre a hivatkozásra ne kattintsunk rá!
- Semmitmondó webcím, gyanúsan olcsó árukkal, hatalmas kedvezményekkel - Gyanús lehet például az „srostore.com” is, ahol közel 90 százalékos kedvezménnyel kínálnak mindent, motorcsónaktól kezdve a golffelszerelésig. Ha ilyet látunk, érdemes az Amazon-on vagy valamelyik megbízható webáruházban leellenőrizni, hogy ott menynyiért adják a terméket, mert csodák nincsenek.
- Adattisztaság - A hamis weboldalak általában nem foglalkoznak a felhasználói adatok helyességével – hiszen soha nem fognak semmit kiszállítani. Az adatok

megfelelőségét egyedül a kártyaadatoknál nézik, amit azonnal le is terhelnek az árucikk árával, azonban szállítás nem történik. Erről tanúskodnak például a scamadviser.com oldalon a hozzászólók panaszai is.



61. ábra: Hamis webáruház, gyanúsan olcsó ár (az objektív valós ára 12.000 EUR körül van)

Ha fenti szempontok megvizsgálása után még mindig kétségeink vannak, akkor ellenőrizzük le a megvásárolandó termék árát más webáruházakban. Ha irreális a különbség, akkor gyanakodjunk! Magát az adott weboldalt is leellenőrizhetjük. Több szolgáltató is foglalkozik azzal, hogy kockázatosnak ítélt weboldalakról szolgáltat információt. Az egyik ilyen a https://transparencyreport.google.com/safe-browsing/search /, de kifejezetten a csaló weboldalak ellenőrzésére szolgál a https://www.scamadviser.com/ és a https://scamdoc.com is.

A másik nagyon egyszerű módszer az, hogy a weboldal címét és a „scam” (csalás) szavakat gépeljük be a keresőprogramunkba. Ha valóban csaló webáruházzal van dolgunk, akkor jó eséllyel már mások is erre a következtetésre jutottak és jelezték akár kommentekben, közösségi oldalakon, vagy akár a fenti csaló weboldalakat listázó oldalak valamelyikén.

Az internetes vásárlásokhoz használjunk elkülönített számlát, amire csak annyi pénzt teszünk, amennyit el akarunk költeni, vagy használjunk internetes kártyát.

Amennyiben megkárosítottak bennünket forduljunk bankunkhoz. Amennyiben azt tapasztaljuk, hogy a kártyaadatainkkal visszaéltek és jogosulatlan tranzakciók történtek, szintén forduljunk bankunkhoz és tiltassuk le az érintett kártyát.

5.7.7 Hamis hírek (fake news) felismerése

A hamis hírek felismerése azért fontos terület, mert nagyjából ugyanazokat a készségeket kell elsajátítani a felismerésükhöz, mintha egy adathalász levelet, vagy csaló webáruházat vizsgálnánk. Bár a hamis hírek közvetlenül nem okozzák az adataink bizalmasságának, sértetlenségének vagy rendelkezésre állásának elvesztését, mégis befolyásolni tudják gondolkodásunkat, ezáltal a világról és egyéb témákról, népcsoportokról, országokról, eseményekről, vagy más, a mindennapi életünkre ható dolgokról alkotott véleményünket. Az alábbiakban pontokba szedjük, hogy milyen szempontok alapján tudjuk eldönteni, hogy hamis vagy valós hírrel állunk szemben:

- Mérlegeljük a forrást, hogy megértsük az oldal küldetését és célját. Rengeteg olyan oldal van, amely más hírportálok nevét kiegészítve próbálja megtéveszteni az olvasókat.
- Nézzük meg a portál többi hírét. Ha jellemzően bulvároš, szenzációhajhász, elfogult, áltudományos, konteós/összeesküvés elméletes, túlzottan szatirikus semmitmondó hírek vannak körbevéve reklámokkal, akkor gyanakodjunk, hogy be akarnak csapni.
- Keressük meg az impresszumot. Az impresszumban találhatók normális esetben az oldal, hírportál szerzői gárdájának (főszerkesztő, kiadó, rovatvezető stb.) elérhetőségei. Ha nincs impresszum, vagy csak egy e-mail cím van ott, akkor gyanakodjunk.
- Ellenőrizzük a szerző kilétét. Keressünk rá a nevére, hogy megtudjuk, egyáltalán létezik-e, és hihető forrásnak számít-e, vagy éppen álnevet használ. Ha nincs szerző, akkor az is beszédes, hiszen az újságírói etikett megköveteli, hogy névvel publikálják a cikkeket.
- Ha vannak hivatkozások, nézzük meg, hogy azok hova mutatnak. Ha reklámokkal teletűzdelt, hasonló szenzációhajhász oldalra, akkor nagy valószínűség szerint átverés a hír.

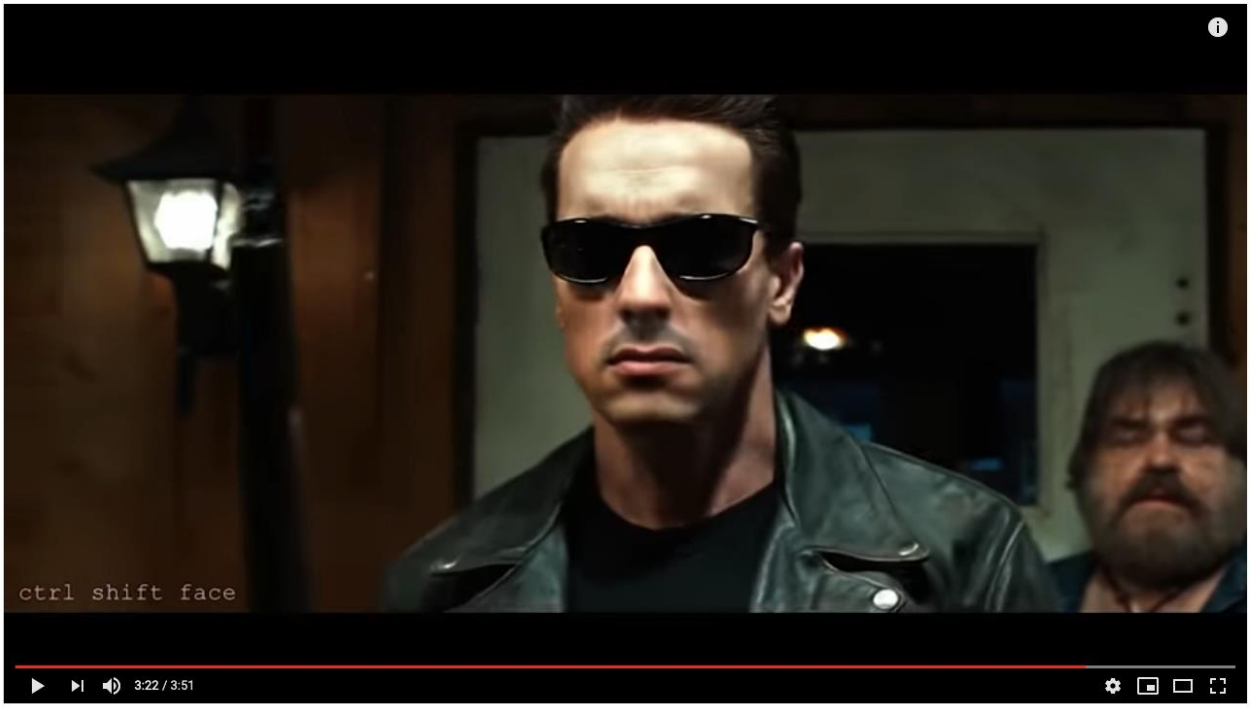
- Ellenőrizzük a dátumot. Ez szintén fontos, hiszen előfordul, hogy egy évekkel korábbi hír kezd el önálló életet élni az interneten. Ha nincs dátum és több gyanús körülmény is van, akkor szinte biztos, hogy nem valós hírrel van dolgunk.
- Tompítsuk saját előítéletünket annak érdekében, hogy megnézzük, a hír befolyással van-e az ítélőképességünkre. Irányul-e bármilyen csoport, népcsoport, ország, eszme, esemény stb. ellen?
- Keressünk rá a hírre más neves hírportálokon. Ha nyoma sincs például egy olyan eseménynek, ami egyébként országos érdeklődésre tartana számot, akkor valószínű, hogy álhírrel van dolgunk.
- Ha a hírhez kép is van mellékelve, mentsük el és töltsük fel a képet a Google képkeresési funkciójába és keressünk rá, hogy máshol, más oldalakon megtalálható-e? Ilyen esetekben gyakran előfordul, hogy a kép egész más esemény, ország vagy hír kapcsán lett publikálva, ráadásul, ha dátumilag is eltérés van, akkor szinte biztos, hogy a kép lopott és valószínű, hogy a hír is hamis.
- Ha olyan hírrel találkozunk a közösségi oldalon, amely a tényleges elolvasás előtt már megosztást kér, akkor gyanakodjunk, hogy álhírrel van dolgunk és az egész csak az adott oldal (és a rajta lévő reklámok) népszerűségét szolgálja.
- Az ilyen hírek címének jellemzői az alábbi szófordulatok: „Nem fogod elhinni…”, „A híres sztárral olyan dolog történt, hogy eláll a szavad…”, „A neves riporter valamit talált, de ami ez után történt, arra nincsenek szavak…” Tehát semmi konkrét nem derül ki a címből, de az olvasó érzelmeire, kíváncsiságára próbál hatni a hír.

Kérjük a kedves olvasót, hogy a fentiek alapján ítélje meg, hogy egy ilyen klasszikus főcím igazi vagy hamis hír lehet? „Egy hatalmas elhagyatott hajóroncsot találtak az Aggteleki Nemzeti Parkban! Mikor átkutatták a fedélzetet feldolgozhatatlan látvány tárult a szemük elé!”

5.7.8 Deepfake, avagy ne higgy a szemednek!

A szó maga a „deep learning” (mély tanulás) és a „fake” (hamis) szavak összevonásából 2017-ben keletkezett. Minél több információt adunk a gépi tanulási módszerrel felvértezett generátor algoritmusnak az eredeti célpontról, az eredmény annál élethűbb, de természetesen egy hamisított videófelvétel lesz. ,. A dolog kicsit hasonlít a „photoshoppolt” fényképekhez, amelyeken szintén nem a valóságos állapotukban láthattuk az ábrázolt személyeket vagy tárgyakat, viszont az eredeti fénykép ismeretében bárki képes egy manipulált újat létrehozni. A hamis videókon látni véljük az általunk ismert szereplőket, azonban vagy eddig

ismeretlen szituációkban, vagy olyan mondanivalóval, amely tőlük eddig ismeretlen vagy szokatlan volt számunkra. Számos hamis videó készült az elmúlt időszakban, mivel a hamisított filmek elkészítése a technológia fejlődésével egyre egyszerűbbé vált.



62. ábra: Deepfake videó részlet, ahol az eredeti Arnold Schwarzenegger által alakított Terminátor arcára Sylvester Stallone arcát hamisították a készítők

Maga a videómanipulációs technológia 1997 óta ismert[42] és bizonyos esetekben – például utószinkron – teljesen elfogadott módszerként jelent meg a szakirodalomban, azonban a technológiának a valós idejű kiterjesztése ezt a módszert különösen veszélyessé teszi. 2016 júniusában Las Vegasban a számítógépes megjelenítéssel és mintafelismeréssel foglalkozó konferencián (Computer Vision and Pattern Recognition, CVPR 2016) a német Max Planck Intézet kutatói olyan módszert mutattak be, amely képes egy éppen most sugárzott videófolyamot valós időben eltéríteni és módosítani, ennek eredményeként egy olyan videót látunk, amelyikben az élő műsorban szereplő személy kizárólag a manipulátor által meghatározott tartalmat közvetíti[43]. A veszély abban rejlik, hogy a hitelességet is valós időben kellene tudnunk megállapítani, ez különösen nehéz problémának tűnik ebben az esetben.

[42] https://www2.eecs.berkeley.edu/Research/Projects/CS/vision/human/bregler-sig97.pdf
[43] https://web.stanford.edu/~zollhoef/papers/CVPR2016_Face2Face/paper.pdf

A jelenség kapcsán számos szakértő megkongatta a vészharangot és „információs apokalipszist", „valóság-apátiát" vagy az információk hitelességének az azonnali és teljes elvesztését prognosztizálta. Egy olyan közegben, ahol a megjelenő információkról nem feltételezhető a hitelesség, valóban nehéz valódi információkhoz jutni, ami okozhatja a tájékoztatásba vetett bizalom elvesztését, aminek pedig egyes következménye az alultájékozottság. Másrészről, ha bármilyen információ hitelessége egyszerűen megkérdőjelezhető csak azáltal, hogy létezik olyan technológia, amellyel ez hamisítható – tehát a látott az biztos hamis, a valódi információk hitelessége is kétségbe vonható.

A hitelesség megállapítása tehát nagyon nehéz lehet számos esetben, de az elektronikus aláírás (különösen a legalább fokozott biztonságú elektronikus aláírás) képes mind a forrás (küldő) eredetiségét, mind pedig a tartalom sértetlenségét megállapíthatóvá tenni rögzített digitális tartalmak (fájlok, folyamok) esetében. Ez azonban nem segít akkor, ha a hamis hír kibocsátója pontosan ezt szándékozik tenni, mivel akkor ő maga fogja hitelesíteni a saját hamis tartalmát. Megnyugtató azonban, hogy a hétköznapok szintjén ma még senki sem szeret másról szóló hamis híreket a saját nevével/címével hitelesítetten közzétenni, ugyanis saját magunkról nem szoktunk szándékosan hamis és hitelesített információt kibocsátani, illetve nem is szoktunk ilyet hitelesíteni. Emlékeztetőül: az elektronikus aláírás képes arra, hogy a kibocsátót és a kibocsátott tartalmat hitelesítse, azaz meg tudja erősíteni, hogy az adott tartalom valóban abból a forrásból származik, amit látunk, és valóban az a tartalom származik onnan, amit látunk, de sajnálatos módon a látottak igazságtartalmának igazolására nem használható.

Ez a védekezési forma így sok esetben alkalmazható lenne, ha a tartalmakat megbízható tanúsítvánnyal hitelesített legalább fokozott biztonságú elektronikus aláírással látnák el a kibocsátáskor. Például az elektronikusan közzétett Magyar Közlöny[44] tartalmát nem szokás megkérdőjelezni annak ellenére, hogy az aláíró nevét vélhetően kevesen ismerik a közlöny olvasói közül, sőt, mivel minősített elektronikus aláírással van a Magyar Közlöny ellátva, az aláírás sikeres ellenőrzése az aláíró személy azonosságát és az aláírt tartalom hitelességét teljes bizonyító erővel igazolja.

Mit lehet tenni a hamisított videók ellen? Egyrészről léteznek olyan egyszerű technikák, amelyekkel a gyengébb minőségű hamisítványok felismerhetők (például a videó lassításával az egyes képkockák közötti átmenetek kidolgozottsága vagy kidolgozatlansága, illetve maga a képkocka élessége vagy elmosódottsága adhat támpontot a valódiságot illetően),

[44] https://magyarkozlony.hu/hivatalos-lapok/58J8ig1eNRRUrayChh6V5d3b410abfd0c/dokumentumok/00d713b096cfd5b140a5770103b711d36569efe0/letoltes

másrészről a gépi tanulás felhasználható a hamis videók felismerésére is (példának erre a DecLarE[45] módszert említhetjük meg, amit 2018 októberében mutattak be). A kritikus gondolkodás itt is előnyös, kétség esetén több, lehetőleg független forrásból keressünk megerősítést, illetve próbálkozzunk meg annak a kérdésnek a megválaszolásával, hogy ki és miért hozhatta létre az éppen megtekintett tartalmat, játszhatott-e szerepet ebben bármilyen manipulációs cél, amit a megtekintés során megjelenő érzelmeink jelezhetnek leginkább.

5.7.9 Internetes zaklatás

Az internetes zaklatás – gyermekeket és felnőtteket is ideértve – az internetes világunknak egyik legnagyobb és egyre gyakoribb problémája. Az internetes zaklatás – bántalmazás a virtuális térben, az infokommunikációs technológia felhasználásával (internetes oldalak, közösségi portálok, fórumok, e-mail, SMS, azonnali üzenetküldők). A zaklatásnak számos típusa ismert és kategorizált:

- zaklatás: támadó, sértő, felzaklató üzenetek küldése sorozatosan,
- lejáratás – rossz hírnév terjesztése: Valótlan pletykák terjesztése, amelyek megszégyenítik, lejáratják a másikat (akár pl. hamis fényképek terjesztése),
- flaming: online „háború”, támadás, veszekedés: dühös, támadó, trágár hozzászólások nyilvános fórumokon (gyakran online politikai, vallási, ideológiai vita),
- identitáslopás: az áldozat e-mail címének, vagy közösségi oldalon a profiljának feltörése azzal a szándékkal, hogy a nevében küldjön sértő, kellemetlen üzenetet másoknak,
- kiközösítés: az online közösség egy tagjának a csoportból való kirekesztése,
- kibeszélés: titkok megosztása, személyes információk nyilvánosságra hozása, elküldése,
- becsapás: a másik becsapása, kellemetlen vagy intim információk kicsalása majd megosztása,
- cyber stalking: fenyegető, megfélemlítő üzenetek küldése, a másik online szokásainak megfigyelése és ezek felhasználása félelemkeltésre, hogy a másik a saját biztonságát veszélyeztetve érezze,

[45] https://arxiv.org/abs/1809.06416

- sexting: szexuálisan provokatív fényképek, videók készítése, és továbbküldése a felvételeken szereplő(k) engedélye nélkül. A téma különösen aktuális, mivel az okostelefonok egyre fiatalabb korosztályok számára elérhetőek és ezzel jelentősen megnő a lehetősége annak, hogy kiskorú készít és/vagy továbbít szexuális tartalmú képeket vagy videókat kiskorúakról, amely tevékenység a Btk. (Büntető Törvénykönyv) 204. § Gyermekpornográfia hatálya alá esik, és extrém esetben, ha mondjuk egy ilyen felvételt valaki megoszt egy iskolai chatcsoportban, akkor ez akár 8 évig terjedő szabadságvesztéssel is büntethető.

Az internetes zaklatás lehetséges okai:

- anonimitás/személytelenség – a támadó azt gondolja, hogy láthatatlan tud lenni, kicsi a lebukás veszélye,
- kevesebb visszajelzés – eldurvulás; amíg a fizikai kontaktusos nézeteltéréseknél a támadó, agresszor látja a másik reakcióit és ez hatással is tud lenni rá, addig az online térben elkövetett zaklatásoknál nincs ilyen azonnali visszajelzés, emiatt a támadó sokkal inkább el tudja ragadtatni magát,
- nincs közösségi visszajelzés – szintén visszautalva a fizikai veszekedésekre, ha az egy valós közösségben történik, akkor a közösség más tagjai is tudnak visszajelzést adni, amivel meg lehet fékezni adott esetben egy eldurvuló zaklatást. Ilyen a legjobb esetben is közösségi oldalakon vagy csoportokban fordul elő, de sajnos elég sok a szemlélődő, passzív résztvevő, akik inkább nem folynak bele a konfliktusba. A valós fizikai konfliktus esetén ezt nehezebben tudják megtenni és inkább beavatkoznak. Az online térben ezt sajnos el tudják kerülni.
- személyes kommunikációban lévő fékek hiánya – személyes kommunikációban azonnal lehet verbális és nonverbális visszajelzést adni, illetve rábírni a támadó felet, hogy hagyja abba, amit csinál,
- az áldozat nem tud menekülni, hiába van otthon például. Az online világból nem lehet elmenekülni – vagy nagyon nehéz. Nem áll meg az online zaklatás az iskolakapuban vagy a munkahely kijáratánál. Emiatt az áldozat fokozottan rosszul érzi magát, ha pedig mégis kilép az adott virtuális közösségi térből, akkor egyrészt minden információforrást elveszít, másrészt kirekesztettnek érezni magát, ami szintén nagyon rossz.
- gyorsan nagy nyilvánosság. Egy közösségi megosztással pillanatok alatt kaphat egy zaklatás nagy nyilvánosságot, ami ebben a mivoltában kikerül az eredeti résztvevők kontrollja alól és akár beláthatatlan következményei is lehetnek.

- nehéz fellépni ellene (felhasználó törlés és tiltás, poszt, fotó törlés, bizonyítás).

Az internetes zaklatás negatív hatással lehet a testi és lelki egészségre, fejlődésre, társas kapcsolatokra, iskolai és sport vagy egyéb teljesítményre egyaránt, és az alábbi következményei lehetnek:

- düh,
- szorongás,
- depresszió,
- magányosság,
- iskolakerülés, szökés,
- pszichoszomatikus betegségek,
- alacsony önértékelés,
- öngyilkossági gondolatok/befejezett öngyilkosság, amire számos példa akad.

Internetes zaklatás kezelési módszerei

- A zaklató felszólítása, hogy hagyja abba! (legfontosabb – visszajelzés adás)
- Azonnali, praktikus segítségnyújtás (tiltás, törlés, bejelentés)
- Segítségkérés: Kék vonal 116-111, http://www.kek-vonal.hu
- http://www.saferinternet.hu [t] – számos kiváló anyag van gyermekeknek, szülőknek, pedagógusoknak a téma feldolgozására.
- Ha kell, akár pszichológushoz, vagy hatósághoz fordulni

Problémát jelent, hogy a gyerekek jelentős része úgy gondolja, hogy jobban ért az internethez és a technológiához, mint a szülője vagy a pedagógusa. Emiatt sajnos nem fogadnak meg jótanácsokat, és nem fogadják el a tiltást, korlátozást büntetést sem.

5.7.9.1 Internetes zaklatás megelőzése

A legfontosabb dolog az internetes zaklatás megelőzése, azért, hogy ismerőseink, családtagjaink, barátaink, de legfőképp gyermekeink ne váljanak se áldozattá, se zaklatóvá. Ennek számos viszonylag egyszerű, ámde időt és energiát igénylő módszere van:

- felkészülni, megismerni a trendeket, szokásokat, képben lenni! Ha nem vagyunk felkészültek, akkor a gyerek/családtag nem fogad el, nem tőlünk kér tanácsot, segítséget!
- beszélgetni a gyerekkel, SOKAT beszélgetni – a bizalom kiépítése nagyon fontos!
- felkészülni a leggyakrabban használt app-ok, szolgáltatások és oldalak BIZTONSÁGOS használatára!
- ellenőrzés: elkérni a telefont, gyerekkel együtt átnézni, internet böngésző előzmények, Youtube előzmények, VIBER/Whatsapp/Snapchat/Tinder Messenger csoportokat!
- Facebookon és más közösségi oldalakon (Twitter, Instagram) legyen bejelölve ismerősként a gyerekünk, hogy tudjuk követni a közösségi aktivitásait!
- használjuk a szülői felügyelet programot és fektessük le a szabályokat! (pl. telefon használat korlátozása, idegenekkel nem ismerkedünk, nem találkozunk, ésszel publikálunk stb.)

5.7.10 Utazásbiztonság – biztonság útközben

A mindennapi életben is számtalan veszélynek vagyunk kitéve, mi magunk is, és ugyanígy ki vannak téve veszélyeknek az informatikai eszközeink és adataink is. Különösen igaz ez akkor, amikor elhagyjuk a jól ismert környezetünket, a mindennapi útvonalainkat és helyszíneinket.

Egy utazásra ritka, hogy készületlenül indulunk el. Mostantól ennek a felkészülésnek része kell, hogy legyen a digitális felkészülés is.

Az első lépés annak végiggondolása, hogy milyen informatikai eszközöket kell magunkkal vinnünk, amire feltétlenül szükségünk lehet. A szállodákban általában van széf, de ezekbe nagy méretű eszközök nem férnek el. Ajánlott nem azt az eszközt, például laptopot magunkkal vinni, amin az összes otthoni vagy céges adatunk van (főleg, ha nincs mentés).

Célszerű az iratainkról egy papíralapú vagy digitális másolatot készíteni. Különösen „macerás” ha külföldön vesznek el az irataink, mert akár a hazautazást is meg tudja gátolni, és

ilyenkor jól jöhet egy másolat. Utazás előtt nézzük meg, hogy a beutazáskor szükséges-e vagy ajánlott-e bejelentkezni a Magyar Nagykövetségre ott-tartózkodásunk ideje alatt. Ez főleg konfliktus sújtotta országokban ajánlott.

Kössünk biztosítást! Sok esetben a bankkártyánkhoz adnak valamilyen alapszintű utazás biztosítást, de ez nem mindig elegendő/megnyugtató. Érdemes olyan biztosítást választani, ahol a műszaki eszközök értékét is megtérítik probléma esetén. Fontos, hogy a biztosítások az adatok értékére, az adatvesztésből fakadó veszteségek megtérítésére nem terjednek ki!

Utazás előtt minden bankkártyánkra állítsunk be limitet és kártyahasználati sms küldést. Ezen kívül vegyük fel a telefonunkba a bankunk bankkártya letiltási telefonszámát vagy ellenőrizhetjük, hogy a mobilbanki applikációnkban ez hogyan működik. Jelezhetjük a bankunknál, hogy külföldre utazunk, nehogy a szokatlan helyszín miatt esetleg letiltsák a pénzügyi műveleteinket. Továbbá lehetőleg több kártyánk legyen, ha bármi történik az egyikkel, ellopják, le kell tiltani vagy fizikailag sérül, akkor legyen másik. Utazás kapcsán arra is érdemes lehet felkészülni, hogy a határon esetleg felkérnek bennünket egy Facebook-bejelentkezésre, vagy a laptop-jelszónk megadására.

ATM-es készpénzfelvételnél legyünk óvatosak, a turisták által látogatott helyeken sokkal gyakoribb a kártyamásolás (ATM skimming), mint bárhol máshol adott városban. Erre utaló jel lehet a ragasztóval összekent "csőr - kártyabeadó nyíláson lévő védelmi eszköz", vagy a nem villogó csőr, illetve bármi, ami nem az ATM-hez illeszkedik formában és színben.

Fontos, hogy ne posztoljuk már a repülőtérről a közösségi oldalakra az utazásunkat, mivel ez felhívás keringőre a betörőknek, hogy nem vagyunk otthon, potenciális célpont az otthonunk. Ha betörnek, akkor jellemzően a nagy értékű tárgyakat veszik magukhoz a betörők – például laptopok, tabletek, és az eszközzel együtt az adataink is elveszhetnek. Ha fentiek ellenére mégis tudatjuk a világgal, hogy nem vagyunk otthon, akkor legyünk nagyon körültekintőek a poszt láthatóságával kapcsolatban!

Érdemes előzetesen felkészülni egy-egy ország kultúrájából. A kulturális szokások eltérése befolyásolhatja, hogy milyen tartalmakat tudunk az interneten megtekinteni, hogy tudunk-e VPN-csatornákat használni, illetve, hogy hol milyen informatikai eszközt használhatunk.

Az eszközeinken remélhetőleg már alapesetben is van hozzáférés-kontroll (jelszó, jelkód, pin kód, ujjlenyomat vagy arcfelismerés), amennyiben nincs, állítsuk be valamelyiket. Ha lehet állítsunk be az eszközeinken háttértár-titkosítást. Így, ha elveszik az eszköz, vagy ellopják, a tolvajok nem fognak tudni sem belépni az eszközünkre, sem kikapcsolt állapotban esetlegesen a háttértár kiszerelésével és más eszközre csatlakoztatásával az adatainkhoz hozzáférni.

Indulás előtt frissítsünk be minden alkalmazást. Előfordultak már olyan esetek, ahol egy hotel WiFijére csatlakozó vendégeknek a támadók preparált rendszerfrissítéseket küldtek, amelyekkel át tudták venni az eszközök irányítását.

Publikus helyeken, például hotelek halljában, kávézók internet sarkaiban lévő számítógépeket lehetőleg ne használjuk – nem tudhatjuk, hogy milyen kártékony programok futnak rajtuk (például billentyűzet naplózó programok, trójai programok) – és ki fér még hozzá ezekhez a gépekhez. Ha mégis muszáj, akkor is csak olyan általános oldalak megtekintésére használjuk őket, ahol nem kell megadni semmilyen azonosítót, jelszót, vagy személyes adatot.

Miközben utazunk fokozottan ügyeljünk az értékeinkre és informatikai eszközeinkre! Alkalom szüli a tolvajt. Egy étteremben, a parkban egy padon, egy pillanatra elég nem figyelni és már el is tűnt az eszközünk. A tolvajok az ellopott eszközöket általában rögtön kikapcsolják, hogy ne lehessen lekövetni őket. Szintén figyelni kell a táskák zsebeire, vagy a hanyagul farzsebbe tett mobilra is. Bár túlzott óvintézkedésnek tűnik, de vannak országok, ahol gyenge a közbiztonság, és akár az utcán a tömegben vagy a közlekedési eszközökön is kikaphatják a kezünkből a telefonunkat – ráadásul erre nagyon összehangolt bandák vannak már.

Egyik tag meglöki az áldozatot, a másik kikapja a telefont a kezéből, harmadik elállja az utat, a negyedik „segítő szándékkal” feltartja, az ötödik pedig már el is tűnt a tömegben. Azt sem fogjuk tudni, hogy mi történt, ki mit csinált. A következő képen egy ilyen rablás videójának egy képkockáját látjuk.

63. ábra: Csoportosan elkövetett mobiltelefon rablás

Ebben a videóban egy ilyen „tökélyre fejlesztett" módszerkerült megörökítésre: https://www.youtube.com/watch?v=0B-DAVYrAso.

A publikus WiFi szolgáltatásokat is érdemes fenntartásokkal kezelni, és maximum olyan információk begyűjtésére használni, ahol nem adunk ki azonosítókat, jelszavakat vagy egyéb személyes adatokat. A publikus WiFi szolgáltatások esetében a WiFi-routeren áthaladó forgalom megfigyelhető. Amennyiben a csatlakozásnál valamilyen tanúsítványt is el kell fogadni, akkor tudjuk, hogy az egyébként titkos „https" forgalmunkat is láthatja az üzemeltető.

Érdemes beruházni egy data rooming (Magyarországon kívül használható adatkeret mobilinternet használatra) csomagra és inkább a mobilszolgáltatónk mobilinternetét használni, mint a publikus WiFiket. Illetve érdemes VPN (Virtual Privat Network – virtuális magánhálózat) szolgáltatást használni, de itt is csak olyan megbízható szolgáltatókét, ahol tisztázottak a felhasználási feltételek és követelmények. Egy friss elemzés szerint az ingyenes VPN szolgáltatók több, mint nyolcvan százaléka nem megfelelően kezeli a felhasználói adatforgalmát. Érdemes előzetesen tájékozódni.

Hazaérkezés után azonnal mentsük le a telefonokról, fényképezgépekről az adatokat, nehogy később véletlenül letöröljük őket. A törölt adathordozókról nem lehetetlen visszaállítani adatokat, de előfordulhat, hogy ez majdnem annyiba kerülne, mint az egész nyaralást megismételni. Legyünk körültekintőek!

5.7.11 Mesterséges intelligencia, és használatának veszélyei

Az elmúlt évek egyik legnépszerűbb témája a mesterséges intelligencia (MI) használata, és a használat veszélyei. Ezeket a veszélyeket számos kategóriába lehet csoportosítani, amelyek közül most a legfontosabbakat felsoroljuk.

- Adatbiztonsági és adatvédelmi veszélyek:
    - adatszivárgás – az MI rendszerek széles körben gyűjthetnek, tárolhatnak és feldolgozhatnak személyes adatokat, és ennek következtében fennáll a veszélye annak, hogy az adatok illetéktelen hozzáférése, lopása vagy kiszivárgása megtörténik.
    - adatbázisok és profilok kialakítása – az MI képes lehet részletes felhasználói profilokat és viselkedési mintázatokat kialakítani, ami sértheti az egyének magánéletét és személyes szabadságát.
    - diszkrimináció és elfogultság (bias) veszélyei , az algoritmusok előítélete – az MI algoritmusok azokat a biasokat is megtanulhatják, amelyek a bemeneti adatokban megtalálhatók, a nem körültekintő adatválasztás miatt. Ennek eredményeként diszkriminatív döntéseket hozhatnak például etnikai, nemi vagy egyéb szempontok alapján.
    - mély tanulás (Deep Learning) korlátai – a mély tanulás alapú rendszerek hajlamosak a túlzott kapcsolódások kialakítására az adatokban, és olyan összefüggéseket is felismerhetnek, amelyek szakmailag vagy társadalmilag nem elfogadottak.
    - az MI poisoning, vagy más néven adatmérgezés (data poisoning) – ez egy olyan technika vagy támadási módszer, amely során rosszindulatú szándékkal módosítják vagy manipulálják a mesterséges intelligencia (MI) rendszert betanító adatokat, vagy a tanítófolyamat során használt adatokat. Ennek lényege, hogy az MI algoritmusok hibás dolgokat tanulnak meg és ebből kifolyólag hibás döntéseket hoznak. Az adatmérgezés legfőbb célja általában az MI rendszer megtévesztése vagy félrevezetése, így olyan döntéseket hoz, amelyek a támadó számára előnyösek, vagy károsak lehetnek mások számára. Például, ha egy képfelismerő MI-t tanítanak be hamis vagy torzított képekkel, akkor az a rendszer az észlelés során a valóságot hamisan és torzítva azonosíthatja, vagy észlelhet a valóságban nem létező objektumokat vagy tulajdonságokat is. Az adatmérgezés akkor különösen veszélyes, ha

olyan döntéseket várunk el az MI-től, ami emberi életekre is veszélyes lehet, ilyen például a következő pontban említett autonóm rendszerek irányítása a közlekedésben,

- MI hallucináció – az "MI hallucináció" egy olyan kifejezés, amelyet azok a helyzetek vagy jelenségek leírására használnak, amikor mesterséges intelligencia (MI) rendszerek olyan információkat vagy adatokat hoznak létre, amelyek látszólag valóságosak vagy értelmesek, de valójában nem tükrözik a valóságot. Ezek a "hallucinációk" abból fakadnak, amikor az MI rendszer hibásan vagy tévesen értelmezi a bemeneti adatokat, vagy amikor túl nagy teret enged a kreativitásnak vagy nem ismer háttérinformációkat és ezért téves következtetéseket von le. Az ilyen fajta MI hallucináció megtéveszthetti a felhasználókat, akik nem rendelkeznek mélyebb tudással az adott témakörrel kapcsolatban. Ez különösen akkor veszélyes, ha kész és hiteles információként tüntetik fel az MI által generált információkat.

- Autonóm rendszerek veszélyei:
  - önvezető járművek - az MI irányította önvezető járművek esetében technikai hibák, biztonsági megszakítások vagy etikai dilemmák merülhetnek fel, például vészfékezési döntések során.
  - autonóm fegyverrendszerek - az MI alapú autonóm fegyverrendszerek veszélyeztethetik a béke és a biztonság stabilitását, mivel emberi beavatkozás nélkül képesek célpontokat kiválasztani és megtámadni.
- Szociális és gazdasági hatások:
  - munkahelyek elvesztése – az automatizáció és az MI berendezések növelhetik a munkahelyi leépítéseket, és gazdasági egyensúlytalanságot okozhatnak.
  - szociális szakadékok – az MI használata fokozhatja a digitális szakadékot, mivel azok, akik nem rendelkeznek hozzáféréssel vagy tudással, hátrányba kerülhetnek.
- Megbízhatóság és felelősség:
  - hibás döntések – az MI hibás döntéseket hozhat, amelyek emberi életekre vagy vagyonokra is kihatnak (például egészségügyben vagy pénzügyekben).

    - felelősség kérdései – az MI által vezérelt rendszerek esetében a felelősség kérdése összetett lehet, és nehéz lehet eldönteni, hogy a felelősség az emberi felhasználóké, a fejlesztőké, az üzemeltetőké vagy az algoritmusoké.
- Szabályozatlanság: az MI gyors fejlődése és alkalmazásának széles körű terjedése miatt gyakran előfordul, hogy a jogi és szabályozási keretek nem tartanak lépést az új technológiával. Ennek eredményeként felmerülhetnek etikai, adatvédelmi, szerzői jogi és egyéb általános jogbizonytalansági problémák. Jelen könyv frissítésének idején volt hír például, hogy számos híres író beperelte az egyik olyan céget, amelyik az írók engedélye nélkül készített olyan adathalmazokat, amelyekkel más MI algoritmusokat tanítottak be. Továbbá a szerzői jog területén született már olyan döntés az Egyesült Államokban, hogy a mesterséges intelligenciát nem illetik meg a szerzői jogok, bármit is hoz létre[46].

Az EU 2020-ban közzétette a Fehér Könyvet a mesterséges intelligenciáról[47], amelyben megjelentek mind az előnyök, mind pedig a hátrányok is:

> „A mesterséges intelligencia egy olyan stratégiai technológia, amely számos előnnyel jár a polgárok, a vállalatok és a társadalom egésze számára, feltéve, hogy emberközpontú, etikus, fenntartható és tiszteletben tartja az alapvető jogokat és értékeket. A mesterséges intelligencia jelentős hatékonyság- és termelékenységnövekedést kínál, amely erősítheti az európai ipar versenyképességét, és javíthatja a polgárok jólétét. Hozzájárulhat a legsürgetőbb társadalmi kihívások megoldásának megtalálásához is, beleértve az éghajlatváltozás és a környezet romlása elleni küzdelmet, a fenntarthatósággal és a demográfiai változásokkal kapcsolatos kihívásokat, valamint demokráciáink védelmét, és ahol szükséges és arányos, a harcot a bűnözés ellen.”

A mesterséges intelligencia keretrendszere ennek mentén jött létre az Európai Unióban[48]. A mesterséges intelligenciáról szóló fehér könyv további szabályozási végrehajtásaként 2022. szeptember 28-án elfogadták a mesterséges intelligenciáért való felelősségről szóló irányelvjavaslatot is[49]. Az oktatásban is nyilvánvaló módon fel lehet használni a mesterséges intelligenciát, így azok számára, akik ebben gondolkodnak, feltétlenül javasolható az EU etikai

[46] https://www.vg.hu/nemzetkozi-gazdasag/2022/02/nem-illeti-meg-szerzoi-jog-a-mesterseges-intelligenciat
[47] https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf
[48] https://digital-strategy.ec.europa.eu/hu/policies/regulatory-framework-ai
[49] https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

iránymutatásának ismerete a mesterséges intelligencia és az adatok oktatási és tanulási célú felhasználásáról is[50].

A biztonsági rendszerek is alkalmaznak ma már mesterséges intelligencia alapú megoldásokat, elegendő csak a biometrikus azonosításokat végző szolgáltatásokra gondolnunk, de számos más olyan szolgáltatást is meg lehetne említeni, amely mesterséges intelligenciát használ (pl. keresők, marketing célú profilozás, orvosi diagnosztikai rendszerek stb.). A mesterséges intelligencia tehát megjelent, megérkezett, és úgy tűnik, hogy velünk is marad még egy darabig. A jövőnk azonban ettől még nem lett kiszámíthatóbb, de remélhetőleg azért ezzel biztonságosabb lesz.

[50] https://op.europa.eu/en/publication-detail/-/publication/d81a0d54-5348-11ed-92ed-01aa75ed71a1/language-hu

6 Mellékletek

6.1 Ajánlott irodalom

Az ajánlott irodalom időbelisége feltűnhet a kedves olvasónak. Fontos megjegyezni, hogy a lenti irodalomlista a mai napig használatos és alapvető szakmai tartalmakat hordoz. Ugyanakkor számos publikáció, riport, tanulmány, értekezés már nem jelenik meg nyomtatott könyv formájában, ezeket az interneten keresztül érhetjük el.

[1] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[2] Andrew S. Tannenbaum: Számítógéphálózatok; Panem–Prentice-Hall, 1999

[3] Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság- és Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék Biztonság Menedzsment Csoport; Az informatikai biztonság fogalmainak gyűjteménye; Ajánlás ; 1.0 változat; 2003

[4] COBIT® 2019 Framework: Introduction and Methodology, ISACA, 2018. ISBN 978-1-60420-763-7

[5] COBIT 4.1 – Control Objectives for Information and Related Technology, 1996-2007 IT Governance Institute

[6] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012. ISBN: 9781604202373

[7] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; August 2005 Version 2.3 CCMB-2005-08-001

[8] Dr. Krasznay Csaba: Kiberbiztonság a XXI. században, Katonai Nemzetbiztonsági Szolgálat, 2022; ISBN: 9786156128126 (PDF)

[9] Kevin Mitnick: A behatolás művészete, PERFACT-PRO Kft.; 2006; ISBN: 9789638647252

[10] Kevin Mitnick: A legkeresettebb hacker, HVG Kiadói Zrt., 2012; ISBN: 9789633040898

[11] Kevin Mitnick: A megtévesztés művészete, PERFACT-PRO KFT.; 2003; ISBN: 9789632065557

[12] Ryan Russell: A Háló kalózai – Hogyan lopjunk kontinenst, Kiskapu Kft., 2005; ISBN: 9789639301993

[13] Simon Singh: Kódkönyv - A rejtjelezés és rejtjelfejtés története, Park Kiadó, 2007; ISBN: 9789635307982

[14] Solymos Ákos: Frici, Fülöp és a hackerek, Underground, 2019; ISBN: 9786150056876

[15] The National Strategy to Secure Cyberspace, February 2003, White House, USA

6.2 Internetes hivatkozások jegyzéke

[a] http://real.mtak.hu/11147/

[b] https://www.nki.gov.hu/

[c] https://www.isaca.org/resources/cobit

[d] https://static.hlt.bme.hu/semantics/external/pages/bit/hu.wikipedia.org/wiki/Sz%c3%a1m%c3%adt%c3%b3g%c3%a9p-architekt%c3%bara.html

[e] http://en.wikipedia.org/wiki/Cloud_computing

[f] http://24.hu/media/2016/08/01/ezek-a-legnepszerubb-weboldalak-a-magyar-es-a-tersegbeli-fiatalok-koreben

[g] http://www.magyarorszag.hu

[h] https://lensesview.com/10-million-passwords-and-usernames-published-online/

[i] https://documentation.help/WinRAR/HELPFileMenu.htm

[j] https://hu.wikipedia.org/wiki/Makr%C3%B3

[k] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016R0679

[l] https://hu.wikipedia.org/wiki/Domain_Name_System

[m] http://hu.wikipedia.org/wiki/Captcha

[n] http://www.howtogeek.com/72130/learn-how-to-securely-delete-files-in-windows/

[o] http://hu.wikipedia.org/wiki/PGP

[p] https://cocosign.com/resource/electronic-signatures-legality-in-the-world/

[q] https://www.pcx.hu/szunetmentes_tap

[r] http://www.backup-utility.com

[s] https://www.linux.com/news/timevault-simplifies-data-backup-ubuntu-users/

[t] http://www.saferinternet.hu

[u] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

[v] https://en.wikipedia.org/wiki/MAC_spoofing

[w] http://www.origo.hu/gazdasag/20180712-a-facebook-az-oroszoknak-is-adott-el-felhasznaloi-adatokat...

[x] http://www.bankszovetseg.hu/Content/Hitelintezeti/034Szeplaki.pdf

[y] https://www.statista.com/statistics/218493/paypals-total-active-registered-accounts-from-2010/

[z] https://www.paypal.com/hu/webapps/mpp/ua/servicedescription-full?locale.x=hu_HU

[aa] https://en.wikipedia.org/wiki/3-D_Secure