

# IT biztonság közérthetően



Neumann János Számítógép-tudományi Társaság

*Erdősi Péter Máté, CISA*  
*Solymos Ákos, CISM, CRISC*

# IT biztonság közérthetően

verzió: 1.3  
2017. június

Kiadja a Neumann János Számítógép-tudományi Társaság (NJSZT)

Készítette a Neumann János Számítógép-tudományi Társaság megbízásából az Időérték Oktatási, Kereskedelmi és Tanácsadó Kft. és az NFS Informatikai és Szolgáltató Bt.

Erdősi Péter Máté CISA és Solymos Ákos CISM, CRISC

Kiadó: Neumann János Számítógép-tudományi Társaság  
1054 Budapest, Báthori u. 16.

Felelős kiadó: Alföldi István ügyvezető igazgató

© Neumann János Számítógép-tudományi Társaság, 2017. június  
Minden jog fenntartva!

**ISBN: 978-615-5036-12-5**



A könyv elkészítését a QUADRON Kibervédelmi Szolgáltató Kft. támogatta.

## Tartalomjegyzék

<b>1. Bevezetés</b>	8
<b>2. Biztonsági alapfogalmak</b>	10
2.1 Biztonság	10
2.2 Kibertér	11
2.3 Nemzeti Kibervédelmi Intézet	12
2.4 A biztonság koncepcionális megközelítése	13
2.5 Információkritériumok	15
<b>3. Információrendszerek</b>	17
3.1 Hardveres infrastruktúra	17
3.2 Alkalmazások, szolgáltatások	18
3.2.1 Ismeretszerzés és kapcsolatteremtés interneten	20
3.2.2 Elektronikus ügyintézés	21
3.3 Számítógép hálózatok	21
<b>4. Fenyegetések, támadások</b>	22
4.1 Rosszindulató szoftverek	23
4.2 Jellemző támadási formák és módszerek	26
<b>5. Fenyegetettségi és támadási trendek az elmúlt évekből</b>	29
5.1 Személyes adatokat érintő incidensek	30
5.2 E-mail fenyegetettségek, kártékony programok és botnetek	31
5.3 Mobileszközök fenyegetettségei	32
5.4 Zsarolóvírusok (Ransomware)	33
<b>6. A védelem kialakítása</b>	34
6.1 Felhasználók felelőssége az incidensek, biztonsági események során	36
6.2 A bizalmasság	36
6.2.1 Bizalmasság az operációs rendszerben	38
6.2.2 Merevlemezek és USB-lemezek titkosítása	39
6.2.3 Titkosítás irodai programcsomagokban	40
6.2.4 Bizalmasság tömörített állományoknál	42
6.3 Hálózat és bizalmasság	42

6.3.1	Hozzáférés-védelem, jelszavak, hitelesítés.....	44
6.3.2	WiFi eszköz biztonsági beállításai .....	48
6.3.3	E-mail .....	51
6.3.4	Azonnali üzenetküldés.....	56
6.3.5	Tűzfalak .....	56
6.4	Adatvédelmi megfontolások .....	57
6.4.1	Védelem böngészés közben .....	59
6.4.2	A látogatott oldalak biztonsága .....	61
6.4.3	Aktív tartalmak és a biztonság .....	64
6.4.4	A böngészőben tárolt adatok biztonsága.....	66
6.4.5	Bizalmassági eszközök közösségi oldalakon .....	70
6.4.6	Az adatok végleges törlése .....	74
6.5	A sértetlenségről.....	75
6.5.1	Digitális aláírás .....	75
6.5.2	Kivonatok (hash-ek) .....	78
6.6	A rendelkezésre állás megteremtése .....	79
6.6.1	Fájlok biztonsági mentése .....	82
6.6.2	Védelem az áramellátás hibái ellen.....	85
6.7	Komplex megközelítést igénylő fenyegetettségek és védelmi megoldások.....	86
6.7.1	Végpontvédelem és vírusvédelem .....	86
6.7.2	Biztonságos Internet bankolás .....	89
6.7.3	Biztonságos bankkártya használat – internetes fizetés .....	90
6.7.4	Internetes zaklatás .....	93
<b>7.</b>	<b>Mellékletek</b> .....	<b>96</b>
7.1	Ajánlott irodalom .....	96
7.2	Internetes hivatkozások jegyzéke.....	97

## Ábrajegyzék

1. ábra Biztonsági koncepció.....	13
2. ábra Felhő-alapú szolgáltatások .....	19
3. ábra Leggyakoribb alkalmazások a "Z" generáció körében.....	21
4. ábra Személyes adatokat érintő incidensek .....	30
5. ábra E-mail fenyegetettségek, kártékony programok és botnetek.....	31
6. ábra Mobileszközök fenyegetettségei.....	32
7. ábra Zsarolóvírusok növekedési trendje.....	33
8. ábra Hozzáférések megadása Windows operációs rendszerben .....	39
9. ábra USB-lemez titkosítása Linuxon .....	40
10. ábra Megnyitási jelszó beállítása Mac Microsoft Word 2016 szövegszerkesztőben.....	41
11. ábra Megnyitási jelszó beállítása Mac Microsoft Excel 2016 szövegszerkesztőben .....	41
12. ábra Jelszó beállítása archiv állomány létrehozásakor .....	42
13. ábra Védett hálózati csatlakozások megjelenítése .....	43
14. ábra Bejelentkezés VPN hálózatba .....	45
15. ábra 25 leggyakrabban használt jelszó .....	46
16. ábra KeePass Jelszóséf .....	48
17. ábra Vezetéknélküli hálózat titkosítás beállítás.....	49
18. ábra Példa nyílt WiFi rendszer beállításaira .....	50
19. ábra MAC szűrés beállítása WiFi eszközön.....	51
20. ábra Adathalász levél példa.....	53
21. ábra Zsarolóvírust tartalmazó levelek "Tárgy/Subject" mezői és eloszlásuk.....	54
22. ábra Zsarolóvírust tartalmazó e-mail hamisított feladóval .....	55
23. ábra Zsarolóvírust tartalmazó levél, a címzett a behamisított feladó.....	56
24. ábra Uniform Resource Locator - URL.....	61
25. ábra McAfee SiteAdvisor – a megbízható weboldalakért .....	63
26. ábra Biztonságos weboldal jele a lakat ikon.....	63
27. ábra Captcha .....	64
28. ábra Böngészési adatok törlése Firefoxban .....	68
29. ábra Inprivate böngésző üzemmód Internet Explorer .....	69
30. ábra Privát böngészés Firefox böngészőben.....	69

31. ábra Inkognító üzemmód Chrome böngészőben.....	70
32. ábra Adatvédelmi beállítások közösségi oldalon .....	71
33. ábra Facebook alkalmazások jogosultságai .....	73
34. ábra Facebook által rólunk tárolt adatok másolatának letöltése .....	73
35. ábra Végleges adattörlés szoftveresen .....	75
36. ábra dDOS támadás megrendelő felület 1. rész .....	80
37. ábra dDOS támadás megrendelő felület 2. rész .....	81
38. ábra dDOS támadás megrendelő felület 3. rész .....	81
39. ábra Windows Backup.....	83
40. ábra Okostelefonok fontos adatainak mentése .....	84
41. ábra Adatok mentése Windows környezetben (Aomei backup)).....	84
42. ábra Szünetmentes otthoni áramellátó eszköz.....	85
43. ábra Teljes rendszervizsgálat Norton Security programmal .....	87
44. ábra Teljes rendszervizsgálat eredménye, ha vírusos a vizsgált számítógép .....	88
45. ábra Tranzakció hitelesítő SMS üzenet.....	89
46. ábra Kártyamásoló eszköz ATM-en.....	91
47. ábra VISA Virtual kártya internetes fizetéshez .....	92

## 1 Bevezetés

Olyan világban élünk, ahol életünk valamennyi, legapróbb része is az infokommunikáció látható vagy láthatatlan együttműködését igényli.

*„A fejlődés ellen nincs gyógymód”* – mondta Neumann János a múlt század ötvenes éveiben – ma már az ezzel járó felelősségre is felhívná a figyelmet.

Naponta olvasunk zsarolóvírusokról, amelyek pénzt követelnek azért, hogy számítógépünket vagy okos eszközünket tovább használhassuk. Naponta olvashatunk hackertámadásokról, amelyek jobb esetben csak egy-egy megcélzott közösségi portált törnek föl, rosszabb esetben akár kiberháborút is jelenthetnek.

A támadók különösen nagy előszeretettel használják fel az otthoni, gyengén védett számítógépeket, amelyek egyenként persze nem jelentenek túl nagy fogást, milliós nagyságrendben azonban már a világ napi életét befolyásoló tényezővé is válhat megtámadásuk. Az otthoni eszközök védelme is nagyon fontos, de ennél talán még fontosabb annak megértése, hogy a munkahelyen használt eszközök biztonság tudatos használata nélkül milyen óriási károk keletkezhetnek. Elég csak arra gondolni, hogy saját tabletjét, okos telefonját a munkahelyi rendszerbe kapcsolva milyen problémákat okozhat valaki, ha nem kellő gondossággal jár el.

A digitalizáció korában egyre kevésbé elképzelhető, hogy ne találkozzunk az élet valamennyi területén az eszközökkel és azok biztonságos használatának követelményével: ma már gyakorlatilag valamennyi munkahely, ezek között a sérülékenységi szempontjából különösen kritikus közszolgálati, kormányzati munkahelyek is érintettek.

Miközben ma már az életünk nagy részét a közösségi oldalakon töltjük, magunkról mindenféle információt megosztva, interneten bankolunk, webáruházakban vásárolunk – és ezek mind törekszenek is arra, hogy biztonságos környezetet teremtsenek, mégis egyre több és professzionálisabb veszélyeztetésnek is ki vagyunk téve, ha nem vagyunk elegendően körültekintőek. Könyvünk alapvetően azt a célt szolgálja, hogy mindenki, különösebb kötöttség nélkül áttekinthesse a veszélyeket és a „kockázatokról és mellékhatásokról” ne kelljen nem várt események bekövetkezése után tájékozódnia.


Könyvünkben ezeket a napjainkban egyre gyakrabban előforduló és megfelelő gondossággal elkerülhető problémákat foglaljuk össze: rosszindulatú szoftverek, e-mail fenyegetettségek, kártékony programok és botnetek, mobileszközök fenyegetettségei, zsarolóvírusok (ransomware), hozzáférés-védelem, WiFi eszköz biztonsági beállításai.



Könyvünk célja összefoglalni valamennyi olyan szempontot, amely felhasználói, hangsúlyozottan nem informatikai tudásra építő nézőpontból, az eszközök tudatos használatával segíthet az eszközök által kiszolgált rendszerek és adatok biztonságának megőrzésében.

Különösen fontosak ezek a készségek abban a világban, amely törvényt is alkotott az információs biztonságról, sőt az Európai Unió által 2018-ban bevezetni szándékozott GDPR (General Data Protection Regulation) miközben a személyes adatok biztonságát kívánja védeni, újabb szempontokat vet fel a saját adatok körütekintő használatával kapcsolatban. A Neumann János Számítógép-tudományi Társaság (NJSZT) jelmondata - „Tudás, Elkötelezettség, Felelősség” - kötelezi a társaságot a civil társadalom infokommunikációs világban való eligazodásának maximális támogatására. A könyvet a téma kiváló szakemberei írták – és a téma fontossága miatt a könyv elkészítésében az NJSZT együttműködik a Nemzeti Kibervédelmi Intézettel, valamint a Nemzeti Közzolgálati Egyetemen alakult Kiberbiztonsági Akadémiával.

A könyvben összefoglalt ismeretek nemcsak arra alkalmasak, hogy a napi gyakorlatban segítsenek elkerülni a rendszereknek sérülést okozó hibákat, hanem arra is, hogy az ECDL informatikai biztonság moduljának tankönyvéül szolgáljon.

Az  az informatikai írástudás felhasználói szintű keretrendszere, amelyet Magyarországon eddig már több mint félmillió ember megismert, és a több mint tíz moduljából az egyik nem véletlenül az informatikai biztonság.

Budapest, 2017. június

Alföldi István, *CGEIT*  
ügyvezető igazgató  
NJSZT

## 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 (étel, ital, lakás) és a jövőben sem várható ebben jelentősebb mértékű változás. Hasonló értelemben szoktuk használni a „közbiztonság” fogalmát is – ha a környezetünkben elvétele fordul elő bűncselekmény, akkor jónak érezzük a közbiztonságot, 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 mind a két esetben arról van szó, hogy a biztonság a szubjektum számára egy kedvező állapot, amelynek megváltozását nem várja, de nem is tudja kizárni. Idealizált, édenkerti esetben ez az állapot örökkön-örökké fennmaradhat. Azonban a világ 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<sup>1</sup>.

A biztonság tehát a minőség és a megbízhatóság mellett a harmadik olyan követelmény, amelyet figyelembe kell venni a hosszútávú működés fenntartása szempontjából. Három **adatbiztonsági követelmény** létezik:

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

A tárgyban további három fogalmat is szoktak használni, amelyek értelmezése olykor nem egyértelmű:

---

<sup>1</sup> [http://uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi\\_szemle/szamok/2013/2013\\_4/2013\\_4\\_alt\\_urmosi.pdf](http://uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2013/2013_4/2013_4_alt_urmosi.pdf)

- **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 információrendszerekben 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 információ-biztonság fogalmával, egyébként szűkebb értelmű nála.
- **információ-biztonság:** tények, utasítások, elképzelések emberi vagy gépi úton formalizált, továbbítási, feldolgozási vagy tárolási célú reprezentánsai bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése. Amennyiben az „adat” fogalmába beleértjük az emberi formalizálást is (beszéd, előadás, beszélgetés), akkor egyenértékű az informatikai biztonság fogalmával, egyébként bővebb nála.

## 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 a Magyarország Nemzeti Kiberbiztonsági Stratégiája is, az 1139/2013. (III. 21.) Kormányhatározat [2] formájában.

A stratégia a kibertér fogalmát így definiálja:

„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információrendszerek, 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 Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.”

Nem hagyható ki a kibertér fogalmából a „kutatási, felsőoktatási és közgyűjteményi hibrindhálózat” 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 feladatokat - alapvetően - az állami és önkormányzati szervek vonatkozásában. Ezen komplex feladatkörének köszönhetően az Intézet az elektronikus információs rendszerek teljes információbiztonsági életciklusára vonatkozóan rendelkezik feladatkörrel, továbbá nyomon tudja követni és segíteni tudja azok alakulását, beleértve a tervezési szakaszt, a szabályozást, az ellenőrzést, valamint az incidenskezelést egyaránt.

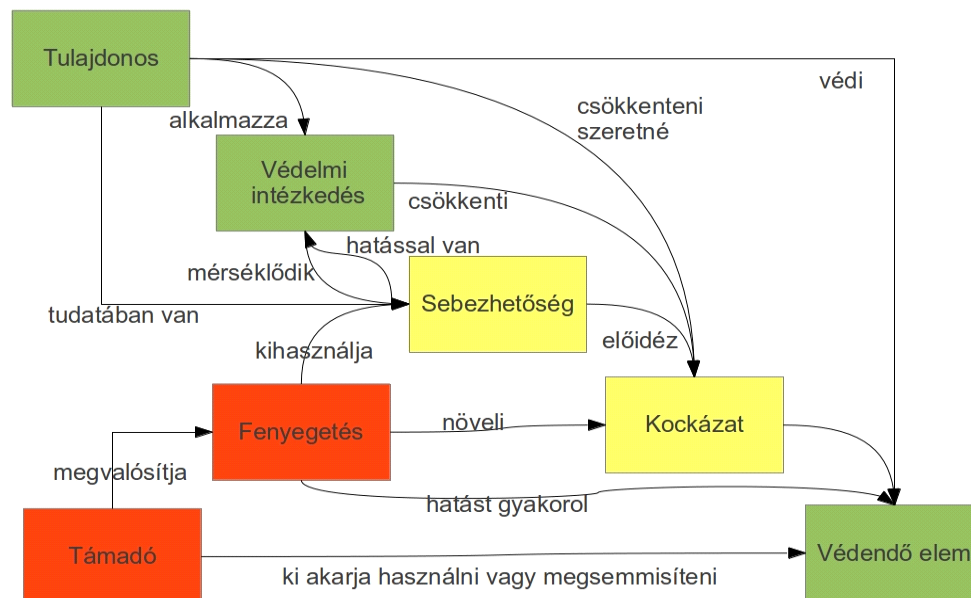
Az NKI részét képező Kormányzati Eseménykezelő Központ az országon belüli koordinációs szervezeteként végzi az internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálását, továbbá közzéteszi a felismert és publikált szoftver sérülékenységeket. Főbb feladatai fentiekén 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. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a teljes magyar kibertér biztonságának erősítéséhez.

További információ az Intézetről a <http://www.govcert.hu/> [q] és a <http://neih.gov.hu> [r] oldalon olvasható.

## 2.4 A biztonság koncepcionális megközelítése

A Common Criteria [3], melyet szoftverrendszerek biztonsági értékelésére dolgoztak ki – és amely ISO 15408 szabványként is ismert, **a biztonság koncepcióját** a 2.3 verziójában fogalmazta meg a rendszerek tulajdonságait is figyelembe véve a maga teljességében. A koncepció tartalmazza a támadót, a támadásokat, a védelmet megvalósító tulajdonost, a védelmi intézkedéseket és a védendő elemeket egyaránt.



1. ábra Biztonsági koncepció

Az ábrán szereplő fogalmak definícióit a következőkben adjuk meg [4] felhasználásával:

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

- **Támadás:** A támadás egy, az erőforrások bizalmassága, sértetlensége és/vagy rendelkezésre állása ellen, egy sebezhetőségből kiinduló, egy fenyegetést megvalósító folyamat.
- **Fenyegetés:** A fenyegetés a támadás lehetősége, vagy a biztonság megsértésének lehetősége, a támadás tárgyát képező erőforrásra.
- **Kockázat:** A kockázat annak a lehetőségnek a valószínűsége, hogy egy fenyegetés támadás útján kárkövetkezményeket okoz. Kárkövetkezmény lehet anyagi, jogi, reputációs, humán erőforrást érintő
- **Védendő elemek:** a szervezet vezetősége (menedzserei) által a küldetést/üzleti 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 következő koncepcionális állítások olvashatók ezek után 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 sebezhetőségre, mérséklük azok hatását a védendő elemekre nézve.
- A támadó esélyt ad a fenyegetések bekövetkezésének, 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 a sikeres támadások számával, valamint a kárkövetkezmények és a védelemre fordított erőforrások számszerűsítésével.

## 2.5 Információkritériumok

Az informatikai rendszerek használatának minden esetben valamely konkrét célja van, nem öncélú. A folyamatok bemeneteik és kimeneteik előállításához információrendszereket használnak, amelyek működése információtechnológiai, vagyis informatikai hardver- és szoftver-alapú megoldásokat igényel. Ennek következtében a folyamatok informatikafüggése – és ebből adódóan az energiafüggése is - kialakul, ezek nélkül a gyakorlatban már nem tudják az információfeldolgozásra épülő feladataikat ellátni.

Az információrendszerek **információkat** dolgoznak fel. Az információ fogalmának meghatározása az adatfeldolgozás fejlődésével együtt változott. Amíg azt gondolták, hogy értelmező tevékenységet csak az ember képes végrehajtani, addig az információt csak az emberi agyban létezőnek gondolták. Miután felismerték az egyes biológiai rendszerek információ-feldolgozási képességét (pl. DNS, dezoxiribonukleinsav), illetve megjelentek a számítógépek és elkezdtek gyorsan, nagy tömegű adatot feldolgozni, ez megváltozott és új tudományterületek kialakulásához vezetett (pl. információtörténet, kommunikáció-elmélet, információ-fizika, adatbázis-kezelés). Az információ (információ) szó hallatán rendezett adatokra vagy összefüggő minta szerint rendezett tényekre utalunk, amelyek között általában nincs éles határvonal. A rendezettség más szóval azt jelenti, hogy az információ minden esetben valamely adatfeldolgozási művelet eredményeként áll elő, hiszen a rendezettséget valahogyan el kell érni.

Az információrendszerek használatának a célja valamely társadalmi, gazdasági vagy magánszféra folyamat támogatása bemeneti-kimeneti információkkal, illetve azok előállítási képességével. Az információk minősége között azonban lehetnek különbségek, melyek erőteljesen befolyásolják a cél mennyiségi és minőségi elérhetőségét. Ezeket a különbségeket az **információ-kritériumok** alapján lehet megérteni.

A célkitűzések elérése érdekében az információknak ki kell elégíteniük bizonyos kontrollkritériumokat. A szélesebb körű minőségi, pénzügyi megbízhatósági, és biztonsági követelmények alapján az alábbi hét megkülönböztethető, egymást néhol minden bizonnyal átfedő információ-kritérium került meghatározásra a szakirodalomban (COBIT 4.1 [5]):

- **hatékonyság:** arra vonatkozik, hogy az információkat az erőforrások optimális (legtermékenyebb és leggazdaságosabb) kihasználásával biztosítsák

- **hatásosság/eredményesség:** azzal foglalkozik, hogy az információk a folyamat szempontjából jelentőséggel bírnak, és hogy az információkat időben, helyes, ellentmondásmentes és használható módon biztosítsák
- **megfelelőség:** a folyamatokat érintő törvények, jogszabályok, szabályozások és szerződéses megállapodások – azaz kívülről előírt jogi és önként vállalt követelmények és belső irányelvek – betartását jelenti, amelyeknek a folyamat a tárgyát képezi
- **megbízhatóság:** a vezetés számára olyan időszerű és pontos információk biztosítása, amelyek az adott szervezet működtetéséhez, pénzügyi megbízhatóságához és irányításához szükségesek
- **bizalmasság:** arra vonatkozik, hogy megakadályozza, a bizalmas információk engedély nélküli megismerését, vagyis fontos információkhoz illetéktelenek ne férjenek hozzá
- **sértetlenség:** az információknak a szervezeti értékek és elvárások szerinti pontosságára, változatlanóságára és teljességére, valamint az információk érvényességére vonatkozik
- **rendelkezésre állás:** azzal foglalkozik, hogy az információk akkor álljanak rendelkezésre, amikor azokra a folyamatnak szüksége van most, és a jövőben; a szükséges erőforrások, és az erőforrások szolgáltatási képességeinek védelmére is vonatkozik

Az információ felhasználhatóságára vonatkozik az első négy kritérium, a biztonságra pedig az utolsó három követelmény vonatkozik. Minden **információbiztonsági** törekvés arra irányul, hogy a három biztonsági követelménynek való megfelelést minden időpillanatban biztosítsák az összes védendő információra és környezetükre egyaránt. Egy szervezet akkor mondhatja el magáról, hogy biztonság tudatosan működik, ha a felhasználók és az egyéb szerepkörökben dolgozók tudatában vannak az alapvető és esetleg szervezetspecifikus fenyegetettségeknek, képesek ezeket felismerni és tudják, hogy mi a teendő egy felismert vagy gyanított incidens esetén, milyen csatornán tudják bejelenteni és felhasználóként mi a követendő magatartás az egyes események kapcsán. Ehhez az állapothoz hosszú út vezet, a szervezet biztonsági kultúráját meg kell teremteni. Felhasználóként tudatában kell lennünk, hogy mi vagyunk az első és legintelligensebb



védelmi vonala a szervezetnek és hogy a biztonság mindenki érdeke, a cég jövője és a munkahely biztonsága múlhat rajtunk.

### 3 Információrendszerek

Az információnak **életciklusa** van, ahogyan azt a COBIT 5 megfogalmazta [7]. 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 előállításához tudás szükséges, amihez a megfelelő információk nélkülözhetetlenek. Az információkat adatok feldolgozásával állítjuk elő, az **adatok** pedig információrendszerekben jönnek létre, tárolódnak és itt dolgozzák fel őket.

Az információrendszerek **számítógépes architektúrákon** [a] 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 összekötési 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

Anélkül, hogy az infokommunikációs technológiai alapismeretek modul anyagát ismertetnénk, meg kell ismételünk azt, hogy 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 a **szoftveres** adatfeldolgozási feladatok ellátására, ehhez különböző szintű programokra lesz szükségük.

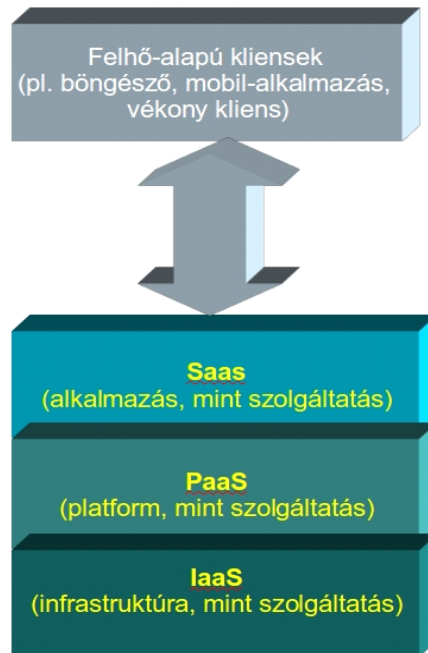
Felépítésükben nem különböznek, de feladatuk különböző, ezért meg lehet különböztetni az adatok feldolgozására szolgáló **számítógépeket**, adatbázis-szervereket, adattárházakat a kommunikációra szolgáló hardverektől (jelismétlő, híd, útválasztó). Kliens-szerver architektúrában értelmezhető felosztás a kiszolgáló architektúra és a kliens-oldal is, ezeket a speciális körülményeket figyelembe vevő programok működtethetők rajtuk.

### 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, megemlíjtük, hogy a hardverek működtetéséhez az úgynevezett meghajtók, vezérlő-programok – driverek – szolgálnak. A számítógép-architektúra teljes funkcionalitásának kihasználását az operációs rendszer teszi lehetővé, míg a felhasználók által igényelt egyes funkciókat megvalósító alkalmazásokat valamely magas szintű programozási nyelven írják és erről fordítják le a számítógép központi feldolgozó egysége által érthető futtatható kódú programmá. Ilyen program például egy szövegszerkesztő, mely a billentyűzet segítségével bevitt karaktersorozatot összefüggő és formázott szöveggé képes tárolni, illetve elvégez a mások által rögzített szövegek megjelenítését is.

Alkalmazásfejlesztések esetén elengedhetetlen, hogy a funkcionális követelmények mellett a biztonsági (ún. nem funkcionális) követelmények is meg legyenek határozva a fejlesztés legkorábbi szakaszától. Ennek elmaradása és/vagy nem megfelelő teszteletlensége 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, 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) [b].



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. GoogleDoc), komplex kommunikációs (telefonálás, levelezés, azonnali üzenetküldés) szolgáltatásokat felhasználni (pl. Skype, Viber, Whatsapp, Gmail) vagy közösségi oldalakon információkat, fájlokat megosztani és megkapni (pl. Facebook, Twitter, Instagram stb.). A **fájl-megosztás** saját gépről is történhet.

Érdeemes 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 múlni fog a biztonságuk. A CaaS számos innovatív információtechnológiai fejlesztést integrál, 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

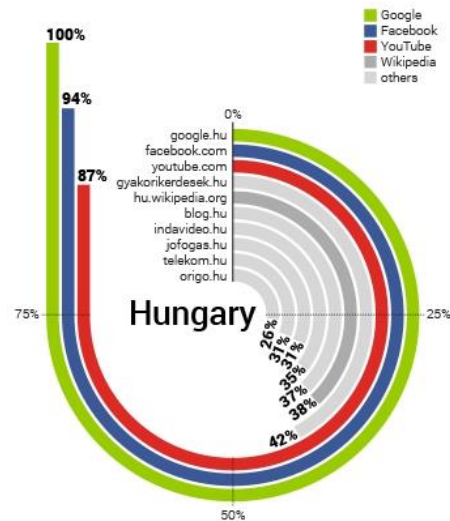
szolgáltatások adatgyűjtései és értékelése, várostervezési megfontolások és még sorolhatnánk.

Ez a biztonsági környezetet is jelentős mértékben megváltoztatta.

### 3.2.1 Ismeretszerzés és kapcsolatteremtés interneten

Az úgynevezett „Z” generáció (2000 után születettek) azon fiatalok összessége, akik számára a technológia, az internetelérés és az azon keresztül a kapcsolatteremtés és fenntartás a mindennapok része, mind az erre használt eszközök, mind a használt szolgáltatások annyira beleivódtak a napi rutinjukba, hogy enélkül gyakorlatilag nem tudják elképzelni sem a létezésüket. Miért fontos ez? Egyrészt azért, mert ezeken a csatornákon és alkalmazásokon keresztül vannak kapcsolatban egymással és a világgal, másrészt innen szerzik az ismereteiket is. És mint a jövő munkavállalói, akik ebben a technológiai (és biztonsági) környezetben szocializálódtak, nehezen illeszkednek be egy konzervatívabb munkahelyre, vagy közösségbe. Teljesen más elvárásokkal érkeznek az úgynevezett nagybetűs életbe, mint a korábbi generációk. A Gemius „Youth on the ‘net” PC-s adatforgalmon alapuló 2016-os kutatása szerint az alábbi weboldak a legnépszerűbbek a 15-24 éves korosztályban [p]:

- [google.hu](http://google.hu)
- [facebook.com](http://facebook.com)
- [youtube.com](http://youtube.com)
- [gyakorikerdesek.hu](http://gyakorikerdesek.hu)
- [hu.wikipedia.org](http://hu.wikipedia.org)
- [blog.hu](http://blog.hu)
- [indavideo.hu](http://indavideo.hu)
- [jofogas.hu](http://jofogas.hu)
- [telekom.hu](http://telekom.hu)
- [origo.hu](http://origo.hu)



3. ábra Leggyakoribb alkalmazások a "Z" generáció körében

Arányaiban az első három (Google, Facebook, Youtube) szolgáltatás a fiatalok 84-100%-a által ismert és használt. A további két helyezett a gyakorikerdesek.hu és a Wikipedia népszerűsége is azt támasztja alá, hogy a fiatalok az Internetet jellemzően két dologra használják: ismeretszerzésre és kapcsolattartásra. Fontos, hogy a tartalomfogyasztásban is jelentős átalakulás történt és a fiatalok elsősorban a videó alapú tartalmakat részesítik előnyben.

Bár itt nem szerepelnek, de a fiatalok számára nélkülözhetetlenek egyéb információforrások is (pl. időjárás, menetrend, stb.), valamint a távtanulást segítő rendszerek és az oktatási intézmények interaktív rendszerei (pl. e-napló, NEPTUN, tananyag közzététele, feladatbeadás, stb.).

### 3.2.2 Elektronikus ügyintézés

Magyarországon az egykapus ügyintézési felületet a <https://magyarorszag.hu> [d] portál biztosítja, ahol egy hiteles regisztrációt követően számos ügy kezdeményezésére van már lehetőségünk teljesen elektronikus formában és több államigazgatási rendszerből tölthetünk le magunkkal kapcsolatosan adatokat is (pl. NAV, OEP).

## 3.3 Számítógép hálózatok

A számítógép-hálózat egy olyan speciális rendszer, amely 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 M2M (A Machine to Machine technológia olyan adatáramlást jelent, mely emberi közreműködés nélkül, gépek között zajlik.) technológiákra.

A hálózatokat fel lehet osztani kiterjedésüket alapul véve a következő három típusra [10]:

**lokális hálózatok, LAN (local area network):** viszonylag kis távolságon intelligens eszközök közötti kommunikációt biztosít, erre a célra telepített fizikai kommunikációs csatornán; hatótávolsága 10 m – 5 km közötti.

**nagyvárosi hálózatok, MAN (metropolitan area network):** megteremti egy intézmény (gazdasági szervezet, üzem, hivatal) épületei közötti összeköttetést egy városban, vagy kb. 50 km-es körzeten belül. Hatótávolsága 1 km – 50 km közötti

**távolsági hálózatok, WAN (wide area network):** földrajzilag távol eső felhasználók közötti összeköttetést - jellemzően nyilvános távközléstechnikai berendezéseken keresztül - biztosító hálózat.

## 4 Fenyegetések, támadások

Az információ olyan érték, amelyek megléte vagy hiánya alapvetően befolyásolja minden folyamatunk elvégezhetőségét és eredményességét. Növelheti a hatékonyságot, ha jó, és teljes improduktivitást 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, vagy a telefonos közlésekre is, amelyeket adott esetben szintén védeni szükséges. Az információ olyan fontos és értékes elemmé vált, hogy be is épült az információtechnológiai **erőforrások** közé a hardver és a szoftver mellé minden keretrendszerben, szabványban. Védeni kell tehát a hardver és a szoftver mellett a fontosnak ítélt információkat is.

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 (információlopás, zombi hálózat, stb.). Ennek minősített esete a **személyazonosság-lopás**, amikor a haszon a támadóé, a büntetés a megtámadotté – hacsak nem tudja ártatlanságát bizonyítani.

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

## 4.1 Rosszindulatú szoftverek

Rosszindulatú szoftvereknek nevezünk minden olyan programot, amelyik a tulajdonos előzetes engedélye nélkül bármilyen tevékenységet akar végezni a számítógépeinken vagy a hálózatra feltöltött adatainkkal. A kifejezés angol változata (**malware**) a „malicious software” kifejezés rövidüléséből eredt. A rosszindulatú programkód tehát számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver. Ezeket károkozási célból 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 más fájlokhoz kapcsolódva önmaguktól terjednek, vagy e-maileken keresztül küldik őket, és károkat okozhatnak a számítógépeken. Kiemelt alfajuk a zsarolóvírusok, amelyek letitkosítják az megfertőzött eszköz (munkaállomás, server, okostelefon stb.) fájljait és váltságdíj ellenében adják meg a titkosítás feloldásához szükséges kulcsot. Bővebben lásd: zsaroló programok.
- **férgek:** a vírushoz hasonló önszorozódó számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá illetve válnak részeivé, addig a férgek önállóan fejtik ki működésüket.
- **Trójai programok:** nevüket az ókori Trója ostrománál alkalmazott hadicsel eszközéről kapták, amely révén egy legálisnak látszó letöltésben egy olyan program bújk meg, ami előbb-utóbb aktivizálódik incidenseket okozva (például hátsó kapukat tölt le 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 kémiszoftverek 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, amelynek 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. Így módon ha egy internetes áruház ér például ilyen támadás, akkor ott nem lehet vásárolni, ergo tényleges bevételkiesés valósul meg.
- kémiszoftver: 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.
- zsaroló programok: a támadó olyan programot juttat be a felhasználó gépére, melyek a fertőzött számítógépeket 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.



- kéretlen levelek: A „spam” elnevezést egy amerikai cég (Hormel Foods) konzervhúskészítményének nevéből kölcsönözték (Spiced Porc and Ham), amely 1937 óta létezik. Az internet világában ez lett az szokásos kifejezés a tömeges e-mailek jelölésére, egy Monthly Python darab nyomán. A kéretlen levelek közös jellemzője, hogy valamely termék 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: az angol kifejezés (botnet) a „**robot**” szóból és „**network**” 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, spam küldésre, 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. Ettől sokkal ritkábban szoktak **fizikai támadó eszközöket** alkalmazni a támadók, mivel ehhez valamilyen személyes jelenlét szükséges, ami a lebukás kockázatát jelentősen megemeli. Azonban sikeresen lehet használni az alábbi eszközöket 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.
  - **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, kifigyelés 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.

## 4.2 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:

- eltérítéssel adathalászat (pharming): a támadó a felhasználó egy adott weboldal felé irányuló forgalmát átirányítja a saját weboldalára 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 (álweboldalak) egy az egyben lemásolják az igaziakat, a felhasználókat gyakran a sikertelennek jelzett bejelentkezési kísérletük után vissza is irányítják a támadók az eredeti weboldalra, hogy a gyanút még jobban eltereljék a csalási kísérletről. Az különbözteti meg az adathalászattól, hogy itt a támadó az áldozata gépére betörve módosítja annak beállításait.
- egyklikkes támadások: 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 letölttetése: 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.)

- adathalászat (phishing): egy valódi weboldal támadók által lemásolt képének felhasználása (álweboldal), amely tartalmában 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 álweboldalak hamisított SSL-tanúsítvánnyal is rendelkezhetnek. Az álweboldalak meglátogatását hamis üzenetekbe rejtett linkekkel érik el (pl. adatváltoztatási kérés a rendszeradminisztrátortól e-mailben, vagy jelszóváltoztatási kérés a banktól egy biztonsági incidenst követően stb.). Ez különbözteti meg az eltérítéssel adathalászattól, mivel itt a támadó az áldozata gépén nem módosít semmit sem.
- Kifigyelés (shoulder surfing): közvetlen megfigyelési technikát jelent, mintha a támadó keresztülnézne a felhasználó vállán, hogy információt szerezhessen. A kifigyelés zsúfolt helyeken hatékony, amikor a felhasználó begépel a PIN-kódját, ügyfél-biztonsági kódját, jelszavát nyilvános helyeken – internetkávézóban vagy könyvtárban stb.
- Szélhámosság (social engineering): 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 dolgozónak vagy rendszeradminisztrátornak adja ki magát, de nem ritka a kezdő munkatárs szindróma is, ami a kezdők felé megnyilvánuló segítőkészséggel él vissza.
- 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 a felhasználó vétlen vagy szándékos tevékenysége következtében kikerülnek a szervezet védett kontrollkörnyezetéből és fentiek miatt ezen bizalmas adatokhoz, információkhoz jogosulatlan hozzáférés történhet. Fontos a feltételes mód – történhet. Mivel az így módon, a szervezet kontrollkörnyezetéből kikerült az adat vagy információ, a szervezetnek nincs 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, ami lehet akár adatlopás, informatikai rendszerek megrongálása vagy más illegális tevékenység.
- 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.

A **hackerek** olyan személyek, akik jól értenek a technikához, és képesek arra, hogy behatoljanak informatikai rendszerekbe és 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 hívunk még „Penetráció-tesztelőknek” vagy „etikus hackereknek”, ők az ügyfelek megbízásából, a feltárt hibákat dokumentálva törnek be a rendszerekbe.

**„Jelszótörés”.** A jelszavak a mai napig az elsődleges hitelesítési adatai sok rendszernek. Egyetlen „faktor”, amit az azonosítón kívül tudni kell a belépéséhez. Mivel azonban a jelszó ellopható, lefigyelhető, feltörhető, ezért kritikus rendszereknél már többfaktoros azonosítást, hitelesítést használnak. A jelszótörés [e] jelentése ennek megfelelően tehát a jelszó nyílt szöveges verziójának megszerzése. Több módszer is ismeretes erre (nyers erő, szótár alapú, szivárványtáblázat stb.) A nyers erő módszer használja fel a lehetséges jelszavak egymás utáni bevitelét a támadás kivitelezése során – ez kétségkívül lehet jelzője a jelszótörésnek, de nem lesz a célja. A jelszótörőnek ugyanis nem az a célkitűzése, hogy sok-sok jelszót próbálgasson, hanem az, hogy gyorsan találjon egy működőképeset a kiszemelt áldozatához. A szivárványtábla egy olyan táblázat, amiben a támadó előre kiszámolja és rögzíti számos különböző karaktersorozat kivonati értékét (hash), így ezeket a támadás során már nem kell kiszámolnia, hanem csak készen felhasználnia. Emiatt erősen ajánlott a hibás bejelentkezések figyelése és bizonyos számú próbálkozás utáni védelem (tiltás, felfüggesztés) életbe léptetése is.

Természetesen lehetnek olyan fenyegetések az adatokra, amelyekről nem tehet senki sem az adott kontextusban, így a **„vis maior”** kategóriába tartozik. Ilyen például az adatok esetében a tűz. Megfontolandó, hogy habár nem „vis maior”, de mégiscsak potenciális

fenyegetést jelentenek az adatokra az emberi tevékenységek a vétlen hibák, gondatlanság révén.

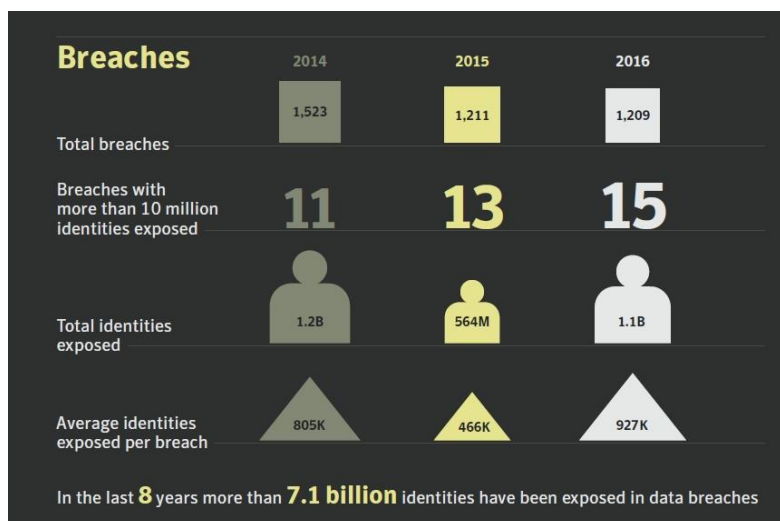
Minden egyes támadási formában közös, hogy az előnyeiket a felhasználók, tulajdonosok rovására akarják érvényesíteni és a Büntető Törvénykönyv (Btk) szerint ma már ezek számítógépes bűncselekményeknek számítanak.

Sajnos a számítógépes bűnözés kifizetődő tevékenységnek tűnik. Elég csak a levélszemét küldéséből befolyó dollármilliárdokat megemlíteni, vagy az egyre emelkedő számú zsarolóvírus aktivitást, amelyből közvetlen bevétele származik a támadóknak, ha az áldozatok fizetnek. Ezen kívül sajnos megjelent a Fraud as a Service (FaaS), amely során 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, kiválasztott célpontok támadása dDOS-szal és még sorolhatnánk.

## 5 Fenyegetettségi és támadási trendek az elmúlt évekből

Számos internetbiztonsággal foglalkozó cég ad ki évről évre úgynevezett Internet Security Threat Report-ot [f]. Ezen fenyegetettségi riportokban bemutatják az általuk tapasztalt és mért internetes fenyegetettségek statisztikáit. Természetesen, mint minden statisztika ez is egy bizonyos nézőpontot és eredményt mutat, ugyanakkor a trendek jól kiolvashatóak belőlük. Jelen dokumentumban a Symantec, a világ egyik legjelentősebb információ- és informatikai biztonsági megoldásokat és szolgáltatásokat nyújtó cégének a fenyegetettségi riportjából mutatunk be pár fontosabb adatot. Fontos, hogy ezen adatok a világméretű információgyűjtő rendszerekből származnak. Érdekes lenne Magyarországra vonatkoztatott adatokat is megjeleníteni, egyelőre azonban ilyenek nem állnak rendelkezésre.

## 5.1 Személyes adatokat érintő incidensek



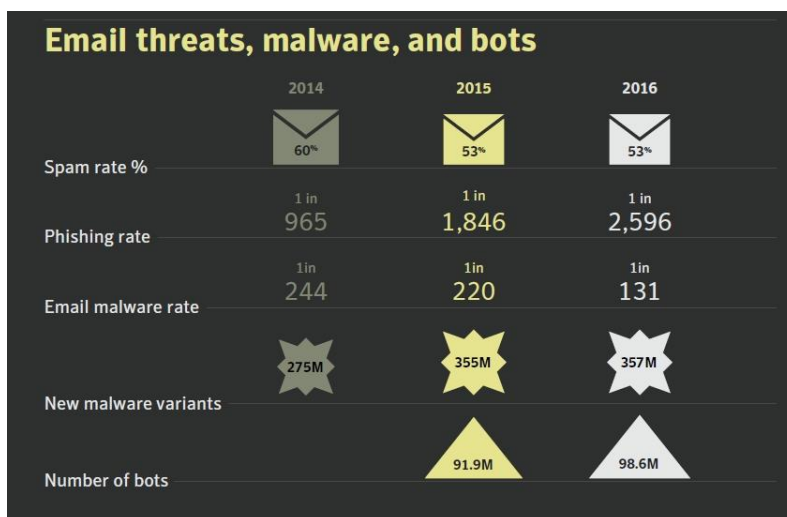
4. ábra Személyes adatokat érintő incidensek

Mint a statisztikából kiolvasható, az ilyen jellegű incidensek száma stagnál, azonban látszik, hogy folyamatosan növekszik azon incidensek száma, ahol több mint 10 millió személyazonosság volt érintett. Ez döbbenetesen magas szám, arányaiban ahhoz mérhetjük mintha Magyarország minden lakosának ellopták volna a személyes adatát egy-egy ilyen incidens során. Az is látszódik, hogy 2015-höz képest megduplázódott az összességében érintett személyes adatok száma, meghaladva az 1,1 milliárdot.

Bár a tényleges incidensek száma csökkent az egy-egy incidensben érintett átlagos felhasználói adat szám több mint a duplájára nőtt a tavalyi évben az előzőhöz képest.

Összességében ez arra utal, hogy a felhasználók egyre gyakrabban használnak olyan internetes szolgáltatásokat, ahol koncentráltan van több millió személyes adat, amely ezen koncentráltágnak köszönhetően sokkal inkább válik a támadók célpontjává. Ezért is fontos, hogy mennyi és milyen személyes adatokat adunk meg a népszerű szolgáltatásokban (Facebook, Twitter, LinkedIn, stb.)

## 5.2 E-mail fenyegetettségek, kártékony programok és botnetek

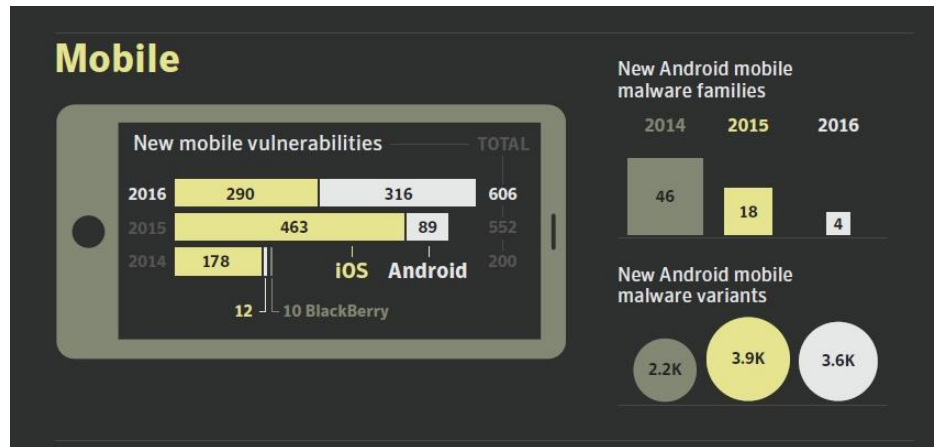


5. ábra E-mail fenyegetettségek, kártékony programok és botnetek

A világ e-mail forgalmának jelentős részét teszik ki a spam-ek, kéretlen levelek. Bár a Symantec statisztikája szerint az összlevél forgalom 53%-a spam, vannak olyan becslések, hogy ez az arány akár 80-90% is lehet valójában. Leolvasható, hogy az elmúlt években jelentősen csökkent az adathalász típusú levelek száma az összes levelszámhoz képest, ugyanakkor a duplájára nőtt a valamilyen kártékony programot (vírus, trójai) tartalmazó levelek száma, 2016-ban minden 131 levélből egy valamilyen kártevőt is kézbesített.

És ehhez kapcsolódik, hogy az új kártevő programok száma is folyamatosan emelkedik. Egyenes következménye a növekvő kártevő fenyegetettségnek, hogy nő a fertőzött számítógépek – és okostelefonok, okoseszközök száma, amelyek pedig így növelik a botnetek számát (Number of bots) és ezáltal tovább növelik az átfogó fenyegetettségeket.

### 5.3 Mobileszközök fenyegetettségei



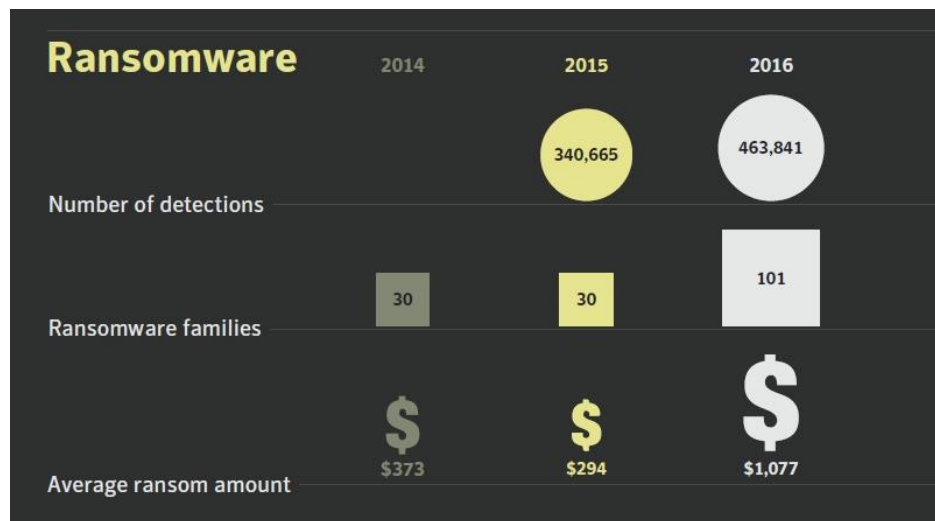
6. ábra Mobileszközök fenyegetettségei

Ahogy terjednek a mobileszközök – főleg az okostelefonokra és táblagépekre gondolva itt – úgy emelkedik a rájuk írt kártevőprogramok száma is. 2016-ban az összához viszonyítva jelentősen nőtt az Android mobil operációs rendszerre írt kártevők száma, mivel ezen eszközökből van számosságában a legtöbb a világban. Ebből is látszódik, hogy a támadók nagyon racionálisak és a hasznonszerzésnél megpróbálják a saját költségeiket is minimalizálni a várható profithoz képest. Ezért is rendkívül fontos, hogy az okoseszközöket is lássuk el megfelelő védelemmel.

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 applikáció boltjából töltsünk le (Google Play, Appstore). Különösen ügyelni kell az okoseszközökön a számos ingyenes program által megjelenített reklámokra, amelyek gyakran ijesztegetik a felhasználókat azzal, hogy vírusos az eszközük, és ezért töltsék le a felkínált vírusirtót. Na pont ezek az ál-vírusirtó programok hordozzák a tényleges fenyegetettséget. Mobileszközökre is elérhetőek olyan komplett védelmi megoldások, amelyek képesek már elloptott/elvesztett eszköz nyomonkövetésére, szülői felügyeleti funkciókra és minden olyan egyéb tevékenységre, amit az asztali PC – munkaállomás környezetben megszokhattunk. A vírusfenyegetettség annyira komoly, hogy már okoseszközökből is szerveztek az internetes bűnözők botneteket.



## 5.4 Zsarolóvírusok (Ransomware)



7. ábra Zsarolóvírusok növekedési trendje

A zsarolóvírusok az elmúlt évek „slágertermékei”. Mint azt fentebb is olvasni lehetett, a zsarolóvírus egyszerűen letitkosítja a gépünk/telefonunk fájljait és csak fizetés után, egy feloldókulcsot visszaküldve férhetünk hozzá újra a fájljainkhoz. Bár az első zsarolóvírust még floppylemezen küldözgették postán, manapság már milliós üzlet a támadóknak. A statisztikákból látszódik, hogy nem csak a darabszámuk, hanem a fajtáik és az általuk begyűjtött pénz is rohamosan növekszik, sajnos további ilyen támadásokra ösztönözve a bűnözőket. Jelen oktatási anyag lezárását megelőzően történt meg az elmúlt évek legnagyobb zsarolóvírus ferzőzése, amikor is egy WannaCry2.0 nevű zsarolóvírus pár nap alatt végigfertőzte a világot. Ez a fertőzés nem csak a kiterjedése miatt volt jelentős, hanem azért is mert, mert egy pár hónapja megismert, de milliányi rendszeren nem javított Windows sérülékenységen keresztül tudott terjedni és ez miatt is számos olyan szolgáltatást érintett, amelyek a világon bárhol élő emberek mindennapjait érintették. A zsarolóvírus által letitkosított fájlok következtében jelentős zavarok és leállások voltak kórházakban, közlekedési rendszerekben, államigazgatásban, telekommunikációban, oktatási- és pénzintézetekben is.

## 6 A védelem kialakítása

Az előző fejezet megmutatta, hogy láthatóan az adatainkat 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 megtörténe ellen (földrengés, hurrikán, céltudatos betörő). Mindkét típusú fenyegetés következményeként az adatok, valamint a tároló 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 felismerjük azt. Nagyon fontos célkitűzés lehet az is, hogy minden pillanatban legyünk képesek arra, hogy a bármilyen okból bekövetkezett információtechnológiai sérülés kárvetkezményét 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, így nem érheti ezeket semmilyen katasztrofális esemény sem. Ezért a védelmet nagyon gondosan kell kiépíteni.

A **biztonság mértékében** 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 felhasználhatja a támadó. Az egyes támadási formákat programokba öntve számos bonyolultabb támadási forma ismert, de ebben az esetben a program működésre bírásához szakismeret is szükséges, ellentétben a programokat lefuttató támadásokkal, ahol a támadónak csak az elindítógombot kell megnyomnia egy egyszerűen kivitelezhető támadás realizálásához. Nyilvánvalóan mindhárom szinthez 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 bejövételét. Ebben segítenek az egyes tartalomellenőrző szoftverek, mint **internet** tartalmát **szűrő** szoftver, weboldalak elérését engedélyező vagy tiltó szoftver, szülői felügyeleti szoftver stb. A tartalomellenőrző szoftver 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 felügyelet szoftver alkalmas.

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. Más szóval, magasabb szintű a biztonság, ha kevesebb a biztonsági incidens. 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 leggyengébben védett elem támadásával lehetséges legtöbb esetben. 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 előírásokban, mivel felette a stratégiai szintű Információbiztonsági Politika, alatta pedig az operatív szintű eljárásrendek találhatók. A szabályzatok közé soroljuk még a katasztrófahelyzetben megteendő intézkedéseket tartalmazó Informatikai Katasztrófatervet is. Ezek otthoni vetülete annak végiggondolása, hogy mit tehetünk az

otthon tárolt adataink védelme érdekében a mindennapokban és extrém helyzetekben (pl. árvíz, lakástűz) is.

## 6.1 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 felhasználó.

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 azért, 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 gyanúsán sétálgató ismeretlenre az irodában. 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, létfontosságú a szervezet számára.

## 6.2 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 ügyfelek adataira, és meg akarják előzni az ügyfelek adataival való visszaélést, valamint az ügyfelek adatainak ellopását, hiszen ennek bekövetkezése súlyos bevétel-kiesést okozhat számukra, ahogyan ezt több példa is bizonyította a közelmúltban. 2018. május 25-től életbe lép az Európai Unió

Általános Adatvédelmi Rendelete (GDPR – General Data Protection Regulation), amely minden olyan cégre és szervezetre, amely személyes adatokat kezel vonatkozni fog. A korábbi szabályokhoz képest némileg szigorodtak az elvárások. Ami jelentőset változott, az a büntetési tétel, ha az adatokért felelős szervezet nem tartja be a szabályokat, vagy ha ez miatt az adatokat érintő incidens következik be.

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 hozzáférnie 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 használunk a titkosításhoz és megoldáshoz, ezért a titkosító kulcs elvesztésével 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 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 általában egy alapszintű titkosítás is megfelelő védelmet nyújt, mivel a védett adatok értéke nem áll arányban azzal az erőforrásszükséglettel, ami az adatok ellopásához és feltöréséhez szükségesek. Konkértan egy hacker nem fogja célzottan az idejét pazarolni arra, hogy az otthoni titkosítással védett családi költségvetést tartalmazó excel táblát feltörje. Vagy ha el is lopja egy tolvaj a pendriveomat, nem lesz elegendő tudása és motivációja, hogy a rajta lévő titkosított word fájlokat feltörje - amik mondjuk a szakdolgozatom anyagait tartalmazzák.

### 6.3 Bizalmasság az operációs rendszerben

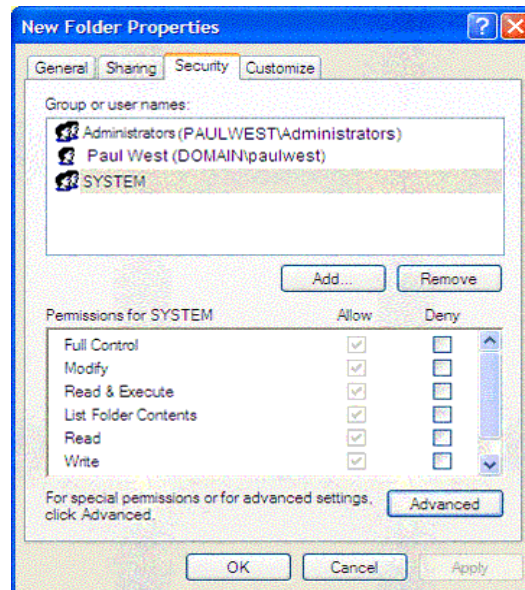
Az operációs rendszerek biztonsága tipikusan fájlok biztonságát jelenti. A fájlok biztonságáról több aspektusból lehet beszélni, a hozzájuk kapcsolódó műveletek révén. Ezek az olvasás, írás, törlés, módosítás. Fontos kérdés, hogy ki rendelkezik ezekkel a **fájl-jogosultságokkal**?

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 (**kititkosítani**) a fájlt értelmes olvasáshoz, illetve a hozzáférés megtiltása. Jelszavas védelmet beállíthatunk irodai programcsomagok által készített dokumentumokhoz (szöveg, táblázat, prezentáció stb.) vagy tömörített fájlokhoz egyaránt (zip, rar stb.). 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 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 megemlíteni azt is, hogy van-e olyan eleme egy fájlnek, 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** [o].

Jól tesszük tehát, ha az operációs rendszerünkben korlátozzuk az egymás adataihoz való **hozzáférést**.



8. ábra Hozzáférések megadása Windows operációs rendszerben

### 6.3.1 Merevlemezek és USB-lemezek titkosítása

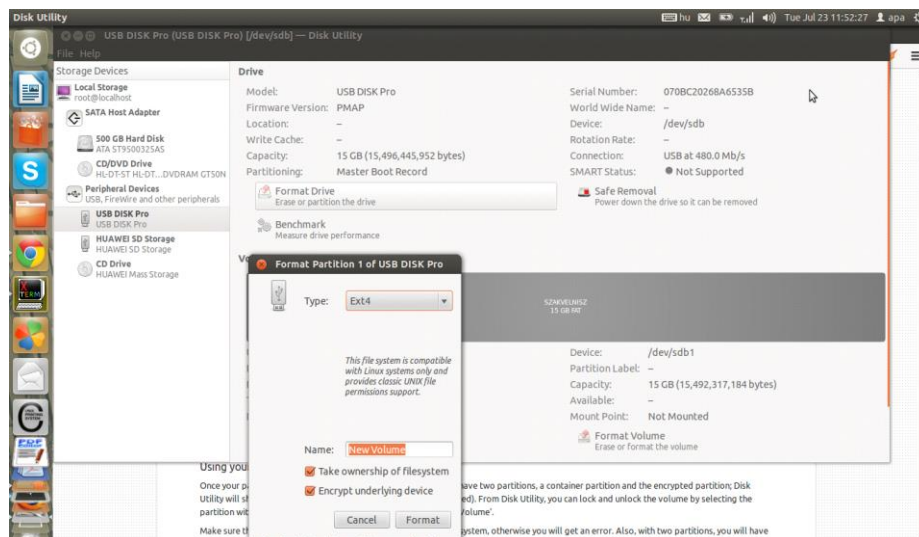
Az adataink mindazok számára alapértelmezett esetben hozzáférhetők, akik a tárolására szolgáló lemezek (belső, külső, felhő, USB) birtokában vannak. Leggyakrabban a jogos tulajdonosa van birtokon belül, de a támadók sokszor sikeresen tudják ezeket a tárolókat – illetve a rajtuk tárolt adatokat távolról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

Az adatok bizalmosságának 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 aggódnunk innentől kezdve az adatok miatt, ha esetleg az eszközt el is lopnák, amennyiben a jelszót megfelelően erősen választottuk, az alkalmazott megfelelően erős kriptográfiai titkosítás visszafejtése 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.

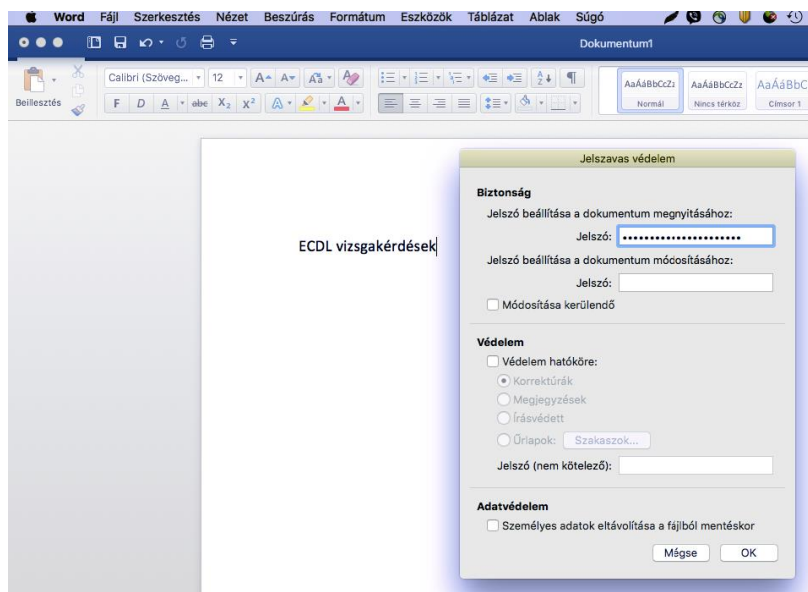


9. ábra USB-lemez titkosítása Linuxon

### 6.3.2 Titkosítás irodai programcsomagokban

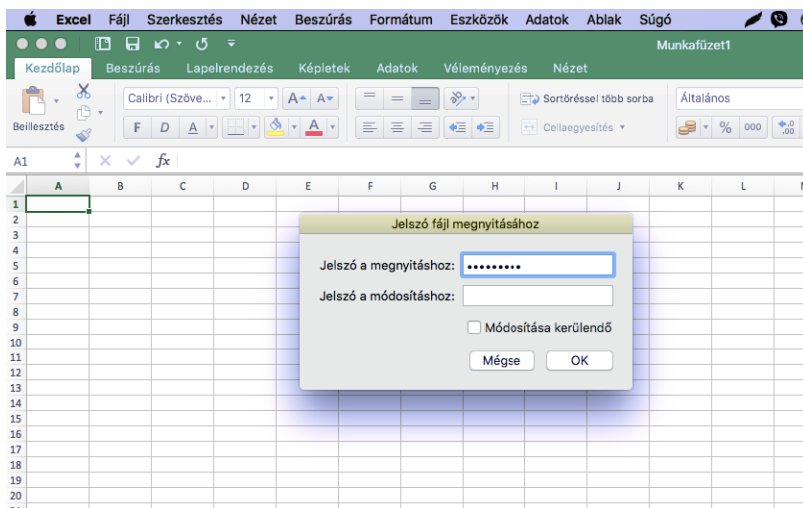
A szövegszerkesztők, táblázatkezelők, irodai programcsomagokban használható programok beépített funkciókat tartalmaznak a szöveg jelszavas védelmének megteremtéséhez, más szóval a **dokumentumtitkosítás**hoz. Amennyiben használjuk ezt a funkciót, a szövegszerkesztő bekér tőlünk egy – megfelelően biztonságos – jelszót, aminek segítségével a teljes dokumentumot kriptográfiailag titkosítja, így azt a jelszót nem ismerő számára teljesen olvashatatlaná 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.





10. ábra Megnyitási jelszó beállítása Mac Microsoft Word 2016 szövegszerkesztőben

Mac Microsoft Word 2016 programban az Eszközök / Dokumentumvédelem menüpontra történő kattintással jelenik meg a jelszót bekérő ablak



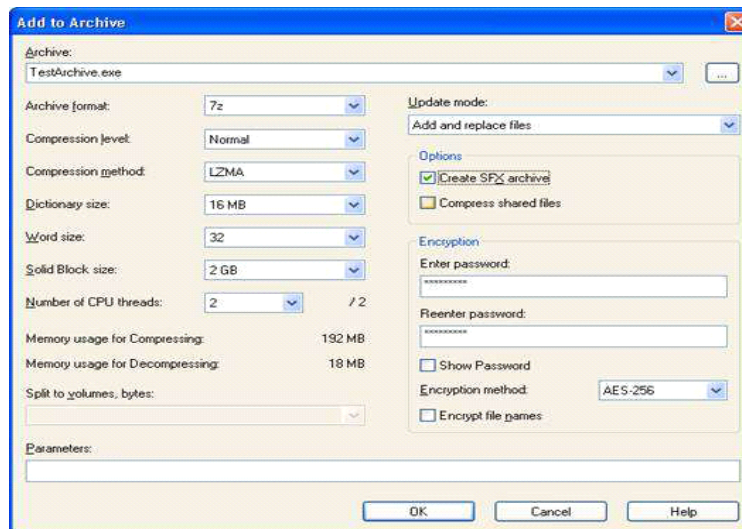
11. ábra Megnyitási jelszó beállítása Mac Microsoft Excel 2016 szövegszerkesztőben

A képen látható Mac Microsoft Excel 2016 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.

### 6.3.3 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.



12. ábra Jelszó beállítása archiv állomány létrehozásakor

A megfelelő jelszó kiválasztása itt sem árt, mivel egy jelszótörő programmal jelentkező támadónak egy 10-számjegyű álló jelszó megfejtéséhez kb. 30 másodpercre van szüksége, egy közepesen erős számítógépen.

## 6.4 Hálózat és bizalmasság

A nyílt internetes kommunikáció során nemcsak a jogosultak láthatnak bele az adatokba. Adatok alatt egyrészt a hálózaton továbbított adatfolyamot, másrészt a hálózaton elérhető eszközökön tárolt adatokat – összefoglaló néven a **hálózati adatok**at 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 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 internet bankolás 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 az adatok olvasását és küldését.

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



13. 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 korlátozás nélkül hozzáférhet, illetőleg tetszés szerint használhatja a számítógépet és annak erőforrásait.

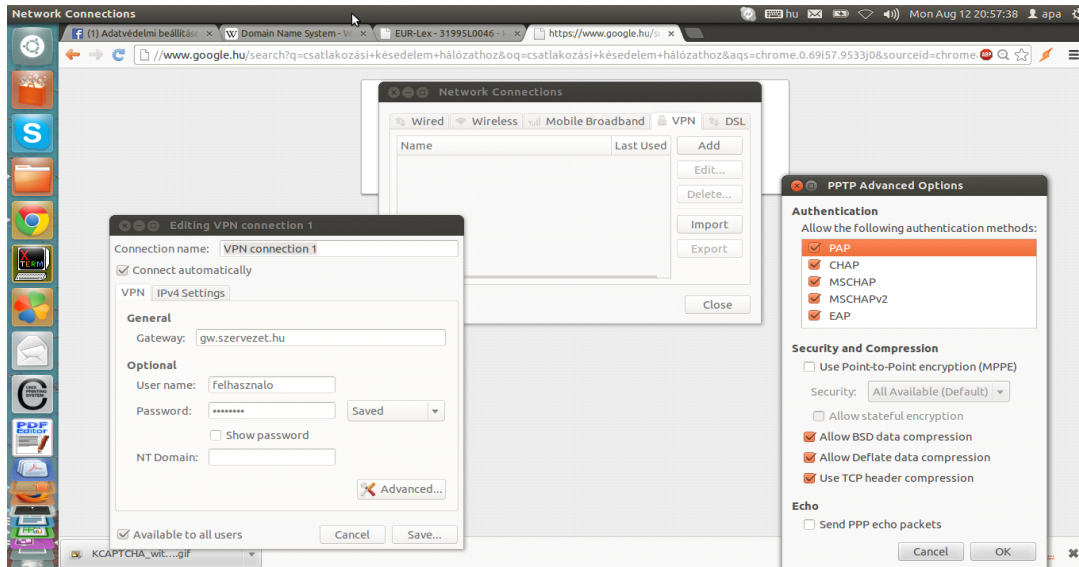
Gyakran felhasználják bejegyzett cégek neveit a személyes biztonsági adatok megszerzéséhez az eltérítéssel adathalászat során. A támadó módosítja áldozata számítógépén például az internetes bankjának a címét, így az áldozat azt hiszi, hogy annak adta meg az adatait, akit lát, nem gondol támadásra.

#### 6.4.1 Hozzáférés-védelem, jelszavak, hitelesítés

A támadások leg többjét hálózaton keresztül követik el abból az egyszerű okból kifolyólag, hogy egy internetre kötött számítógépet okoseszközt és okostelefont az egész internet közössége lát, míg egy számítógép esetén, a számítógépet tartalmazó helyiségbe, otthoni gépek esetén a lakásunkba fizikailag belépők száma igen erősen korlátozott szokott lenni. 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 kikapartják 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) kifigyelnek a tolvajok, hogy ki pakol laptopnak tűnő táskát csomagtartóba, és vagy ott helyben, vagy a következő parkolásnál elloppják azt. Mire a tulaj visszatér, az eszköznek hiúlt helye. Sokszor a tulaj azt sem tudja, hogy honnan lopták el az eszközt. Ilyen esetekre jó tanács az, hogy legyen titkosított a háttértár, az eszköz legyen védve jelszóval, a telefonon is legyen képernyőzár, a SIM kártyán pedig PIN kód. És nem utolsósorban ne tároljunk nem mentett adatokat a hordozható eszközeinken, hiszen telefont tudunk venni másikat, de például a gyermekünk első lépéseit megörökítő videót soha többet nem vehetjük fel újra.

A hálózatoknak több típusa van, jellemzően a kiterjedés, a hozzáférés fizikai típusa és a korlátozása tekintetében osztályozhatók. Kiterjedés tekintetében vannak **helyi hálózatok** (LAN), nagy kiterjedésű hálózatok (WAN), hozzáférés típusa szerint megkülönböztetünk vezetékes és vezeték nélküli – más szóval drótnélküli – hálózatokat, illetve a hozzáférés vonatkozásában léteznek nyilvános és titkosított, virtuális magánhálózatok (**VPN**) is. A VPN kialakításához kell egy olyan szoftver, amely a két végpontot titkosított csatornán

összeköti. . A helyi hálózatok lehetnek önálló kialakításúak és funkcionálhatnak más hálózatok önálló részeként is, **alhálózat**ként.



14. 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 adminisztrátori** 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 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.

Számos, a hálózat biztonságát fenyegető veszély létezik. 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 különböztetünk meg:

- többször használatos jelszó: egyszer megadjuk 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 legkésebb példája a bankok Internetbankolás során alkalmazott belépési SMS jelszava, illetve tranzakció hitelesítő SMS jelszava.
- biometria 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 késleltetni a támadás bekövetkezését, mert a rossz jelszavak feltörését vagy kitalálását pillanatok alatt el lehet végezni. A jelszóhasználati rossz szokások bemutatására számos elemzés készült itthon és a nagyvilágban is.

A következő elemzés angol nyelvterületen készült és a 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.

1 123456 (nincs változás)	14 111111 (+1)
2 password (nincs változás)	15 1qaz2wsx (új)
3 12345678 (+1 helyezés)	16 dragon (-7)
4 qwerty (+1)	17 master (+2)
5 12345 (-2 helyezés)	18 monkey (-6)
6 123456789 (nincs változás)	19 letmein (-6)
7 football (+3)	20 login (új)
8 1234 (-1)	21 princess (új)
9 1234567 (+2)	22 qwertyuiop (új)
10 baseball (-2)	23 23. solo (új)
11 welcome (új)	24 passw0rd (új)
12 1234567890 (új)	25 starwars (új)
13 abc123 (+1)	

15. ábra 25 leggyakrabban használt jelszó

A biometria védelem viszonylag ritka otthoni felhasználásban, de 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.

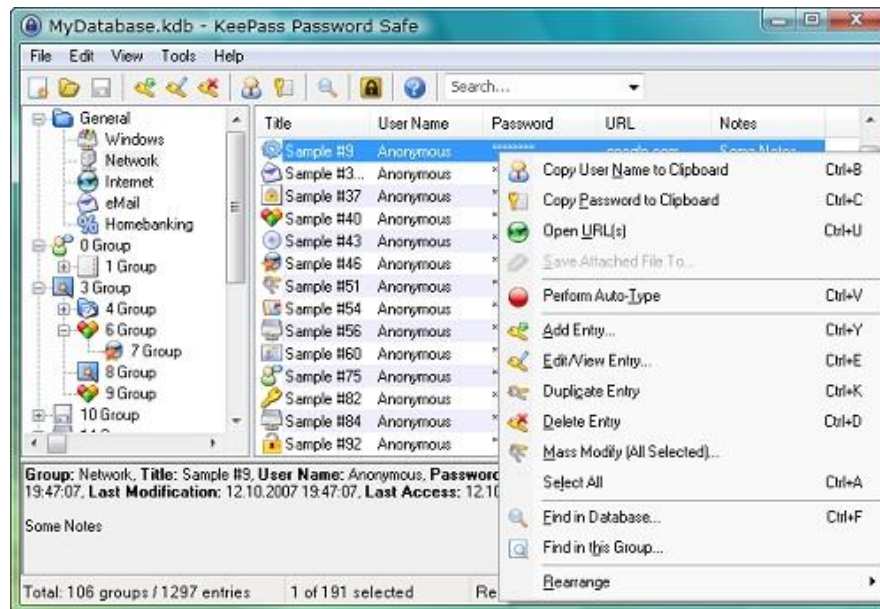
A fizikai védelem témakörébe tartozik valamelyest a webkamerák védelme is. A számítógépekhez kapcsolt vagy beépített webkamerákat egy külső támadó a saját irányítása alá tudja vonni bizonyos támadásokkal - még akkor is, ha nem ég a webkamera működését jelző lámpa, így erősen javasoljuk a webkamerák „megvakítását” használaton kívül (pl. egy ragasztócsíkkal való leragasztását vagy egy papírdarabbal való lefedését).

#### **6.4.1.1 Jelszóséf**

A jelszóséfek olyan alkalmazások, amelyek egy titkosított adatállományban eltárolják a felhasználók által alkalmazott jelszavakat és a hozzájuk kapcsolódó egyéb információkat (kapcsolódó weboldal, vagy alkalmazás, felhasználónév, jelszólejárati idő, megjegyzés). A jelszóséf 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 hozzáférni.

Az egyik legnépszerűbb 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 12 másodpercen belül törlődik a vágólapról, meggátolva, hogy más alkalmazás hozzáférjen.





16. ábra KeePass Jelszószer

Munkahelyi környezetben érdemes megérdeklődni az információvédelemmel kapcsolatos területtől, hogy mi a céges szabály az ilyen jelszószer alkalmazásokkal 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 szerben tároltuk a jelszavakat. Fentiek miatt elsősorban otthoni használatra javasolt.

#### 6.4.2 WiFi eszköz biztonsági beállításai

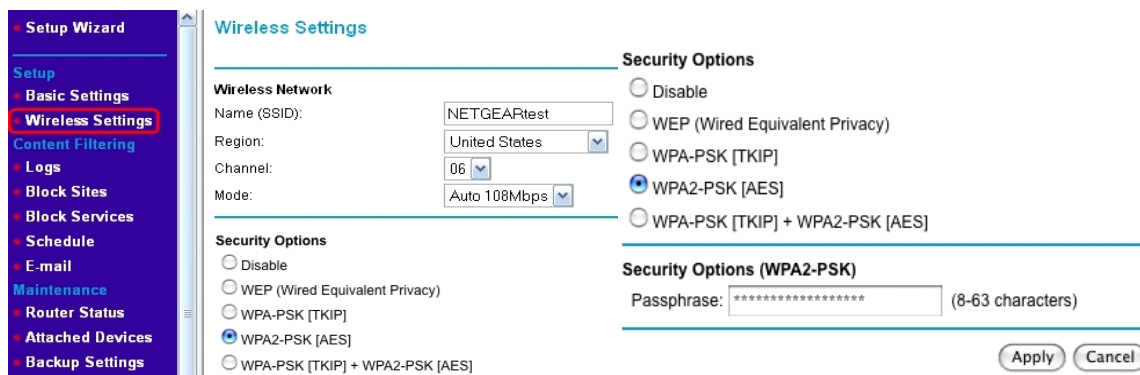
Az otthoni hálózatok kiépítésében is teret nyertek a vezeték nélküli technológiák, mivel kényelmesek és egyszerű telepíteni őket. A biztonságukról azonban alapértelmezésben nem gondoskodnak, sőt, a gyári beállítások minden támadó számára ismertek, amivel nem okoz nekik gondot bármelyik nem megfelelően védett otthoni hálózatot ugródeszkeként 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 hálózat (**WEP** – Wired Equivalent Privacy – már nem tekinthető biztonságosnak), a WiFi védett hozzáférés (**WPA** – WiFi Protected Access – ebből is a WPA2 szabvány, ami jelenleg elfogadott, mint biztonságos módszer) 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 és WPA2) 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). A WPA tartalmazza az IEEE 802.11i szabvány főbb szabályait, és egy átmeneti megoldásnak szánták, amíg a 802.11i szabványt véglegesítik.

A „Personal” (WPA2-PSK) módban, amit 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.



The screenshot shows the 'Wireless Settings' page of a Netgear router. On the left is a 'Setup Wizard' sidebar with options like Setup, Basic Settings, Wireless Settings (highlighted), Content Filtering, Logs, Block Sites, Block Services, Schedule, E-mail, Maintenance, Router Status, Attached Devices, and Backup Settings. The main area is titled 'Wireless Settings' and contains the following fields and options:

- Wireless Network:**
  - Name (SSID): NETGEARtest
  - Region: United States
  - Channel: 06
  - Mode: Auto 108Mbps
- Security Options:**
  - ☐ Disable
  - ☐ WEP (Wired Equivalent Privacy)
  - ☐ WPA-PSK [TKIP]
  - ☒ WPA2-PSK [AES]
  - ☐ WPA-PSK [TKIP] + WPA2-PSK [AES]
- Security Options (WPA2-PSK):**
  - Passphrase: (8-63 characters)

At the bottom right are 'Apply' and 'Cancel' buttons.

17. ábra Vezetéknélküli hálózat titkosítás beállítás

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

### Wireless Settings

☒ Enable 2.4GHz 54Mbps 802.11g Radio

---

**Wireless Network**

Name (SSID)

Region

Channel

Wireless Mode

---

**Security Configuration**

Security mode

Cipher Type ☒ Disable ☐ WEP ☐ AES ☐ TKIP

---

**Security Encryption (WEP) Key**

Encryption Strength

Passphrase

key 1:

key 2:

key 3:

key 4:

### Advanced 11g Wireless Settings

**Wireless Router Settings**

☒ Enable SSID Broadcast

☒ Enable Super G Mode

☒ Enable eXtended Range(XR)

☒ Enable Adaptive Radio(AR)

Transmit Power

Fragmentation Threshold (256 - 2346)

CTS/RTS Threshold (256 - 2346)

Preamble Mode

DTIM(1 - 5)

Qos

---

**Wireless Card Access List**

18. 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, másrésről a saját gépünk is csak akkor tud kommunikálni az eszközön keresztül, ha előtte hozzáadtuk a jogosult eszközök listájához.

### Wireless Card Access Setup

#### Available Wireless Cards

Device Name	MAC Address
-------------	-------------

#### Wireless Card Entry

Device Name:	Squeezebox
MAC Address:	00:04:20:1e:00:b3

Add

Cancel

Refresh

19. 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 lehetséges. 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.

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 ezen szoftverek 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.

#### 6.4.3 E-mail

Nagyon gyakori kommunikációs forma (sok százmillió keletkezik naponta belőlük az üzleti, otthoni és kormányzati területeken) az internetes kommunikáció során az egész világon az

elektronikus levelezés használata. Bár manapság kezdik átvenni ez e-mailezés funkcióját az azonnali üzenetküldési szolgáltatások (Facebook Messenger, Viber, Whatsapp, Skype). Az egyszerű e-mail szolgáltatások és programok nyílt szöveggént küldik a leveleket a hálózaton keresztül. Mivel egy e-mail keresztülhalad számos informatikai rendszeren, míg a címzettjéhez elér – fontos tudni, hogy ezen levelek bizalmassági szintje megegyezik egy postai levelezőlappal. Bárki, aki hozzáfér, olvashatja azt. Ezért azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet, csupán az elektronikus levél titkosítása biztosíthatja. Ide kívánczik még az e-mail aláírás, mint fogalom. Az **e-mail aláírás** (nem tévesztendő össze a levelek elektronikus 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 kitétséget 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 csomagértékesítő levelenél 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. Nagyon gyakori támadás az, amikor egy szöveges fájlba egy makró-vírust rejtenek el, ami a szöveg megnyitásakor aktivizálódik. **Makró**nak 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. 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 hasonló oldalra csalják az áldozatot, ahol az megadja az azonosító adatait és esetleg még egyéb adatokat is, amivel aztán a csálók később megpróbálnak visszaélni. Ide tartozik a banki adatokat bekérő hamisított elektronikus levelek témaköre is. Kaphatunk egy e-mailt, 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 kezelni, 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 egyrésztől intézkedést tud tenni az incidens megállítására, másrésztől az elkövetők kézre kerítését is elindíthatja – ami sosem a mi feladatunk, ne is próbálkozzunk vele, mert esetleg a Btk. szerinti tiltott tevékenységekbe futhatunk bele.



20. ábra Adathalász levél példa

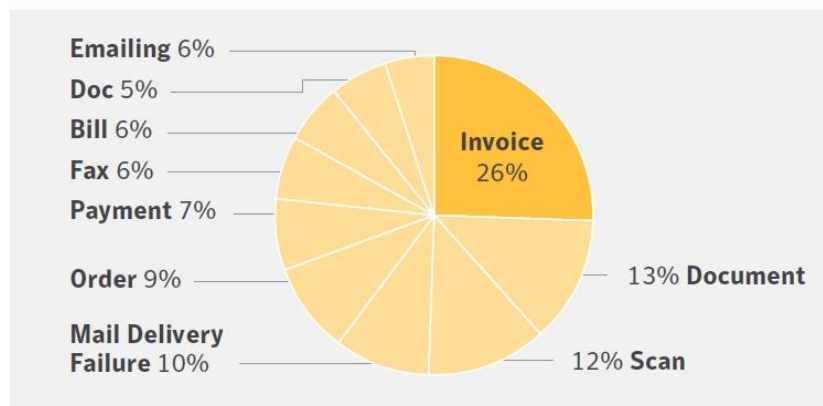
Fenti példában – túl azon, hogy egy bank sem küld ilyen olvashatatlan levelet az ügyfeleinek – azt fontos kiemelnünk, hogy jól látszódik, hogy a félkövér, kék, aláhúzott levélszövegben lévő hivatkozás és a valós URL – weboldalcím különbözik. Ha rávisszük az egerünket az emailekben található hivatkozásokra, akkor pár másodperc múlva megjelenik a tényleges hivatkozás. Ha ez nem egyezik pontosan, vagy nagyon eltérő weboldalnak

tűnik, akkor semiképp se kattintsunk rá. Fent például árulkodó a ....hu.nr0.us/... tényleges domain név végződés. Miért küldene egy magyar bank egy amerikai domain alatt futó weboldalra?

Kiemelten szeretnénk felhívni a figyelmet a zsarolóvírusokra, mivel ezen 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 ha letöltődött elkezd áldatlan tevékenységét.

Épp ezért életbevágó, hogy felismerjük az ilyen leveleket. A Symantec cég statisztikája szerint 89%-ban angolul íródtak az ilyen levelek, a tárgy mezőben pedig az alábbi szavak vannak:



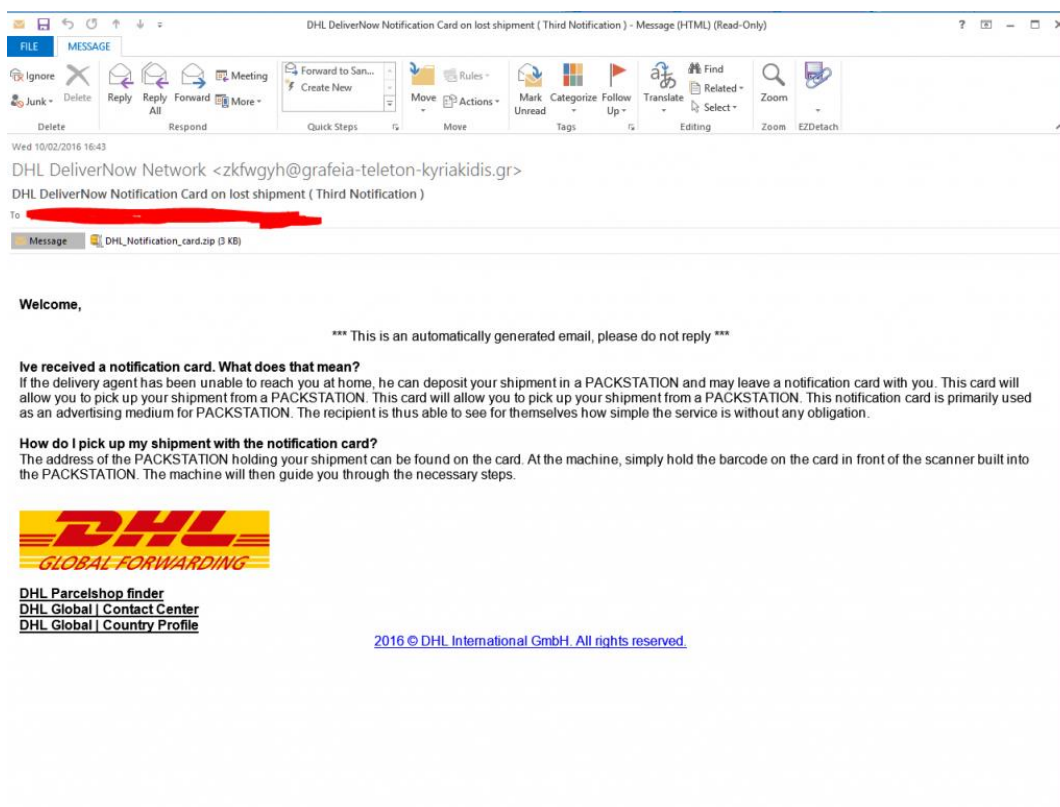
21. ábra Zsarolóvírust tartalmazó levelek "Tárgy/Subject" mezői és eloszlásuk

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 (invoice) érkezett, ráadásul egy külföldi cégtől? A második legjellemzőbb, hogy egy névtelen dokumentum van a csatolmányban, ami megint felkeltheti az érdeklődést, hogy mi is lehet? De ugyanez a célja a többi témának is. Bár itt a statisztikában nem jelenik meg, de sokszor előfordul, hogy valamilyen csomagküldő cég értesítésének álcázzák a vírust. 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 nyeremény értesítésekre is, ahol több milliós nyereménnyel kecsegtetnek, mert valaki, vagy valami kisorsolta a felhasználó e-mail címét. Ilyen nincs. Ha nem játszottunk nem is nyerhetünk! Ha nincs milliomos afrikai bankár nagybácsink, akkor nem is örökölhettünk tőle mesés vagyont.

Amiről felismerhetjük az ilyen leveleket:

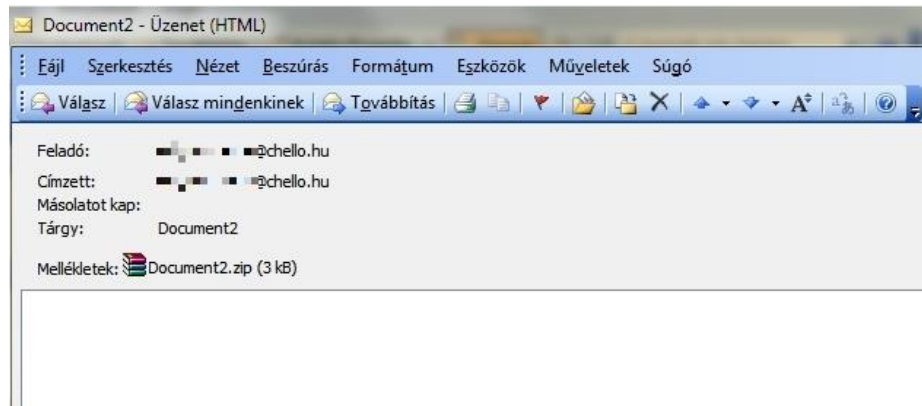
A feladó és a hozzá kapcsolódó e-mail cím nem függ össze. Lenti példában – elnézést a morbiditásért, a DHL nevében egy görög temetkezési vállalat címéről küldte a csaló az üzenetét, nyilvánvalóan hamis a levél.



22. 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.





23. ábra Zsarolóvírust tartalmazó levél, a címzett a behamisított feladó.

#### 6.4.4 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. 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 fájlhozzáférés. 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).

#### 6.4.5 Tűzfalak

A tűzfalak olyan hardveres vagy szoftveres eszközök, melyek egy előre definiált szabályrendszer alapján intézkednek 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 az 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 **betörésektől**, 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 engedélyoznünk 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.

## 6.5 Adatvédelmi megfontolások

Személyi biztonságról akkor beszélhetünk, ha minden adatunk (legyen az 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 – ekkor általában az adatkezelőnek be kell jelentkeznie az Adatvédelmi Nyilvántartásba, mint regisztrált adatkezelő, 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

össességét és elfogadott kockázati szinten való működését jelenti, amelyben az adatok és információk bizalmassága, sértetlensége és rendelkezésre állása biztosított.

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) [m] a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Ezt fogja követni 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)”. 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 tananyagnak 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 az olvasó, akkor azért érdemes utánanézni, mert a jövőben az előírások és a büntetési tételek szigorodnak.

A GDPR létrejöttének célja volt az is, hogy az EU államolgárainak 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 indokoltá 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 az egészségügyi 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 tekinthetők, ez miatt mind a célzottan támadóknak, a célzottabb reklámok küldőinek vagy esetlegesen zsarolóknak sokkal nagyobb értéket tudnak képviselni.

A képzett támadók sokféle módon szerezhetik be a szükséges információkat, például telefonhívásokkal (kikérdezés), adathalászattal (phishing), eltérítéssel adathalászattal

(pharming), kifizetéssel (shoulder surfing), vagy személyesen, megtévesztéssel (szélhámosság – social engineering). A szélhámosság módszerei változatosak, nagyon gyakori például az, hogy a szélhámosságok valamilyen ürügy révén (pl. üzleti tárgyalás) bejutnak a helyszínre és ott szétnéznak további adatok után kutatva. Ugyanilyen gyakran történik az meg, hogy a szélhámosság **információbúvárkodást** 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 tulaját 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 hasznót.

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 felülettel előlépett közösségi oldalakon elvégzünk néhány beállítást és figyelembe vesszünk néhány szabályt is.

### 6.5.1 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, amely a WWW szabványos nyelvének tekinthető, vannak definiálva. A HTML formátumú linkek (kereszthivatkozások) segítségével a dokumentumok kapcsolati hálót alkotnak az interneten. A böngészőt eredetileg arra találták ki, hogy szövegeket, majd képeket keressen az interneten és azokat jelenítse is meg – ez a **böngészés**. Időközben a böngészők már további grafikákat is meg tudnak jeleníteni úgynevezett beépülők (plugin) segítségével, e-maileket lehet velük küldeni, és videokonferenciákat lehet tartani, és még sok más egyébre is használhatók.

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. 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 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/vagy használni. A szoftverfrissítések telepítésének az a leglényegesebb oka, hogy ezzel lehetőséget kapunk kijavítani egy program hibáját vagy biztonsággi kockázatát.

Ezen kívül, mivel a böngészők a weboldalak HTML nyelven megírt kódját értelmezik és jelenítik meg ezért sajnos a forráskódba beszúrt olyan parancsokat vagy mini programokat is értelmezik és lefuttatják, amelyekről a felhasználónak nincs is tudomása, mivel magán a weboldal megjelenítésében nem okoz 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 mini programot (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 ez miatt nagyobb arányban fognak megfertőződni, akkor ezt a támadást 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, vagy a böngészők fekete listára teszik az oldalt és jelzik a felhasználónak, hogy az oldal rosszindulatú programot terjeszt. Az ilyen fertőzés ellen a

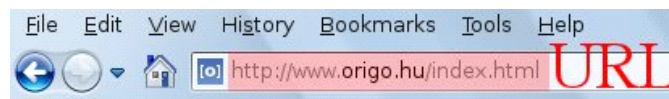
legjobb módszer a naprakész vírusirtó program, amely már letöltés előtt, vagy közben megfogja a kártevőt és figyelmezteti a felhasználót. Sajnos ilyen fertőzési próbálkozással bármilyen weboldalon összefuthatunk egy papírbolt weboldalától az iskolai weboldalakon át egy magánszemély privát oldaláig bezárólag. Nem kell, hogy illegális vagy felnőtt tartalmakat megosztó oldalakra látogassunk.

Az internet-használat 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, 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, mint internet-kávézó, nyílt hozzáférési pontok, hogy megtanuljuk hogyan kell személyes adatainkat törölni a böngészőből, különös tekintettel a böngészési előzményekre, könyvjelzőkre, ideiglenesen tárolt internet fájlokra, az elmentett jelszavakra, sütikre, automatikusan kitöltött űrlap-adatokra. Ez akkor is fontos, amikor ilyen helyeken a webalapú levelező fiókunkat használjuk.

## 6.5.2 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 - több százezer oldallal bővül. A nyomtatott sajtó (kiadók), nyomtatott publikációk, egyetemek, magánszemélyek, múzeumok, nemzeti és nemzetközi szervezetek, egyesületek, vállalatok stb. kínálnak számtalan információt.



24. ábra Uniform Resource Locator - URL

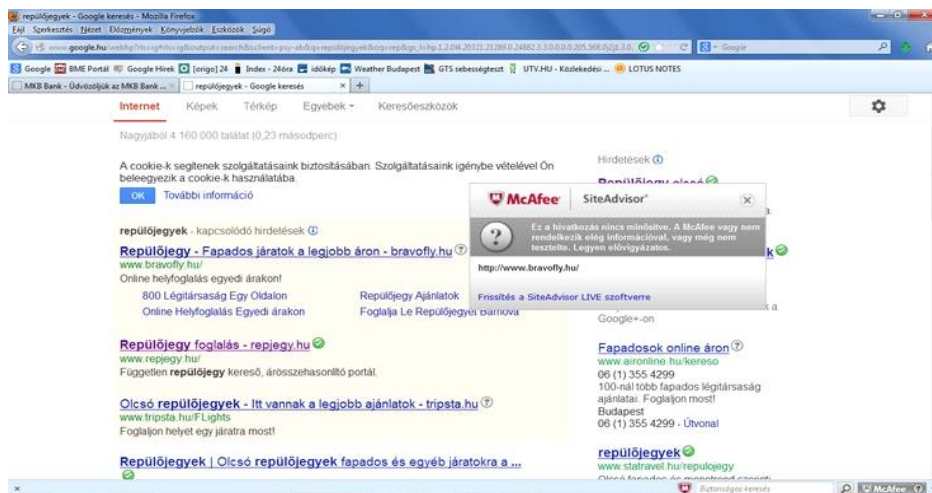
Minden weboldalnak van egy neve, az úgynevezett URL (Uniform Resource Locator), amit böngészővel lehet elérni, azaz a böngésző címsávjába kell beírni. A névhez egy IP-címnek is kell tartoznia, ami alapján a hálózati kapcsolat létrejöhet. Az URL áll egy protokoll-megnevezésből (http://), egy doménnévből (www.origo.hu) és egy oldalnéből (index.html).

A nevek és címek összerendelését segíti a **DNS**, Domain Name System, magyarul a doménnév-rendszer [n]. A DNS rendszer a domainekeket (tartományokat) kezelő, a világon több ezer szerverre elosztott hierarchikus adatbázis-rendszer. Ezek a domainekek vagy tartományok úgynevezett zónákra vannak elosztva, ezekért egymástól független adminisztrátorok 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) szerveret takarhat csupán. Az egyes tartományokat (pl. .hu) felosztották zónákra (pl. ecdl.hu), ahol minden egyes IP-címet a zóna-felelős menedzsel és rendel hozzá. A zónába a tartományon keresztül vezet az út, tehát a rendszer lelke a legfelső szintű tartomány-vezérlő 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 (193.225.14.73). Ez nyilván sokkal kényelmetlenebb megoldás.

A World Wide Web-en általában az ún. 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.

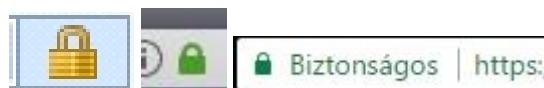
A támadók jellemzően az internet kevésbé ellenőrzött részein bújnak meg, **álweboldalak**at készítenek (melyek megszólalásig hasonlítanak az eredetire, de mögöttük már a támadó áll), illegális tartalmakat árulnak, vagy rosszindulatú programokat, szkripteket (parancssori programok), linkeket szeretnének letölteni/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, amiket a védelmi programok képesek többé-kevésbé beazonosítani, és a felhasználót erre figyelmeztetni. Az egyik ilyen védelmi szolgáltatás a „SiteAdvisor”, ami a weboldalak minősíti és a minősítés alapján tanácsokkal látja el a felhasználót az oldallal kapcsolatban.





25. ábra McAfee SiteAdvisor – a megbízható weboldalakért

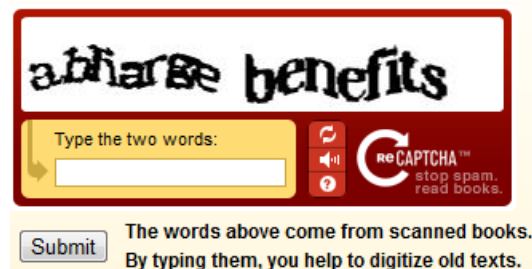
Például egy online pénzügyi tranzakció elvégzésekor, vagy személyes adataink megadásakor, azonosító és jelszó megadásakor a weboldal biztonságának biztosításához ragaszkodni kell. Ennek leggyakoribb eszköze a biztonságos böngészés, a https (secure http) protokoll használata. Tipikusan a nyilvános adatokon végrehajtódó és nyilvános adatokat szolgáltató keresőmotoros weboldalaknál található http előtag, mert ezeket nem szükséges védett oldalon megjeleníteni. 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.



26. 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.

Szintén az automatizált támadások elleni védelemre szolgál a „**captcha**” [k]. 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. Leggyakrabban egy olyan módon eltorzított szöveg felismerését jelenti, mely meghaladja egy számítógépes program képességeit, de nem okoz gondot az embernek.



27. ábra Captcha

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

### 6.5.3 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), Javaappletek, ActiveX Control-ok, JavaScript, VBScript és a Flash.

- Sütik: A sütik (cookie) egy kis adatbázist képeznek, amelyek a felhasználó PC-jén elraktározódnak olyan információkkal, amelyek összefüggésben állnak a meglátogatott internetes oldalakkal. A sütiket azért kell blokkolni a böngészőnkben, hogy nyugodtan böngészhessünk ismeretlen weblapokon, a kifizetés legkisebb veszélye nélkül. Például, ha egy korábban látogatott weboldalra lépünk és azt tapasztaljuk, hogy a bejelentkezési mező már ki van töltve, akkor biztosak lehetünk



benne, hogy ez egy sütiben el van tárolva a böngészőnkben. A sütik képesek elraktározni a látogatott weboldalak címeit, azon kulcsszavakat, amelyekre kereséseket indítottunk és képesek eltárolni a különböző weboldalakon történő bejelentkezéseink adatait is. A jelszavainkat is.

- **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 független a hardvertől és az operációs rendszertől, nagy népszerűségnek örvendett a Java, 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 Javán alapuló script nyelv, olyan programozási nyelv, amely a felhasználónál szövegformában van jelen, és külön 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 weboldalat 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. Napjainkban egyre kevesebb az olyan weboldal, amelyen nincs jelen valamilyen formában a flash. A Flash alapvetően egy grafikai szerkesztő, amely animációt és interaktivitást is lehetővé tesz. Mivel a Flash Player igen elterjedt, így a támadók ezen programok biztonsági réseit is kihasználják, hogy az áldozat gépére valamilyen káros programot telepítsenek vagy az áldozat gépéről információkat szerezzenek.

Fordítsunk kiemelt figyelmet az aktív tartalmakat megjelenítő programjaink frissítésére, mivel időről időre ismertté válnak sérülékenységek, amelyeket ezen programokra vonatkoznak. Mivel ezen programok gyakorlatilag milliányi 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, melyek 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”). Ennek hatására a felhasználó 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 szintet növelte ezáltal.

#### 6.5.4 A böngészőben tárolt adatok biztonsága

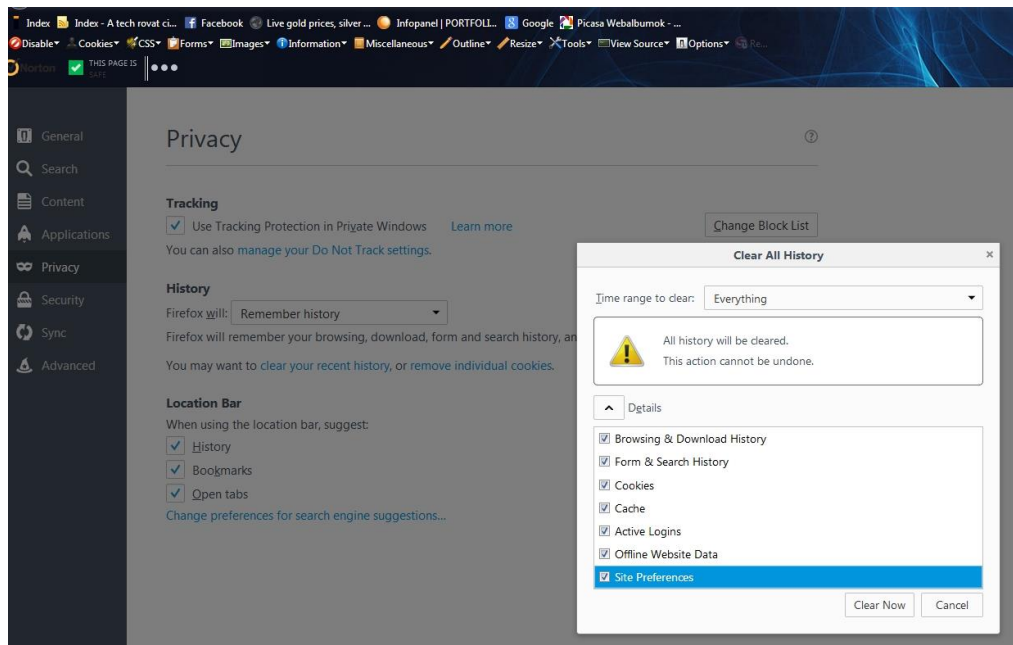
Böngészés során – akár tudunk róla, akár nem – számos adat és szokás naplózódik a meglátogatott oldalak kapcsán.

- 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 saját gépünkön tárolódnak. A sütik (cookie) egy kis adatbázist képeznek, amelyek a

felhasználó PC-jén elraktározódnak, természetesen csak akkor, ha ezt a felhasználó le nem tiltja, ugyanis alapértelmezetten szinte minden böngésző támogatja. Ebben a kis adatbázisban olyan információk raktározódnak el, amelyek összefüggésben állnak a meglátogatott internetes oldalakkal. Ez akkor is észrevehető, ha az online űrlapot a felhasználó elkezdi kitölteni. Olyan adatokat nem kell beírnia, amiket egyszer már megadott, mert a süti automatikusan felkínálja a korábban eltárolt adatokat ismételt felhasználásra. Sütiket (cookie) a felhasználó felismerésén kívül arra is alkalmazznak, hogy internetes oldalakat a felhasználó személyes kívánsága szerint a saját kényelme szerint lehessen kialakítani (profilok).

- 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.

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.



28. 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 árt.

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



## Az InPrivate be van kapcsolva

Amikor az InPrivate-böngészés be van kapcsolva, ez a jelzés látható

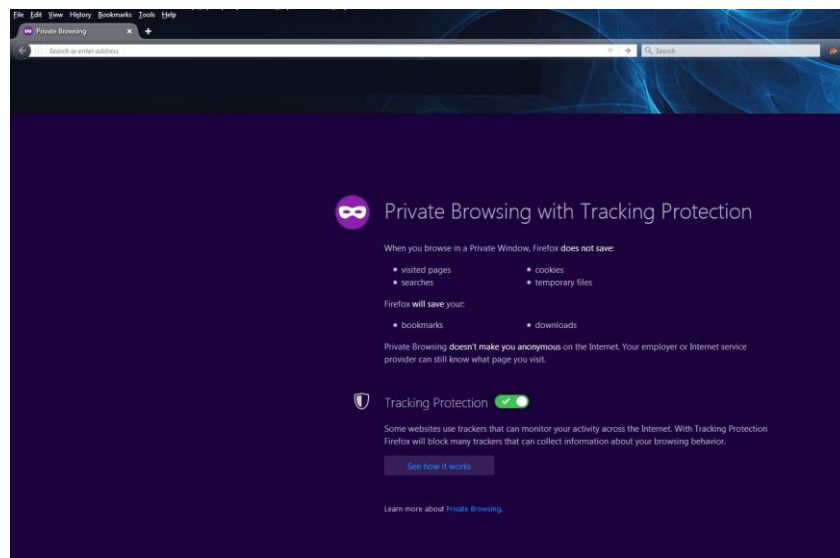


Az *InPrivate-böngészés* megakadályozza, hogy az Internet Explorer eltárolja a böngészési munkamenet adatait (többek között a cookie-kat, az ideiglenes internetfájlokat, az előzményeket és más adatokat). Az eszköztárak és bővítmények alapértelmezés szerint le lesznek tiltva. További információért tekintse meg a Súgót.

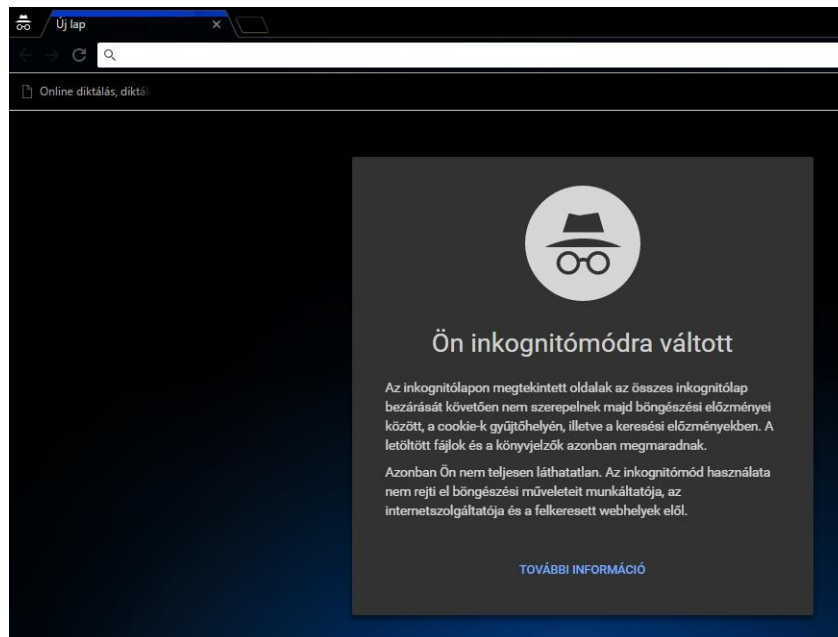
Az InPrivate-böngészés kikapcsolásához zárja be ezt a böngészőablakot.

További tudnivalók az InPrivate-böngészésről | Az Internet Explorer adatvédelmi nyilatkozata az interneten.

29. ábra Inprivate böngésző üzemmód Internet Explorer



30. ábra Privát böngészés Firefox böngészőben



31. ábra Inkognitó üzemmód Chrome böngészőben

### 6.5.5 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.

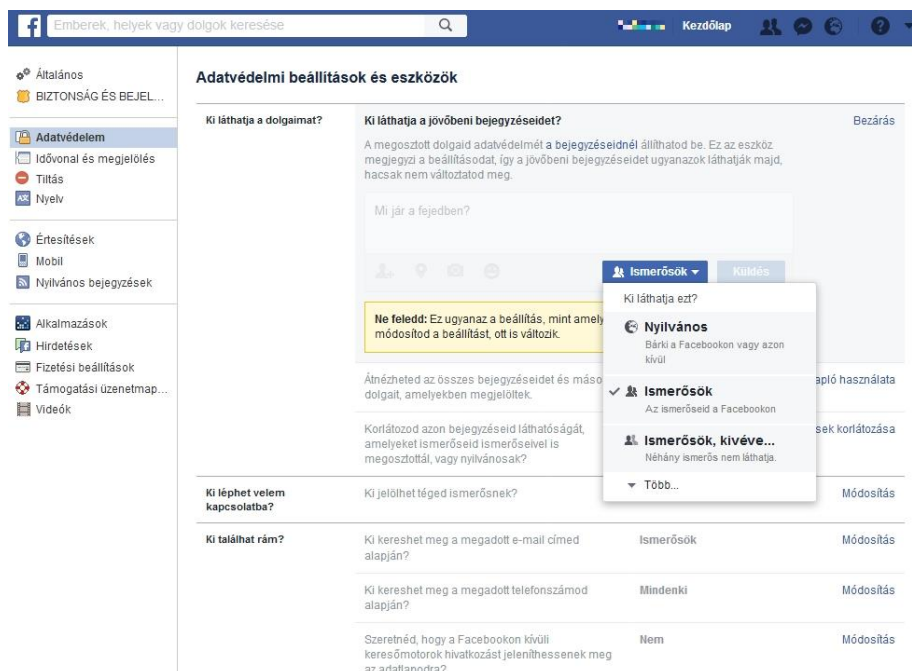
Ilyen veszélyt kevésbé rejt a zenei érdeklődés, az otthoni cím és a kedvenc televízióműsor megadása, mivel ezek egyrésztől több helyről hozzáférhető adatok, másrésztől többek által megismerhető adatok, mint a becenev. Egy szexuális bűnöző számára

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 kapcsolat-felvételt ne engedélyezzük senki ismeretlennek, csak annak, akit már valaki az ismerősi körünkben – valamilyen módon – hitelesített saját ismerőseként.



32. ábra Adatvédelmi beállítások közösségi oldalon

Az előbbi képen 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 három témakör köré csoportosulnak a beállítások – például – az egyik legkedveltebb közösségi oldalon, a Facebookon:

- Ki láthatja a dolgaimat?
- Ki léphet velem kapcsolatba?
- Ki találhat rám?

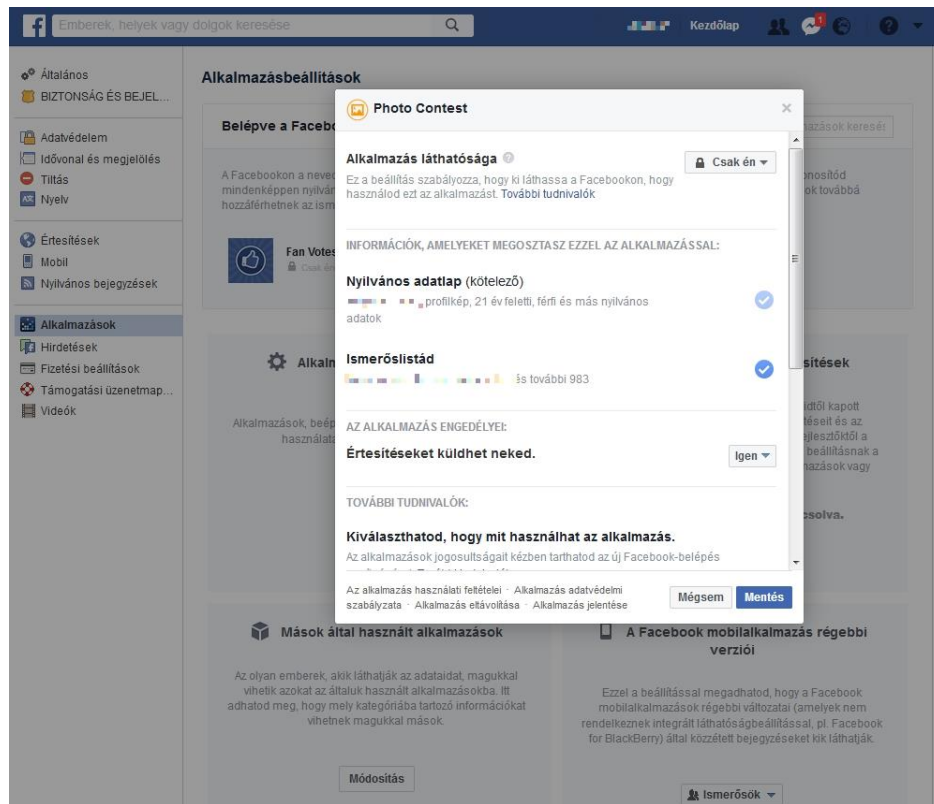
A Facebookon ezen kívül számos egyéb módon is növelhetjük a biztonságunkat. Érdemes megfontolnunk, hogy engedjük-e és ha igen milyen kontroll mellett, hogy mások is írjanak az idővonalunkra, vagy mások megjelölhessenek minket képeken.

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 felhasználók azt látják, hogy jéé, milyen érdekeset írt az ismerősöm, rákattint és már ő is megfertőződött és így tovább - láncreakció szerűen.

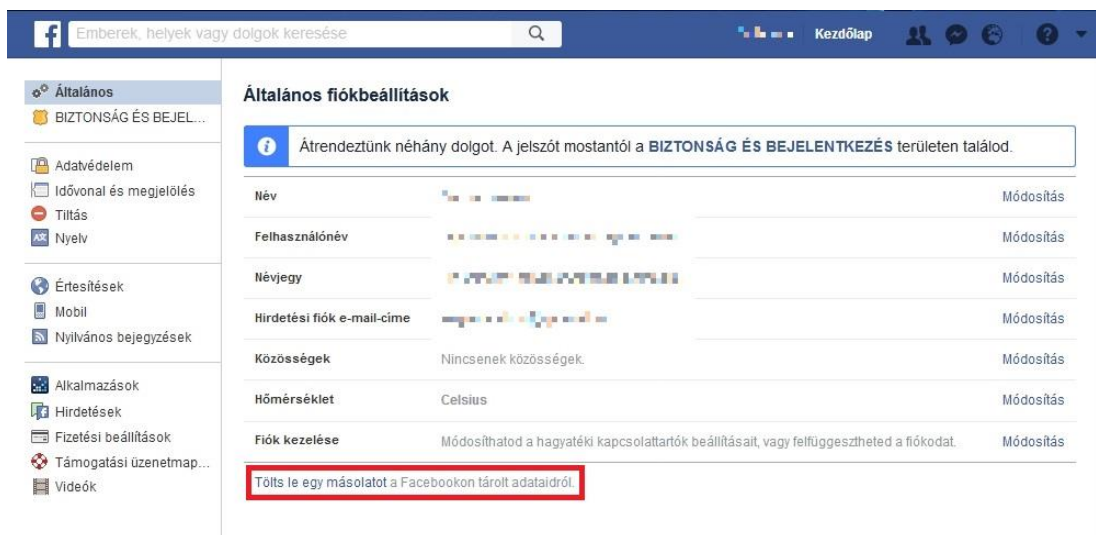
Amennyiben használunk Facebookos alkalmazásokat időnként vizsgáljuk felül, hogy tényleg használjuk-e őket és ha nem, akkor töröljük, ha pedig igen, akkor nézzük végig, hogy mihez akar az alkalmazás hozzáférni és amit problémásnak gondolunk, azt tiltsuk le.





33. ábra Facebook alkalmazások jogosultságai

Ha tudni szeretnénk, hogy milyen adatokat és tartalmakat tárol rólunk a Facebook, akkor van lehetőségünk ennek letöltésére:



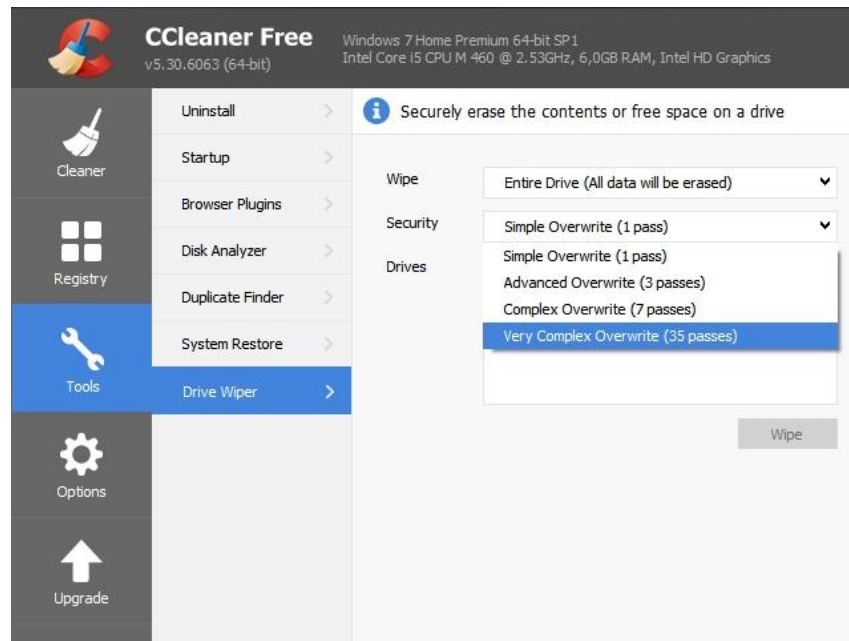
34. ábra Facebook által rólunk tárolt adatok másolatának letöltése

### 6.5.6 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) **bedarálása**, szétroncsolása fizikailag (hard delete). Ugyanígy az adatok végleges törlését eredményezi a merevlemezek **elektromágneses törlése** (degaussing) – ami erős mágneses mező gerjesztésével tünteti el a mágnesezett adathordozókról az adatokat, gyakorlatilag felülmágnesezi azokat – ez főle 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 [g] 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, okosTV-vel 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 szoftveres adatmegsemmisítő szoftver használata majd a gyári beállítások visszaállítása.

A következő ábra a CCleaner szoftvernek mutatja be azt a beállítását, amikor a merevlemez szabad területén esetleg ottmaradt korábbi adatokat 7-szeres felülírással törli – illetve teszi véglegesen elérhetetlenné.



35. ábra Végleges adattörlés szoftveresen

## 6.6 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.

### 6.6.1 Digitális aláírás

A digitális aláírás egy olyan titkosított kód, amely egy személy azonosságát társítja ahhoz a fájlhoz, amit aláírt, más szóval hitelesíti. A **hitelesítés** ugyanis az állított azonosság megerősítése, így a **hitelesség** az eredet és a küldő meg nem változását jelenti. A digitális aláírás szabatosabban megfogalmazva egy – aszimmetrikus kriptográfiai algoritmuson alapuló – matematikai számsor, amelynek előállítási eszköze a **digitális aláírás séma** 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, amit a hitelesítésszolgáltatók digitális

tanúsítványba foglalnak az aláíró személy azonosítása és hitelesítése után. A **digitális tanúsítvány** ennél fogva igazolja, hogy az üzenet küldője valóban az, akinek állítja magát. 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 [1] titkosításra és hitelesítésre készített programcsomag részeként használható digitális tanúsítványokat jelöli.

A digitális tanúsítványok 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 eredt – arra használatos, hogy valaki az eszközeinek birtoklását hitelesítse általuk és **biztonságos kapcsolódást** 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,
- 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 alacsony szintűen írták ma már digitálisan, hogy a támadók addig se tudják észrevétlenül módosítani ezeket a tartalmakat, amíg eljutnak a felhasználók gépeire (kódalírás). A telepítések előtt érdemes elolvasni azt az üzenetet, mely megmutatja a telepítendő szoftver íróját is. Másrészt 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. Ilyen ügyintézési terület ma Magyarországon például a cégeljárás.

### 6.6.2 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 bájtól pár/sok terrabájtig is akár), így a hatékony aláíráskészítéshez szükségessé vált egy olyan eljárás közbeiktatása, mely az aláírandó adat méretétől függetlenül 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-ének nevezünk.

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

- 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 – például tekintsünk 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) különbsége ad lehetőséget.

## 6.7 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
- végpontvédelem a működésbiztonság megőrzése számára

Az áramellátást szünetmentes tápegységek [h] 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 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
- mennyire van védve a hálózat a szolgáltatás-megtagadásos támadások ellen (DoS, Denial of Service)

A **DoS-támadások** 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 (ez hatványozottan sikerülhet, ha hibás az adatcsomag és a szerver oldalnak több idő feldolgozni vagy mondjuk egy-egy hibás feldolgozásnál végtelen ciklusba kerül), hogy más felhasználók kérésének feldolgozására a szervernek ne maradjon kapacitása, így az lelassul a külső szemlélő számára, vagy megszűnik válaszolni. Otthoni felhasználóknak jó hír, hogy az erre irányuló védelem megteremtése a szolgáltató feladata.



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? Sajnos vannak ilyen bűnszervezetek, aki az otthoni felhasználók millióinak számítógépét 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. Sajnos ezen eszközök védelmével a felhasználók és a gyártók még nem kielégítően foglalkoznak, pedig fontos lenne.

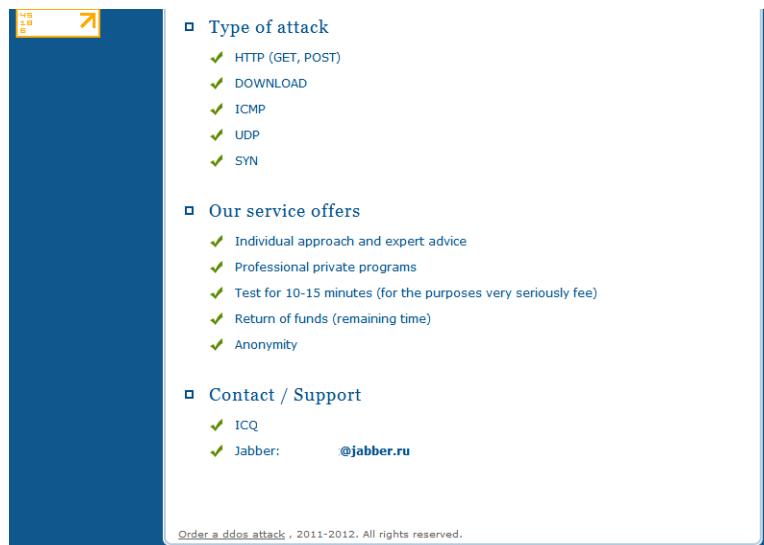
Dos és dDoS támadások esetén az adott internetes szolgáltatás nem elérhető. Ha valakinek az üzleti működése múlik egy honlapon, akkor érdemes felkészülni egy ilyen támadásra. Hiszen ha nem elérhető a webáruház például, akkor nincs bevétel.

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



36. ábra dDOS támadás megrendelő felület 1. rész





37. ábra dDOS támadás megrendelő felület 2. rész



38. 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 adatokat, 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, **mentéseket**. A

hardver meghibásodása (olvasófej, mágneslemez felülete, mágnesezettség), vagy az eszköz (telefon, laptop) elveszése, ellopása következtében ezek az adatok megsérülhetnek, megsemmisülhetnek annyira, hogy a teljes visszaállításukra lehetőség nem lesz.

### 6.7.1 Fájlok biztonsági mentése

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

Az adatvesztés ellen az adatok megőrzése, a mentések létezése nyújthat egyedül védelmet. A mentések tervezésénél az alábbiakat kell megfontolás tárgyává tennünk a helyes mentés megtervezéséhez:

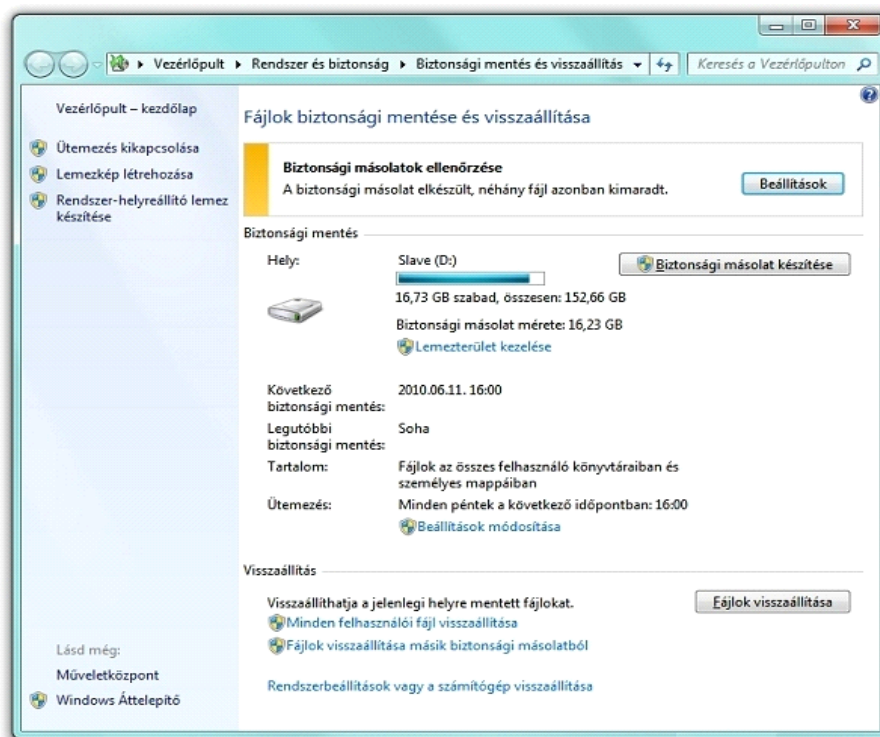
- Mekkora adatmennyiséget kell mentenünk?
- Milyen gyakran változnak meg a mentendő adatok? Milyen gyakran kell elmenteni őket ahhoz, hogy lehetőleg ne legyen súlyos adatvesztés?
- Hány példányban kell a mentést elvégezni?
- Mikor kell a mentést elvégezni, más szóval mikorra lehetséges ütemezni a mentést ahhoz, hogy ne zavarjon senkit sem – és befejeződjön a következő napi mentés elindítása előtt?
- Meddig kell megőrizni a mentéseket?
- Hol tároljuk a mentéseket?
- Hogyan kell a mentéseket biztonságosan megsemmisíteni?

Windows rendszerben a mentést a beépített automatikus biztonsági mentési eszköz, a Windows Backup [i] biztosítja 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 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 [j] alkalmazás is. 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 atékony megoldás lehet a fájlok manuális másolása, például egy külső merevlemezre, vagy egy nem állandó jelleggel felcsatlakoztatott felhő alapú tárhelyre.

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 tönkre megy, 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.



39. 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 ezen eszközön is rengeteg fontos adatot tárolunk. Telefonszámok és egyéb kontakt adatok, sms-ek, fényképek, videók. Gondoskodni kell az okostelefonok adatainak mentéséről is. Erre szintén vannak célszoftverek, különböző funkcionalitással.



40. ábra Okostelefonok fontos adatainak mentése



41. ábra Adatok mentése Windows környezetben (Aomei backup)

A mentések gyakoriságát úgy válasszuk meg, hogy egyrészt ne jelentsen többletterhet, másrészt 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.

## 6.7.2 Védelem az áramellátás hibái ellen

A szünetmentes áramellátó berendezések használata számítástechnikai és ipari környezetben, vagyis otthon és a munkahelyen ma már elengedhetlenné vált. Nem szívesen vállalnánk fel ugyanis egy áramszünet, illetve a feszültség-ingadozással járó zavarok hátrányos, költséges következményeit. Az **elektromos hálózatról** üzemeltetett eszközök működése függ a hálózat működésétől, más szóval attól, hogy van-e áram. Az otthoni eszközök java része kizárólag az elektromos hálózatról működik, amely meghibásodása esetén 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 kárösszeg, melyet az áramszünetek és a hálózati áramellátás ingadozásai, túlfeszültségei okozhatnak.

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. Illetve 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.



42. ábra Szünetmentes otthoni áramellátó eszköz

## 6.8 Komplex megközelítést igénylő fenyegetettségek és védelmi megoldások

### 6.8.1 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 mint kiberfegyverek 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, addigra mára már az összetett támadások ellen hasonlóan összetett, többféle fenyegetéstől is megóvó végpontvédelemre van szükség.

#### 6.8.1.1 Vírusvédelem

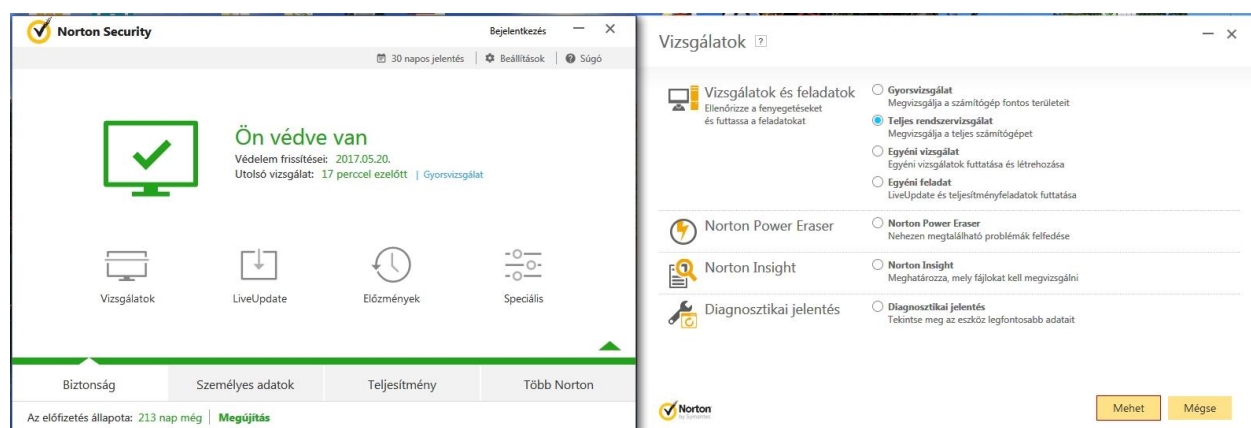
A vírusirtó szoftverek alkalmazása a legismertebb és több mint 90%-ban elterjedt védekezési módszer. Hatékonyan véd a **fertőzés** ellen. A fertőzés szó alatt itt egy speciális rosszindulatú program operációs rendszerbeli fájlokhoz való hozzákapcsolódását értjük. A vírusirtó programok több lehetőséget ajánlanak fel a fertőzött fájlok kezelésére, a végleges törléstől a karanténba helyezésen át a helybenhagyásig terjednek a **fertőzésmentesítés** eszközei.

A **karantén** az operációs rendszerben egy olyan 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 fertőzésmentesíteni, így nem tudjuk megszabadítani a gépet fertőzéstől, mert valamiért a vírusirtó program erre nem képes.

Minden vírusirtónak van egy állandóan működő része, ami az aktuális forgalmat szűri és nem engedi be a felismert mintát tartalmazó fájlokat, illetve különböző mélységű ütemezett kereséseket is végre lehet hajtani, a leginkább üresjáratú időpontokban. Ezeket a felismeréseket a vírusdefiníciós fájlban tárolt mintákkal való összehasonlítás teszi lehetővé. Azért, hogy a legújabb vírusok ellen is védettek legyünk, rendszeres időközönként javasolt

a vírusdefiníciós fájlokat letölteni. Ez biztosítja azt, hogy az új fenyegetések elleni védelem naprakészen maradhat, mivel a letöltés által frissülnek a definíciós fájlok.

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 indoklást, hogy egyre elterjedtebbek az úgynevezett nulladik napi sérülékenységeket kihasználó kártevők, illetve a támadók eszköztárából fakadóan olyan gyorsan tudják mutálni és kiküldeni, terjesztetni 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.



43. ábra Teljes rendszervizsgálat Norton Security programmal



Teljes rendszervizsgálat ?

**X Fenyegetés észlelhető**

\* Javasolt műveletek

Cím	Kockázat	Állapot	Művelet
JS.Downloader teljesen megoldva	Magas	Teljesen megoldva	✓
JS.Downloader teljesen megoldva	Magas	Teljesen megoldva	✓
Trojan.Horse teljesen megoldva	Magas	Teljesen megoldva	✓
Ransom.Cryptodefense teljesen megoldva	Magas	Teljesen megoldva	✓
Trojan.Zbot teljesen megoldva	Magas	Teljesen megoldva	✓
Downloader.Upatre teljesen megoldva	Magas	Teljesen megoldva	✓

A karanténba zárt fájlokat [itt](#) állíthatja vissza.

[Eredmények összegzése](#)
[Eredmények exportálása](#)
[Bezárás](#)
[Összes alkalmazása](#)

44. 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 védelem fenntartásához naprakészen kell tartani a vírusdefiníciós fájlokat, ami rendszeres internet-kapcsolatot és frissítési tevékenységeket igényel.

### 6.8.1.2 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 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 érhetőek el.

Nem mehetünk el szó nélkül az egyre elterjedtebb okostelefonok védelme mellett sem. Az okostelefonok is ugyanúgy számítógépek, mint nagyobb társaik épp ezért ugyanúgy fenyegetettek, mint az asztali munkállomások vagy laptopok. Okostelefonokra is elérhetőek végpontvédelmi megoldások – fizetők és ingyenesek egyaránt. Rengeteg



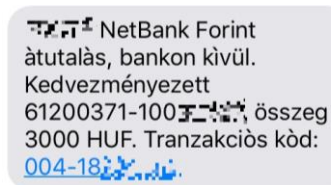
olyan kártevő program van – és számuk rohamosan nő, amely a legelterjedtebb okostelefon platformra az Androidra íródott. Természetesen nem kivétel a Windows és az iOS platform sem ez alól. Az okostelefonok szinte éjjel nappal online vannak, elérik az Internetet – és ezzel együtt ezen eszközök is elérhetőek 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! Lehetőleg valamilyen neves gyártó alkalmazását töltsük le a hivatalos forrásokból (Google Play, AppStore, Windows Central) és használjuk rendszeresen, mint a nagy számítógépeken (frissítések, online ellenőrzés, rendszeres teljes keresés).

## 6.8.2 Biztonságos Internet bankolás

Manapság egy elterjedtebb az Internetes bankszámlakezelés. A bankok mindent megtesznek azért, hogy ezen szolgáltatásuk megfelelő védelmet nyújtson az ügyfelek számára. Egyrészt ez saját üzleti érdekük is, másrészt a Pénzügyi Felügyelet is szigorúan ellenőrzi a bankok által megtett erőfeszítéseket.

Internetes bankolás felhasználói oldalról vizsgálva két kritikus pontot hordoz. Az egyik a belépés, a másik a különböző pénzügyi műveletek végrehajtása.

Az internetbanki belépésre a hazai bankok évek óta kínálnak megerősített, úgynevezett kétfaktoros bejelentkezést. Ilyen lehet az SMS-ben érkező egyszerhasználatos jelszó, a bank által adott hardveres véletlenszám generátor (token), illetve a chipkártyás beléptetés. Vannak bankok, ahol ezen megerősített belépési módok nem kötelezőek, de választhatóak. 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 többfaktoron alapuló módszerrel megerősítve fogadják be. Legegyszerűbb példa az utalás, ahol a beküldött megbízást követően egy megerősítő tranzakciós kódot küld a bank. Az SMS-ben benne van a célszámla, az utalandó összeg és a legvégén a tranzakciós kód.



45. ábra Tranzakció hitelesítő SMS üzenet

Mivel ez minden esetben a felhasználó telefonszámára érkezik meg, még ha egy támadónak sikerült is belépnie a felhasználó netbankjába, ha az utaláshoz szükséges tranzakciókódot nem adja meg az ügyfél – mert feltűnik neki, hogy nem ő akart utalni, vagy nem oda, nem ekkora összeget, akkor a tranzakció nem fog létrejönni, nem lesz anyagi veszteség. Ha ilyet tapasztalunk, akkor azonnal értesítsük bankunkat és várjuk meg, amíg megvizsgálják bejelentésünket.

Annak érdekében, hogy a felhasználó internetbanki adatait ne lehessen ellopni, minden bank az Internetbanki oldalán biztonsági figyelmeztetéseket tesz közzé, amit érdemes megfogadni és alkalmazni.

### 6.8.3 Biztonságos bankkártya használat – internetes fizetés

#### 6.8.3.1 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. (Forrás: [www.bankracio.hu](http://www.bankracio.hu))

Fontos, hogy a bankkártyán fizikailag leolvasható adatok (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, mégkevésbé szabad a kártyára írni. PIN kód begépelésnél 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 és hasonló kódokat válasszuk.

ATM készpénzfelvételénél mindig győződjünk meg arról, hogy a kártyabeadónyílásra 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 dugjuk be a kártyát, értesítsük a bankot.



46. 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, az máris a támadók birtokában van.

Internetes fizetéshez nem szükséges a kártya fizikai jelenléte, elég ha a kártyán szereplő adatokat ismerjük. Éppen ezért fontos, hogy amikor fizikailag fizetünk a kártyával, ne engedjük, hogy elvigyék, ne tévesszük szem elől, mert ezidő 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.

### 6.8.3.2 Biztonságos internetes fizetés

A világban egyre elterjedtebb az online vásárlás. A különböző webáruházakban megvásárolt termékek esetében választhatjuk az utánvétes fizetést, de a leggyakrabban valamilyen elektronikus fizetési megoldást választunk. Ezen elektronikus fizetési eljárások mögött jellemzően egy bankkártya van, ami mögött pedig a bankszámlánk.

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 nincs rajta sem mágnescsík, sem chip, tehát készpénzfelvételre vagy POS terminálos fizetésre nem alkalmas. Csak a kártyaadatok érdekesek. A virtuális kártya általában vagy a főszámlánkhöz 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 időzárás limitnél 24 vagy 48 óra után visszaállnak az alaplimitre – jellemzően 1Ft-ra. Így ha el is lopják a kártyaadatainkat valamelyik kereskedő számítógépes rendszeréből, nem férnek hozzá a számlán tartott összegünkhöz.



47. ábra VISA Virtual kártya internetes fizetéshez

Egyik legjellemzőbb internetes fizetési módszer még a PayPal, amely egy virtuális számla, amely mögé szintén valamilyen bankkártyát kell megadni. Ha nagyon biztonságosak akarunk lenni, akkor megadhatunk virtual 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.

Nagyon fontos, hogy akár fizikailag, akár internetes fizetésre 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 kártyaügyfélszolgálatának telefonszáma az azonnali kártyatiltáshoz.

#### 6.8.4 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)

##### 6.8.4.1 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
- Sexting: szexuálisan provokatív fényképek, videók készítése, és továbbküldése

##### 6.8.4.2 Internetes zaklatás lehetséges okai:

- Anonymitás/személytelenség., A támadó azt gondolja, hogy láthatatlan tud lenni, kicsi a lebukás veszélye
- Kevesebb visszajelzés – eldurvulás. Míg 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, ez miatt 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 rábírní 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. Ez miatt az áldozat fokozottan rosszul érzni magát, ha pedig mégis kilép az adott virtuális közösségi térből, akkor egyrészt minden információforrást elveszít, másrészt kirekesztettnek érzni 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 beléthatatlan következményei is lehetnek.
- Nehéz fellépni ellene (felhasználó törlés és tiltás, poszt, fotó törlés, bizonyítás).

#### 6.8.4.3 Internetes zaklatás lehetséges következményei:

Az internetes zaklatás negatív hatással lehet a testi és lelki egészségre, fejlődésre, társas kapcsolatokra, iskolai és sport vagy egyéb teljesítményre egyaránt.

- Düh
- Szorongás
- Depresszió
- Önsértés
- Magányosság
- Iskolakerülés, szökés
- Pszichoszomatikus betegségek
- Alacsony önértékelés
- Öngyilkossági gondolatok/befejezett öngyilkosság (Sajnos számos példa van arra, hogy internetes zaklatás öngyilkosságba torkollott.)

#### 6.8.4.4 Internetes zaklatás kezelési módszerei:

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

Probléma a kezelési módokkal, hogy a gyerekek jelentős része úgy gondolja, hogy jobban ért az Internethez és a technológiához, mint a szülője – pedagógusa. Ez miatt sajnos nem fogadnak meg jótanácsokat és nem fogadják el a tiltást, korlátozást büntetést sem.

#### 6.8.4.5 Internetes zaklatás megelőzése

A legfontosabb dolog az internetes zaklatás megelőzése, hogy 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 nem fogad el, nem tőlünk kér tanácsot, segítséget!
- Beszélgetni a gyerekkel, SOKAT beszélgetni – bizalom kiépítése nagyon fontos!
- Felkészíteni a leggyakrabban használt app-ok, szolgáltatások és oldalak BIZTONSÁGOS használatára.
- Ellenőrzés: Elkérni a telefont, gyerekekkel együtt átnézni, Internet böngésző előzmények, Youtube előzmények, VIBER/Whatsapp/Snapchat/Tinder Messenger csoportokat,
- Facebookon és más közösségi oldalakon legyen ismerős a gyerek
- Kövessük a Twitteren, Instagrammon.
- Szülői felügyelet program használata.
- Szabályok lefektetése (pl. telefon használat korlátozása, idegenekkel nem ismerkedünk, nem találkozunk, ésszel publikálunk stb.)

## 7 Mellékletek

### 7.1 Ajánlott irodalom

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

[2] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

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

[4] 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

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

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

[7] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012

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

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

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

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

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



## 7.2 Internetes hivatkozások jegyzéke

- [a] <http://hu.wikipedia.org/wiki/Számítógép-architektúra>
- [b] [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing)
- [c] Global Use of Electronic Authenticity; Erdősi Péter Máté, SSRN, 2013;  
[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2264335](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2264335)
- [d] <http://www.magyarorszag.hu>
- [d] <http://www.saferinternet.hu>
- [e] jelszótörés - 10 millió jelszó <https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495>
- [f] Symantec Report  
[https://digitalhubshare.symantec.com/content/dam/Atlas/campaigns-and-launches/FY17/Threat%20Protection/ISTR22\\_Main-FINAL-APR24.pdf?aid=elq\\_&om\\_sem\\_kw=elq\\_18292472&om\\_ext\\_cid=biz\\_email\\_elq\\_](https://digitalhubshare.symantec.com/content/dam/Atlas/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-APR24.pdf?aid=elq_&om_sem_kw=elq_18292472&om_ext_cid=biz_email_elq_)
- [g] Biztonságos törlés <http://www.howtogeek.com/72130/learn-how-to-securely-delete-files-in-windows/>
- [h] Szünetmentes táp <http://www.extor.hu/szunetmentes-aramellato-berendezesek/kompakt-ups-otthonra-kis-irodaba>
- [i] Windows Backup <http://www.backup-utility.com>
- [j] TimeVault <http://www.tucows.com/preview/722287/Time-Vault>
- [k] captcha <http://hu.wikipedia.org/wiki/Captcha>
- [l] PGP <http://hu.wikipedia.org/wiki/PGP>
- [m] Adatvédelmi irányelv (GDPR) <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679>
- [n] DNS [https://hu.wikipedia.org/wiki/Domain\\_Name\\_System](https://hu.wikipedia.org/wiki/Domain_Name_System)

- [o] makró <http://wiki.prog.hu/wiki/Makr%C3%B3>
- [p] legnépszerűbb weboldalak <http://24.hu/media/2016/08/01/ezek-a-legnepszerubb-weboldalak-a-magyar-es-a-tersegbeli-fiatalok-koreben>
- [q] Kormányzati Eseménykezelő  
Központ <http://www.govcert.hu/>
- [r] Nemzeti Elektronikus  
Információbiztonsági Hatóság <http://neih.gov.hu>