ECDL/ICDL
IT Biztonság
verzió: 1.1

ECDL Magyarország

ECDL Hungary Approved Courseware

Rendelkezünk a vásárlói biztonságot jelentő tudással.

2011-ben 5,5 milliárd támadást blokkoltunk.

A Symantec páratlan rálátással rendelkezik a fenyegetések világára. Több mint 64,6 millió érzékelőnk figyeli a támadásokat több mint 200 országban és területen, nap mint nap. Miért ne használná fel a tudásbázisunkat a vásárlói bizalom növelésére, és ne teremtene új értékesítési lehetőségeket? A fenyegetésértékelések kialakításának köszönhetően fény derül az egyes környezetek gyengeségeire és kritikus pontjaira. Senki más nem rendelkezik ilyen szintű felderítéssel és ilyen védelmi megoldásokkal a vásárlók érdekében.

Bizalommal a hálózatok világában. Symantec™

Erdősi Péter Máté, CISA
NJSZT Informatikai biztonsági szakértő

ECDL/ICDL
IT Biztonság

verzió: 1.1
2013. szeptember 23.

A KKV-KAT ÉRŐ FENYEGETÉSEK MEGDUPLÁZÓDTAK

Egy kíbertámadás pillanatok alatt tönkreteheti vállalkozását

73% ennyi KKV-t ért már rossz-indulatú támadás[1]

36% a támadásoknak a kis-és középvállal-kozásokat célozza[2]

UP 81%

5.5 millió rosszindulatú támadás[3]

UP 36%

4 500 új web-alapú támadás naponta[3]

UP 41%

403 millió új rosszindulatú virus változat[3]

Védje ügyfeleit - és saját vállalkozását

EGYSZERŰ. GYORS. HATÉKONY.

89%-a

a KKV-knak tekinti az IT-t üzletileg fontosnak és használ felhő alapú megoldást a legfontosabb üzleti folyamatokra[4]

63%-a

a KKV-knak nem rendelkezik állandó informatikussal[5]

Ingyenes, 30-napos próbaváltozatot innen tölthet le:
go.symantec.com/sepsbe2013

Forrás: 1. Symantec SMB Information Protection Survey 2010 2. Symantec Intelligence Report, June 2012 3. Symantec Internet Security Threat Report Volume 17, April 2012 4. AMI Segmentation Study 2012 5. "The Accidental Entrepreneur," Forrester Custom Research prepared for Symantec, May 2012

Symantec.

IDŐÉRTÉK
Oktatási, Kereskedelmi és Tanácsadó Kft.

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

Szakmai lektor: Dr. Muha Lajos
ECDL lektor: Ziegler Tünde
Grafika és tördelés: Pilinyi Zsolt
Kiadó: Neumann János Számítógép-tudományi Társaság
1054 Budapest, Báthori u. 16.

Felelős kiadó: Alföldi István ügyvezető igazgató

ISBN: 978-615-5036-07-1

Symantec. | Website Security Solutions

Norton SECURED powered by Symantec

ONLINE BIZTONSÁG

MIRE FIGYELJÜNK?

Symantec. | Website Security Solutions

Norton SECURED powered by Symantec

CDSYS

COMPLIANCE DATA SYSTEMS Kft.

További információért keresse a Compliance Data Systems Kft. munkatársait a 06-1-700-4450-es telefonszámon, vagy az info@cdsys.hu email címen.
www.cdsys.hu

Tartalomjegyzék

1. Bevezetés ... *11*

2. Biztonsági alapfogalmak ... *14*

2.1 Kibertér ... *14*
2.2 Biztonság ... 16
2.3 Koncepcionális megközelítés ... 18
2.4 Információkritériumok ... *21*

3. Információrendszerek ... *24*

3.1 Hardver ... *24*
3.2 Alkalmazások ... *25*
3.3 Szolgáltatások ... *25*
3.3.1 Ismeretszerzés és kapcsolatteremtés interneten ... *27*
3.3.2 Elektronikus ügyintézés ... *28*
3.3.2.1 e-Europe ... *28*
3.3.2.2 Hiteles e-ügyintézés ... *29*
3.3.2.3 Környezet kímélése ... *30*
3.4 Hálózati elemek ... *31*

4. Fenyegetések, támadások ... *35*

5. A védelem kialakítása ... *43*

5.1 A bizalmasság ... *45*
5.1.1 Bizalmasság az operációs rendszerben ... *46*
5.1.1.1 Merevlemezek és USB-lemezek titkosítása, rejtjelzése ... *48*
5.1.1.2 Titkosítás irodai programcsomagokban ... *50*
5.1.1.3 Bizalmasság tömörített állományoknál ... *52*
5.1.2 Hálózat és bizalmasság ... *54*
5.1.2.1 Hozzáférés-védelem, jelszavak ... *55*
5.1.2.2 WiFi eszköz biztonsági beállításai ... *58*
5.1.2.3 E-mail ... *62*
5.1.2.4 Azonnali üzenetküldés ... *63*
5.1.2.5 Tűzfalak ... *64*
5.1.3 Adatvédelmi megfontolások ... *65*
5.1.3.1 Védelem böngészés közben ... *67*

5.1.3.1.1 A látogatott oldalak biztonsága *68*
5.1.3.1.2 Aktív tartalmak és a biztonság *71*
5.1.3.1.3 A böngészőben tárolt adatok biztonsága *73*
5.1.3.2 Bizalmasság védelme a közösségi oldalakon *75*
5.1.4 Az adatok végleges törlése *77*
5.2 A sértetlenségről *78*
5.2.1 Digitális aláírás *79*
5.2.2 Kivonatok *82*
5.3 A rendelkezésre állás megteremtése *83*
5.3.1 Fájlok biztonsági mentése *84*
5.3.2 Védelem az áramellátás hibái ellen *87*
5.3.3 Vírusvédelem *88*
6. Mellékletek *89*
6.1 Ajánlott irodalom *89*
6.2 Internetes hivatkozások jegyzéke *91*
6.3 Fogalomtár *94*

Ábrák jegyzéke

1. ábra: Biztonsági koncepció *19*
2. ábra: Felhő-alapú szolgáltatások *26*
3. ábra: A TCP/IP és az ISO OSI összehasonlítása *34*
4. ábra: Sérülékenységek száma 2006-2012 között *42*
5. ábra: Hozzáférések megadása Windows operációs rendszerben *47*
6. ábra: USB-lemez titkosítása Windows TrueCrypt programmal *49*
7. ábra: USB-lemez titkosítása Linuxon *49*
8. ábra: Titkosítási jelszó beállítása szövegszerkesztőben – MS Word *50*
9. ábra: Olvasási jelszó beállítása szövegszerkesztőben - LibreOffice *51*
10. ábra: Jelszó beállítása táblázatkezelőben - LibreOffice *51*
11. ábra: Jelszó beállítása táblázatkezelőben – MS Excel *52*
12. ábra: Jelszó beállítása tömörítés közben - Windows *53*
13. ábra: Jelszó beállítása tömörítés közben - Linux *53*
14. ábra: Védett hálózati csatlakozások jelölése *55*
15. ábra: Bejelentkezés VPN hálózatba *56*
16. ábra: A 10.000 leggyakoribb jelszó weboldala *58*
17. ábra: WiFi titkosítási beállítások *59*
18. ábra: MAC szűrés beállítása WiFi eszközön *60*
19. ábra: Példa nyílt WiFi rendszer beállításaira *61*
20. ábra: Uniform Resource Locator - URL *69*
21. ábra: McAfee SiteAdvisor – a megbízható weboldalakért *70*
22. ábra: Captcha *71*
23. ábra: Böngészési adatok törlése Firefoxban *74*
24. ábra: Adatvédelmi beállítások közösségi oldalon *76*
25. ábra: Végleges adattörlés szoftveresen *78*
26. ábra: Windows Backup *85*
27. ábra: Adatok mentése Linuxon *86*
28. ábra: Szünetmentes otthoni áramellátó eszköz *87*

Táblázatok jegyzéke

1. táblázat: Környezetvédelem az e-Kormányzati Akciótervben *31*
2. táblázat: Támadások és támadási szintek *43*

A vírusok tönkretehetik vállalkozását. Mi megállítjuk a vírusokat.

Bemutatjuk a Symantec Endpoint Protection Small Business Edition 2013-at

Egy vírus néhány perc alatt képes tönkretenni vállalatát. Mi pontosan ilyen gyorsan nyújtunk védelmet az Ön számára. A Symantec Endpoint Protection Small Business Edition 2013 egyszerű, gyors és hatékony megoldás, amely védelmet nyújt a vírusokkal és a kártékony programokkal szemben, és mindössze néhány perc alatt üzembe helyezhető. Az üzembe állításhoz nincs szükség további hardver telepítésére, speciális informatikai személyzetre vagy előképzettségre.

- Egyszerű, gyors és hatékony
- Percek alatt telepíthető
- Bármikor, további költségek nélkül áttérhet a felhőalapú változatra

Tesztelje ingyenesen! Látogasson el a **go.symantec.com/stopthreats** oldalra, és töltse le a 30 napos ingyenes próbaverziót!

Symantec™

1. Bevezetés

Ez az új biztonságspecifikus modul az otthoni és a munkahelyi felhasználók számára jött létre, nem feltétlenül az IT szakemberek lettek megcélozva ezáltal. A modul elsajátítása képessé teszi a jelentős időt online eltöltő, vagy a munkához szükséges tanfolyamokat számítógépen végző illetve otthoni számítógép-felhasználókat arra, hogy megvédjék magukat és adataikat számos csalárd rosszindulatú tevékenységtől. Ezt a modult egyaránt hasznosnak véljük egyéni felhasználóknak, munkaadóknak és pedagógusoknak. Azonban hangsúlyozni kell, hogy az informatikai biztonság ugyanolyan külön szakma, mint a rendszergazdai vagy alkalmazás-fejlesztői, ezért ez a jegyzet arra nem vállalkozhat, hogy megtanítja ezt a kétségkívül nagyon szép és igen nehéz szakmát. Mindazonáltal sokkal közelebb lesz a biztonságos állapothoz az, aki alkalmazza az ebben a jegyzetben leírtakat, mint az, aki nem tud ezekről a jelenségekről, trendekről, védelmi mechanizmusokról.

Az internetes támadások száma és súlya megnövekedett az utóbbi időben. A támadók különösen nagy előszeretettel használják fel az otthoni, gyengén védett számítógépeket a támadásaik kivitelezésére. Ebben segíti őket egyrészről az, hogy a felhasználók által jellemzően használt szoftvertermékekhez a támadók is könnyen hozzáférnek, másrészről az, hogy az informatikai biztonság még nem épült be a képzési rendszerbe. A biztonság így csak korlátozottan van jelen a mindennapjainkban és az sem biztos, hogy amit tudunk, az hiteles forrásból származik. Egyetlen egy otthoni számítógép megszerzése talán nem okoz nagy problémát – gondolnánk – de néhány millió vagy tízmillió számítógép feletti irányítás megszerzése már jelentős számítási kapacitáshoz juttatja a támadókat. Ezek ellen ma már minden számítógép-felhasználónak szükséges védekeznie, ezért a modul tematikájában az informatikai jártasságot – az alapszintű digitális írástudást – magától értetődőnek tekintettük. Szeretnénk eloszlatni a félreértést: a támadónak nem „X.Y” számítógépére van általában szüksége, hanem „millió gépre, köztük X.Y. számítógépére is”.

A modulban szereplő készségek és ismeretek halmaza nagyon fontos a jelenlegi technológiai helyzetben, mivel ma már egyre többen használják a számítógépeket kommunikálásra, információk megosztására és termékek és szolgáltatások online megvásárlására. Ennek következtében a kiberbűnözés egyre szélesebb körben terjed, és a támadási módszerek, mint például az adathalászat, levélszemét-küldés és a biztonsági intézkedések megkerülése kifinomultabbá válnak. Az új technoló-

giák megkönnyítik a támadók számára a kifinomult támadások végrehajtását viszonylag alacsony költség és erőforrás-felhasználás mellett, emiatt a megtámadottak köre egyre szélesebb lesz. A megtámadottak pedig egyre több időt töltenek majd el a támadások következményeinek felszámolásával, ahelyett hogy a feladataikat végeznék.

Az ECDL/ICDL IT Biztonság jegyzet elsajátításával az érdeklődők képesek lesznek:

- általános fogalmak ismeretére, ezen belül
  - *megérteni és azonosítani a napi szintű infokommunikációs eszközhasználat alapjául szolgáló legfontosabb fogalmakat,*
  - *megérteni az információk és adatok védelmének fontosságára, a fizikai biztonságra, személyes adatok védelmére és eltulajdonításának megakadályozására vonatkozó kulcsfogalmakat,*
  - *megérteni a hálózati típusokat, a kapcsolatok formáit és a hálózat-specifikus témákat, beleértve a tűzfalakat,*
  - *megérteni az e-mailekre és azonnali üzenetküldőkre vonatkozó biztonsági kérdéseket;*

- biztonságos tevékenységek végzésére, ideértve
  - *biztonságosan és megbízhatóan használni az internetet,*
  - *megfelelően kezelni az adatokat és az információkat,*
  - *megvédeni a számítógépet, eszközöket vagy hálózatot a rosszindulatú programoktól és jogosulatlan hozzáférésektől,*
  - *biztonságosan böngészni a World Wide Web-en és biztonságosan kommunikálni az interneten;*

- biztonságot segítő (biztosító) eszközök alkalmazására, felhasználására, különösen
  - *megfelelő technikákat és alkalmazásokat használni a biztonságos hálózati kapcsolat fenntartására,*
  - *biztonságosan és megfelelően menteni, visszaállítani és törölni az adatokat, valamint biztonságosan selejtezni azt eszközöket.*

Különösen fontosak ezek a készségek abban a világban, mely törvényt is alkotott az információbiztonságról. Így az információbiztonság többé már nem egyéni probléma, hanem társadalmi igény. Kívánunk biztonságos és folyamatos internetezést, számítógépes munkát, szolgáltatások igénybe vételét és otthoni felhasználást az új évezredben, a biztonságigényes digitális világban.

Budapest, 2013. szeptember 6.

Alföldi István, *CGEIT*
ügyvezető igazgató
NJSZT

Erdősi Péter Máté, *CISA*

2. Biztonsági alapfogalmak

2.1 Kibertér

Miért jelentkezik ma már társadalmi szinten az információbiztonsági igény? A mai társadalmi rendszerek – ideértve a gazdaságban, a kormányzatban, önkormányzatban, tudományban és otthon működő rendszereket egyaránt – függenek az információtechnológiától, és ez a függés az egyes rendszerek összekapcsolódásával, a **kibertér** (cyberspace) létrejöttével világméretűvé vált. Nem hagyható ki a kibertér fogalmából a kutatási, felsőoktatási és közgyűjteményi rendszer (NIIF: Nemzeti Információs Infrastruktúra Fejlesztési Program) sem, a kormányzati, nemzetvédelmi és üzleti szempontok mellett, hiszen jelentős feladatokat töltenek be a társadalomban és az innovációban. A kibertér fogalmának meghatározásához hívjuk segítségül a 2003 februárjában kiadott Amerikai Nemzeti Kibertér-védelmi Stratégia *[1]*[1] bevezető sorait:

> *„Az üzleti folyamatoknak, a kormányzat működtetésének és a nemzetvédelemnek a módja végérvényesen megváltozott. Ezek a tevékenységek ma már információtechnológiai infrastruktúrák összefüggő hálózatától függenek, amit kibertérnek hívnak. A Nemzeti Kibertér-védelmi Stratégia ennek az infrastruktúrának a védelmére nyújt egy keretet, ami létfontosságú az amerikai gazdaság, biztonság és életmód fenntartásához.*
>
> *...*
>
> *A kibertér védelme különösen nehéz stratégiai kihívás, mely összehangolt és fókuszált erőfeszítéseket követel meg az egész társadalomtól – a szövetségi kormányzattól, állami és helyi kormányzatoktól, a magánszektortól és az Amerikai néptől egyaránt."*

Magyarország is felismerte a kibertér fontosságát, ezért megjelent a Magyarország Nemzeti Kiberbiztonsági Stratégiája is, az 1139/2013. (III. 21.) Kormányhatározat *[2]* formájában.

1 *A továbbiakban az irodalomjegyzékre történő hivatkozásokat szögletes zárójelek között adjuk meg (pl. [1], [a])*

„A stratégia összhangban az 1035/2012. (II. 21.) Korm. határozattal elfogadott Magyarország Nemzeti Biztonsági Stratégiájával, abból kiindulva kifejti annak a kiberbiztonságról szóló 31. pontjában meghatározott törekvéseket és megfogalmazott kormányzati felelősséget. Gyökereiben a 2001-ben elfogadott Budapesti Konvencióig nyúlik vissza („Convention on Cybercrime"), mely nemzetközi egyezmény napjainkban is referenciaként használt, nemzetközileg elfogadott alapelveket fogalmaz meg. A stratégia egyben igazodik az Európai Parlament által 2012. november 22-én elfogadott,„A kiber-biztonságról és védelemről szóló", 2012/2096(INI) számú határozatában a tagállamok felé megfogalmazott ajánlásokhoz, valamint az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én „Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" címmel közzétett közös közleményhez. A stratégia illeszkedik továbbá a NATO 2010 novemberében elfogadott Stratégiai Koncepciójához, a Szövetség 2011 júniusában elfogadott Kibervédelmi Politikájához és ennek végrehajtási tervéhez, valamint a 2010. november 19–20-ai lisszaboni és a 2012. május 20–21-ei chicagói NATO-csúcs dokumentumaiban megfogalmazott Szövetségi kibervédelmi elvekhez és célokhoz."

A stratégia a kibertér fogalmát hasonló módon definiálta, mint az amerikai stratégiai dokumentum:

„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."

Az Infotörvény *[15]* globális kibertér alatt a következőt érti:

> *„Globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese”*

Vegyük észre, hogy a kibertér fel lett a fentiek által osztva folyamatokra, infrastruktúrákra és adatokra-információkra. Ez azért lényeges, mert a kibertérben sokszor előfordul olyan eset, amikor az adott országban csak a kibertéren keresztül érkező adat jelenik meg, és az adatot szolgáltató szervezet semmilyen eszközt nem birtokol, tárol vagy üzemeltet az adott ország földrajzi területén, így ezekre ráhatást nehezen tud tenni az információt megjelenítő ország hatósága.

2.2 Biztonság

Az élet számos területén sokszor használjuk azt a fogalmat, hogy „**biztonság**” (security). 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 elvétve 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** (threat) 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. A biztonság iránti szabályozási igényt jól jelzi a 2013. évi L. törvény, az állami és önkormányzati szervek elektronikus információbiztonságáról (Infotörvény). A törvény a biztonságot az elektronikus információs rendszerek aspektusából közelíti meg. Nagyon fontos elem, hogy a törvény alkalmazásában **elektronikus információs rendszer** az adatok, információk kezelésére használt **eszközök** (környezeti infrastruktúra, hardver, hálózat és adathordozók), **eljárások** (szabályozás, szoftver és kapcsolódó folyamatok), valamint

az ezeket kezelő **személyek** együttese. A fogalmakhoz ezen kívül felhasználtuk egy módszertani alapokon nyugvó informatikai biztonsági rendszertan *[am]* egyes elemeit is. A rendszertan szerint a biztonság olyan kedvező állapotot jelöl, amelyben „*zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg*".

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

1. **bizalmasság** (confidentiality): röviden annyit jelent, hogy valamit csak az arra jogosultak ismerhetnek meg, korlátozott a megismerése jogosultak köre; vagy ahogyan az Infotörvény fogalmazza meg – az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

2. **sértetlenség, vagy integritás** (integrity): röviden úgy mondanánk, hogy valami az eredeti állapotának megfelel és teljes. Az Infotörvény értelmezésében az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

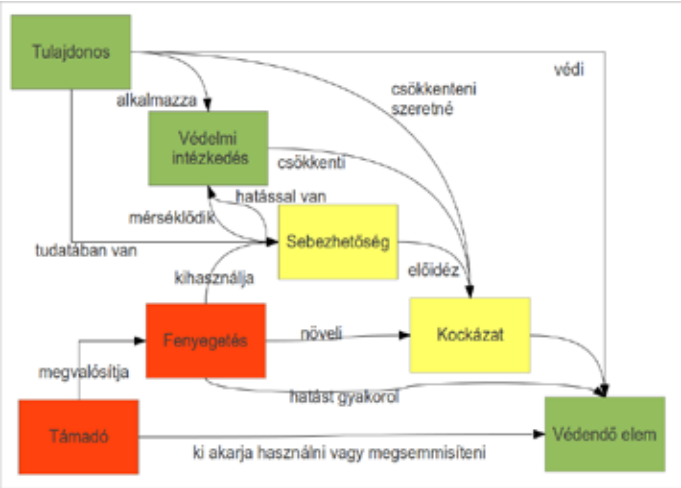
3. **rendelkezésre állás** (availability): lényegében annyit jelent, hogy a szükséges infrastruktúrák valamint adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van, vagy ahogyan az Infotörvény fogalmazza meg, annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

A védelem feladata tehát a védendő elemek biztonságát megteremteni, ami más szóval annyit tesz, hogy a hardverek, szoftverek, eljárások, szabályzatok stb. bizalmasságát, sértetlenségét és rendelkezésre állását kell biztosítani. A védelem feladatai ezzel kapcsolatosan sokrétűek lehetnek, ideértve a megelőzést és korai figyelmeztetést, észlelést, reagálást, valamint incidens- vagy krízismenedzsmentet egyaránt.

Az információbiztonságot és az informatikai biztonságot – néha még a szakemberek is – gyakran összekeverik egymással, sőt időnként az adatvédelemmel, a személyes adatok védelmével is. Az adatvédelem kifejezés – érdekes módon az angol nyelvben (data protection) is kizárólag a személyes adatok védelmére van fenntartva, a személyiségi jogokkal összefüggő tevékenység. Az **információbiztonság** és az **informatikai biztonság** különbözik egymástól. Az információbiztonság értelmezésünkben a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Ez alapján az informatikai biztonság „csak" az informatikai rendszerekben kezelt adatok, és az azt kezelő rendszer védelmét jelenti. Mivel angolul általában az információvédelemre, illetve az informatikai védelemre, sőt néha a kommunikációs, információs és más elektronikus rendszerek védelmére is az „information security" kifejezést használják, az egyes fordítások még inkább zavarossá teszik a képet. Általában a szövegkörnyezet teszi egyértelművé, hogy információvédelemről vagy informatikai védelemről van-e ott szó.

2.3 Koncepcionális megközelítés

A biztonságra vonatkozóan számos szabvány és ajánlás létezik. Ilyenek például informatikai rendszerekre vonatkozóan az ISO 27000 szabványcsaládba tartozó szabványok és a NIST SP 800-53 szabvány is. A Common Criteria *[3]*, melyet az informatika eszközök, termékek biztonsági értékelésére dolgoztak ki – és amely ISO 15408 szabványként is ismert, **a biztonság koncepcióját** (security concept) a 2.3 verziójában fogalmazta meg a rendszerek tulajdonságait is figyelembe véve a maga teljességében a koncepciót bemutató ábráján. 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 felhasznált fogalmak definícióit a következőkben adjuk meg *[4]* felhasználásával:

- **Védelmi intézkedés** (security countermeasure, control): a fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési vagy technikai eszközökkel alkalmazott intézkedés.

- **Sebezhetőség vagy sérülékenység** (vulnerability): 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** (attack): A támadás egy az erőforrások bizalmassága, sértetlensége és/vagy rendelkezésre állása ellen, egy sérülékenységből kiinduló, egy fenyegetést megvalósító folyamat.

- **Fenyegetés** (threat): A fenyegetés a támadás lehetősége, vagy a biztonság megsértésének lehetősége, a támadás tárgyát képező erőforrásra.

- **Kockázat** (risk): A kockázat annak a lehetőségnek a valószínűsége, hogy egy fenyegetés támadás útján kárkövetkezményeket okoz.

Védendő elemek (assets): a szervezet vezetősége (menedzserei) által a küldetést megvalósító, illetve az informatikai feladatok végrehajtásához rendelt emberek, eszközök (eljárások, technológia és adatok).

Az ábrából a következő koncepcionális állítások olvashatók ezek után ki:

1. A támadó rosszindulatú tevékenységeket akar végezni a védendő elemeken.

2. A tulajdonos meg akarja védeni a védendő elemeit.

3. A tulajdonos tisztában van a sérülékenységekkel, ezért védelmi intézkedéseket alkalmaz.

4. A védelmi intézkedések csökkentik a kockázatokat.

5. A sérülékenységek idézik elő a kockázatokat.

6. A védelmi intézkedések hatnak a sérülékenységekre, mérséklik azok hatását a védendő elemekre nézve.

7. A támadó esélyt ad a fenyegetések bekövetkezésének, ami növeli a kockázatot.

8. A fenyegetések a sérülékenységeket használják ki.

A támadások működési mechanizmusa tehát az, hogy a támadó megkeresi a védeni kívánt informatikai rendszer sebezhető pontjait – sérülékenységeit, amelyeken keresztül támadásokat próbál meg realizálni. A tulajdonos a **biztonsági kockázatok**at (security risks) védelmi intézkedésekkel csökkenti, melyek lefedik a sérülékenysé-

gek (vulnerabilities) által jelentett gyengeségeket. A biztonság innentől kezdve mérhető, mégpedig a sikeres támadások számával, valamint a kárkövetkezmények és a védelemre fordított erőforrások számszerűsítésével.

2.4 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 információval kapcsolatos alapvető fogalmakat *[6]* az adatokban, a tudásban, tapasztalatban és bölcsességben látja. 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 Infotörvény *[15]* különbséget tesz adat és információ között is, az alábbi módon:

- **adat** (data): az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas

- **információ** (information): bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.

Ezzel kapcsolatosan megemlítjük, hogy a 2000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről az I. függelék a) pontjában szintén megadja az információ meghatározását, mely szerint az információ olyan ismeretanyagot jelent, amelyet bármilyen formában továbbítani lehet.

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 **információkritériumok** 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, változatlanságára 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 az első négy kritérium, a biztonságra pedig az utolsó három követelmény vonatkozik. Minden információbiztonsági törekvés arra irányul, hogy a három biztonsági követelménynek való megfelelőséget minden időpillanatban biztosítsák az összes védendő információra és környezetükre egyaránt.

Könnyen belátható, hogy azzal az információval, amelyik magasabb szinten felel meg a fenti kritériumoknak, hatékonyabb, összetettebb rendszerek működtethetők gyorsabban, pontosabban, kevesebb erőforrás felhasználásával – közismert példaként említjük a lottószelvények feldolgozási folyamatát ma és 1763-ban, amikor az első 5/90 lottójátékokat Budán és Pozsonyban megtartották.

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 előállításhoz 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 rendszereken** *[α]* 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 Hardver

Anélkül, hogy az infokommunikációs technológiai alapismeretek modul anyagát ismertetnénk, meg kell ismételnünk 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 **számítógép**eket, 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

A hardveres egységek összeszerelésüket követően még nem képesek szofisztikált felhasználói utasításokat végrehajtani, ezeket teszik majd lehetővé a különböző programok, szoftverek, alkalmazások. Anélkül, hogy mély technikai részletekbe mennénk, megemlítjük, hogy a hardverek működtetéséhez az úgynevezett meghajtók, vezérlő-programok – driverek – szolgálnak. A számítógép-architektúra teljes funkcionalitásának kihasználását az operációs rendszer teszi lehetővé, míg a felhasználók által igényelt egyes funkciókat megvalósító **alkalmazások**at 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 szövegként képes tárolni, illetve elvégzi a mások által rögzített szövegek megjelenítését is.

3.3 Szolgáltatások

A kibertér és a virtualizáció fejlődésével megszületett az igény, hogy a felhasználók ne csak a saját gépeiken legyenek képesek szoftvereket, egyedi alkalmazásokat futtatni, hanem legyen lehetőségük a különböző alkalmazásokat távolban, a **felhőben** futtatni és csak az adatokat mozgatni a helyi és a távoli számítógépek között, vagyis mindez **szolgáltatásként** jelenjen meg a felhasználó számára. 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 üzenet-küldés) szolgáltatásokat felhasználni (pl. Skype, Gmail) vagy közösségi oldalakon információkat, fájlokat megosztani és megkapni (pl. Facebook, Iwiw, Twitter stb.). A **fájl-megosztás** saját gépről is történhet.

Ez a biztonsági környezetet is jelentős mértékben megváltoztatta.

3.3.1 Ismeretszerzés és kapcsolatteremtés interneten

Az otthoni internetezés védelme egyre fontosabbá lesz tanulmányi szempontból is, hiszen már 2010-ben a diákok az interneten töltött idejüknek majdnem az ötödét (19%) töltötték tanulással és 43%-ot kommunikálással – érdekes, hogy a játék csupán 18% időt foglalt el a felmérés szerint *[c]*. Megfordítva a dolgot, a számítógép és az internet elérhetetlensége a tanulást és a kommunikációt nehezíti meg a diákok számára. A felmérés alapján a legnépszerűbb 16 weboldal az alábbi volt (alfabetikus sorrendben):

• Blogger	• Startlap játékok
• Facebook	• Sulinet Digitális Tudástár
• Farmville	• Teamspeak
• Honfoglaló	• The Sims3
• Index.hu	• Travian
• Origo angol-magyar szótár	• Wikipedia
• SecondLife	• World of Warcraft
• Skype	• YouTube

Nem lehet kihagyni a tájékozódást (pl. időjárás, menetrend, stb.), a távtanulást segítő rendszereket és az oktatási intézmények interaktív rendszereit sem (pl. e-napló, NEPTUN, tananyag közzététele, feladatbeadás, stb.) ebből a felsorolásból.

3.3.2 Elektronikus ügyintézés

3.3.2.1 e-Europe

Az Európai Tanács felkérésére az Európai Bizottság 1999-ben kidolgozott egy akciótervet, mely azt a célt szolgálta, hogy Európa mielőbb kiaknázhassa az új gazdaság, illetve az internet adta lehetőségeket.

Ezt e-Europe névvel illették és a következő területeken (klaszter) tartalmazott végrehajtandó tevékenységeket:

1. Olcsóbb, gyorsabb és biztonságosabb internet
   a. Olcsóbb és gyorsabb internet hozzáférés
   b. Gyors internet a kutatóknak és diákoknak
   c. Biztonságos hálózatok és intelligens kártyák
2. Befektetés az emberekbe és az ismeretekbe
   a. Az európai ifjúság beléptetése a digitális korszakba
   b. Munka a tudás-alapú gazdaságban
   c. Mindenki részvétele a tudás-alapú gazdaságban
3. Az internet használatának ösztönzése
   a. Az e-kereskedelem elősegítése
   b. Elektronikus közigazgatás: elektronikus hozzáféré a közszolgáltatásokhoz
   c. Távegészségügy
   d. Digitális tartalom a globális hálózatoknak
   e. Intelligens közlekedési rendszerek

A tervet időről-időre felülvizsgálják és a következő időszakra mindig olyan tevékenységeket adnak meg, mely a korábbi tapasztalatokra épül.

Magyarországon az egykapus ügyintézési felületet a *https://magyarorszag.hu [e]* 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).

3.3.2.2 Hiteles e-ügyintézés

Az Európai e-Kormányzati Akcióterv 2011-2015 dokumentum *[8]* kimondja, hogy a cselekvési terv célja annak elérése, hogy a nemzeti és uniós politikai intézkedések a lehető legnagyobb mértékben kiegészítsék egymást. További célja a hagyományos e-kormányzatról való átállás támogatása olyan új, nyílt, rugalmas és együttműködésen alapuló akadálymentes e-kormányzati szolgáltatásokra, amelyek helyi, regionális, nemzeti és európai szinten segítenek bevonni a lakosságot és a vállalkozásokat a politika alakításába.

Az e-kormányzat terén való európai szintű együttműködés szorgalmazását komoly politikai és gazdasági megfontolások indokolják. Az együttes fellépés a közforrások hatékonyabb felhasználása és az állami kiadások csökkentése révén segítséget jelenthet a gazdasági válság leküzdésében. Az e-kormányzati szolgáltatások pedig gazdaságosabban fejleszthetők a köz- és magánforrások összevonásával és koordinációjával. Az akcióterv két kulcsfontosságú célkitűzés elérésével foglalkozik (melyeket a Digital Agenda for Europe – Digitális Európai Menetrend - dokumentumban fogalmaztak meg):

1. 1. Számos olyan határon átnyúló kulcsfontosságú szolgáltatás legyen elérhető 2015-re, mely lehetővé teszi a vállalkozóknak, hogy Európában bárhol vállalkozhassanak a származási helyüktől függetlenül, továbbá lehetővé teszi a polgárok számára a tanulást, munkavállalást, letelepedést és nyugdíjba vonulást bárhol az Európai Unió területén.

2. 2. Az eKormányzati szolgáltatásokat kezdje el használni az EU polgárainak legalább a fele (50%).

Mivel az e-kormányzati szolgáltatások a vállalkozások számára is nagy jelentőséggel bírnak, a cselekvési tervben a fenti célkitűzés kiegészítették azzal, hogy 2015-ig a vállalkozások 80%-a vegyen igénybe e-kormányzati szolgáltatásokat.

A teljesen elektronikus szolgáltatások használata nem nélkülözheti az elektronikus azonosíthatóságot (eID) és az elektronikus hitelességet a teljes bizonyító erő és az írásbeliség fenntartásához. Az előnyökre jól rávilágít az a felmérés *[d]*, mely szerint a válaszolók 97,5%-a gondolja úgy, hogy a teljesen elektronikus ügyintézés lecsökkenti az ügyek intézésének az ügyfelektől megkövetelt időtartamát, valamint 85% azt is gondolja, hogy az ügyintézés költségei (utazás, sorban állás, munkahelyről való elszabadulás stb.) csökkennének, ha teljesen elektronikusan lehetne az ügyeiket elintézni.

Jó hazai példa a cégeljárással kapcsolatos ügyek teljes elektronikus útra terelése, melyet követően a cégbejegyzéshez szükséges iratokat, dokumentumokat a céges eljárásban közreműködő ügyvédek kizárólag elektronikus úton küldhetik be a cégbíróságokhoz és a költségtérítés megfizetése is kizárólag elektronikus formában történhet. Továbbá a közjegyzők ma már munkájuk egy részét kizárólag teljesen elektronikus formában, minősített digitális aláírás és időbélyeg használatával végezhetik csak el.

3.3.2.3 Környezet kímélése

Első ránézésre nem információbiztonsági kérdés a környezetvédelem, de ha az infrastruktúra elektromos rendszerektől való függőségét, az energia-függőséget vagy a szélsőséges időjárási események következtében fellépő fizikai veszélyeket is számításba vesszük, akkor nem hátrány figyelembe venni az információtechnológia alkalmazhatóságát ilyen célból sem.

Csak megemlítjük, hogy az Európai e-Kormányzati Akcióterv 2011-2015 dokumentum tartalmaz ilyen irányú felvetéseket is, mégpedig:

> *„Az alábbiakban javasolt intézkedéstervezet célként tűzi ki a tagállami közigazgatások tevékenységéhez kapcsolódó szén-dioxid-kibocsátás csökkentését, melynek eszköze lehet például az elektronikus archiválás bevezetése, a hivatalos utak videokonferenciákkal történő helyettesítése stb.”*

Ennek érdekében az Akcióterv a következő két feladatot fogalmazta meg:

Határidő	Tevékenység
2012	A Bizottság tanulmányt készít az e-kormányzat kibocsátáscsökkentő potenciáljáról és az ehhez kapcsolódó bevált gyakorlatokról.
2013	A tagállamok mutatókat és értékelési eljárásokat határoznak meg és fogadnak el annak mérésére, hogy kormányzataik szén-dioxid-kibocsátása milyen mértékben csökkent az e-kormányzati szolgáltatások bevezetése nyomán.

1. táblázat: Környezetvédelem az e-Kormányzati Akciótervben

3.4 Hálózati elemek

A **hálózat modellezéséhez** a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization) OSI (Open System Interconnection, Nyílt Rendszerek Összekapcsolása) ajánlását használjuk fel *[9]*, mely kiválóan alkalmas minden hálózati forgalom modellezésére.

Az OSI modell **hét réteget** tartalmaz, melyek a fizikai átvitelt biztosító közegtől a felhasználó által látott felület felé rendben az alábbiak:

1. **fizikai réteg**: melynek az a feladata, hogy a biteket mechanikai és elektromos eljárásokkal továbbítsa a kommunikációs csatornán, és ha a küldő 1-et küldött, akkor a fogadó is 1-et lásson, hasonlóképpen ha 0 lett elküldve, akkor 0 is érkezzen meg.

2. **adatkapcsolati réteg**: az a feladata, hogy a fizikai réteg szolgáltatásait felhasználva a felette levő rétegnek hibamentes átvitelt biztosítson, az adatforgalom keretekre tördelésével.

3. **hálózati réteg**: feladata az egyes adatcsomagok eljuttatása a forrásállomástól a célállomásig, beleértve az útvonal megkeresését és meghatározását.

4. **szállítási réteg**: feladata a viszony rétegtől kapott adatokat feldarabolni a hálózati réteg számára küldhető csomagokká és viszont, biztosítani, hogy a hálózaton keresztül megkapott csomagokat értelmezhető formában állítsa elő a viszony rétegnek további feldolgozásra.

5. **viszony réteg**: feladata a felhasználók között számítógépes viszonyok (session) létrehozása. Ennek segítségével lehet például belépni egy távoli rendszerbe vagy fájlokat mozgatni távoli gépek között.

6. **megjelenítési réteg**: feladata az adatok szabványos módon történő kódolása annak érdekében, hogy az adatokat eltérő módon kódoló számítógépek is tudjanak egymással kommunikálni.

7. **alkalmazási réteg**: a széles körben használt protokollok egységes, standardizált szintje. Ezt használják különböző fizikai terminálokhoz illetve különböző fájlrendszerek közötti fájlátvitel esetében, ideértve az elektronikus levelezést, távoli bejelentkezést, könyvtárakban való keresést is.

A tényleges hálózati kommunikációt megvalósító elemek működése a fenti hét réteg segítségével modellezhető. A hálózati kommunikáció minden rétegben támadható, ezért minden rétegben el kell gondolkodni a védelmen is.

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

1. **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.

2. **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

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

Az internetes kommunikáció során először egy lokális (otthoni, munkahelyi, hivatali, iskolai, nyilvános) hálózathoz csatlakozik a felhasználó egy alkalmazás segítségével, ahol a hálózaton keresztül éri el a távol lévő szolgáltatásokat, leggyakrabban **TCP/IP** (Transmission Control Protocol / Internet Protocol) protokollt használva. A TCP/IP egy olyan réteges hálózati modell amely a világméretű hálózat, az INTERNET alapjául szolgál. Négy rétegből áll: alkalmazási, transzport (TCP/UDP), hálózati (internet, IP) és hálózati elérési (network interface) – ezek mindegyike megfeleltethető az OSI modell alkalmazási, szállítási, hálózati, valamint adatkapcsolati és fizikai rétegének (ahogyan azt a 3. ábra mutatja). A rétegek működését legjobban úgy szemléltethetjük, hogy az alkalmazás a felhasználó által elküldeni kívánt adatot odaadja továbbításra az alatta levő rétegnek, aki azt szintén becsomagolja, a saját nyelvére „lefordítja" és megint továbbadja a soron következő rétegnek, míg el nem érkezünk a hálózati réteghez. Hálózati szinten már csak a fizikai közegen átvinni kívánt elektromos jeleket kell továbbítani. Ezt az internet, vagyis az internetnek a küldő és a fogadó között elhelyezkedő **hálózati eszközök** eljuttatják a fogadó oldalra, ahol az ottani hálózat visszafordítja a kapott jeleket adattá, a lenti rétegektől felfelé, egészen az alkalmazásig. Esetenként a hálózati csatoló késedelemmel küldi ki az adatot a fizikai közegre, ami **hálózati csatlakozási késedelmet** okozhat ugyan, de a felhasználó számára csak rosszul beállított rendszerek esetében lesz látható. A mobil eszközök fejlődésével a hálózati csatlakozást ma már nem kizárólag asztali számítógéppel lehetséges megvalósítani, hanem minden olyan eszközzel, mely rendelkezik hálózati csatoló kártyával (NIC: Network Interface Card). Ezek a csatolókártyák lehetnek külön elemek és beépülő áramkörök is az egyes eszközökben.

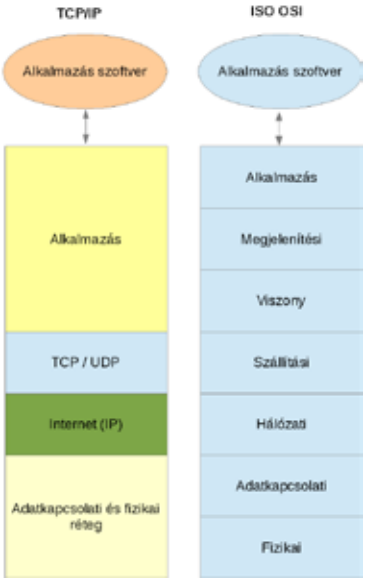
Mindkét esetben közös tulajdonságuk, hogy a fizikai átviteli közeghez, vagyis a fizikai réteghez való hozzáférést biztosítják. Egy számítógépnek több interfésze is lehet (jellemzően vezetékes és vezeték nélküli). Minden NIC a gyártó által biztosított egyedi címmel rendelkezik, ez a MAC-address.

A felhasználó hálózati csatlakozása egyrészről az ISO OSI 2. réteg szintjén a **Média Hozzáférési Kontroll** (**MAC**, Media Access Control) címmel történik, másrészről a hálózati kapcsolatot az ISO OSI 3. réteg szintjén az internet-protokoll címe (IP cím) azonosítja, mely révén a hálózati csomagok egyrészről eljutnak a lokális eszköztől (forrás) egy távoli helyre (cél), majd ez teszi lehetővé azt, hogy a

válasz onnan vissza is érkezzen a küldő IP címére.

A támadók az internetes protokollok tulajdonságait maximálisan ismerik és a gyengeségeit is képesek kihasználni. Például a címek hamisításával el tudják azt érni, hogy a címeken alapuló védelem hatástalan marad, hiszen a hamis címet hiába tiltja a megtámadott, ha a rejtett valódi címről a támadás tovább folytatódik. A helyes védelem kiválasztásához tehát a védelemnek is elengedhetetlen a hálózat áttekintő, modell-szintű ismerete.

A TCPI/IP protokoll összehasonlítását az OSI rétegeivel az alábbi ábra *[t]* segítségével lehetséges megtenni, így vethetjük össze a **hálózat** elméleti modelljét (jobb oldal) a gyakorlati implementációval (baloldal):



3. ábra: A TCP/IP és az ISO OSI összehasonlítása

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 **erőforrás**ok közé a hardver és a szoftver mellé minden keretrendszerben, szabványban. Védeni kell tehát a hardver és a szoftver mellett a fontosnak ítélt információkat is.

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

1. **rombolás**: károkozás a megtámadottnak, a működési folyamataihoz szükséges erőforrások sérülésének előidézésével (beleértve az információt is)

2. **haszonszerzés**: az erőforrások eltulajdonításával saját szakállukra megszerezni azt a hasznot, ami a más erőforrásai illegális felhasználásával elérhető (információ-lopás, zombi hálózat, stb.). Ennek minősített esete a **személyazonosság-lopás**, amikor a haszon a támadóé, a büntetés a megtámadotté – hacsak nem tudja ártatlanságát bizonyítani.

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** (**viruses**): olyan programok, amelyek más fájlokhoz kapcsolódva önmaguktól terjednek, vagy e-maileken keresztül küldik őket, és károkat okozhatnak a számítógépeken

- **férgek** (**worms**): a vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá illetve válnak részeivé, addig a férgek önállóan fejtik ki működésüket.

- **trójaik** (**trojans**): nevüket az ókori Trója ostrománál alkalmazott hadicsel eszközéről kapták, amely révén egy legálisnak látszó letöltésben egy olyan program bújik meg, ami előbb-utóbb aktivizálódik incidenseket okozva (például hátsó kapukat tölt le vagy rosszindulatú programokat indít el).

- **hátsó kapuk** (**backdoors**): szoftverekbe épített olyan kiegészítések, amelyek bizonyos kiválasztott személyek részére hozzáférést engednek az egyes programokhoz, a számítógéphez, vagy az azokon kezelt adatokhoz. A hátsó kapuk egy részét a szoftverek fejlesztői tudatosan, szervizcélokkal építik be, míg kisebb részük programozási hiba következtében teszi lehetővé a hozzáférési szabályok kikerülését a jogosulatlan hozzáférést így megszerző támadóknak. Ezen kívül léteznek kifejezetten hátsó kapuk nyitásának céljával létrehozott támadóprogramok is, amelyeket általában vírusok, illetve kémszoftverek részeként terjesztenek a felhasználó tudta nélkül. Ezek támadási célú használata azért veszélyes, mert minden egyes esetben rosszindulatú programkódok telepítéséhez vezethet. A hátsó kapu a rendszerbiztonság megkerülésével működik, így az egyébként kialakított védelem itt nem fog érvényesülni.

- **rendszerszinten rejtőző programok** (**rootkit**): 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.

- **telefonszám-intervallum modemes tárcsázó** (**diallers**): olyan számítógépes program, mely telefonszámokat hív fel egy előre definiált lista szerint abból a célból, hogy a hívott oldalon található számítógépes modemeket felderítse és megjegyezze egy későbbi támadáshoz.

- **szolgáltatás-megtagadási támadást indító programok** (**Denial of Service**, **DoS**): 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.

- **kémszoftver** (**spyware**): 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** (**ransomware**): 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.

- **kéretlen levelek** (**spam**): A „spam” elnevezést egy amerikai cég (Hormel Foods) konzervhús-készítményének nevéből kölcsönözték (**S**piced **P**orc and H**am**), amely 1937 óta létezik. Az internet világában ez lett az szokásos kifejezés a **tömeges e-mailek** jelölésére. 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.

- **zombi hálózati szoftverek** (**botnet**): az angol kifejezés a „robot" szóból származik és annyit jelent, mint dolgozni. 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 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 **adatlopás**ra is használni, hiszen a felhasználó gépére észrevétlenül feltelepül és ott bármilyen tevékenységet folytathat.

A rosszindulatú programok leggyakrabban az interneten keresztül kerül 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** (**keystroke-logging**): 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** (**spycam**): 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 más érzékeny információk eltulajdonítására, kifigylés közben. Hátránya a személyes jelenlét, illetve a fizikai elhelyezés szüségessége. Egyes esetekben a támadók a számítógépek beépített vagy hozzákapcsolódó webkameráit képesek a felhasználó tudta nélkül

bekapcsolni, rejtett kameraként használni és azokon keresztül adatokat ellopni a felhasználó környezetéből.

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

- **eltérítéses adathalászat** (**pharming**): a támadó a felhasználó egy adott weboldal felé irányuló forgalmát átirányítja a saját weboldalára 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 elterelje a csalási kísérletről. Az különbözteti meg az adathalászattól, hogy itt a támadó az áldozata gépére betörve módosítja annak beállításait.

- **egyklikkes támadások** (**one-click attack**): a támadók azt a bizalmi kapcsolatot használják ki, ami a felhasználó böngészője és a felhasználó által meglátogatott weboldal között fennáll. A támadónak a felhasználó környezetébe kell bejuttatnia a támadó kódot, amit a weboldal a felhasználó hiteles kérésének értelmez és megpróbál általában automatikusan végrehajtani. A támadás akkor sikeres, ha a támadó pontos üzenetet tud küldeni a weboldalnak és nincs olyan biztonsági szűrés bekapcsolva, mely a támadó által – ebben az esetben vakon – elküldött üzenetek hitelességét ellenőrizné.

- **csatolmányokba rejtett rosszindulatú programok letöltetése** (**malware download as attachments**): 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 eltérítéses 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 begépeli 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.

A **kiberbűnözés** szó a kibertéren keresztül, számítógép-használat közben elkövethető jogellenes bűncselekményekre utal. Ilyenek lesznek például az adathalászat és a **bankkártya adat**ok (név, szám, lejárat, cvc) ellopása online.

A **hackerek** olyan személyek, akik jól értenek a technikához, és azért hatolnak be a rendszerekbe, hogy a rendszert magát megértsék, a biztonsági veszélyekre a rendszer üzemeltetőit figyelmeztessék, vagy csupán kedvükre finomhangolják a programokat – ez a **hackelés**. Ha úgy vesszük, a hackerek igen kíváncsi emberek. Amíg csak olyan rendszerekbe hatolnak be, amelyekhez hozzáférési joguk van, addig nincs probléma. Csak akkor számítanak illegális behatolóknak, ha hozzáférési illetőség, engedély nélkül hatolnak be, például egy egyetem fő számítógépébe, hogy megnézzék, hogy is működik az – ez illegális, még jobbító szándékkal is. Azokat a hackereket, akik bizonyos cégek megbízásából megpróbálják kifigyelni a biztonsági hézagokat, „Penetráció-tesztelőknek” vagy „**etikus hackerek**nek”

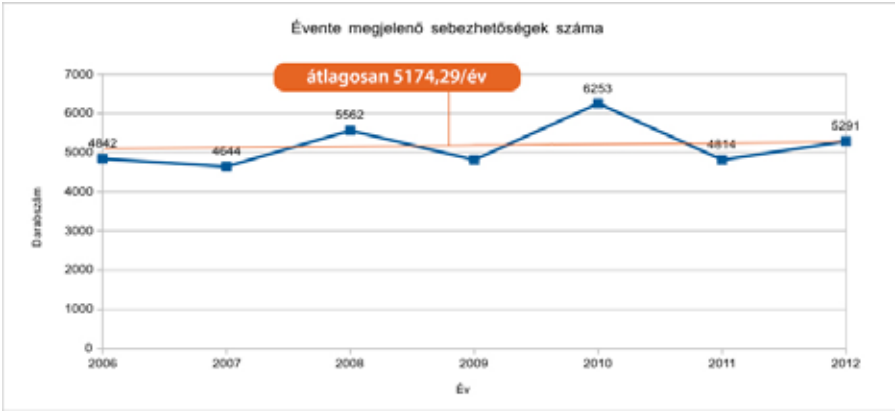
nevezik. Ők legálisan tevékenykednek, hiszen megbízásra cselekszenek, és tartják magukat az előírásokhoz. Azon kívül biztosítva vannak, ha a feltörési kísérlet során károk keletkeznének. Ha ezek a feltételek fennállnak, akkor ezt **etikus hackelés**nek nevezzük.

A rossz szándékú hackereket **crackerek**nek nevezik. Gyakorlatilag ugyanolyan tudásszinttel rendelkeznek, mint a hackerek, de a motivációjuk eltérő. Idegen rendszerekbe hatolnak be károk okozása vagy haszonszerzés céljából. Törlik, megváltoztatják, a védett adatállományokat, programokat, vagy visszaélnek azokkal, ezeket a tevékenységeket **crackelés**nek nevezzük. Ilyen behatolás nyomán milliós nagyságrendű károk is keletkezhetnek.

A "**jelszócrackelés**" jelentése ennek megfelelően tehát jelszó nyílt szöveges verziójának megszerzése. Több módszer is ismeretes erre (nyers erő, szótár, szivárványtáblázat stb.) A nyers erő módszer használja fel a lehetséges jelszavak egymás utáni bevitelét a támadás kivitelezése során – ez kétségkívül lehet jelzője a jelszócrackelésnek, de nem lesz a célja. A jelszócrackernek 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 Btk. szerint ma már ezek számítógépes bűncselekményeknek számítanak. A Symantec minden évben közzéteszi a biztonsági fenyegetésekről szóló riportját *[u]*. A 2013-as kiadásban a következő adatokat találhatjuk a sérülékenységek számának alakulása tekintetében 2006-2012 között:



4. ábra: Sérülékenységek száma 2006-2012 között

Ezeket a számokat elemezve azt kapjuk, hogy az elmúlt hét év során minden egyes nap több mint 14 új sérülékenység jelent meg az informatikában, ami a felhasználók biztonságát kisebb-nagyobb mértékben veszélyeztette. Ez azt jelenti, hogy a biztonság önmagában nem fog hosszú ideig fennállni, a fennmaradásáért folyamatosan tennünk kell.

Annál is inkább, mert a számítógépes bűnözés olykor igen kifizetődőnek tűnhet. Elég csak a levélszemét küldéséből befolyó dollármilliárdokat megemlíteni, vagy az **online emelt díjas tárcsázó program**ok esetét, amikor a felhasználó telefonját megfertőzve egy emelt díjas számot tárcsázó programmal, a támadók osztoztak a hívások költségein. A támadásnak az ad különös érdekességet, hogy itt a támadók nem maguk hajtották be a költségeket, hanem egy teljesen legális, népszerű telekommunikációs szolgáltatói rendszert vettek erre igénybe.

5. 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 (tűz, típushiba), és vannak olyanok, amelyek bekövetkezését nem láthatjuk előre és nem is tehetünk semmit a megtörténése ellen (földrengés, hurrikán, céltudatos betörő). Mindkét típusú fenyegetés következményeként az adatok, valamint a tároló és a feldolgozó eszközök is megsérülhetnek, ellophatják őket, vagy megsemmisülhetnek. Cél az, hogy ahol lehet, a fenyegetés megvalósulását megakadályozzuk, 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 kárkövetkezményét gyorsan meg tudjuk szüntetni, vagy le tudjuk csökkenteni az elviselhető szintre. Ez csak akkor fog a gyakorlatban a kellő mértékben működni, ha megvannak az ehhez szükséges információk, 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

2. táblázat: Támadások és támadási szintek

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 bejövetelét. 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**, más szóval a védelemhez? 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, alkalmazá-

sok) biztonságáról – vagyis ezek bizalmasságáról, sértetlenségéről és rendelkezésre állásáról – kell a megfelelő mértékben gondoskodni.

A védelem szabályait Informatikai vagy Információbiztonsági Szabályzatban (**IBSZ**) szokták rögzíteni, mely 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.

5.1 A bizalmasság

Az üzleti életben nagyon jelentős az üzleti titok védelme, ennek az az oka, hogy a vállalatok nagyon odafigyelnek az ügyfeleikre és az ügyfeleik adataira, és meg akarják előzni az **ügyfelek adataival való visszaélést**, valamint az ügyfeleik adatainak ellopását, hiszen ennek bekövetkezése súlyos bevétel-kiesést okozhat számukra, ahogyan ezt több példa is bizonyította a közelmúltban.

Az adatokhoz való jogosulatlan hozzáférést alapesetben a **jelszó**használat akadályozza meg. A jogosulatlan adat-hozzáférés ellen ezen túlmenően a **titkosítás**, **rejtjelzés** is védelmet nyújt. A kettő között az a különbség, hogy a jelszavas védelemnél a támadónak a védelem esetleges megkerülésével mégis sikerülhet hozzáfernie a védendő adatokhoz (például másik operációs rendszerrel olvassa be a jelszóval védett adatokat), míg rejtjelzés alkalmazásával hiába fér hozzá a titkosított adatokhoz, azt 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.

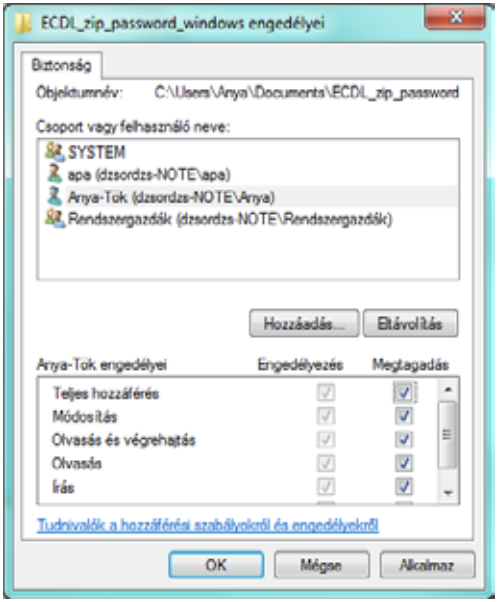
Bizalmasságról akkor beszélhetünk, ha az adataink egy részének megismerhetőségét korlátozzuk, és minden időpillanatban tudjuk, hogy ki van feljogosítva az egyes adatokhoz történő **hozzáférés**re. A bizalmasság megteremtését lehetséges saját és felhő környezetben is értelmezni. Amennyiben a saját gépeinken tárolt adatokról van szó, lehetőségünk van hozzáférés-védelmet kialakítani (jelszavasat, erősebb esetekben tokeneset[2] vagy tanúsítvány alapút). 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.

5.1.1 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?

2 *Token: hardveres biztonsági eszköz, birtoklás alapú hitelesítési eljárásban alkalmazzák.*



5. ábra: Hozzáférések megadása Windows operációs rendszerben

Az olvasást megakadályozza a titkosító program általi **fájltitkosítás** – amikor esetleg megnyithatjuk a fájlt, de értelmezni nem tudjuk. Ilyen a szövegszerkesztőben való megnyitás jelszóhoz való kötése – amikor a jelszó ismerete nélkül itt sem tudjuk megnyitni (**kititkosítani**) a fájlt értelmes olvasáshoz, valamint ugyanilyen eredményt nyújt a hozzáférés megtiltása is. 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 fájlnak, amit a rosszindulatú támadás során fel lehet

arra használni, hogy a tulajdonos tudta nélkül írjanak bele a fájlba vagy a rendszerbe – ilyenek lehetnek például a **makrók** *[ak]*.

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

5.1.1.1 Merevlemezek és USB-lemezek titkosítása, rejtjelzése

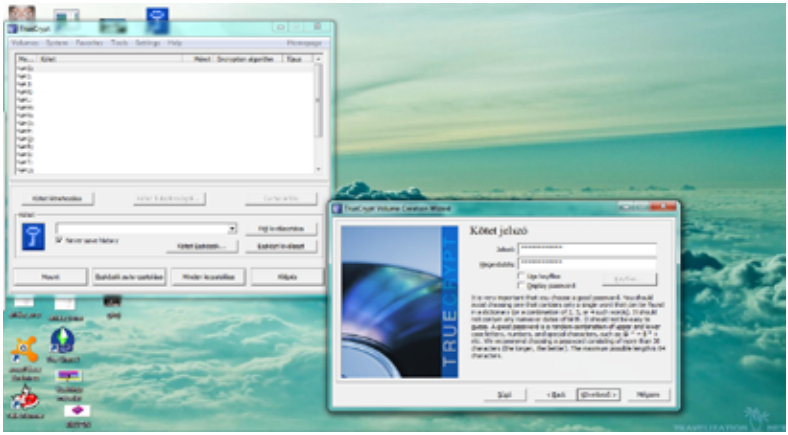
Az adataink mindazok számára alapértelmezett esetben hozzáférhetők, akik a tárolására szolgáló lemezek (belső, külső, felhő, USB) birtokában vannak. Leggyakrabban a jogos tulajdonosa van birtokon belül, de a támadók sokszor sikeresen tudják ezeket a tárolókat – illetve a rajtuk tárolt adatokat távolról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

Az adatok bizalmasságának legáltalánosabb védelmére a rejtjelzést használják. Lehetséges titkosítani mind a számítógépek merevlemezét, mind pedig egy külsőleg csatlakoztatható USB-eszközt is.

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 rejtjelzett partíciót el tudjuk érni. Rendszerindításra nem felkészített lemez teljes mértékben titkosítható.

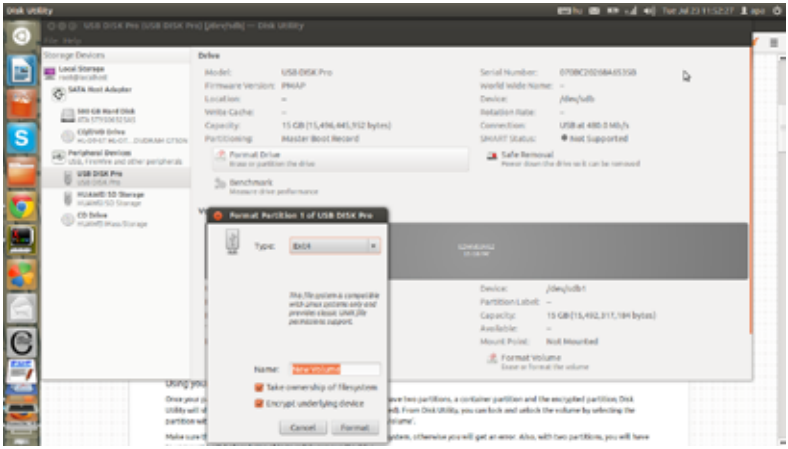
A rejtjelzés előnye az, hogy nem kell aggódnunk innentől kezdve az adatok miatt, ha esetleg az eszközt el is lopnák, amennyiben a jelszót megfelelően erősre választottuk, az alkalmazott megfelelően erős kriptográfiai titkosítás visszafejtése meghaladja a támadók erőforrás-lehetőségeit.

Természetesen itt is vigyáznunk kell a jelszó rendelkezésre állásának megmaradására, mert enélkül a titkosított adatok előlünk is el lesznek rejtve a továbbiakban.



6. ábra: USB-lemez titkosítása Windows TrueCrypt programmal

Az USB lemezek titkosítása működik más operációs rendszerek alatt is, például ahogyan ezt Linux Disk Utility programja az alábbi ábrán be is mutatja.

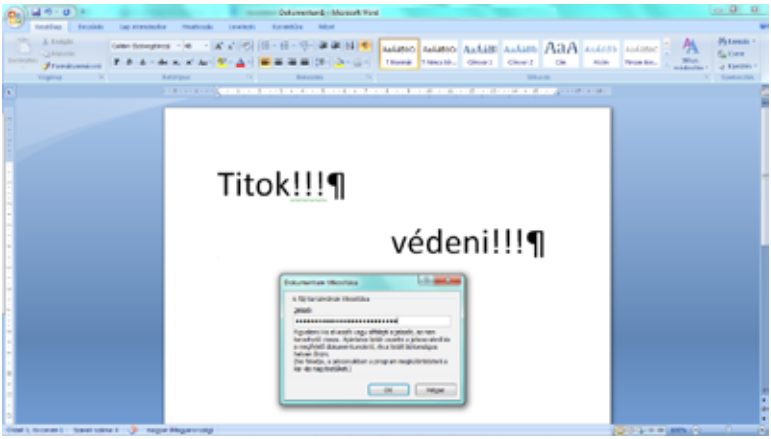


7. ábra: USB-lemez titkosítása Linuxon

5.1.1.2 Titkosítás irodai programcsomagokban

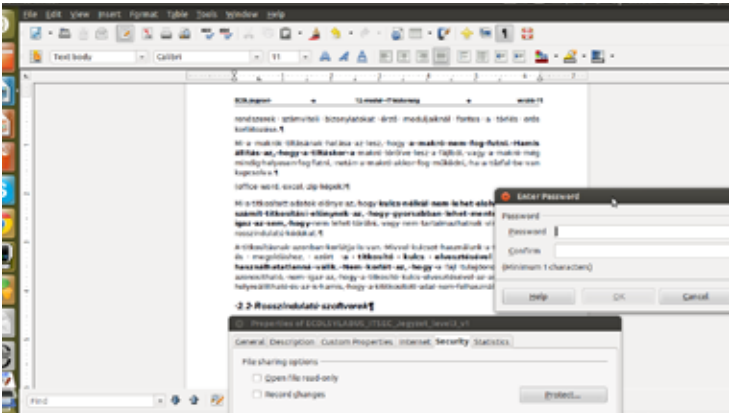
A szövegszerkesztők, táblázatkezelők, irodai programcsomagokban használható programok beépített funkciókat tartalmaznak a szöveg jelszavas védelmének megteremtéséhez, más szóval a **dokumentum-titkosítás**hoz. Amennyiben használjuk ezt a funkciót, a szövegszerkesztő bekér tőlünk egy – megfelelően biztonságos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

A következő ábrán az MS WORD 2007 verziójának dokumentum-titkosítási funkciója látható, melyet az Office gomb / Előkészítés / Dokumentum titkosítása parancs segítségével érhetünk el.



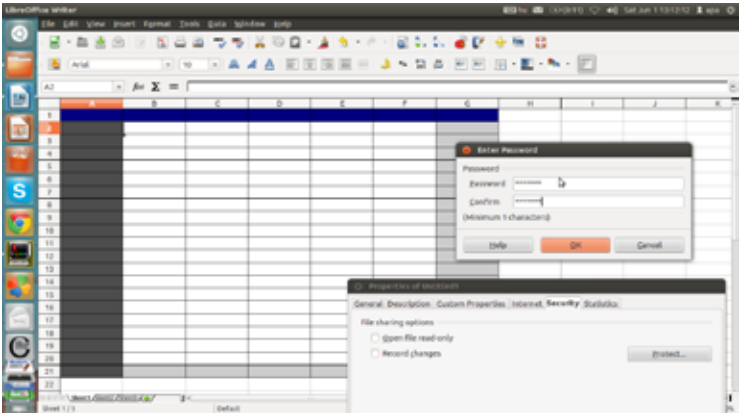
8. ábra: Titkosítási jelszó beállítása szövegszerkesztőben – MS Word

Ezt a beállítást nemcsak a Windows támogatja, minden szövegszerkesztő képes a dokumentumokat titkosítani, hogy csak a megfelelő jelszó birtokában lehessen a védett szöveget elolvasni.



9. ábra: Olvasási jelszó beállítása szövegszerkesztőben - LibreOffice

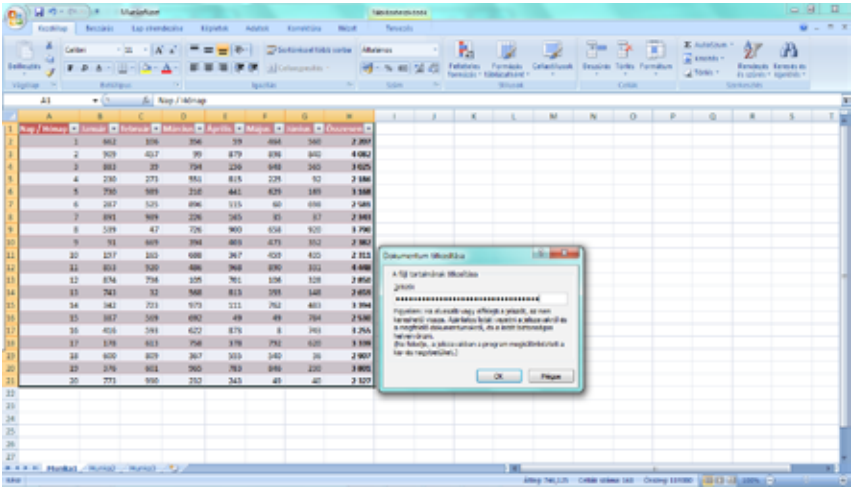
Nem lehet elégszer elismételni, hogy a biztonság kulcsa itt is a jelszó megfelelő megválasztása, hiszen egy gyenge jelszóval a védelem pillanatok alatt feltörhető.



10. ábra: Jelszó beállítása táblázatkezelőben - LibreOffice

A fenti képen látható LibreOffice 3.5 angol nyelvű verzióban a File menü / Properties menüpont / Security fül / Protect nyomógomb megnyomásával jelenik meg a legalább egy karaktert kötelezően tartalmazó jelszót bekérő ablak.

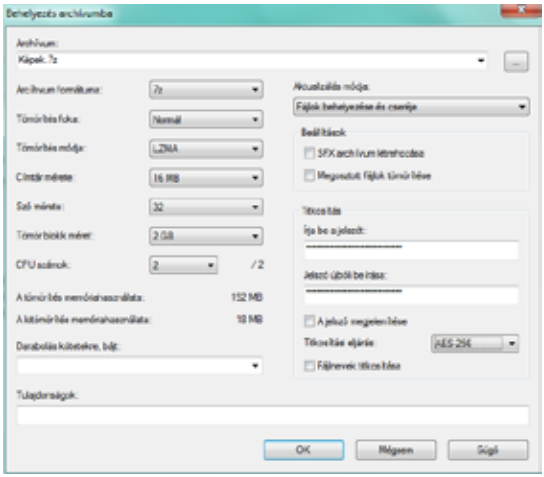
Ugyanezt megtehetjük az MS Excel programnál is, teljesen ugyanilyen módszert követve. A következő ábrán az MS EXCEL 2007 verziójának dokumentum-titkosítási funkciója látható, melyet itt is az Office gomb / Előkészítés / Dokumentum titkosítása parancs segítségével érhetünk el. Az eltérő irodai szoftvercsomagok eltérően helyezhetik el a dokumentum-titkosításra vonatkozó parancsaikat, olykor szükség lehet a Súgó <*F1*> használatára is.



11. ábra: Jelszó beállítása táblázatkezelőben – MS Excel

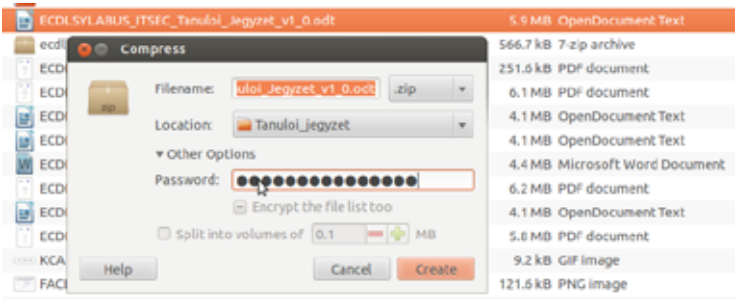
5.1.1.3 Bizalmasság tömörített állományoknál

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 **fájltömörítéshez**, az alábbi kép jobboldalán találhatunk ehhez segítséget.



12. ábra: Jelszó beállítása tömörítés közben - Windows

A tömörítőprogramok más rendszerekben is képesek jelszavakat használni a védelem érdekében, ahogyan ezt a következő ábra mutatja be a Linux Nautilus fájlkezelőjének Compress parancsa esetében.



13. ábra: Jelszó beállítása tömörítés közben - Linux

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

5.1.2 Hálózat és bizalmasság

A nyílt internetes kommunikáció során nemcsak a jogosultak láthatnak bele az adatokba. Adatok alatt egyrészről a hálózaton továbbított adatfolyamot, másrészről a hálózaton elérhető eszközökön tárolt adatokat – összefoglaló néven a **hálózati adatokat** értjük. A támadók a hozzáférés-védelmi rendszerek és a protokollok gyengeségeit, 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 adatokat (ügyfélszám, felhasználói név, jelszó). A bankok számos esetben szabályrendszereket fogalmaznak meg a felhasználók számára, a biztonság érdekében. Ha egyszer a külső szabályokat leképezték például belső informatikai biztonsági szabályzatokra, akkor ezek nagyon fontosak lesznek, mivel követendő szabályokat adnak a felhasználók számára. A szabályok kikényszerítését **tűzfalak** végzik. Az otthoni felhasználás során mint az elektronikus szolgáltatásokat (pl. internetes bankolást) igénybe vevő ügyfelek találkozhatunk betartandó biztonsági előírásokkal, de a tűzfalakról otthon sem feledkezhetünk meg.

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.

14. ábra: Védett hálózati csatlakozások jelölése

A hálózatra való csatlakozásnak a biztonsági kihatása egyszerűen szólva az, hogy megfertőződhet a számítógép rosszindulatú szoftverekkel. A hálózatra történő csatlakozás biztonsági vonatkozása ennél fogva a személyes adatok védelme köré csoportosul, hiszen a netre kötött gépeken tárolt adatokhoz a külső támadó egy sikeres támadás során korlátozás nélkül hozzáférhet.

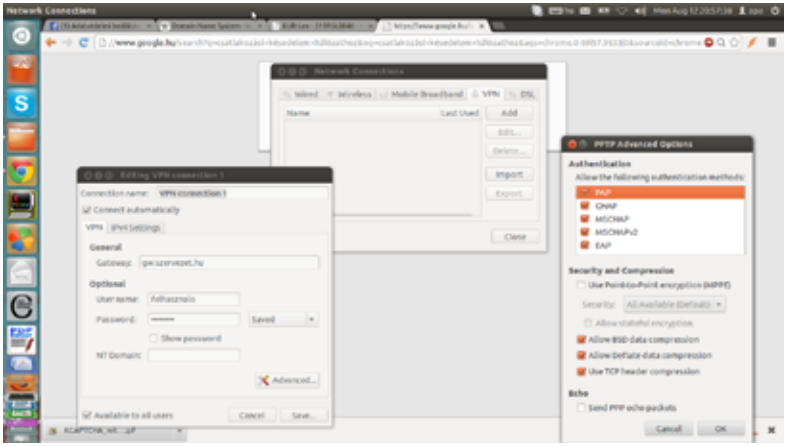
Gyakran felhasználják bejegyzett cégek neveit a személyes biztonsági adatok megszerzéséhez az eltérítéses adathalászat során. A támadó módosítja áldozata számítógépén például az internetes bankjának a címét, így az áldozat azt hiszi, hogy annak adta meg az adatait, akit lát és nem gondol támadásra. Jellemző módon az adatok megszerzéséhez hamisított weboldalakat használnak, mivel egy internetes weboldalt nagyon könnyű lemásolni.

5.1.2.1 Hozzáférés-védelem, jelszavak

A támadások legtöbbjét hálózaton keresztül követik el abból az egyszerű okból kifolyólag, hogy egy internetre kötött számítógépet az egész internet közössége lát, míg a számítógépet tartalmazó helyiségbe, otthoni gépek esetén a lakásunkba fizikailag belépők száma igen erősen korlátozott szokott lenni. Ezért a hálózatok logikai védelme (tűzfal, tartalomszűrő, adatszivárgás-elleni védelem) sokkal nagyobb jelentőségű, mint a **fizikai védelem**, de ez utóbbit sem szabad természetesen elhanyagolni, mert ugyan kevesebb a fizikai veszélyforrás, de sokkal nagyobb kárt tud okozni a megvalósulásuk, mint egy hálózati behatolás.

A hálózatoknak több típusa van, jellemzően a kiterjedése, a hozzáférés fizikai típusa és a korlátozása tekintetében osztályozhatók. Kiterjedés tekintetében vannak **helyi hálózat**ok (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-hez kell egy olyan szoftver,

ami ezt támogatja és a tűzfalon is át tud menni. A helyi hálózatok lehetnek önálló kialakításúak és funkcionálhatnak más hálózatok önálló részeiként is, **alhálózat**ként.



15. ábra: Bejelentkezés VPN hálózatba

Általában minden hálózatnál van valaki, aki kiosztja és visszavonja a fájl- és eszközhozzáféréseket – ha egynél több személynek kell hozzáférést adni a saját zárt hálózatunkhoz, ezáltal megvalósítottunk egy **hálózati adminisztrátor**i szerepkört, aki a hálózaton belüli hitelesítés, feljogosítás és számonkérés kezelésére van feljogosítva, és feladata fenntartani a szükséges adathozzáférést a hálózaton.

A hozzáférés alapja az **azonosítás**, **hitelesítés** és a **feljogosítás**. Azonosítás során először azonosítani szükséges az erőforrásokat használni kívánó felhasználót (tipikusan a felhasználói név megadásával), majd a rendszer meg kíván arról győződni, hogy tényleg az a felhasználó próbál meg bejelentkezni, akinek a hozzáférést kiosztották, ezért hitelesíti a bejelentkezőt (leggyakrabban többször használatos jelszavak megadásával) és ha a felhasználói név – jelszó pár érvényes, a rendszer a meghatározott erőforrások használatát engedélyezi (pl. nyomtató, internet, hálózati alkalmazások stb.). A hitelesítés lehet **tudásalapú** (pl. jelszavak, kifejezések megadása), **eszközalapú** (pl. tokenes jelszógenerátor) vagy **biometriai** (ilyen az ujjlenyomat, retinalenyomat, hang stb. alkalmazása).

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 jelszókezelés szabályait ajánlott betartani, mint a jelszavak másokkal való nem megosztása, időszakos megváltoztatása, megfelelő jelszó-hossz, megfelelő jelszókarakterek – betűk, számok és speciális karakterek – együttes használata. A jelszavak tulajdonságainak használatát javasolt kikényszeríteni.

A jelszavak használatakor három hitelesítés-típust különbözetünk meg:

1. **többször használatos jelszó alapú**: egyszer megadjuk (pl. karaktersorozat, összekötési útvonal), beállítjuk és annyiszor használhatjuk, ahányszor akarjuk

2. **egyszer használatos jelszó** (**OTP** – **one time password**) alapú: ezt a jelszót a felhasználó saját maga generálja és a generálás után csupán egyetlen egyszer használhatja fel – jellemzően egy token, hardveres eszköz szükséges hozzá.

3. **biometriai alapú hitelesítés**: az ember valamely fiziológiai jellemzője (pl. ujjlenyomat, hang, retina, tenyérlenyomat stb.) szolgál hitelesítésre.

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 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.

A biometriai védelem viszonylag ritka otthoni felhasználásban, de a kritikus biztonságú helyszíneken alapértelmezett a használatuk a bizalmasság védelme érdekében. Ilyen védelmi technika az ujjlenyomat, kézgeometria, tenyérlenyomat

beolvasása, hangazonosítás vagy retina-szkenner a hozzáférés-védelemben.

16. ábra: A 10.000 leggyakoribb jelszó weboldala

Az eszközök fizikai biztonságának növelésére használható módszer például a **biztonsági kábel**ek alkalmazása, hogy a támadó ne tudja egyszerűen ellopni az eszközöket, fizikailag legyen meggátolva benne. Gyakran szokták alkalmazni a lelakatolást a hordozható számítógépek esetében is, a lopás megnehezítésére.
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).

5.1.2.2 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 ugródeszkaként felhasználni a további támadásaikhoz.

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), a WiFi védett hozzáférés (**WPA** – WiFi Protected Access) 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 WiFi 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 WPA úgy lett kialakítva, hogy együttműködjön az összes vezeték nélküli hálózati illesztővel, de az első generációs vezeték nélküli elérés pontokkal nem minden esetben működik. A WPA2 a teljes szabványt tartalmazza, de emiatt nem működik néhány régebbi hálózat kártyával sem.

Mindkét megoldás megfelelő biztonságot nyújthat, két jelentős problémával:

- Vagy a WPA-nak, vagy WPA2-nek engedélyezettnek kell lennie a WEP-en kívül. De a telepítések és beállítások során inkább a WEP van bekapcsolva alapértelmezettként, mint az elsődleges biztonsági protokoll.

- A „Personal” (WPA-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.

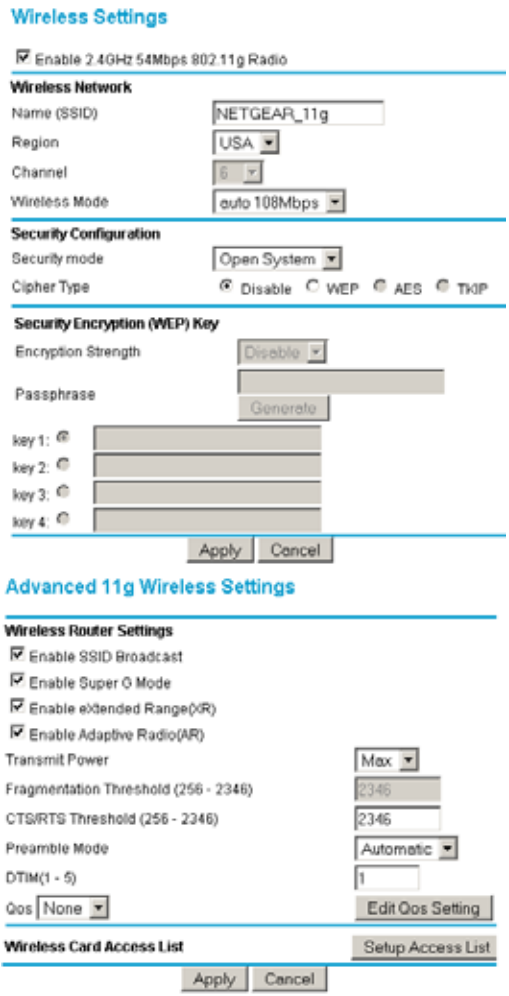
17. ábra: WiFi titkosítási beállítások

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

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

18. ábra: MAC szűrés beállítása WiFi eszközön

Ezt 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.



19. ábra: Példa nyílt WiFi rendszer beállításaira

5.1.2.3 E-mail

Nagyon gyakori kommunikációs forma (sok százmillió keletkezik naponta belőlük az üzleti, otthoni és kormányzati területeken) az internetes kommunikáció során az egész világon elektronikus levelezés használata. A levelezéshez használt legelterjedtebb protokoll az **SMTP** *[ah]*.

Az SMTP a Simple Mail Transfer Protocol rövidítése, ami egy de facto szabvány kommunikációs protokoll az e-mailek interneten történő továbbítására. Ez egy viszonylag egyszerű, szövegek átvitelére tervezett protokoll, ahol egy üzenetnek egy vagy több címzettje is lehet. Az SMTP szolgáltatás a TCP (Transmission Control Protocol) 25-ös portját használja. Az SMTP-t 1982-ben definiálták először az RFC 821 dokumentumban (Request for Comments). Az SMTP akkor működik a leghatékonyabban, ha a fogadó gép bármikor elérhető. A Sendmail volt az első levéltovábbító ügynök (mail transfer agent) ami megvalósította az SMTP-t. Ezt az SMTP-t használja az exim, az IBM által fejlesztett Postfix, D. J. Bernstein által fejlesztett qmail és a Microsoft Exchange Server.

Az SMTP kezdetben csak a hétbites ASCII karaktereket ismerte, nem tudott mit kezdeni a bináris fájlokkal. A felhasználók alkalmi megoldásokat vettek igénybe ilyen esetekben. Azóta már kifejlesztették a MIME kódolást, amivel bináris fájlok is „utazhatnak" a levelekben. Ma már minden SMTP kiszolgáló támogatja a 8 bites, azaz a 8BITMIME kiterjesztésű leveleket, ami bináris formában tárolja / küldi az üzeneteket. Az SMTP nyílt szövegként küldi a leveleket a hálózaton keresztül, ezért azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet, csupán az elektronikus levél titkosítása biztosíthatja. Egy fogalom kívánkozik még ide, az e-mail aláírás. Az **e-mail aláírás** (nem tévesztendő össze a levelek digitális aláírásával) egy olyan előre megírt szöveg, melyet minden egyes kimenő e-mail végére a levelező programunk automatikusan beilleszt. Tipikusan ilyen az elköszönő szöveg, pl. „üdv, Péter".

E-mail vonatkozásában a legnagyobb kitettséget a rosszindulatú programkódoknak egy még ismeretlen tartalmú, megbízhatónak látszó, hamisított levélhez hozzáfűzött levélcsatolmány megnyitása jelenti. 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 tartalma-

zó 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.

Az adathalászat során értékes információk megszerzéséért általában félrevezetnek valakit az online személyazonosságról. 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 vonatkozóan kétkedve és bizalmatlanul javasolt kezelnünk, és az elutasítás után mérlegelhetjük az incidens jelzését is a bank vagy szolgáltató felé. Ez utóbbi azért fontos, mert az ügyfelek tömeges visszajelzései alapján az érintett szervezet egyrészről intézkedést tud tenni az incidens megállítására, másrészről az elkövetők kézre kerítését is elindíthatja – ami sosem a mi feladatunk, ne is próbálkozzunk vele, mert esetleg a Btk. szerinti tiltott tevékenységekbe futhatunk bele.

5.1.2.4 Azonnali üzenetküldés

A valós idejű szöveges kommunikáció két vagy több személy között az azonnali üzenetküldés. Sok közösségi program része (Iwiw, Facebook, Skype), 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 fájl-hozzáférés. A védelem itt elsősorban bizalmasságot biztosító módszerekkel valósítható meg, mint az **adattitkosítás** vagy **adat-rejtjelzés** (ami még csak elvétve jellemző a valós üzenetküldőkre), fontos információk titokban tartása, fájl-megosztás korlátozása és természetesen figyelni illik a program integritására, vagyis észlelhetővé kell tenni azt, ha valaki a tudtunk nélkül átírná

az azonnali üzenetküldő szoftverét, ami a gépünkön fut (erre szolgál a kódaláírás, amit a digitális aláírásoknál tárgyalunk).

5.1.2.5 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.
Három fajtájával érdemes megismerkedni:

1. **Csomagszűrő tűzfal** (**packet filter**): a hálózat alsóbb, csomagokból álló szintjein döntenek egyes csomagok átengedéséről vagy eldobásáról, amit csomagszűrésnek nevezünk. Megjegyzendő, hogy egyes szakemberek a csomagszűrőt nem is tekintik tűzfalnak.

2. **Alkalmazás-szintű tűzfal** (**proxy**): hasonlóan a csomagszűréshez, az alkalmazások adatforgalmát naplózza, esetenként az engedélyezésről vagy tiltásról is dönt, de már az alkalmazás szintjén, az alkalmazás által fogadott és küldött formátumú adatokra köztes elemként *[al]*. Ez magasabb szintű tartalomellenőrzést biztosít, mint a csomagszűrés. A proxyk biztonsági szerepet is játszhatnak (pl. tűzfalak), de gyakran a cél csupán az ellenőrizhetőség és naplózhatóság (például ha az internetet csak HTTP proxy-n át érhetik el, a tevékenységeket ellenőrizni és megfigyelni is lehet ezáltal).

3. **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 csomagszűrők és proxyk lehetnek különálló hardveres-szoftveres egységek, de 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 engedélyeznünk kell.

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

A tűzfalnak van egy ismert korlátja, mégpedig nem értesít automatikusan a hálózati behatoláskor.

5.1.3 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.

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**) *[ai]* a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. A szabályozás a következők miatt jött létre:

- mivel a Közösségnek a Szerződésben megállapított, és az Európai Unióról szóló szerződés által módosított célkitűzései között szerepel az Európa népei közötti egyre szorosabb egység megteremtése, a Közösséghez tartozó államok közötti szorosabb kapcsolatok szorgalmazása, az Európát megosztó határok felszámolására tett közös intézkedések megtételével a gazdasági és társadalmi fejlődés biztosítása, az európai népek életkörülményei javításának folyamatos ösztönzése, a béke és a szabadság megőrzése, valamint megszilárdítása, továbbá a demokrácia biztosítása azon alapvető jogok alapján, amelyeket a tagállamok alkotmánya, jogszabályai, valamint az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény elismer;

- mivel az adatfeldolgozási rendszerek célja az emberek szolgálata; mivel a természetes személyek nemzetiségétől és lakóhelyétől függetlenül tiszteletben kell tartaniuk e személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat, és hozzá kell járulniuk a gazdasági és társadalmi fejlődéshez, a kereskedelem fejlődéséhez, valamint az egyének jólétéhez;

- mivel egy olyan belső piac kialakítása és működése, amelyben a Szerződés 7a. cikkének megfelelően biztosított az áruk, a személyek, a szolgáltatások és a tőke szabad mozgása, nem csak azt kívánja meg, hogy a személyes adatok szabadon áramolhassanak egyik tagállamból a másikba, hanem azt is, hogy az egyének alapvető jogai biztosítva legyenek;

- mivel a Közösségben a gazdasági és társadalmi tevékenység számos területén egyre többször folyamodnak a személyes adatok feldolgozásához; mivel az informatika terén elért haladás az ilyen adatok feldolgozását és cseréjét lényegesen megkönnyíti;

Más dolog, amikor haszonszerzési célból csalással, számítógépes rendszerekhez való hozzáféréssel szereznek – jellemzően pénzügyi – adatokat rólunk, hiszen a feketepiacon a számlaadatoknak értéke van, nem is kicsi. A képzett támadók sokféle módon szerezhetik be a szükséges információkat, például telefonhívásokkal (kikérdezés), adathalászattal (phishing), eltérítéses adathalászattal (pharming), kifigyeléssel (shoulder surfing), vagy személyesen, megtévesztéssel (szélhámosság). A szélhámosság módszerei változatosak, nagyon gyakori például az, hogy a szélhámosok valamilyen ürügy révén (pl. üzleti tárgyalás) bejutnak a helyszínre

és ott szétnéznek további adatok után kutatva. Ugyanilyen gyakran történik az meg, hogy a szélhámos **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.

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

5.1.3.1 Védelem böngészés közben

Egy webböngészővel egyszerűen meg lehet az egyik internet oldalról egy másikat látogatni, mert a böngésző értelmezi 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 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 frissítés**eket, vagy ha a szoftver erre nem ad lehetőséget, úgy mindig a legfrissebb szoftververzióját telepíteni és/vagy használni. A szoftverfrissítések telepítésének az a leglényegesebb oka, hogy ezzel lehetőséget kapunk kijavítani egy program hibáját vagy biztonsági kockázatát.

Az internethasználat biztonsága alapvető fontosságú digitális értékeink védelméhez. Nagyon fontos tudatában lenni annak, hogy bizonyos online tevékenységeket (vásárlás, pénzügyi tranzakciók, internetes bankolás, internetes számlafizetés) csak biztonságos weboldalakon szabad végrehajtani. Meg kell tanulni azt, 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 internetkávézó, 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 fiók**unkat használjuk.

5.1.3.1.1 A látogatott oldalak biztonsága

A WWW tulajdonképpen elkülönített dokumentumokat fog össze hálózatban. Linkek (kereszthivatkozások) segítségével fogalomról fogalomra, dokumentumról dokumentumra 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.

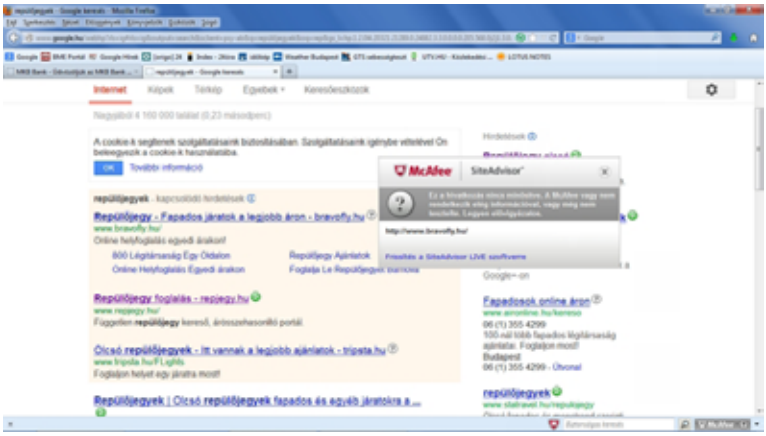
20. ábra: Uniform Resource Locator - URL

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://, ftp://, https://, file:// stb.), egy doménnévből (www.origo.hu) és egy oldalnévből (index.html).

A nevek és címek összerendelését segíti a **DNS**, Domain Name System, magyarul a doménnév-rendszer *[aj]*. A DNS rendszer a domaineket (tartományokat) kezelő, a világon több ezer szerverre elosztott hierarchikus adatbázis-rendszer. Ezek a domainek vagy tartományok úgynevezett zónákra vannak elosztva, ezekért egymástól független adminisztrátorok felelősek. A nevek rendezése a múltban nagyon szigorúan kötődött a **DNS-végződéshez**, 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) szervert 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 Weben 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, álweboldalakat 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 többékevésbé beazonosítani, és a felhasználót erre figyelmeztetni. Az egyik ilyen védelmi szolgáltatás a „SiteAdvisor", ami a weboldalakat minősíti és a minősítés alapján tanácsokkal látja el a felhasználót az oldallal kapcsolatosan.



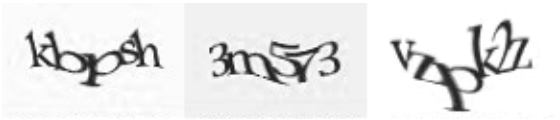
21. ábra: McAfee SiteAdvisor – a megbízható weboldalakért

Például egy online pénzügyi tranzakció elvégzésekor 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 (időzár), ez megnehezíti egy esetleges lehallgató dolgát is.

A biztonságos weboldal jele a lakat-ikon, egy lezárt lakat jelzi azt (a https-en kívül), hogy itt most titkosított forgalomról van szó.

Szintén az automatizált támadások elleni védelemre szolgál a „**captcha**" *[af]*. 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.



22. ábra: Captcha

5.1.3.1.2 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 böngészőkben, hogy nyugodtan böngészhessünk ismeretlen weblapokon, a kifigyelés legkisebb veszélye nélkül.

- **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 e célra alkalmazott értelmezőprogram (interpretáló) által lehet alkalmazni. Alkalmazható például űrlapok kitöltésének ellenőrzésére, látogatottság számlálásra vagy képek cseréjére (ha rávisszem az egér mutatóját egy képre, akkor egy másik jelenik meg). Fontos veszélye, hogy lehetővé teszi ActiveX Control-ok aktivizálását, amelyeket már egyszer a számítógépre telepítettünk, és ezáltal ugyanolyan jogokkal bírnak, mint a helyi telepítésű program.

- **VBScript**: A VBScript ugyancsak a Microsoft által kifejlesztett programozási nyelv, amely a Visual Basic programozási nyelvre támaszkodik és szorosan kapcsolódik a Windows operációs rendszerekhez. VBScripttel is ki lehet egészíteni a weboldalakat aktív elemekkel. Mindenesetre az Internet Explorer az egyetlen böngésző, amely kiegészítők nélkül képes a VBScriptet a weboldalakon működtetni. Szintén képes ActiveX vezérlésére.

- **Flash**: 1996-ban vezette be a Macromedia (jelenleg az Adobe) a flash-technológiát, ami nagyon gyorsan teret hódított. 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.

Az aktív programokon keresztül kémprogramok telepíthetők 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. 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. A felhasználó döntése marad, hogy mit tart esetenként fontosabbnak és mire van felkészülve egy kényelemből bekövetkező incidenst követően.

5.1.3.1.3 A böngészőben tárolt adatok biztonsága

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

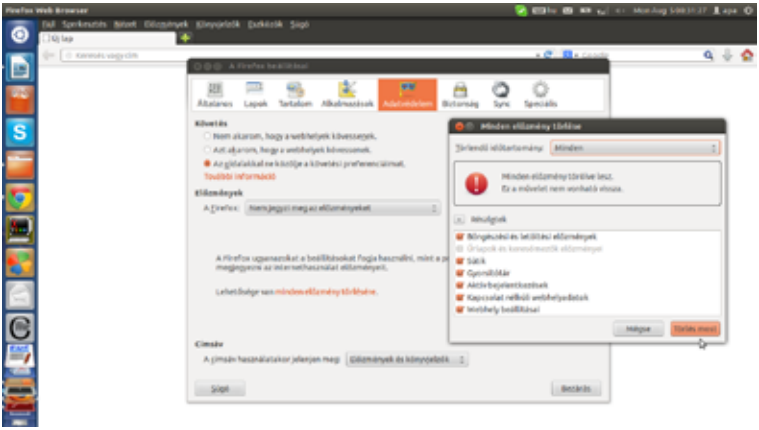
- **előzmények**: a meglátogatott oldalak listája időrendi sorrendben.

- **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 in-

formációk 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 alkalmaznak, 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.



23. ábra: Böngészési adatok törlése Firefoxban

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

Az **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.

5.1.3.2 Bizalmasság védelme a 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.

Mindezt azért, hogy a lehetséges veszélyeket képesek legyünk elkerülni, mint 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 adatokat adunk meg a közösségi hálózatokon és ezen belül a kapcsolati hálónkon, amit kevesen ismerhetnek, mint például a lakcímünk. Ilyen veszélyt kevésbé rejt a zenei érdeklődés, az otthoni cím és a kedvenc televízióműsor megadása, mivel ezek egyrészről több helyről hozzáférhető adatok, másrészről többek által megismerhető adatok, mint a becenév. Egy szexuális bűnöző számára megkönnyítheti a szexuális kizsákmányolás előkészítését minden apró információ, amit megadunk a közösségi oldalakon, ez egy ismert és nagyon veszélyes fenyegetés itt.

Az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk az, hogy a személyes adatokat bárki megnézheti. A közösségi média használatakor nemcsak azok olvashatják adatainkat,

akik barátságosan viseltetnek irányunkban, hanem azok is, akiknek esetleg valamelyik megnyilvánulásunk nem tetszik, és ezt internetes zaklatásban fejezik ki.

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

1. barátaink megválasztásánál óvatosan járunk el vagy a kellemetlen barátot töröljük, és

2. 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

3. 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.

24. 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.

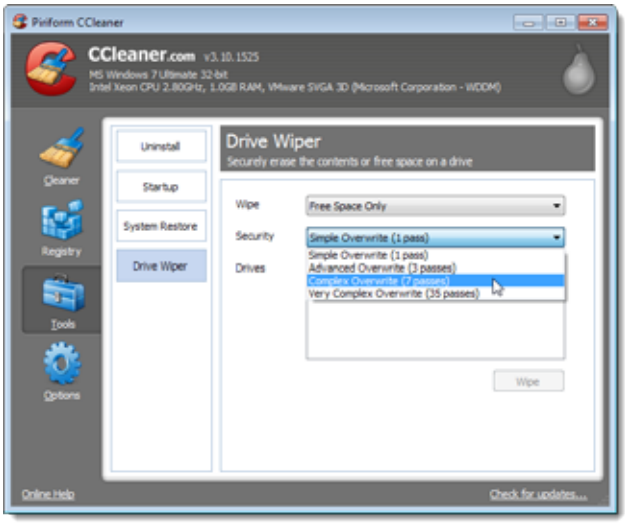
Az alábbi három témakör köré csoportosulnak a beállítások – például – az egyik legkedveltebb közösségi oldalon, a Facebookon:

1. *Ki láthatja a dolgaimat?*
2. *Ki léphet kapcsolatba velem?*
3. *Ki találhat rám?*

5.1.4 Az adatok végleges törlése

Az adatok **visszaállíthatatlan törlés**ére, 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 **Lomtár**ba mozgatása (soft delete), csupán az elérésüket, kilistázásukat szünteti meg a könyvtárban. A visszaállíthatatlan törlésre egy jó módszer az adatokat tartalmazó lemez (CD, DVD) **bedarálás**a fizikailag (hard delete). Ugyanígy az adatok végleges törlését eredményezi a merevlemezek **elektromágneses törlés**e (degaussing) – ami erős mágneses mező gerjesztésével tünteti el a mágnesezett adathordozókról az adatokat, gyakorlatilag felülmágnesezi azokat. Megfelelő lehet **szoftveres adatmegsemmisítő eszközök** használata is, de csak akkor, ha a célszoftverek *[y]* többszörös felülírás alkalmazásával teszik véglegesen olvashatatlanná a korábbi adatokat.

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.



25. ábra: Végleges adattörlés szoftveresen

5.2 A sértetlenségről

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

5.2.1 Digitális aláírás

A digitális aláírás egy olyan 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 *[ag]* 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. 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:

1. az aláírandó adatokból elkészül annak fix (általában 160–512 bit) hosszúságú kivonata,

2. a kivonatot az aláíró algoritmus és a titkos kulcs segítségével rejtjelezi az alkalmazás, és ez lesz a digitális aláírás,

3. az aláírás kezdeti ellenőrzése automatikusan megtörténik,

4. 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:

I. a fogadó az adatokból elkészít egy új kivonatot,

II. a digitális aláírásból a nyilvános kulcs segítségével visszaállítja az eredeti kivonatot,

III. a fogadó az új kivonatot és az eredeti kivonatot összehasonlítja, és ha egyezik, akkor az aláírás rendben van, ha nem egyezik, akkor pedig az aláírás elfogadását – alapesetben – megtagadja.

A digitális aláírás sikeres ellenőrzéséből az alábbiak következnek:

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

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

- × az adatok a küldés során megváltoztak,
- × az ellenőrzéskor más kulcsot vagy algoritmust használtak,
- × a tanúsítványt nem tette a fogadó még megbízhatóvá a saját rendszerében,
- × a tanúsítvány lejárt,
- × a nyilvános kulcshoz tartozó tanúsítvány hibás.

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

Hol alkalmazzák ezt a technológiát elsősorban? A programozók a fejlesztett kódokat alá szokták írni ma már digitálisan, hogy a támadók addig se tudják észrevétlen módosítani ezeket a tartalmakat, amíg eljutnak a felhasználók gépeire (kódaláírás). A telepítések előtt érdemes elolvasni azt az üzenetet, mely megmutatja a telepítendő szoftver íróját is. Másrészről a teljesen elektronikus ügyintézés nem képzelhető el másként, csak digitális aláírással, hiszen így tud meggyőződni az ügy-

intéző a beküldött nyomtatvány aláírójának személyazonosságáról anélkül, hogy az ügyfél személyesen is megjelenne előtte. Ilyen ügyintézési terület ma Magyarországon például a cégeljárás.

5.2.2 Kivonatok

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

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

1. **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.

2. **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.

3. **Ütközés-mentesség** (**collision resistance**): gyakorlatilag lehetetlen két olyan üzenetet találni a lehetséges üzenetek halmazában, melyeknek a kivonata megegyezik. Ez a tulajdonság fogja megvédeni az aláírást az előre megválasztott üzenetek típusú támadásoktól - amikor a támadó az előre elküldött üzenetet íratja alá, de az általa másodikként megtalált üzenetre cserélné ki az aláírt üzenetet. Erre az üzenetek halmaza és a lehetséges hash értékek halmaza méretének lényeges (sok-sok nagyságrendnyi) különbözősége ad lehetőséget.

5.3 A rendelkezésre állás megteremtése

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

1. áramellátás a hardver számára
2. adatok és szoftverek az alkalmazások számára
3. hálózati sávszélesség biztosítása az elérhetőség érdekében
4. vírusvédelem a működésbiztonság megőrzése számára

Az áramellátást szünetmentes tápegységek *[a]* 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:

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

A **DoS-támadások** kivitelezésekor a támadók valódinak látszó kérésekkel bombázzák egy időben a szervert, de nem foglalkoznak a válaszokkal, mert a cél a folyamatos kérésekkel a szervert annyira leterhelni, hogy más felhasználók kérésének feldolgozására a szervernek ne maradjon kapacitása, így az lelassul a külső szemlélő számára, vagy megszűnik válaszolni. Otthoni felhasználóknak jó hír, hogy az erre irányuló védelem megteremtése a szolgáltató feladata.

Ettől nehezebb kérdés az, 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 (fájlnak) csak egyetlen egy példánya keletkezik és nem készítenek róla másolatokat, **fájlmentés**eket. A hardver meghibásodása (olvasófej, mágneslemez felülete, mágnesezettség) következtében ezek az adatok megsérülhetnek, megsemmisülhetnek annyira, hogy a teljes visszaállításukra lehetőség nem lesz.

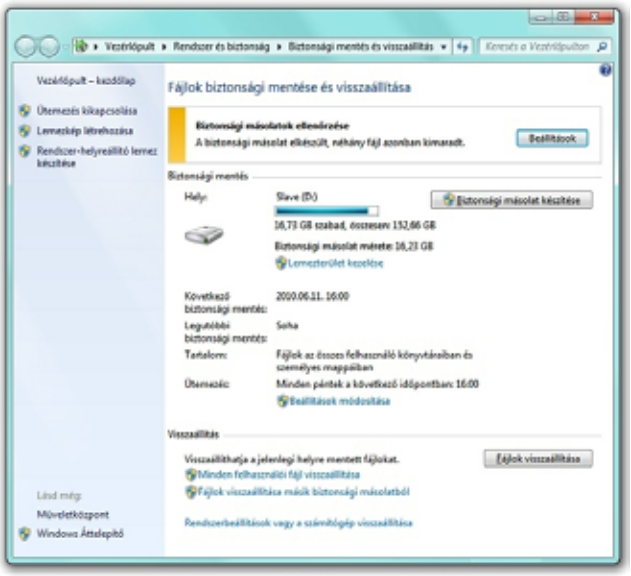
5.3.1 Fájlok biztonsági mentése

Az adataink a számítógépen 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 megfontolni:

1. Mekkora adatmennyiséget kell mentenünk?
2. Milyen gyakran változnak meg a mentendő adatok?
3. Hány példányban kell a mentést elvégezni?
4. Mikor kell a mentést elvégezni, hogy befejeződjön a következő mentés elindítása előtt?
5. Meddig kell megőrizni a mentéseket?
6. Hogyan kell a mentéseket biztonságosan megsemmisíteni?

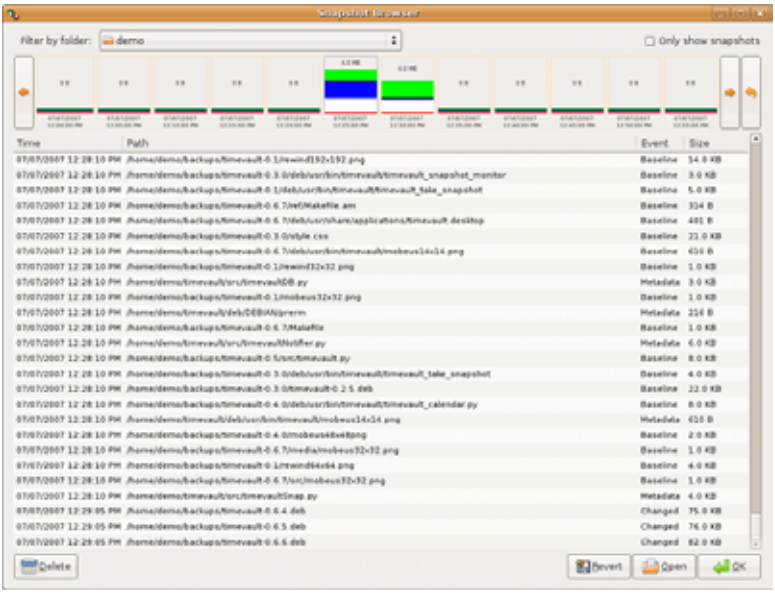
Windows rendszerben a mentést a beépített automatikus biztonsági mentési eszköz, a Windows Backup *[ab]* biztosítja legegyszerűbb módon. A Windows Backup a teljes rendszert lementi olyan formában, hogy egy visszaállítás után a működés ettől a ponttól fog újraindulni. Tekintettel arra, hogy ez a módszer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

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 *[ac]* 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.



26. ábra: Windows Backup

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



27. ábra: Adatok mentése Linuxon

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

5.3.2 Védelem az áramellátás hibái ellen

A szünetmentes áramellátó berendezések használata számítástechnikai és ipari környezetben, vagyis otthon és a munkahelyen ma már elengedhetetlenné vált. Nem szívesen vállaljuk fel ugyanis egy áramszünet, illetve a feszültségingadozással járó zavarok hátrányos, költséges következményeit. Az **elektromos hálózat**ról üzemeltetett eszközök működése függ a hálózat működésétől, más szóval attól, hogy van-e áram. Az otthoni eszközök java része kizárólag az elektromos hálózatról működik, 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 károsszeg, 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. Az otthoni védelemre példa az alábbi kis teljesítményű és méretű szünetmentes áramellátást biztosító egység.

28. ábra: Szünetmentes otthoni áramellátó eszköz

5.3.3 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 fertőzés-mentesíteni, 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 üresjárati időpontokban. Ezeket a felismeréseket a **vírusdefiníciós fájl**ban 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.

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

6. Mellékletek

6.1 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] Tom Stonier: Információ és az univerzum belső szerkezete;
Springer Hungarica, 1993

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

[8] EUROPEAN COMMISSION, Brussels, 15.12.2010, COM(2010) 743 final;
The European eGovernment Action Plan 2011-2015;
Harnessing ICT to promote smart,
sustainable & innovative Government SEC(2010) 1539 final

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

[10] James Martin – Kathleen K. Chapman: Lokális hálózatok,
Novotrade Kiadó kft. - Prentice Hall, 1992

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

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

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

[14] PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ,
Felhasználói szintű informatikai biztonsági képzés,
2010-2013. Utolsó frissítés: 2013. június 10.

[15] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

6.2 Internetes hivatkozások jegyzéke

Az internetes hivatkozások 2013. szeptember 23-i állapot szerint lettek rögzítve. Előfordulhat, hogy az idő múlásával egyes linkek megváltoznak, vagy eltűnnek. A szerző garanciát ezekért nem vállalhat, a változásokat a könyv felülvizsgálásakor tervezi kezelni.

[a] *http://hu.wikipedia.org/wiki/Számítógép-architektúra*

[b] *http://en.wikipedia.org/wiki/Cloud_computing*

[c] *http://www.slideshare.net/tothmozer/internethasznalati-szokasok-3374155*

[d] Global Use of Electronic Authenticity; Erdősi Péter Máté, SSRN, 2013; *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2264335*

[e] Kormányportál *http://www.magyarorszag.hu*

[f] Vörös Október Támadás *http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies*

[g] Vörös Október Támadás ábra *http://www.securelist.com/en/images/vlill/kaspersky_lab_infographic_red_october_victims_by_country.png*

[h] COBIT *http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx*

[i] Common Criteria *http://www.commoncriteriaportal.org/*

[j] Infobiztonsági törvény *http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=160206.240508*

[k] Kibertér-védelmi stratégia *http://www.cert-hungary.hu/node/195*

[l] CERT Hungary *http://www.cert-hungary.hu/node/3*

[m] ISO 2700x
http://www.27000.org/

[n] ECDL Elektronikus hitelesség, elektronikus aláírás modul
http://njszt.hu/ecdl/syllabus/elektronikus-hitelesseg-elektronikus-alairas

[o] saferinternet.hu
http://saferinternet.hu

[p] Top 10.000 jelszó
https://xato.net/passwords/more-top-worst-passwords/

[q] Linux SAG(The Linux System Administrator's Guide)
http://www.tldp.org/LDP/sag/sag.pdf

[r] Linux Security Administrator's Guide,
http://www.linuxtopia.org/online_books/linux_administrators_security_guide/

[s] MS Office jelszavas védelem
http://office.microsoft.com/hu-hu/excel-help/dokumentumok-munkafuzetek-es-bemutatok-vedelme-jelszoval-engedelyekkel-es-egyeb-korlatozasokkal-HA010354324.aspx

[t] TCP/IP és ISO
http://www.ciscoworld.hu/tcpip-es-osi-modell-attekintese/

[u] Symantec Report
http://www.symantec.com/security_response/publications/threatreport.jsp

[v] Hozzáférés Windowsban
http://technet.microsoft.com/en-us/library/bb456977.aspx

[w] Android MAC-cím
http://optimum.custhelp.com/app/answers/detail/a_id/2820/~/finding-the-mac-address-on-an-android-phone-or-android-tablet

[x] WiFi biztonság
http://www.wikihow.com/Add-a-Password-to-Your-Wireless-Internet-Connection-(WiFi)

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

[z] Jelszavas RAR védelem
http://www.wikihow.com/Add-a-Password-to-a-RAR-File

[aa] Szünetmentes táp
http://www.extor.hu/szunetmentes-aramellato-berendezesek/kompakt-ups-otthonra-kis-irodaba

[ab] Windows Backup
http://techcorner.hu/pcworld/backup-ami-elerheto.html

[ac] TimeVault
http://www.tucows.com/preview/722287/Time-Vault

[ad] NetGear WiFi
http://logitech-en-amr.custhelp.com/app/answers/detail/a_id/16648/~/configuring-a-netgear-router-to-work-with-my-squeezebox-touch

[ae] Linksys WiFi
http://kb.linksys.com/Linksys/ukp.aspx?pid=80&vw=1&articleid=19073

[af] captcha
http://hu.wikipedia.org/wiki/Captcha

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

[ah] SMTP
http://hu.wikipedia.org/wiki/SMTP

[ai] Adatvédelmi irányelv
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:hu:HTML

[aj] DNS
https://hu.wikipedia.org/wiki/Domain_Name_System

[ak] makró
http://wiki.prog.hu/wiki/Makr%C3%B3

[al] proxy szerver
http://hu.wikipedia.org/wiki/Proxy_szerver

[am] IT biztonsági módszertan
http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/10_Muha_Lajos.pdf

6.3 Fogalomtár

A

ActiveX, *71*
adat, *21*
adat-rejtjelzés, *63*
adathalászat, *40*
adatlopás, *38*
adattitkosítás, *63*
adatvédelem, *65*
alhálózat, *56*
Alkalmazás-szintű tűzfal, *64*
Alkalmazások, *25*
automatikus frissítés, *68*
automatikus kiegészítés, *75*
azonosítás, *56*
álweboldal, *40*

B

bankkártya adat, *40*
bedarálás, *77*
billentyűzet-leütéseket naplózó eszközök, *38*
biometriai alapú hitelesítés, *57*
bizalmasság, *17*
Biztonság, *16*
Biztonság koncepciója, *18*
biztonság megteremtése, *63*
Biztonság mértéke, *43*
biztonsági kábel, *58*
biztonsági kockázat, *20*
biztonsági követelmény, *17*
biztonságos háttér-adattároló, *86*
biztonságos kapcsolódás, *79*
biztonságos weboldal, *68*
bonyolult fájlnevek, *85*
Böngészés, *73*

C

captcha, *71*
crackelés, *41*
crackerek, *41*
csatolmányokba rejtett rosszindulatú programok letöltetése, *39*
Csomagszűrő tűzfal, *64*

D

Diallers
  online emelt díjas tárcsázó program, *42*
  telefonszám-intervallum modemes tárcsázó, *37*
digitális aláírás séma, *79*
Digitális Európai Menetrend, *29*
digitális tanúsítvány, *79*
DNS
  DNS, *69*
  Domain Name System, *69*
  doménnév-rendszer, *69*
DNS-végződés, *69*

dokumentum-titkosítás, *50*
DoS
Denial of Service, *37*
DoS, *37*
szolgáltatás-megtagadási támadást indító programok, *37*
DoS-támadások, *84*

E

e-Europe, *28*
e-mail aláírás, *62*
egyklikkes támadások, *39*
elektromágneses törlés, *77*
elektromos hálózat, *87*
elektronikus információs rendszer, *16*
eltérítéses adathalászat, *39*
erőforrás, *44*
érzékeny információk, *38*
etikus hackelés, *41*
etikus hackerek, *40*
Európai Adatvédelmi Irányelv, *65*
Európai e-Kormányzati Akcióterv 2011-2015, *29*

F

fájl-jogosultságok, *46*
fájl-megosztás, *26*
fájlmentés, *84*
fájltitkosítás, *47*
felhő, *25*
feljogosítás, *56*
Fenyegetés, *35*
férgek, *36*
fertőzés, *88*
fertőzésmentesítés, *88*
fizikai adatmegsemmisítés, *77*
fizikai támadó eszközök, *38*
fizikai védelem, *55*
Flash, *73*

H

hackelés, *40*
hackerek, *40*
Hálózat, *31*
hálózat modellezés, *31*
hálózati adat, *54*
hálózati adminisztrátor, *56*
hálózati betörés, *65*
hálózati csatlakozási késedelem, *33*
hálózati eszközök, *33*
Hardver, *24*
Hash
hash, *82*
kivonat, *82*
lenyomat, *82*
hátsó kapuk, *36*
hitelesítés, *56*, *79*
hitelesség, *79*
Hozzáférés, *55*
HTML
HTML, *67*
HyperText Markup Language, *67*

HTTP
HTTP, *69*
Hypertext Transfer Protocol, *69*

I

IBSZ
IBSZ, *45*
információ, *21*
információ életciklusa, *24*
információbiztonság, *18*
információbúvárkodás, *67*
Információkritériumok, *21*
informatikai biztonság, *18*
internetes zaklatás, *75*
internetszűrő, *44*

J

Java appletek, *72*
Javascript, *72*
jelszó, *50*
jelszócrackelés, *41*
jogosulatlan hozzáférés, *45*

K

karantén, *88*
kémszoftver, *37*
kéretlen reklámszoftverek, *38*
kiberbűnözés, *40*
Kibertér, *14*
kifigyelés, *40*
kikérdezés, *67*
kititkosítás, *51*
Kockázat, *20*

L

LAN
helyi hálózat, *55*
lokális hálózatok, LAN, *32*
Lomtár, *77*

M

MAC
MAC, *33*
Media Access Control, *33*
Média Hozzáférési Kontroll, *33*
makró, *43*, *48*
Malware
malicious software, *35*
malware, *35*
Rosszindulatú szoftverek, *35*

N

nagyvárosi hálózatok, MAN, *32*
NIC
hálózati csatoló kártya, *33*
Network Interface Card, *33*
NIC, *33*
nyilt WiFi, *61*

O

OSI modell, *31*
OTP
egyszer használatos jelszó, *57*
one time password, *57*
OTP, *57*

P

Patch
- bugfix, *68*
- javítócsomag, *68*
- patch, *68*
- update, *68*

PGP tanúsítvány, *79*

PSK
- előre kiosztott forgalomtitkosító kulcson alapuló védelem, *59*
- Pre-Shared Key, *59*
- PSK, *59*

R

regisztrált adatkezelő, *65*

rejtett kamerák, *38*

rendelkezésre állás, *17*

Rootkit
- rendszerszinten rejtőző programok, *37*
- rendszerszinten tevékenykedő kártékony kódok, *36*
- rootkit, *37*

S

Sebezhetőség vagy sérülékenység, *19*

sértetlenség, *17*

SMTP
- Simple Mail Transfer Protocol, *62*
- SMTP, *62*

Social engineering
- social engineering, *40*
- szélhámosság, *40*

Spam
- kéretlen levelek, *37*
- spam, *37*

Sütik, *71*

SZ

szabály-alapú tűzfalrendszer, *43*

számítógép, *24*

számítógépes rendszer, *24*

Személyi tűzfal, *64*

szoftver, *24*

szoftveres adatmegsemmisítő eszközök, *77*

Szolgáltatás, *25*

szülői felügyelet szoftver, *44*

T

Támadás, *19*

tartalomellenőrző szoftver, *44*

távolsági hálózatok, WAN, *33*

TCP/IP, *33*

titkosítás, rejtjelzés, *45*

titkosító kulcs, *45*

többször használatos jelszó, *57*

trójaik, *36*

Tűzfal, *64*

U

URL
- Uniform Resource Locator, *69*
- URL, *69*

Ü

ügyfelek adataival való visszaélés, *45*

V

VBScript, *72*
Védelmi intézkedés, *19*
Védendő elemek, *20*
veszély, *16*
vírusdefiníciós fájl, *88*
vírusirtó, *88*
vírusok, *36*
vis maior, *41*
visszaállíthatatlan törlés, *77*
VPN, *55*

W

webalapú levelező fiók, *68*
WEP
  vezetékes kapcsolódással megegyező bizalmasságú hálózat, *59*
  WEP, 59
  Wired Equivalent Privacy, *59*
WPA
  WiFi Protected Access, *59*
  WiFi védett hozzáférés, *59*
  WPA, *59*
Www
  World Wide Web, *69*
  WWW, *68*

X

X509v3 tanusítvány, *79*

Z

zombi hálózati szoftverek, *38*
zsaroló programok, *37*