Nemzeti
Közszolgálati Egyetem
Közigazgatás-tudományi Kar

TÖRLEY GÁBOR

ADATBIZTONSÁG A KÖZIGAZGATÁSBAN

Egyetemi jegyzet

Budapest, 2013

Lektorálta
Dr. Péterfalvi Attila

Készült:
a Társadalmi Megújulás Operatív Program
TÁMOP-4.2.1/B-09/1/KMR-2010-0005 projekt,
Hatékony állam, szakértő közigazgatás, regionális fejlesztések
a versenyképes társadalomért alprojekt,
Közigazgatási szervezet és e-kormányzás műhely munkájának keretében

Készült a Nemzeti Közszolgálati Egyetem, Közigazgatási-tudományi
Karának megbízásából

Kiadja:
FÁMA Zrt. – Nemzeti Közszolgálati és Tankönyv Kiadó

ISBN: 978-615-5344-05-3

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai
Szociális Alap társfinanszírozásával valósul meg.

Tartalomjegyzék

Bevezetés

Ez a tankönyv az adatbiztonság világába és annak gyakorlati megvalósításába vezeti be az Olvasót. Tudván, hogy az olvasók, a közigazgatás leendő dolgozói nem informatikai szakemberek, ezért – az elmélet közérthető ismertetése mellett – nagy hangsúlyt fektetek a gyakorlati módszerek leírására.

Az elvek felsorolásával, a sok képpel, példával – néha elrettentő példával – az a célom, hogy a könyv tudásanyagát felhasználva növeljem a hallgatók tudatosságát, éberségét és egészséges félelmét, azért, hogy megtanulják, hogyan tudnak először a saját személyes adataikra figyelni, hiszen e nélkül nem lehetne rájuk bízni mások személyes adatainak kezelését, amely a munkájuk szerves része lesz majd.

Jó tanulást és jó olvasást kívánok!

Budapest, 2012. március 15.

Törley Gábor

1. Informatikai védelem, informatikai biztonság

A fejezet címében olvasható két fogalom tisztázása érdekében először meg kell értenünk a védelem és a biztonság fogalmát és egymáshoz való viszonyát.

Általában a biztonság alatt egy rendszer állapotát értjük. Olyan kedvező állapotot, amelynek megváltozása nem valószínű, de nem is lehet kizárni azt.[1] Ezt a kedvező állapotot védelmi intézkedésekkel tudjuk elérni. A védelem tehát eszköze annak, hogy a kedvező állapot – a biztonság – létrejöjjön és tartósan megmaradjon.

A biztonság és a védelem cél–eszköz viszonyban áll egymással. A védelem célja a biztonság kedvező állapotának megteremtése és fenntartása, s minél hatékonyabb a védelem, annál hatékonyabb és tartósabb a biztonság.

Legyen szó bármilyen szervezetről, intézményről, a biztonság állapota számos összetevővel, működési tényezővel kapcsolatban merülhet fel. Így például beszélhetünk a szervezeti felépítés és a szervezeti működés biztonságáról, ha a szervezet kialakítása a hatékony és stabil működés irányába hat. Nincs túl sok vagy túl kevés bürokratikus szint, s a szervezet – különösebb megrázkódtatás nélkül – képes alkalmazkodni a környezetből vagy az újabb feladatokból adódó változásokhoz. A szervezeti felépítés és működés biztonságának megteremtése irányába ható védelmi intézkedések például a szervezeti felépítés pontos megtervezése, a humánerőforrás-stratégia kialakítása, a megfelelően működtetett minőségbiztosítás stb.

---

1 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 3. p.

Egy másik biztonsági kategória a gazdasági–pénzügyi biztonság. Ez akkor áll fenn, ha rendelkezésre állnak a működéshez szükséges megfelelő anyagi és tárgyi források. E nélkül a szervezet kényszerpályára kerülhet az informatikai erőforrások rendszerbe állítása, alkalmazása és védelme terén is. A gazdasági–pénzügyi biztonság megteremtésére irányuló védelmi intézkedéseket – elsősorban a közigazgatásban – számos külső tényező is befolyásolja, így nehéz lenne azt állítani, hogy a szigorú gazdálkodás mint védelmi eszköz eredménye lenne a gazdasági–pénzügyi biztonság, bár kétségkívül hozzájárul annak megteremtéséhez. A pénzügyi biztonság megteremtésére irányuló védelmi intézkedéseket alapvetően befolyásolja a működési környezet, illetve az ehhez kapcsolódó biztonsági kategória, a működési környezet biztonsága. Profitorientált szervezet esetén a gazdasági biztonságot, a gazdasági folyamatok kiszámíthatóságát értjük ez alatt. Nem profitorientált, végrehajtó szervezetek esetén, mint amilyen a közigazgatási szervek többsége, a gazdasági környezetnél jelentősebb és közvetlenebb befolyásoló hatással bír azon jogszabályi háttér biztonsága, amely alapvetően meghatározza a felépítést, működést, feladatmegosztást. Látszik, hogy a biztonsági kategória megvalósítása érdekében kifejtett védelem részben a szervezeteken kívül esik, így a védelmi intézkedéseket a működési környezetben és az azt befolyásoló szervezeteknél kell keresnünk.

A vagyonbiztonság fogalmának meghatározásával közelebb kerülünk az információs rendszerekhez. Ez a fogalom azt jelenti, hogy a szervezet céljának megvalósításához szükséges vagyoni erőforrások (épületek, berendezési tárgyak, vagyonvédelmi eszközök, munkaeszközök, az információs rendszerek fizikai összetevői) bizalmasságának, sértetlenségének és rendelkezésre állásának fenyegetettsége minimális, azaz csekély esélye van annak, hogy a kedvező állapot megváltozzon,[2] tehát a vagyoni

2 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 6. p.

erőforrásokat csak az arra illetékesek használhatják (például az épületekbe, helyiségekbe csak a jogosultak léphetnek be), a vagyoni erőforrások megfelelnek az eredeti állapotuknak (sértetlenek, ide nem értve persze a szükségszerűen bekövetkező amortizációt), és adott időben, adott helyen rendelkezésre állnak, használhatók, szolgáltatásokat nyújthatnak.

Végül, de nem utolsósorban a biztonsági kategóriák közé sorolhatjuk az informatikai biztonságot. A fogalom meghatározásához az informatika definíciójából kell kiindulnunk. Az informatika az adatok rögzítésével, kezelésével, rendszerezésével, továbbításával foglalkozik,[3] s nem kizárólag a számítógéppel történő információkezelést és feldolgozást öleli fel: vannak technológia-független részei, elvei, szabályai, eszközei is. Általában ismerjük azt a kijelentést, miszerint „minden információ adat, de nem minden adat információ". Ebből megállapíthatjuk azt, hogy az informatika központi fogalma az információ, illetve az ezt is tartalmazó tágabb kategória: az adat. Az informatika az információ és az adat köré csoportosítja interdiszciplináris és sokszor technológia-független eszközeit, elveit.

Ezzel meg is érkeztünk e könyv fő témájához, az adat kezeléséhez, feldolgozásához, védelméhez és biztonságához. Az informatikai biztonság is technológia-független és interdiszciplináris fogalom.[4] Technológia-független azért, mert adatot, információt kezelni nemcsak számítógéppel vagy kommunikációs eszközökkel lehet, hanem papíralapon is. Interdiszciplináris azért, mert az információs és kommunikációs technológiák eszközein kívül felöleli a szervezés- és vezetéstant, a jogtudományt, a szociológiát, a pénzügytant, a közgazdaságtant és egyéb tudományterületeket.

3 Dr. Horváth Katalin – Kohány András – Dr. Orbán Anna: *7. modul. A közigazgatási informatika alapjai.* Informatikai és Közigazgatás c. tankönyvsorozat. Budapest, 2003. 10. p.

4 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 10. p.

Ez a tankönyv – Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényből indulva ki – azokat az elsősorban számítástechnikai és kommunikációs technológiákkal megvalósuló módszereket és eszközöket mutatja be, amelyek segítségével az adatalany érdekében meg lehet védeni az adatot.

Az informatikai biztonság és az informatikai védelem fogalma legalább két nézőpontból közelíthető meg. Ez azt jelenti, hogy az embert a középpontjába állító jogi oldal és az adatot a középpontjába állító műszaki, technikai oldal folyamatos versenyben van egymással, ugyanakkor egymást kiegészítve működnek. A rendszerváltás előtt az informatikai védelem megvalósítását és szabályozását tekintve a technikai oldalra helyeződött nagyobb hangsúly. A rendszerváltást követően azonban az embert a középpontba állító, az emberi jogi gondolkodás és az individuum érdekében megvalósított adatvédelem (a szó szoros értelmében) lett az uralkodó irányzat. Ma tehát az informatikai védelem két oldala egymást kiegészítve lép fel az adatalany érdekében: védi az egyént, a személyiséget (jogi szabályokkal és garanciákkal) és ennek érdekében az adatot (műszaki, technikai eszközökkel). Ez a szemléletmód Nyugat-Európában a II. világháború után, fokozatos fejlődés nyomán bontakozott ki, míg Magyarországon csak a rendszerváltás után.

Az informatikai biztonság tehát kétféle megközelítésben írható le:

- Jogilag – az embert, az adatalanyt a középpontba állítva: például jogi eszközök (törvények): az információs szabadságjogok (információs önrendelkezési jog és információszabadság), valamint az egyéb emberi és személyhez fűződő jogok (például az emberi méltósághoz való jog).
- Műszaki, technikai értelemben – az adatalany érdekében az adatot a középpontba állítva: az a kedvező állapot, amikor minimális a szervezet, az információs rendszer informatikai erőforrásai

bizalmasságának, sértetlenségének és rendelkezésre állásának fenyegetettsége, azaz csekély a kedvező állapot megváltozásának a valószínűsége.[5]

Az informatikai védelem az informatikai biztonság megteremtésének eszköze, az informatikai biztonság pedig az informatikai védelem eredménye. A cél és az eszköz megjelölését követően azonban a terminológiában némi fogalmi zavar keletkezhet.[6] Az informatikai védelem két oldalának angol tükörfordítása ugyanis nem egészen igazodik a tartalomhoz. Az adatvédelem az informatikai védelemnek az embert, az adatalanyt a középpontjába állító vetülete (data protection). Ez azonban valójában nem az adat, hanem az adatalany védelmét jelenti (tehát a jogi oldalról szól). Az informatikai védelemnek az adatot a középpontjába állító vetülete az adatbiztonság (data security). Ez azonban valójában nem biztonsági, hanem védelmi kategória, nem cél, hanem eszköz: az adatalany védelme érdekében az adat védelmének műszaki, technikai eszköze. A fogalom e pontos meghatározása mutatja az adatalany védelméhez képest alárendelt szerepét is. (Sajnos, a fogalom téves elnevezése és ezért sokszor téves értelmezése folytán az adatbiztonságot sok szakember célnak, nem pedig eszköznek tekinti még ma is.)

■ ■ ■

5 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 6. p.

6 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete*. Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 11. p.

2. Az adatbiztonság fogalma, összetevői

Ahogy a bevezetésben láttuk, az adatbiztonság nem biztonsági, hanem védelmi kategória, azon védelmi módszerek összessége, amelyeket az adatokon hajtanak végre az adatalany, illetve az érintett, valamint az adatkezelő védelme érdekében. Ez alatt érthetünk egyfajta „műszaki, technikai személyiségvédelmet".

Az adatbiztonság fogalmának meghatározásakor Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényből (a továbbiakban: Infotv.) érdemes kiindulnunk – a műszaki, technikai szakirodalom ugyanis gyakran nincs tekintettel az adatbiztonság jogi vonatkozásaira, és a legtöbbször figyelmen kívül hagyja, hogy maga a fogalom az előző Avtv.[7] megszületése óta kétharmados törvényben van definiálva. A definíció idővel változott, bővült, de ma is része a jelenlegi törvénynek. A 2012. január 1-je óta hatályos Infotv. 7. §-ában olvashatunk az adatbiztonság követelményéről,[8] sokkal bővebben, mint a korábbi törvényben:

„7. § *(1) Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.*

(2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási

7 Személyes adatok védelméről és a közérdekű adatok nyilvánosságáról 1992. évi LXIII. törvény

8 Magyar Közlöny, 2011/88. szám, 25449. p., http://kozlony.magyarorszag.hu/pdf/9906 – letöltve: 2011.10.27.

szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
(3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
(4) A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.
(5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja
a) a jogosulatlan adatbevitel megakadályozását;
b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.
(6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek."

Az első bekezdés deklarálja a célt, illetve azt is, hogy kik kötelesek megtervezni és végrehajtani az adatkezelési műveleteket oly módon, hogy ezt a célt elérjék. Nevezetesen: az adatkezelő felelős azért, hogy úgy legyenek megtervezve és végrehajtva az adatkezelési cselekmények,[9] hogy biztosítva legyen az adatalanyok magánszférájának védelme, tehát a személyes adatok védelme.

A második bekezdés arról ad tájékoztatást, hogy kik kötelesek gondoskodni az adatbiztonságról, kiknek kell megtenniük az adat védelmével kapcsolatos intézkedéseket a célból, hogy ezek az intézkedések megfeleljenek az Infotv.-nek, illetve az egyéb adat- és titokvédelmi szabályoknak. Tehát az adatkezelőnek és tevékenységi körében az adatfeldolgozónak – a jogszabályok és az adatkezelő által meghatározott keretek között – kell gondoskodnia az adatok biztonságáról. Szintén ebben a bekezdésben találjuk a védelmi intézkedések lehetséges irányait: technikai és szervezési intézkedések, eljárási szabályok.

A harmadik bekezdés nem sorolja fel a lehetséges védelmi intézkedéseket, hiszen azok tárháza a technika fejlődésével folyamatosan változik és bővül, így rövid időközönként módosítani kellene a törvényt, ami irreális lenne. Ezért az Infotv. példálózva arról rendelkezik, hogy az adatbiztonság keretében mi ellen kell az adatokat megvédeni, a védelmi intézkedéseknek mire kell irányulniuk. Itt szeretném kiemelni a véletlen megsemmisülés és sérülés esetét. Hogyan értelmezhető a véletlen fogalma egy programozott környezetben? Elektronikus adatfeldolgozás esetén ugyanis maga az adatfeldolgozás művelete olyan környezetben történik, ahol programozott akciókra (felhasználói kérésekre, utasításokra) programozott reakciók (adatfeldolgozási műveletek) következnek be.[10] Egy ilyen rendszerben azért nehézkes a véletlen fogal-

9 Infotv. 3. § 10.

10 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 65. p.

mának definiálása, mert az adat megsemmisülése, sérülése, felhasználói hiba (ismerethiány, rossz szoftverhasználat) vagy programozói hiba (az adatfeldolgozást végző szoftver programhibája, amikor a szoftver nem a felhasználói kézikönyvben leírtaknak megfelelően működik), esetleg vis maior (árvíz, belvíz, tűzvész, földrengés, vihar stb.) következménye lehet. Az egyes vis maior eseteket, azaz az adatkezelő, illetve az adatfeldolgozó tevékenységi körén kívül eső, külső, elháríthatatlan okokat, csapásokat át lehet minősíteni jogilag véletlenné, azonban kell lennie valamilyen intézkedési tervnek, szabálynak vis maior esetére is. Alapszabály, hogy az adatkezelő köteles megtérítenie az okozott kárt, ha megszegte az adatbiztonság követelményeit, azonban mentesül a felelősség alól, „ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő".[11]

A negyedik bekezdés szerint megfelelő technikai védelemmel kell biztosítani, hogy eltérő céllal rendelkező elektronikus nyilvántartásokat ne lehessen közvetlenül össze kapcsolni és az érintetthez rendelni.[12]

A paragrafus utolsó előtti bekezdése a személyes adatok automatizált feldolgozásával foglalkozik. Eszerint az adatkezelőnek biztosítania kell, hogy például jogosulatlan személyek ne vihessenek be és ne használhassanak fel adatokat, üzemzavar esetén a rendszert helyre lehessen állítani. Naplózni kell azt, hogy kik, mikor, milyen adatokat vittek be a nyilvántartásba, kiknek továbbították az adatokat, vagy milyen hibák fordultak elő.

Az informatikai biztonság fogalmából és az Infotv. rendelkezéseiből kiindulva tehát összefoglalhatjuk azokat a védelmi módszereket, amelyekkel az adat biztonsága megvalósítható: ezek az adatbiztonság összetevői. A védelmi módszerek felvázolásánál az adatbiztonság központi kategóriájából, az adatból kell kiindulnunk.

11 Infotv. 23. § (1)

12 http://www.adatvedelmiszakerto.hu/2011/09/az-adatbiztonsag-kovetelmenye-az-uj-adatvedelmi-torvenyben – letöltve: 2011.10.27.

Így beszélhetünk szervezési intézkedésekben megvalósuló adminisztratív védelemről, amely az adat védelmének legkülső körét, a szervezet (adatkezelő, adatfeldolgozó) és a szervezetet körülvevő környezet szabályozását, vezetését jelenti.

A fenti normaszöveg említést tesz az eljárási szabályokban megnyilvánuló védelmi intézkedésekről. Ide tartoznak a szervezetek (adatkezelők és adatfeldolgozók) által megalkotott titok- és adatvédelmi, valamint adatbiztonsági szabályzatok.

A normaszöveg által említett harmadik védelmi módszer a technikai, műszaki védelem. Ezt a módszert két részre oszthatjuk: fizikai és logikai védelemre. A fizikai védelem körébe vonhatók az adatot közvetlenül körülvevő tárgyiasult tényezők, így a környezeti infrastruktúra, épületek, helyiségek, vezetékek, hardverek, adathordozók, dokumentumok védelme. A logikai védelem körébe az adatok, a szoftverek, valamint a kommunikáció védelmét sorolhatjuk.

Végül külön érdemes foglalkozni az informatikai biztonsági rendszerek leggyengébb láncszemével, az emberrel. Ide sorolhatjuk azokat a védelmi módszereket, amelyek az emberek megbíizhatatlanságával, pontatlanságával szemben védik az adatokat. Ide tartozik különösen a teljesítménykövetés,[13] valamint az emberek gyengeségére alapuló hackertámadások elleni védelmi módszerek. Ezeket a humán védelem kategóriájában foglalhatjuk össze.

A védelmi módszereket a későbbiekben részletezni fogom.

Az adat biztonsága egyenes arányban áll az adat védelmével és fordított arányban a kényelemmel. Ebből következik, hogy annál nagyobb az adat biztonsága, minél hatékonyabb annak védelme. Így kijelenthetjük, hogy a teljes biztonság (ha ez egyáltalán elérhető a gyakorlatban) a felhasználók számára nagy kényelmetlenséggel járna, viszont, ha az informatikai rendszerek kényelmes használata a cél, akkor le kell

13 Természetesen a 36/2005. (X. 5.) AB határozat figyelembevételével.

mondanunk a védelemről.[14] Ez az elv valójában az információs rendszer használhatósága és az adat, az adatalany védelme közötti kapcsolatot jelzi. Az adatbiztonságot úgy kell kialakítani, a védelmi módszereket, intézkedéseket úgy kell megválasztani, hogy mind az adatalany, mind az adat védelme megvalósuljon, azonban a szükséges intézkedések ne tegyék nehézkessé, lassúvá, esetleg lehetetlenné az informatikai rendszer mindennapos használatát. Ennek ellenére a törvény szövegéből következik, hogy ha sorrendiséget kellene felállítani, elsőbbséget kap az adatalany magánszférájának biztonsága, majd a személyes adatok védelme, aztán az egyéb adatkörök, titokkörök védelme és legutolsó sorban következne az ezek megvalósítására vonatkozó eszköztár, az adat biztonsága. Másképp fogalmazva, az adatalany védelmével járó követelmények határozzák meg az adat védelmének eszközeit és nem fordítva.

Ez a tétel azonban nem mindig igaz. Az Infotv. nem tartalmazza azt az ár--érték, pontosabban kár--érték deklarációt, amely az Adatvédelmi Irányelvben jelent meg: „Tekintettel a technika vívmányaira és alkalmazásuk költségeire, ezen [adatbiztonsági] intézkedéseknek olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatkezelés által jelentett kockázatoknak és a védendő adatok jellegének."[15] A védendő adatok jellege szerinti adatbiztonság azt jelenti, hogy a különböző adatkörök és titokkategóriák között egyfajta sorrendiséget kell felállítani a védelem erőssége szempontjából. Néhány kérdést még így sem lehet eldönteni, például az állam titka vagy a magánszféra titka érdemel-e erősebb védelmet. Azért ennek ellenére a magyar jogi szabályozásból is kirajzolódik valamiféle sorrendiség. Így kijelenthetjük, hogy a személyes adatok védelménél erősebb védelmi intézkedéseket kell alkalmazni a különleges adatok és az egészségügyi személyes adatok esetén.

14 Peter Norton – Mike Stockman: *A hálózati biztonság alapjairól.* Kiskapu Kiadó, Budapest, 2000. 10. p.

15 Adatvédelmi Irányelv, 17. cikk (1)

Viszont ugyancsak nem dönthető el például az sem, hogy a közérdekű adatok a személyes adatokkal egyenlő, erősebb vagy pusztán csak másfajta védelemben részesülhetnek.

Az Adatvédelmi Irányelv alapján az adatkezelés által jelentett kockázatokat is figyelembe kell venni az adatbiztonság kialakításakor, azaz a lehetséges támadások, támadási felületek nagyságát és a támadással bekövetkezhető kár mértékét is. Tehát végtelen pénz elköltésével akár végtelen biztonság is elérhető, legalábbis elméletben. Az Adatvédelmi Irányelv szerint az adatbiztonságra csak annyi pénzt érdemes elkölteni, amennyi legfeljebb a bekövetkezhető kár nagysága. Ez azonban ismét hasonló kérdéseket vet fel, mint amelyeket az előző bekezdésben tettem fel: Mennyi az adat pénzben kifejezett értéke? Értékesebb-e a személyes adat, mint az államtitok? (Amerikai privacy-védők részéről történnek kísérletek arra, hogy az adat, a személyes adat valódi, piaci értékét megállapítsák, és az interneten elérhető adat-érték kalkulátorokkal nyilvánossá és kiszámíthatóvá tegyék.[16])

Mivel a jogszabály nem definiálja a kár–érték arányt, így azt a gyakorlat kényszeríti ki. „A védelem kialakítása során felmérésre, elemzésre kerülnek a kockázati tényezők, lehetséges támadások és azok várható kockázata is. A következő lépés ezek módszeres megszüntetése. Az összes kockázat megszüntethető, így gyakorlatilag végtelen biztonság is elérhető, de ennek végtelen ára van. Csakhogy a felhasználók nem költenek többet rendszerük védelmére, mint amennyit az valójában ér. A gyakorlati megvalósítás során elért és a tökéletes biztonság közötti rést maradványkockázatnak nevezzük, amelynek létezését és esetleges következményeit a rendszer tulajdonosának és üzemeltetőjének tudomásul kell vennie."[17]

16 http://www.gportal.hu/gindex.php?pg=198341 – letöltve: 2011.10.27.
A személyes adatok értékét kiszámító kalkulátor a http://turbulence.org/Works/swipe/swipe_data_cal.html weblapon érhető el. Letöltve: 2011.11.05.

17 Az idézet Virasztó Tamás: *Titkosítás és adatrejtés. Biztonságos kommunikáció és algoritmikus adatvédelem* c. könyvének mottója. NetAcademia Kft., Budapest, 2004.

2.1. Informatikai biztonsági kockázatok – a közelmúlt eseményeinek tükrében

2.1.1. 2007. Észtország[18]

Észtország fővárosában és észak-keleti részében 2007. április 26–28. között az észt kormány intézkedése – „Tallin felszabadítóinak szovjet emlékműve" áthelyezése – miatt zavargások kezdődtek. Ezt követően rendszeres internetes támadásokat szerveztek az Észt Parlament, bankok, minisztériumok, illetve újságok és elektronikus hírközlők honlapjai ellen. A cél a weboldalak blokkolása és a hivatalos kommunikációs vonalak elvágása volt. Ezek mellett az interneten propagandaüzenetekben szólítottak fel fegyveres ellenállásra és további erőszakra.

Mi sem jelezte jobban a cselekmény súlyosságát, mint az, hogy az észt hálózaton az adatforgalom sokszor órákon át a normális ezerszerese volt. Az ország internetes forgalmát irányító központok naponta többször leálltak a túlterhelés miatt, az állami szervek hálózatait le kellett választani az internetről. A banki rendszerek megbénultak, a pénzügyi tranzakciók rendszeresen akadoztak.

Május 15-én a tömeges internetes támadások miatt az ország második legnagyobb bankjának fel kellett függesztenie azon szolgáltatásait, hogy külföldről is el lehessen érni a pénzintézet egyes rendszereit. Egy másik bank nyilvánosságra hozta a támadások miatti veszteségeit: több mint 1 millió dolláros forgalomkiesést szenvedett el.

Az elemzők szerint az akciók túlságosan is jól össze voltak hangolva ahhoz, hogy mind-össze néhány rosszindulatú programozót feltételezzenek a háttérben. Néhány támadást sikerült orosz szerverekig visszavezetni, sőt, az Európai Parlament állásfoglalása szerint a támadások

18 Muha Lajos: *Kiberháború az orosz–észt viszony kapcsán*. Hacktivity 2007 Konferencia, Budapest, Magyarország, 2007. 09. 22–23. p.

az orosz közigazgatás IP címeiről érkeztek, de az alkalmazott technika miatt nehéz meghatározni a pontos forrásokat.[19]

A beavatkozást sem az észtek, sem az EU, sem a NATO nem minősítette katonai akciónak.

2.1.2. 2008. Grúz–orosz háború

2008 augusztusában kitört a grúz–orosz háború Dél-Oszétia hovatartozása miatt. A háború során mindkét fél intenzív információs csatát is vívott, az internetet is felhasználva, annak ellenére, hogy az infrastruktúra igen szegényes volt, az online tájékoztatás kiiktatását elsődleges fontosságúnak tartották. A grúz kormány lehetetlenné tette az orosz weboldalak elérését Grúziából, és a háború részvevőinek weboldalai folyamatos hacker-célpontok voltak, tehát mindkét fél bevetette ezt az eszközt.

2.1.3. 2009. Dél-Korea

2009 júliusában dél-koreai magán- és kormányzati oldalak ellen indult összehangolt támadás. A célpontok hírportálok, a közigazgatás, bankok honlapjai, online aukciós oldalak, az országban állomásozó amerikai csapatok honlapjai voltak. Feltételezések szerint egy észak-koreai vagy egy vele szimpatizáló kisebb hackercsoport állt a támadás mögött.[20] Tanulság: néhány ember különösebb hadászati tudás nélkül is képes károkat, fennakadásokat okozni egy informatikailag fejletlen államnak.

19 Muha Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme.* (Doktori értekezés) 2007. 50. p.

20 Kovács László – Krasznay Csaba: *Digitális Mohács. Kibertámadási forgatókönyv Magyarország ellen.* Hadmérnök, IV. évfolyam, 2009/4. (december)

2.2. Kritikus infrastruktúra

A kritikus infrastruktúra fogalma a 2080/2008. Kormányhatározat[21] szerint a következő: „Kritikus infrastruktúra alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra-elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt, minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában." A kritikus információs infrastruktúra az Európai Unió Zöld Könyve[22] szerint „azon infokommunikációs rendszerek, melyek magukban kritikus infrastruktúrák, vagy ilyenek működéséhez elengedhetetlenül szükségesek".

A kormányhatározat 10 ágazat 43 alágazatát sorolja a kritikus infrastruktúrák közé, melyek mindegyike kivétel nélkül, kisebb vagy nagyobb mértékben függ az információs rendszerektől.

Kovács László és Krasznay Csaba *Digitális Mohács* című forgatókönyve a következő sorrendben határozza meg a megtámadni kívánt célokat:

- elektronikus média;
- műsorszórás;
- internetes média;
- pénzügy – beleértve a közigazgatási rendszerek kapcsolatát a Magyar Államkincstárral;
- közlekedés;

21 http://pvir.bm.hu/jog/File/2080_2008%20Korm.%20hat.doc, 4. oldal – letöltve: 2011.10.28.

22 Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, 7. p. – http://eur-lex.europa.eu/LexUriServ/site/hu/com/2005/com2005_0576hu01.pdf – letöltve: 2011.10.28.

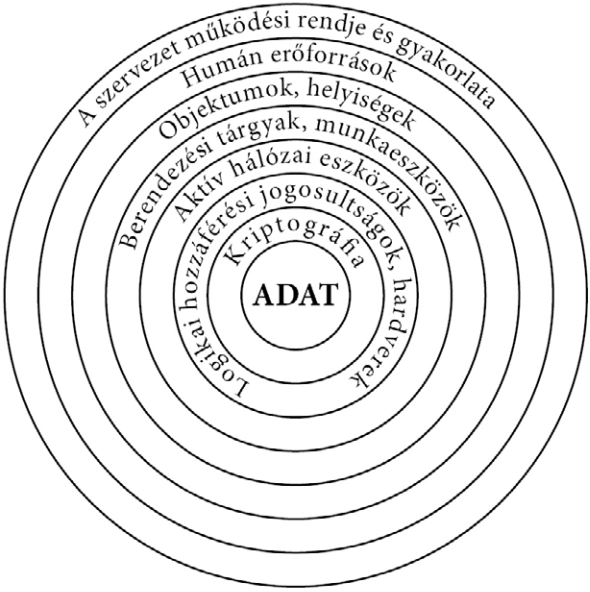
- telekommunikáció;
- internet;
- villamosenergia-szolgáltatás.

Ezekből következik, hogy a magyar közigazgatás intézményeinek jelentős része kritikus infrastruktúrának minősül, de mindenképpen függ tőle. Fontos, hogy ezen intézmények rendelkezzenek a szükséges védelmi módszerekkel – nem csak a kibertámadások ellen!

■ ■ ■

3. Az informatikai biztonsági környezet

Az adat védelmére tett technikai, műszaki, szervezési és eljárási intézkedések az informatikai biztonsági környezetben érvényesülnek. Az adat felől közelítve az informatikai biztonsági környezet fogalmát, ide tartozik valamennyi, az adatot logikailag és fizikailag körülvevő eszköz, tárgy, objektum, intézkedés stb.



1. ábra: Informatikai biztonsági környezet[23]

23 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 91. p.

Ha az informatikai biztonsági környezet helyesen van kialakítva, elemei az adat körül héjszerűen, körkörösen helyezkednek el. (Lásd: 1. ábra.) A külső kört a szervezet (adatkezelő, adatfeldolgozó) működési rendje és gyakorlata alkotja. Ide tartoznak például a szervezeti működés kialakításának kérdései és mindazok a szervezési feladatok, amelyek belső tényezőktől függenek. A második kört a humán erőforrások alkotják; itt találhatók a megbízhatósággal, teljesítménykövetéssel kapcsolatos védelmi intézkedések. A harmadik kört az objektumok, helyiségek alkotják. Itt az adat – és tegyük hozzá: a vagyon – védelme érdekében megvalósítandó belépés- és mozgás-ellenőrzési intézkedések, vagyon- és személyvédelmi intézkedések, természeti csapások elleni intézkedések vannakk. A negyedik kört a helyiségeken belül elhelyezett berendezési tárgyak és munkához szükséges eszközök alkotják, s itt sorakoznak az adat fizikai tárolásával kapcsolatos védelmi intézkedéseksorakoznak. Ennél beljebb már az adatforgalmat közvetlenül lebonyolító, aktív hálózati eszközöket és egyéb hardvereket találjuk. E körben a fizikai és logikai hálózatvédelem és a számítógépek fizikai és logikai védelme valósul meg. A hatodik körben a védelmi módszerek már az adat logikai védelmét szolgálják a különböző rendszerekhez, szoftverekhez, illetve magához az adathoz való hozzáférési jogosultságok meghatározásával. A legbelső kör az adat védelme érdekében magával az adattal végzett műveleteket jelenti; itt a kriptográfia eszközeit alkalmazzák.

3.1. Bizalmasság, sértetlenség és rendelkezésre állás

A Közigazgatási Informatikai Bizottság (KIB) 25. számú ajánlása[24] a következőképp definiálja az informatikai biztonságot és a hozzá kapcsolódó fogalmakat:

24 A KIB 25. számú ajánlása, 23–24. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

3.1.1. Informatikai biztonság

Az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az infokommunikációs rendszerben kezelt[25] adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Egyszerűsítve: az informatikai rendszerekben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme.

3.1.2. Bizalmasság

Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

3.1.3. Sértetlenség

Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

3.1.4. Rendelkezésre állás

Az informatikai rendszerelem – ide értve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a szükséges időben és időtartamra használható.

25 Az adatok kezelése az alkalmazott eljárástól függetlenül: adatok gyűjtése, felvétele, tárolása, feldolgozása (megváltoztatás, átalakítás, összegzés, elemzés stb.), továbbítása, törlése, hasznosítása (ideértve például a nyilvánosságra hozatalt is) és felhasználásuk megakadályozása.

3.1.5. Zárt védelem

Zárt a védelem, ha az összes releváns fenyegetést figyelembe veszi.

3.1.6. Teljes körű védelem

Teljes körű a védelem, ha az informatikai rendszer összes elemére kiterjed.

3.1.7. Folytonos védelem

Folytonos a védelem, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

3.1.8. Kockázattal arányos védelem

A kockázatokkal arányos a védelem, ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

A továbbiakban az egyszerűsített meghatározást fogom használni.

Az bizalmasság, sértetlenség és rendelkezésre állás elveit az adatot körülvevő biztonsági környezet valamennyi körében érvényesítik. Ezt könnyű belátni. Vegyük például egy egyetem tanulmányi rendszerét. Tegyük fel, hogy csak a bizalmasság elve nem teljesül. Ez azt jelentené, hogy bárki hozzáférhetne a felhasználók (oktatók, hallgatók, tanulmányi hivatal munkatársai stb.) személyes adataihoz, és jogosultságaival (vissza)élhetne.

Ha csak a sértetlenség elve nem teljesülne, akkor nem lehetne megbízni például abban, hogy a vizsgán megszerzett érdemjegy nem fog-e „véletlenül" megváltozni vagy törlődni. Ugyanez lenne a helyzet a személyes adatokkal kapcsolatban is.

Ha csak a rendelkezésre állás elve nem teljesülne, akkor semmit sem érne a tanulmányi rendszer, ha vizsgára jelentkezéskor folyton leállna a túl sok konkurens felhasználó miatt.

A példa ne vezesse félre az Olvasót, a bizalmasság, sértetlenség és a rendelkezésre állás elve nem csak az információtechnológiai eszközökön alkalmazandó, hiszen az informatikai biztonság fogalma technológia-semleges, az informatikai biztonsági környezet összes elemére érvényes. Ezt a későbbi példáknál látni fogjuk.

Könnyen megérthetjük, hogy nem emelhetjük ki egyik elvet sem a többi közül, nem tehetjük fontosabbá egyiket a másiknál, hiszen ha csak bármelyik sérül, már nem beszélhetünk a biztonság állapotáról.

Ha az informatikai biztonsági környezet valamely eleme olyan állapotban van, hogy fennáll a bizalmasság, a sértetlenség vagy a rendelkezésre állás sérülése, akkor az adott elem a fenyegetettség állapotába került.

A fenyegetettség állapota az informatikai biztonsági környezetben mindig valamilyen veszélyforrásból kiindulva következik be. A veszélyforrás jelentkezhet az informatikai biztonsági környezeten belül, például lehet valamilyen nem kellően megszervezett vagy végrehajtott védelmi intézkedés, cselekmény, hibásan működő hardver vagy szoftver, a valóságnak meg nem felelő (esetleg módosított) adat, az adatkezelési tevékenység ellátására alkalmatlan objektum vagy helyiség, bizalmasságában sérült humán erőforrás. A veszélyforrás azonban eredhet az informatikai biztonsági környezeten kívülről is, így lehet valamilyen külső ráhatás, természeti csapás, robbanás a szervezet működési környezetében stb. Ezek a külső veszélyforrások általában a vis maior kategóriájába tartoznak ugyan, az adatbiztonság azonban éppen arra irányul, hogy az adatokat ezek egy része ellen is védje.

A fentebb röviden vázolt veszélyforrásokról és az azok elleni védekezésről szólnak a következő fejezetek.

■ ■ ■

4. Szervezeti és működési veszélyforrások, védelmi módszerek

A szervezeti és működési veszélyforrások a szervezet működési rendjében és gyakorlatában keresendők. E tényezők közül tekintsük át a legfontosabbakat az alábbiakban.

Az egyik alapvető veszélyforrás a biztonsági szervezet hiánya vagy elégtelen kialakítása. Ha nincs a szervezeten belül elkülönült, az adatbiztonságért felelős egység vagy személy, a védelmi intézkedések is elmaradnak, vagy kellő összehangolás és megtervezés hiányában elszigetelt projektekben valósulnak meg. Ilyen módon veszélynek vannak kitéve az adatok és az adatalanyok is, hiszen a szervezet nincsen felkészülve egy esetleges támadásra.

Szintén komoly veszélyforrást jelenthet az, ha van ugyan biztonsági szervezet, de az diszfunkcionálisan működik, mert nincs megfelelően kialakítva. Ilyen gyakran előforduló alapvető hiba, hogy a biztonsági szervezet nem a megfelelő szinten helyezkedik el a szervezeti hierarchiában, esetleg nem is valamelyik adatbiztonsággal kapcsolatos szervezeti egység alá van rendelve. Ilyen módon a befolyását nem tudja kiterjeszteni az egész szervezetre, és így ez a megoldás nem teszi lehetővé összehangolt védelem, egységes szervezeti védelmi reakciók kialakítását.

A szervezet működési rendjében és gyakorlatában rejlő veszélyforrásként fogalmazhatók meg a titokvédelmi és iratkezelési hiányosságok (beleértve az elektronikus dokumentumok kezelésének rendjét is). Ezek a veszélyforrások akkor jelentkeznek, ha a szükséges titokvédelmi és iratkezelési szabályzatok nincsenek kidolgozva, így a különböző

titokkategóriák kezelése ad hoc módon, elszigetelt megoldásokkal történik. Ekkor az adatkezelés jogi, hozzáférés-jogosultsági és adatbiztonsági menete nem illeszkedik bele a szervezeti működés napi rutinjába, nem válik mindenre kiterjedő tevékenységgé.

Talán még ennél is súlyosabb veszélyforrást jelent az, ha ki vannak ugyan dolgozva a szükséges szabályzatok, azonban az adott intézmény dolgozói nem tartják be azokat egy helytelen, de a számítógép-használók körében annál inkább elterjedt gondolkodásmód következtében: „Miért védjem az adatokat, ki az, aki engem meg akarna támadni?" Ez a gondolkodásmód a humán erőforrások bizalmasságának és rendelkezésre állásának sérülésén keresztül hat a szervezet napi működési gyakorlatára, és egyúttal befolyásolja az adat biztonságát.

Ami az iratkezelési rendet illeti, egyaránt kell figyelnünk a hagyományos, papíralapú, valamint az elektronikus iratok kezelésére. A hagyományos iratok kezelésénél a legnehezebb rész a védendő adatokat tartalmazó iratok tárolásának, illetve megsemmisítésének rendje. A fenyegetettség állapotát idézheti elő ugyanis az iratokban található adatok jellegének meg nem felelő tárolási mód és az iratmegsemmisítés helytelen gyakorlata is (például a megsemmisítendő iratokat kiteszik a folyosóra, vagy egyszerűen kidobják a szemétbe).

Fontos megemlíteni a harmadik felekkel kötött szerződésekből eredő veszélyforrásokat. Ilyen szerződések általában az információs rendszer fejlesztésére (például új szoftverek, hardverek telepítése), az informatikai biztonsági környezet elemeivel való műveletvégzésre (például új klímaberendezést kap a szerverszoba) vagy adatfeldolgozásra vonatkoznak. Ezen szerződések támadási lehetőségét kínálnak akkor, amikor nem határozzák meg kellőképpen, azaz a védendő adatok jellegének megfelelően a teljesítő félnek az informatikai biztonsági környezetbe való fizikai és logikai belépési és hozzáférési jogosultságait, vagy nem rögzítik egyértelműen és a teljes műveletre kiterjedően az adatfeldolgozás kereteit.

4.1. A helyi biztonsági felügyelet / biztonsági vezető

Az informatikai biztonság olyan felelősség, amelyben egy intézmény vezetésének valamennyi tagja osztozik. Mivel a szervezetet érintő összes szervezési intézkedésről a vezetés dönt, az adatvédelemért, az adatbiztonságért felelős szervezeti egységet (kisebb szervezetnél ez alatt az adatvédelmi és adatbiztonsági felelőst) közvetlenül a szervezet vezetője alá kell rendelni. A védelemért felelős szervezeti egységnek (helyi biztonsági felügyeletnek) az adatvédelmet és az adatbiztonságot együttesen, egymásra tekintettel kell érvényesítenie, semmiképpen sem emelheti az adatbiztonságot az adatalany védelme fölé. Ezért a védelemmel foglalkozó szervezeti egység olyan szakembergárdából kell, hogy álljon, ahol egyformán művelik mindkét tudományterületet (tehát az adatvédelmi joghoz is értenek és az adatbiztonsághoz is). A valóság az, hogy ilyen szakemberekből ma még igen kevés áll rendelkezésre, ezért többnyire az egyik, illetve a másik szakterülethez értő szakembereket alkalmaznak, akiknek együttes döntése alapján alakul ki a szervezet adatvédelmi és adatbiztonsági stratégiája és technikája.

A minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.) szerint „a minősített adatot kezelő szervnél a minősített adat védelmével kapcsolatos feladatok végrehajtását és koordinálását a minősített adatot kezelő szerv vezetője által kinevezett biztonsági vezető végzi. Amennyiben a minősített adatok mennyisége indokolja, az ezek védelmével kapcsolatos feladatok ellátására külön szervezeti egységként helyi biztonsági felügyelet is kijelölhető. Ebben az esetben a helyi biztonsági felügyeletet a biztonsági vezető vezeti."[26] A 90/2010. (III. 26.) Kormányrendelet 5. §-a alapján a biztonsági vezetőnek legalább felsőfokú iskolai végzettséggel, a minősített adatok kezelésének vagy védelmének területén szerzett legalább egy év szakmai

26 Mavtv. 23. § (2)-(3)

gyakorlattal, a kezelt minősített adatok minősítési szintjének megfelelő szintű személyi biztonsági tanúsítvánnyal, illetve aláírt titoktartási nyilatkozattal kell rendelkeznie. A biztonsági vezető köteles a biztonsági vezetők részére tartandó képzésen és továbbképzésen részt venni. A személyi biztonsági tanúsítványról az 5. fejezetben olvashatunk bővebben.

A biztonsági vezető legfontosabb feladatai közé tartozik, hogy elkészítse a biztonsági szabályzatot, majd gondoskodjon annak naprakészen tartásáról és betartatásáról,;[27] írásban meghatározza a biztonsági személyzet feladatait,;[28] jegyzőkönyv felvétele mellett évente ellenőrzi a minősített adat védelmére vonatkozó személyi, fizikai, adminisztratív biztonsági rendelkezések megtartását,;[29] kezelje a személyi biztonsági tanúsítványok kiadását, meghosszabbítását és visszavonását.[30] Mindezen kívül a fizikai és az adminisztratív biztonság körébe tartozó feladatai közé tartozik például a biztonságtechnikai rendszerek és eszközök évi karbantartása; a biztonsági tárolók tartalékkulcsainak és a kódoknak az őrzése (ezt rábízhatja másra is); a kódok megváltoztatásának nyilvántartása,;[31] a más szervtől kapott, valamint a saját készítésű, minősített adatot tartalmazó adathordozó ügyviteli érdeket nem képviselő, többes sorszámú példányai megsemmisítésének előzetes jóváhagyása, amennyiben erre a minősített adatot kezelő szerv vezetője felhatalmazta.[32]

A KIB 25. számú ajánlása[33] szerint érdemes létrehozni egy úgynevezett vezetői fórumot, amely szavatolja, hogy a biztonsági kezdemé-

27 90/2010. (III. 26.) Kormányrendelet 58. § (2)
28 90/2010. (III. 26.) Kormányrendelet 28. § (1)
29 90/2010. (III. 26.) Kormányrendelet 6. § (1)
30 90/2010. (III. 26.) Kormányrendelet 10-12. §, Mavtv. 17. § (2)
31 90/2010. (III. 26.) Kormányrendelet 33. § (2)
32 90/2010. (III. 26.) Kormányrendelet 56. § (2)
33 A KIB 25. számú ajánlása, 40–41. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

nyezéseket a vezetés jól érzékelhető támogatása kísérje. Ezen fórum hatáskörébe tartozik:

a) javaslattétel az informatikai vezető testület számára a stratégiai tervezéshez, az informatikai biztonsági célok megfogalmazásához és azok szervezeti integrációjához;
b) az informatikai biztonsági irányelvek és feladatok vizsgálata és jóváhagyása, a megvalósításhoz szükséges humán és anyagi erőforrások biztosítása;
c) az informatikai biztonsági intézkedések teljes körű bevezetésének koordinációja és biztosítása szervezeti szinten;
d) a bevezetett informatikai biztonsági intézkedések, irányelvek hatékonyságának folyamatos felülvizsgálata;
e) az információs erőforrások súlyos veszélyhelyzeteknek való kitettségében bekövetkező jelentős változások nyomon követése;
f) az informatikai biztonsági események nyomon követése;
g) az informatikai biztonság fokozását szolgáló jelentős kezdeményezések jóváhagyása;
h) az Informatikai Biztonsági Vezető személyének kijelölése, feladat- és hatáskörének meghatározása;
i) az informatikai biztonsági tudatosság fenntartása a szervezetnél (például felhasználói tanfolyamok szervezésével, illetve könnyen értelmezhető, csak az eszenciákat tartalmazó informatikai biztonsági „kisokos” kiadásával).

A szervezeten belül érvényesülő informatikai védelem alapvető dokumentuma az adatvédelmi és adatbiztonsági szabályzat. Ez a dokumentum azokat a rendszabályokat tartalmazza, amelyek mentén a szervezet működése szerveződik az informatikai védelem és az informatikai biztonság terén, és amelynek a fenti ajánlás szerint legalább az alábbiakra ki kell térnie:

a) a szervezet vezetésének egyértelmű nyilatkozata az informatikai biztonság szabályozott kialakítására, illetve fenntartására;

b) az informatikai biztonság alapvető fogalmaira;
c) az informatikai biztonsággal kapcsolatos feladat- és hatáskörökre, felelősségekre, a biztonsági események jelentésének rendjére;
d) elvek, követelmények, kötelező eljárások, szabványok.

E dokumentumban ugyancsak szabályozni kell az adatokhoz való hozzáférés jogi és technikai feltételeit, úgy, hogy a műszaki megoldásokat a jogszabályok érvényesítése szolgálatába állítják. Ennek keretében rendelkezni kell az informatikai biztonsági környezet elemeiről és azok védelméről is.

Mindannyian tudjuk, hogy egy szabályzat annyit ér, amennyit betartanak belőle, ezért nagy szükség van az adatvédelmi és adatbiztonsági tudatosság növelésére, amelyre kiváló eszköz a már említett tanfolyamok rendszeres szervezése.

A harmadik felekkel kötött szerződések esetében előre meg kell egyezni az alkalmazott védelmi intézkedésekben, és meg kell határozni a védelmi intézkedéseket. A külső személynek adott hozzáférés további részvevőket is magában foglalhat, ezért a szerződésnek az ilyen hozzáférésekre is ki kell térnie, tartalmaznia kell a hozzájárulást más résztvevőkre, továbbá meg kell határoznia a számukra engedélyezett hozzáférés feltételeit.

■ ■ ■

5. Humán veszélyforrások és védelmi módszerek

Az informatikai biztonsági környezetben a humán veszélyforrások két irányból jelentkezhetnek: Egyrészt belülről, amely esetben a humán erőforrások bizalmassága, sértetlensége és rendelkezésre állása sérül. Másrészt viszont humán veszélyforrásnak tekinthetjük a kívülről eredő, az informatikai biztonság kedvező állapotának megváltoztatását célul kitűző szándékos emberi magatartásokat, cselekményeket.

A belülről jelentkező veszélyforrások alapja általában a nem megfelelő szintű adatvédelmi és adatbiztonsági tudatosság, amelynek következményei az adatvédelmi és adatbiztonsági szabályok be nem tartása, a veszély túlzott lekicsinylése, ilyen módon a túlzott biztonságérzet kialakulása („Miért pont engem támadnának meg?" – gondolkodásmód). Ebből erednek a korántsem csak legendákban szereplő sárga cetlik, amelyek a jelszavakat tartalmazzák, és jól láthatóan virítanak a számítógépek monitorán vagy kevésbé jól láthatóan a fiókokban. Ez a magatartás teret enged a kívülről eredő humán veszélyforrásoknak is.

Ennél is súlyosabb belső veszélyforrásnak tekinthető, ha maga a felhasználó fordul az informatikai biztonsági környezet valamelyik eleme ellen. Itt külön kell választani a véletlen (de nem vétlen) és szándékos károkozást. A gondatlanságból elkövetett károkozás általában valamilyen szervezési hibára vagy inkompetenciára vezethető vissza (például ha elhanyagolják a leendő munkavállalók megbízhatóságáról, tudásáról, informatikai előéletéről való megfelelő meggyőződést). Sajnos, gyakrabban fordul elő, hogy az – esetleg elbocsátott – alkalmazott valamely okból bosszúból vagy nyereségvágyból fenyegeti az informatikai biztonsági környezet elemeinek biztonságát.

Az informatikai biztonsági rendszeren kívüli humán veszélyforrások közé szokták sorolni a tömegjelenségeket, például a megmozdulásokat 2006 őszén Budapesten vagy 2011 augusztusában Londonban. E jelenségek értékelése túlmutat az informatikai biztonsági környezeten, amelyhez a politikai, társadalmi alaprendszer elemzésére lenne szükség, amit viszont nem e tankönyv hivatott megtenni. Véleményem szerint az ilyen fajta jelenségek ritkák, de ezekre is válaszreakciókkal kell rendelkeznie egy szervezetnek.

Szintén a kívülről eredő humán veszélyforrások közé sorolhatjuk azokat a szándékos emberi magatartásokat, amelyek egy informatikai biztonsági környezetben fennálló biztonsági kedvező állapot megváltoztatására irányulnak. A szakirodalom eltérő értékelést ad és különböző elnevezéseket használ ezekre a cselekedetekre és az elkövetők személyére is. Korántsem a teljesség igényével emeljünk ki három elkövetői kört, illetve tevékenységfajtát.

- **Hacking, hacker:** A hacker tevékenysége általában nem közvetlenül pusztításra, rombolásra irányul, hanem pusztán arra, hogy bebizonyítsa, valamely adatbiztonsági intézkedés nem állja meg a helyét az informatikai biztonsági környezetben, azaz nem alkalmas a biztonság kedvező állapotának a tartós fenntartására.[34] A hackinghez általában nem kapcsolódik nyereségvágy, de bőséges példát találunk az ellenkezőjére is.
- **Cracking, cracker:** A cracker olyan, a számítástechnikához magas színvonalon értő személy, aki tudását elsősorban a saját céljaira használja fel, visszaél vele, és másokat károsít meg. Számítógépekre hatol be jogtalanul, adatokat szerez meg és használ fel elsősorban anyagi javakért, esetleg társai elismerésének reményében. A cracker az általa birtokolt információval (például kódok,

34 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 97. p.

jelszavak, titkosítási kulcsok) visszaél,[35] és ezáltal szoftvereket és rendszereket használ illegálisan, adatokat szerez meg és hoz nyilvánosságra, illetve összehangolt támadással nagyobb rendszerek működését lehetetleníti el.

- **Script kiddie:** általában olyan, komoly szaktudással nem rendelkező fiatal gyerekről van szó, aki hackerek által megalkotott eljárások alapján mások által megírt programokat („szkripteket") használ arra, hogy vandálkodjon (például mások hálózati kapcsolatát vagy gépének működését megzavarja, gépekre betörve az ott levő tartalmakat törölje vagy megváltoztassa), számítógépekre illegális hozzáférést szerezzen és annak erőforrásait engedély nélkül használja.[36]

A hacker fogalma azért is érdekes, mert kezdetben nem kapcsolódott hozzá pejoratív jelentés: a számítástechnika hőskorában a hatalmas szakmai tudással rendelkező szakemberek nevezték magukat hackernek. A mai hackerekre is jellemző a hatalmas szakmai tudás, azonban tevékenységük – az informatikai rendszerekbe való behatolás, biztonsági intézkedések kikerülése vagy kiiktatása – bűncselekmény, még akkor is, ha nem irányul közvetlen károkozásra.

A hackerek és crackerek sokszor a humán erőforrások – dolgozók, felhasználók – óvatlanságát használják ki, hogy célt érjenek. Ugyanis igen gyakran nem a technikai, hanem „az emberi esendőség az, amely miatt megszakad az informatikai biztonság védelmi rendszere. A jó szándékú, ám tudatlan alkalmazottakat könnyen kihasználják a hackerek, akik tudják, a háttérből mely szálakat kell mozgatni."[37] Ilyenkor a hacker vagy cracker az informatikai biztonsági környezeten belül lévő emberektől szerez meg adatokat (jelszavakat, kódokat stb.) félre-

35 http://hu.wikipedia.org/wiki/Cracker – letöltve: 2011.10.29.
36 http://hu.wikipedia.org/wiki/Hacker#Script_kiddie – letöltve: 2011.10.29.
37 Jeff Crume: *Az internetes biztonság belülről. Amit a hekkerek titkolnak.* Szak Kiadó, Budapest, 2003. 75. p.

vezetéssel vagy a humán erőforrások bizalmassága, sértetlensége ellen irányuló közvetlen támadással, azaz kényszerítéssel, zsarolással.[38] A félrevezetésre példa, amikor a támadó olyan személynek adja ki magát, aki létezik az informatikai biztonsági környezetben (például rendszergazda, karbantartó, operátor, helpdeskes ügyintéző) vagy azon kívül (például postás, pizzafutár, szerelő). Korunk egyik legnagyobb hackere, Kevin Mitnick is használt ilyen megtévesztő módszereket.[39]

A félrevezetés másik formája, az úgynevezett phising, magyarul adathalászat: személyes adatok ellopása elektronikus módon, törvénytelen cselekedet végrehajtása céljából. A leggyakrabban eltulajdonított adatok: kulcsszavak, bankkártya-adatok. A félrevezetés történhet kéretlen levélben vagy honlapon, és legtöbbször valamilyen félrevezető üzleti ajánlattal, fizetési felszólítással vagy adakozási kérelemmel kezdődik.[40]

Script kiddie-k tevékenységére volt példa a VBS. Kurnyikova vírus.[41] (Az e-mail üzeneteken keresztül terjedő internet-férget Jan de Wit, egy 20 éves holland fiatalember készítette 2000-ben, programozási tudás nélkül. Miután rájött, hogy a vírus elszabadult és az egész világon terjed, 2000 szeptemberében feladta magát a rendőrségen. Csak az FBI 55 amerikai vállalatnál 166 000 dolláros kárt derített fel. A holland bíróság 2002-ben jogerősen – az enyhítő körülményeket is figyelembe véve – 150 órányi közmunkára ítélte a fiatalembert.[42])

38 Peter Norton – Mike Stockman: *A hálózati biztonság alapjairól.* Kiskapu Kiadó, Budapest, 2000. 36–37. p.

39 Erről lásd bővebben: Kazári Csaba: *Hacker, cracker, warez.* Computer Panoráma Kiadó, Budapest, 2003. 51–170. p.

40 http://www.ofe.hu/inet/ofe/hu/fogalmak/fogalom.html?phraseid=2173 – letöltve: 2011.10.29.

41 Szappanos Gábor: *Kirándulás a számítástechnika sötét oldalára.* VirusBuster Kft., Budapest, 2003. 10. p.

42 Létai János: *Elutasították az Anna Kurnyikova-vírus szerzőjének fellebbezését.* HWSW Online informatikai hírmagazin, 2002. október 29., http://www.hwsw.hu/hir.php3?id=18263 – letöltve: 2011.10.29.

A humán védelmi módszerek közül az egyik legfontosabb a leendő munkavállaló megbízhatóságáról való meggyőződés. Ez különösen igaz azoknál a közigazgatási szerveknél, ahol minősített adatok kezelése folyik. A Mavtv. alapján szükséges az érintett munkavállaló nemzetbiztonsági ellenőrzésének lefolytatása. Az ellenőrzés pozitív eredménye „az a tanúsítvány, amely érvényességi idejének lejártáig meghatározza, hogy valamely természetes személy milyen legmagasabb minősítési szintű adat felhasználására kaphat felhasználói engedélyt".[43] „A minősített adat felhasználásához szükséges személyi biztonsági tanúsítvány nem adható ki, illetve a már kiadott tanúsítványt vissza kell vonni, ha a nemzetbiztonsági ellenőrzés alapján készített szakvélemény kockázati tényezőt tartalmaz. A személyi biztonsági tanúsítvány a szakvélemény kiállításától számított 5 évig érvényes."[44]

A munkavállalók megbízhatóságáról a KIB 25. számú ajánlása[45] szerint időben három alkalommal lehet meggyőződni: a leendő munkavállaló alkalmazása előtt, közben és után vagy annak változásakor.

Az alkalmazás előtt: Az emberi hibákból, vétlen vagy szándékos károkozásból, lopásból, illetve az eszközök, létesítmények nem megfelelő használatából eredő kockázatokat mérsékelni kell. A következőket vegyük figyelembe:

a) A biztonsági követelményeket a munkaerő-felvételnél, a szerződésekben, valamint az egyén foglalkoztatása során egyaránt érvényesíteni kell.
b) A munkaerő-felvételi eljárás során – törvényes keretek között – olyan vizsgálatokat kell lefolytatni, melyek egyértelmű képet adnak a jelentkező alkalmasságáról az informatikai biztonság szempontjából. Ez különösen fontos olyan munkakörök esetében,

43 Mavtv. 3. § 11.
44 Mavtv. 10. § (3)
45 A KIB 25. számú ajánlása, 76., 79., 84. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

amelyek kiemelt fontosságúak ezen szempont alapján. Minden munkavállalónak, a rendszerek külső használóinak (a velük kötött szerződés alapján) alá kell írniuk egy titoktartási nyilatkozatot.

c) A munkavállalótól csak olyan nyilatkozat megtétele vagy olyan adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely nem sérti a személyiségi jogait, a munkaviszony szempontjából lényeges tájékoztatást nyújthat, és az érintett írásban hozzájárult.

Valamennyi munkaterületre részletes munkaköri leírást kell készíteni, amely tartalmazza az adott munkaterületre vonatkozó biztonsági követelményeket, egyértelműen megjelölve a kötelességeket és a felelősségeket is.

Fontos, hogy a munkavállalók szerepei, azaz, hogy pontosan miből is áll a munkájuk, terjedelmükben hozzárendelhetők legyenek a munkakörökhöz, és ezáltal el lehessen azokat határolni egymástól, hogy minden munkavállaló csak a szigorúan rá vonatkozó feladatot hajtsa végre.

A ki- és beléptetési folyamatokkal kapcsolatban összehangolt munkára van szükség a humánerőforrás-gazdálkodás és a biztonsági szakértők között, hogy minél tovább fent lehessen tartani a biztonság kedvező állapotát. Ehhez fontos, hogy a hozzáférési jogok pontosan meg legyenek határozva, és érvényre jussanak be- és kilépéskor is.

A felvételi eljárás során a leendő munkatársakat ellenőrző vizsgálatok alá kell vetni, természetesen figyelembe véve az összes ide vonatkozó titoktartási, személyes adatvédelmi és alkalmazáson alapuló jogszabályt. A vizsgálat foglalja magába:

a) az üzleti és személyi referenciák meglétét,
b) a felvételre jelentkező életrajzának ellenőrzését a lehető legnagyobb teljességgel és pontossággal,
c) a legmagasabb iskolai végzettség (szakképzettség) megerősítését,

d) a hatóság által kibocsátott azonosító irat ellenőrzését (személyi igazolvány vagy útlevél),
e) részletesebb ellenőrzéseket, mint például a hitelképesség ellenőrzése vagy erkölcsi bizonyítvány kérése.

Alkalmazni lehet viselkedési szabálygyűjteményt, etikai kódexet is, így meghatározható az alkalmazottak, szerződő felek felelőssége a bizalmasságot, az adatvédelmet, az etikát, a szervezet berendezéseinek megfelelő használatát illetően.

Gyakorlati tapasztalat, hogy egyes nagyvállalatoknál a belépő szocializációs tréningen „esik át" az alkalmazás előtt. Az ilyen tanfolyamokba az informatikai biztonsági oktatást is érdemes beleilleszteni. Az eljárás előnye, hogy az új munkatárs már az első munkanapján teljes tudatában van információvédelmi felelősségének.[46]

Az alkalmazás alatt: Elengedhetetlen, hogy a munkatársak kellőképpen motiválva legyenek arra, hogy betartsák a biztonsági előírásokat. Ha ez nem történik meg, akkor az alkalmazottak és a szerződő felek akaratlanul is jelentős kárt okozhatnak! A helytelen személyzeti politika, a gyenge vezetés a munkatársakat alulmotiválttá teszi; ha a felhasználó nem érzi önnön fontosságát az adott szervezetnél, a szükséges biztonsági intézkedéseket is kevésbé veszi figyelembe. Tapasztalati tény, hogy az a munkatárs, aki nincs kellőképpen motiválva, sokkal több informatikai biztonsági eseményt okoz.

Ennek legegyszerűbb gyakorlati megvalósítása a rendszeres oktatás, ahol naprakész információkkal lehet ellátni a munkatársakat. A szervezetnek ehhez megfelelő képzési tervvel kell rendelkeznie. Azt is érdemes megfontolni, hogy egy éppen induló tevékenység (projekt) igényel-e különleges biztonsági képzést.

46 A KIB 25. számú ajánlása, 79. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

A humán védelem másik fontos eleme olyan jogosultsági rendszer felépítése, amely feladatfüggő, és a szükséges tudás elvére épül. Mind a fizikai, mind a logikai védelem területén ki kell építeni. A feladatfüggés elve azt jelenti, hogy a dolgozók jogosultságai az ellátandó feladathoz, nem pedig a szervezeti hierarchiában elfoglalt helyhez igazodnak. A szükséges tudás elvén pedig azt értjük, hogy a dolgozó a feladatkörön belül is csak akkor kaphat hozzáférést, jogosultságot, ha elegendő ismerettel rendelkezik a jogosultsággal járó műveletek biztonságos elvégzéséhez. Így mindenki csak annyit lát a rendszerből és csak olyan adatokhoz fér hozzá, amelyek feltétlenül szükségesek a munkájának elvégzéséhez, ily módon pedig a lehető legkisebb kárt tudja okozni. Ezt az elvet más néven a legkevesebb jogosultság elvének is nevezik. Egy ilyen jogosultsági rendszer kiépítése magába foglalja a folyamattervezést. Nem történhet meg, hogy egy folyamatot csak egy személy ellenőrizzen és manipuláljon. Például egy könyvelési osztályon más személy fogadja a számlákat, és más kezdeményezi azok kifizetését.

Az alkalmazás megszűnésekor vagy változásakor: A munkaviszony megszüntetése, illetve a szervezeten belüli megváltozása nagyjából azonos biztonsági kategória, mivel mindkettő az éppen használt adatfeldolgozó eszközök és jogosultságok leadásával jár. Láttuk korábban, hogy a munkatársak feladatainak elhatárolása alapvető biztonsági követelmény, éppen ezért a felhasználói jogosultságok megvonása az adott szervezeti területen teljes mértékben indokolt. A cégen belül másik szervezeti egységhez áthelyezett munkatársat ilyen szempontok alapján gyakorlatilag azonosan kell kezelni a kilépő munkatárssal.

Át kell gondolni azokat a felelősségeket és jogi következményeket, amelyek a munkaviszony megszűnését követően még meghatározott ideig érvényesek, például ha a munkavállaló titoktartási nyilatkozatot tett. Ezeket érdemes szerződésben rögzíteni.

Biztonsági szempontból szükséges, hogy a felelős vezetők tudassák az alkalmazottakkal, az ügyfelekkel, a szerződő felekkel a személyzeti

változásokat, és kezdeményezzék a távozó munkatárs ügyfeleket, szerződő feleket érintő jogosultságainak (például belépési engedélyek, távoli hozzáférések) teljes körű visszavonását. Az adatfeldolgozó eszközök hozzáférési jogait minősített esetben akár még a felmondási idő alatt is ajánlatos csökkenteni vagy megszüntetni.

Természetesen ilyen intézkedést csak különféle kockázati tényezők elemzése után hoznak meg:[47]

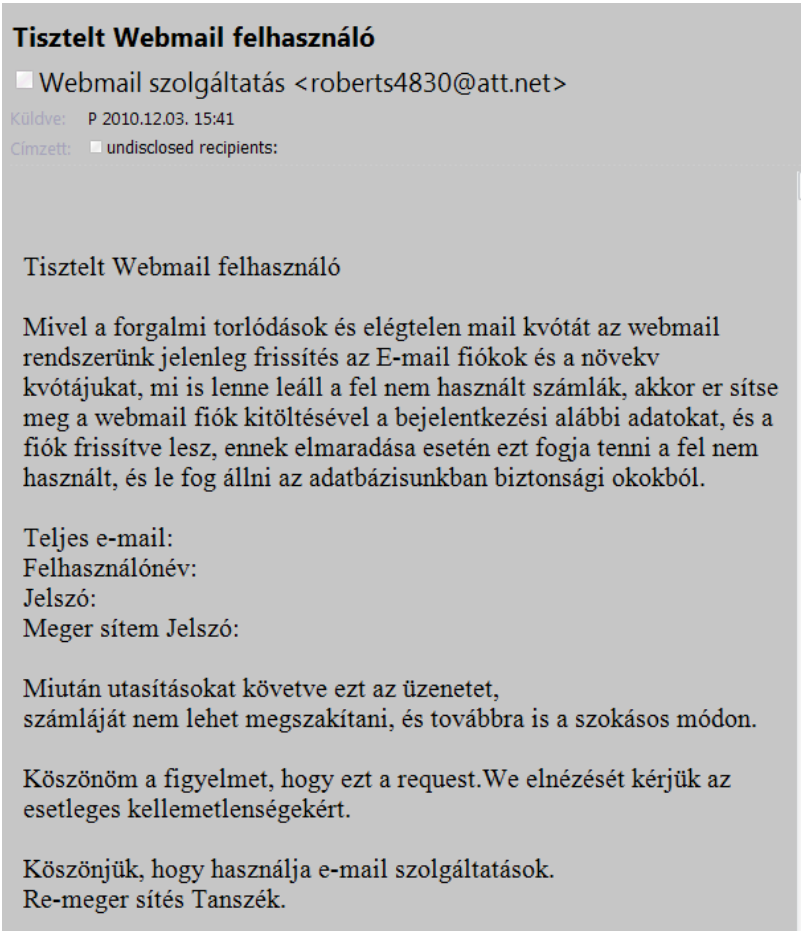
a) Ki kezdeményezte a munkaviszony megszüntetését, és a mi megszűnés indoka?
b) Milyen mértékű az alkalmazott vagy a szerződő fél jelenlegi felelőssége?
c) Mennyi a számára pillanatnyilag hozzáférhető vagyontárgyak értéke?

Az alkalmazott új munkakörbe való helyezésénél érdemes hasonló módon eljárni, mint a munkaviszony megszűnésekor. Fontos, hogy a hozzáférési jogok átadása, megszüntetése mindig dokumentálva legyen!

Adathalászat elleni védelem: Véleményem szerint néhány alapelv betartásával és pár lépés végiggondolásával könnyedén lehet védekezni az adathalászat ellen. A legfontosabb alapelv az, hogy bank, közösségi hálózat, e-mail vagy szolgáltató ***soha nem fog tőlünk írásban vagy írott formában*** jelszót vagy PIN kódot kérni. Ezeket a kódokat gyakorlatilag csak mi ismerjük (rosszabb esetben tároljuk) „szöveges formában". Az informatikai rendszerek ezeket az adatokat kódolva tárolják.

Három példát fogok bemutatni. Az első (lásd: 2. ábra) azt akarja elhitetni velünk, hogy biztonsági frissítés miatt kell megadnunk a felhasználói adatokat, köztük a jelszavunkat is (ráadásul kétszer!).

47 A KIB 25. számú ajánlása, 85–86. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.



Tisztelt Webmail felhasználó

Webmail szolgáltatás <roberts4830@att.net>

Küldve: P 2010.12.03. 15:41

Címzett: undisclosed recipients:

Tisztelt Webmail felhasználó

Mivel a forgalmi torlódások és elégtelen mail kvótát az webmail rendszerünk jelenleg frissítés az E-mail fiókok és a növekv kvótájukat, mi is lenne leáll a fel nem használt számlák, akkor er sítse meg a webmail fiók kitöltésével a bejelentkezési alábbi adatokat, és a fiók frissítve lesz, ennek elmaradása esetén ezt fogja tenni a fel nem használt, és le fog állni az adatbázisunkban biztonsági okokból.

Teljes e-mail:
Felhasználónév:
Jelszó:
Meger sítem Jelszó:

Miután utasításokat követve ezt az üzenetet,
számláját nem lehet megszakítani, és továbbra is a szokásos módon.

Köszönöm a figyelmet, hogy ezt a request.We elnézését kérjük az esetleges kellemetlenségekért.

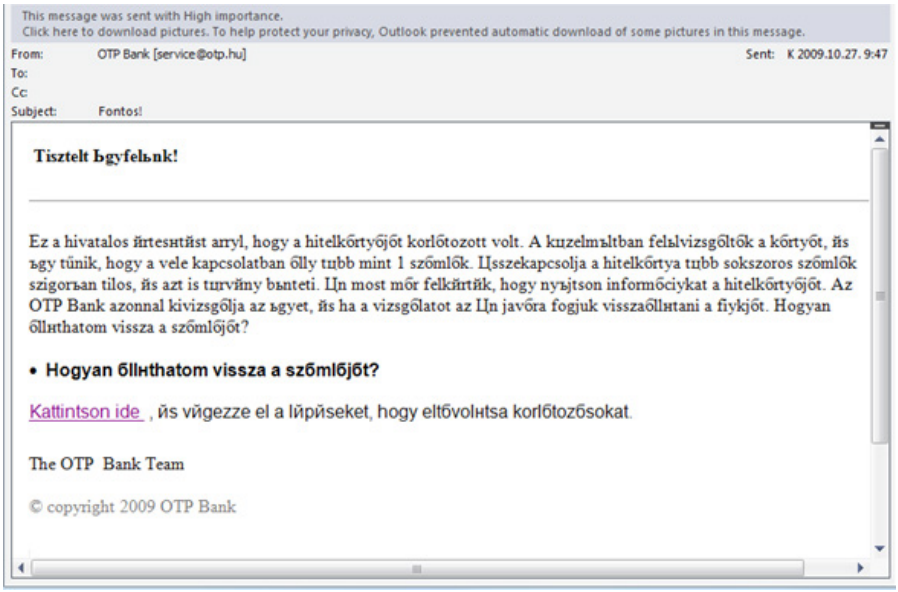
Köszönjük, hogy használja e-mail szolgáltatások.
Re-meger sítés Tanszék.

2. ábra: E-mail adathalász példa

Ez a levél elég hamar „megbukik”, ugyanis a küldő e-mail címe nem arra utal, hogy a levelezésszolgáltató címe lenne, illetve gondok vannak a magyarságával. Látszik rajta, hogy valamilyen fordítóprogrammal készült. Ekkor már mindenképp gyanút kell fognunk, és érdemes azonnal törölni a levelet.

A második példa „klasszikus" banki adathalász levél (lásd: 3-4. ábra). Itt az e-mail cím akár hihető is lehetne, de a levél szövegében sok gyanús karakter van (cirill betűk), és a nyelvhelyesség is hagy kívánnivalót maga után. Ilyen jellegű leveleknél soha ne kattintsunk a levél által megadott linkre, mert már maga a weboldal is kártékony kódokat tartalmazhat. Az ilyen weboldalaknak az a céljuk, hogy a meghatározott szövegmezőben adjuk meg a jelszavunkat, és a Belépés gombra kattintva küldjük az adathalászoknak.

A 4. ábrán látszik a levél által hivatkozott weboldal, amely hasonlít a bank eredeti oldalára. Ilyenkor érdemes ellenőrizni a webcímet, és abból látszódni fog, hogy az valójában nem a bank oldala.


This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: OTP Bank [service@otp.hu] Sent: K 2009.10.27. 9:47
To:
Cc:
Subject: Fontos!

Tisztelt Ьgyfelьnk!

Ez a hivatalos йrtesнtйst arryl, hogy a hitelkбrtyбjбt korlбtozott volt. A kцzelmъltban felьlvizsgбltбk a kбrtyбt, йs ъgy tűnik, hogy a vele kapcsolatban бlly tъbb mint 1 szбmlбk. Цsszekapcsolja a hitelkбrtya tъbb sokszoros szбmlбk szigorъan tilos, йs azt is tцrvйny bьnteti. Цn most mбr felkйrtйk, hogy nyьjtson informбciykat a hitelkбrtyбjбt. Az OTP Bank azonnal kivizsgбlja az ъgyet, йs ha a vizsgбlatot az Цn javбra fogjuk visszaбllнtani a fiykjбt. Hogyan бllнthatom vissza a szбmlбjбt?

- **Hogyan бllнthatom vissza a szбmlбjбt?**

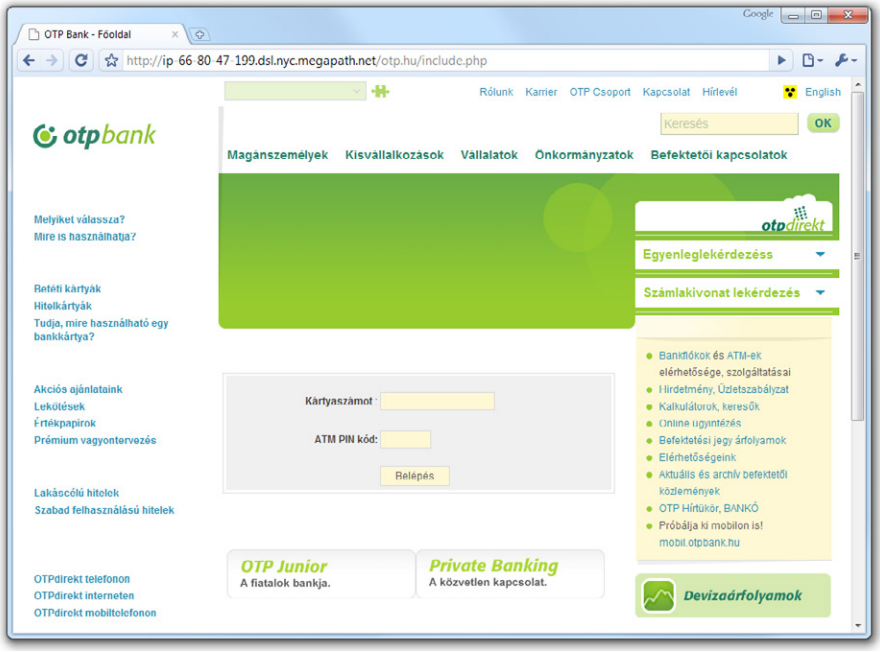
Kattintson ide , йs vйgezze el a lйpйseket, hogy eltбvolнtsa korlбtozбsokat.

The OTP Bank Team

© copyright 2009 OTP Bank

3. ábra: Banki adathalász levél[48]

48 http://spamblog.hu/wp-content/uploads/2009/10/image7.png – letöltve: 2011.11.04.

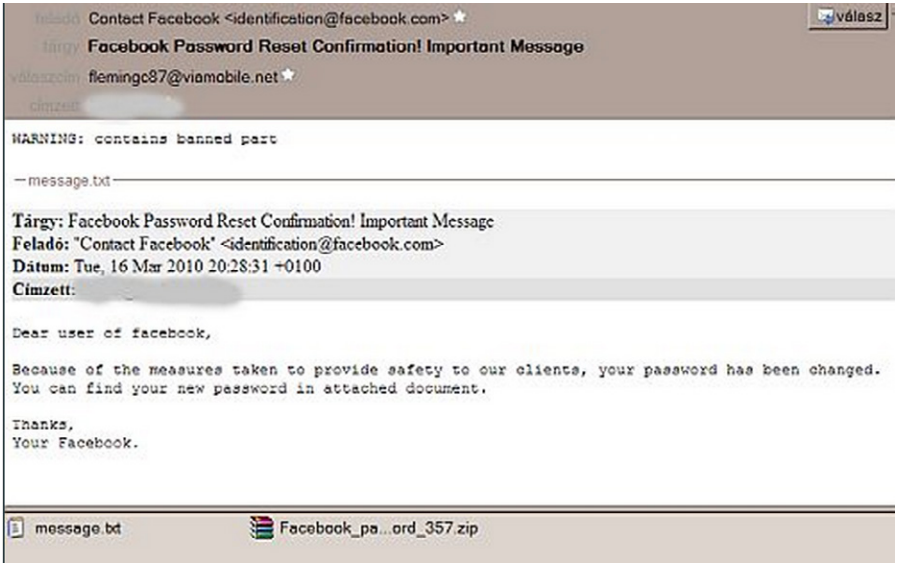


4. ábra: Erre az oldalra jutnánk a levél nyomán[49]

A harmadik példa a legjobb. (Lásd: 5. ábra.) Ez egy közösségi oldalról jött, és ha valaki angol nyelven használja az adott közösségi oldalt, akkor a levél nyelve nem lesz gyanús. Az feladó e-mail címe is hitelesnek tűnik, bár furcsa, hogy a levél válaszcíme eltér tőle.

Ez a levél nem hivatkozást küld, hanem csatolmányt, és ha lefuttatnánk a tömörített fájlban levő programot, kártékony programokkal, vírusokkal árasztanánk el számítógépünket. Fontos alapelv ezzel kapcsolatban a jelszó megváltoztatása, amelyet mindig az adott közösségi oldal vagy e-mail szolgáltató saját weboldalán lehet megtenni.

49 http://spamblog.hu/wp-content/uploads/2009/10/image8.png – letöltve: 2011.11.04.



5. ábra: Adathalász levél közösségi oldaltól[50]

■ ■ ■

50 http://itcafe.hu/dl/cnt/2010-03/58128/facebook.jpg – letöltve: 2011.11.04.

6. Az adatkezelő tevékenységi körén kívül eső veszélyforrások és védelmi módszerek

Az adatkezelő tevékenységi körén kívül eső veszélyforrások közé azokat a dolgokat, történéseket soroljuk, amelyeket az adatban esett kárt szemlélve a vis maior kategóriájában foglalhatnánk össze. Hangsúlyozni szeretném azonban, hogy az adatkezelő nem tárhatja szét a kezét például egy természeti katasztrófát követően azzal az indokkal, hogy „nem számított erre", ezért nem dolgozott ki semmilyen védelmi intézkedést. A helyzet az, hogy a „hagyományos" vis maior kategóriák ellen kell és egy része ellen igen jól lehet is védekezni adatbiztonsági intézkedésekkel.

A külső veszélyforrások egyik köre a természeti csapások: árvíz, belvíz, villámcsapás, földcsuszamlás, földrengés, tűzhányó-kitörés, tűzvész, szél stb. Ezek a veszélyforrások adatvesztést, áramköri meghibásodást okozhatnak, illetve bekövetkezhet az információs rendszer részleges vagy teljes pusztulása.[51] Ilyen esetben az informatikai biztonsági környezet elemeinek, illetve maguknak a védendő adatoknak a sértetlensége, rendelkezésre állása kerül veszélybe.

A veszélyforrások másik köre a szervezetet körülvevő – fizikai – működési környezetből ered. Ide sorolhatók az áramellátás zavarai, az áramellátás hibája vagy megszűnése, a működési környezetben bekövetkező, de a szervezetre is hatással lévő robbanás, robbantás, valamint

51 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 23–24. p.

az építési vagy más munkálatokból eredő gondatlan károkozás.[52] Ezek közül az áramellátási zavarok a leggyakoribbak. A szervezetnek az effajta veszélyforrásokra is védelmi mechanizmust, megfelelő válaszreakciót, eljárást kell kidolgoznia. Nyilvánvaló, hogy van olyan eset (például robbantás), amely ellen a szervezet általában védtelen. E veszélyforrások közös jellemzője az, hogy valamennyit emberi tevékenység vagy mulasztás okozza, a felelősséget megállapítani azonban nem lehet, vagy csak gondatlanság okán állapítható meg. Ha ugyanis e veszélyforrások szándékosság folytán következnek be, akkor crackingről vagy még súlyosabb bűncselekményekről beszélhetünk (terrortámadás, életellenes bűncselekmények).

A fenti veszélyforrások ellen leginkább fizikai védelmi mechanizmusokkal készülhetünk fel, amelyeket a következő fejezetben fogok ismertetni. Egy intézkedést érdemes mégis kiemelni, mégpedig a kockázatáthárítást. Az informatikai rendszerekre biztosítás köthető, amely ugyan nem véd a vis maior bekövetkezésétől, azonban ha mégis bekövetkezik a baj, nem nulláról, a „romokból" kell újrakezdeni, hanem a biztosítás már nyújt valamilyen kezdő alapot az újjáépítéshez, a helyreállításhoz. Sajnos, ez az a védelmi módszer, amelyet a legkevésbé alkalmaznak…

■ ■ ■

52 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 23–24. p.

7. Fizikai veszélyforrások és védelmi módszerek

A fizikai és környezeti biztonság megteremtése, illetve fenntartása érdekében a vonatkozó jogszabályok, biztonsági és tűzvédelmi szabványok, valamint a helyi szabályzatok, rendelkezések előírásainak maradéktalanul meg kell felelni. Ebből az következik, előfordulhat, hogy biztonsági ellenőrzés (audit) során vagy szabványosítási eljárásban azért marasztalják el a szervezetet, mert olyan egyszerű tárgy nem felelt meg a szabványoknak, egyéb biztonsági előírásoknak, mint például az ajtók zárja, a kültéri ablakok rácsozata vagy a beléptető rendszer.

A fejezetben felhasznált, később ismertetendő példákat nem egy James Bond filmből kölcsönöztem. Szeretném felhívni az Olvasók figyelmét, hogy ma már néhány ezer forintból lehet olyan eszközt gyártani/venni, amellyel igen komoly károkat lehet okozni.

A fizikai veszélyforrások között tartjuk számon az informatikai biztonsági környezet elemeit fenyegető, fizikai, tárgyiasult eszközökkel megvalósítható cselekményeket, történéseket, állapotokat. Ezek egy része a fizikai eszközökhöz, helyiségekhez való jogosulatlan hozzáférésre, azaz a bizalmasság megsértésére, más része pedig ezen eszközök rendelkezésre állásának megszakítására, vagyis azok megrongálására vagy megsemmisítésére irányul.

7.1. Jogosulatlan fizikai hozzáférés

A jogosulatlan fizikai hozzáférés típusai közül az aktív és a passzív hozzáférést különböztetjük meg. Az aktív hozzáférés alatt mindig valamilyen tevőleges cselekményt értünk. Ilyen például az objektumba,

helyiségbe történő illetéktelen belépés, az objektumon belüli és kívüli jogosulatlan mozgás, és ide sorolható mindezek legdurvább formája, az erőszakos behatolás. Ezt a veszélyforrást a humán erőforrások gondatlansága is előidézheti például az objektum őrizet nélkül hagyásával.[53]

A passzív hozzáférés célja nem a fizikai rombolás, hanem az informatikai biztonsági környezet fizikáját, fizikai tulajdonságait, illetve a humán erőforrások fiziológiáját használja ki, hogy adatokat megrongáljon, -szerezzen vagy -semmisítsen. Ilyen passzív fizikai hozzáférést jelentő veszélyforrás az akusztikus hozzáférés, az emberi beszéd lehallgatása, amelytől informatikai szempontból elsősorban bizalmas információk, jelszavak, kódok megszerzése remélhető. Az ide tartozó eszközök a következők:[54]

- puskamikrofon, amely nagy teljesítményű, erősítővel ellátott mikrofon (lásd: 6. ábra);
- optikai lézersugár, amely azt használja ki, hogy egy szobában történő beszélgetés hanghullámai üvegrezgést eredményeznek; az ablaküvegre irányított lézersugarat az üvegrezgés modulálva veri vissza, így a beszéd a vételi oldalon megfelelő készülékkel érthetővé tehető (lásd: 7. ábra);
- rádiófrekvenciás, miniatűr antennával ellátott adó (és a lehallgató oldalán: vevő) eszközök, amelyek azt használják ki, hogy a rádióhullámok egyszerűen előállíthatók, nagy távolságra jutnak el, és könnyen áthatolnak az épületek falain[55] (lásd: 8. ábra);
- szintén a rádiófrekvenciás technológián alapulnak a telefonvonalra és telefonba, valamint egyéb eszközökbe (például számítógépes

53 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek.* BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 24–26. p.

54 Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-Kerszöv Kiadó, Budapest, 2000. 273–294. p.

55 Andrew S. Tanenbaum: *Számítógép-hálózatok.* Panem Könyvkiadó Kft., Budapest, 2004. 131–132. p.

egér, USB pendrive, hálózati elosztó, számológép) szerelhető hangrögzítő és hangtovábbító (lehallgató) berendezések (lásd: 9. ábra).

6. ábra: Puskamikrofon[56]

7. ábra: Optikai lézersugár[57]

56 A képek hivatkozásai sorrendben: http://www.mikrofondot.hu/images/super/Rode-NTG-2-puskamikrofon-allvanyon.jpg, http://www.kiralyportal.hu/termekkepek/elado_hasznalt_em2_600pl_puskamikrofon_termikrofon_mono_vese__es_gomb_karakterisztika_kapcsoloval_valtoztathato_erzekeles_1_ceruzaelemmel_mukodik_tokeletes_minimalis_kis_karcok_vannak_rajt_8000ft_nagy891.jpg – letöltve: 2011.10.31.

57 A kép hivatkozása: http://hardverapro.hu/dl/uad/2009-01/510859pic.jpg – letöltve: 2011.10.31.

8. ábra: Rádiófrekvenciás lehallgató eszközök[58]

9. ábra: Egyéb lehallgató eszközök[59]

Német kutatók érdekes dolgot fedeztek fel: mikrofonnal is le lehet hallgatni a mátrixnyomtatók keltette zajt. Az új lehallgatási módszerrel egyelőre 72%-os pontossággal lehet felismerni a szöveget, de egy jól megválasztott szótárral akár 95%-os pontosságra is fel lehet

58 A képek hivatkozása sorrendben: http://www.minikamerak.hu/wp content/uploads/2011/01/ Radiofrekvencias.jpg, http://3.bp.blogspot.com/_Zzcqr-sQV-_c/TJEeX08krtI/AAAAAAAAA2A/VgwfC44bahU/s320/lehalgato1.jpg, http://www.spycentrum.com/Katalog/FM/fm2.jpg – letöltve: 2011.10.31.

59 A képek hivatkozása sorrendben: http://aboltom.com/images/124.gsm_spy_audio_bug_mouse.jpg, http://www.poloska.com/pics150/line10.jpg – letöltve: 2011.10.31.

javítani.[60] Ez elég jó arány ahhoz, hogy fontos információkat lehessen megszerezni.

Szintén a passzív fizikai hozzáférés kategóriájába tartozik az elektromágneses hozzáférés. Ennek alapja az, hogy a számítógép elektronikus áramköreiben mozgó elektronok elektromágneses hullámokat keltenek maguk körül, amelyek a szabad térben tovaterjednek.[61] A számítógépek fémháza antennaként erősíti fel ezeket a hullámokat.

7.2. A fizikai rendelkezésre állás megszakadása

Amikor az informatikai biztonsági környezet fizikai elemei részlegesen vagy teljesen működésképtelenné, használhatatlanná válnak, akkor a fizikai rendelkezésre állás részleges vagy teljes megszakadásáról beszélünk. A számítógépeket tekintve, a fenti példákból kiindulva azt mondhatjuk, hogy előállítható olyan, rádiófrekvenciás jeleket kibocsátó eszköz, amely kiégetheti a számítógép áramköreit.[62] Előállítható olyan elektromágneses hullámokat gerjesztő eszköz is, amely a hardvereken (például mágneses adattárolású háttértárak) a mágneses jeleket torzítja el, semmisíti meg, ilyen módon törölve a tartalmakat. Egyik eszköz sem nagyobb egy mobiltelefonnál.

A fizikai rendelkezésre állás megszakadását gyakran az informatikai biztonsági környezetben található informatikai eszközök megbízhatatlansága okozza. Előfordul, hogy ezek az eszközök nem felelnek

60 http://www.adatvedelmiszakerto.hu/2010/08/adatbiztonsag-mikrofonnal-lehet-lehallgatni-a-nyomtatokat – letöltve: 2011.10.31.

61 Andrew S. Tanenbaum: *Számítógép-hálózatok*. Panem Könyvkiadó Kft., Budapest, 2004. 128. p.

62 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 102. p.

meg azoknak a minőségi követelményeknek, amelyek az adatbiztonság kialakításához és fenntartásához szükségesek.

Ha sok számítógép van egy légtérben, akkor gondot okozhat az általuk termelt hő elvezetése. Zárt térben a nem megfelelő légállapot hőmérsékletemelkedést okoz. A 36–40 Celsius fokos levegő már kárt okozhat a nyomtatott áramkörökben (processzorok, memóriák stb.). A számítógépek általában rendelkeznek olyan védelmi mechanizmussal, hogy bizonyos processzorhőmérséklet felett leállítsák magukat, de ekkor is megszakad rendelkezésre állásuk.

Az energiaellátás zavarai is okozhatják a fizikai rendelkezésre állás megszakadását. Ezek közé soroljuk az áram- és feszültségingadozást, a túláramot és az áramkimaradást. Ugyancsak nem tesznek jót a pillanatnyi (tizedmásodperces), ismétlődő áramkimaradások. Mindezek adatvesztést, a háttértárak fizikai sérülését, az áramkörök sérülését okozhatják.

Szintén a fizikai rendelkezésre állás megszakadásához vezethetnek az adatkezelő tevékenységi körén kívül eső veszélyforrások, azaz a természeti csapások és a szervezet működési környezetéből eredő veszélyforrások.

Veszélyforrásnak tekintendő, ugyanis a fizikai rendelkezésre állás megszakadásához vagy az üzemzavar helyreállításának meghosszabbodásához vezethet a dokumentációk (üzemeltetési és felhasználói kézikönyvek, hardver- és szoftver-leírások) hiánya. Ilyen esetben a szakembereknek nehéz kivédeniük egy váratlan támadást, illetve ha a rendelkezésre állás már megszakadt, akkor „autodidakta" módon sokkal lassabb ideig tart a rendszer tanulmányozása és a megfelelő intézkedések meghozatala.

7.3. Fizikai védelmi módszerek

A fizikai védelmi módszerek közé az objektum- és vagyonvédelemmel kapcsolatos intézkedéseket, eszközöket soroljuk. Habár ezek a módszerek közvetlenül a vagyonbiztonság megteremtését szolgálják, az

informatikai biztonsági környezet tárgyiasult elemein keresztül azonban szoros kapcsolatban vannak az informatikai biztonsággal is. A védendő adatok jellege szerint érdemes külön biztonsági területeket kijelölni. Ezeket a területeket külön kockázatelemzés után lehet meghatározni. Gondoskodni kell az illetéktelen behatolást, hozzáférést, károkozást és beavatkozást megakadályozó fizikai-mechanikai, elektronikai és személyi védelem szükséges méretű – együttes – alkalmazásáról.[63]

A védelemnek arányban kell állnia a megállapított kockázatokkal. Az objektumok bizalmasságának megőrzése, a dokumentumok és adathordozók védelme érdekében szükség van megfelelő be- és kiléptetési, valamint megfigyelési szabályok érvényesítésére.

A védelemigényes helyiségekbe való belépési jogosultságot a legkisebb jogosultság elve szerint kell meghatározni, tehát a személyek munkaköréhez kapcsolódóan. A KIB 25. ajánlása szerint alapvető követelmények a következők:[64]

- A szervezet adatfeldolgozó helyiségeinek határoló falazata fizikailag legyen ellenálló, a külső falak, nyílászárók megfelelő felépítésűek legyenek.
- Fontos, hogy a felügyelet nélküli helyiségek nyílászárói zárva legyenek.
- Ablakok esetében – ha szükséges – ajánlatos külső mechanikai védelmi eszközöket (például rács) alkalmazni, különösen a földszinti helyiségek esetében.
- Fogadószemélyzettel vagy ha szükséges, biztonsági őrrel ellátott ügyfélteret, recepciót, tárgyalóhelyet a produktív munkaterületektől és az adatfeldolgozó egységektől kellő távolságban kell kialakítani.

63 A KIB 25. számú ajánlása, 88. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

64 A KIB 25. számú ajánlása, 89. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

- A fizikai biztonság fontos eleme a tűzvédelem, a biztonsági határoknak, falaknak, nyílászáróknak a nemzetközi előírásokban, szabványokban rögzített tűzállósággal kell rendelkezniük.
- A megfelelő behatolásjelző rendszer a biztonság alappillére, fontos, hogy minden olyan terület, ahol adatfeldolgozást, adatkezelést végeznek, megfelelően felosztott behatolásvédelmi rendszerrel legyen felszerelve. Napjaink riasztóközpontjai lehetővé teszik a különböző biztonsági zónák (ún. partíciók) létrehozását az adott telephelyen belül. A területileg megosztott, jól particionált biztonsági rendszer támogatja a szervezeten belüli feladatelhatárolást is.
- Fontos, hogy a szervezet által kezelt adatfeldolgozó eszközöket fizikailag el kell választani azoktól, amelyeket harmadik fél kezel.

Minősített esetben a védendő adat körül érdemes több biztonsági zónát kialakítani, mert ily módon növelhető a fizikai védelem.

Belépés-, kilépés- és mozgásellenőrzés: Fontos alapelv, hogy az adott biztonsági zónához jogosultsággal nem rendelkező **munkatársakat**, illetve a vendégeket ki- és belépéskor regisztrálni kell. A belépés előtt ellenőrizni kell a belépő által megjelölt belépési célt.

A fokozott vagy kiemelt biztonsági zónához tartozó helyiségekben a belépési jogosultsággal rendelkező személyek ki- és belépését is naplózni kell. A belépés ellenőrzését a beléptető rendszer kártyáján túl egyéb hitelesítési eljárások alkalmazásával (például PIN kód, biometriai azonosító eljárások) is meg kell erősíteni.

Érdemes jól megkülönböztethető azonosító kártyákat csináltatni külön a munkatársaknak és külön a vendégeknek, s azok viselését kötelezővé tenni.

Az objektum kerítésén belüli, illetve az épületeken belüli mozgás ellenőrzésére a kamerás és térfigyelő rendszereket alkalmazzák. E célra az egyik legelterjedtebb eszköz az ún. CCTV rendszer (= Closed Chain Television System, azaz zártláncú televíziós rendszer), amely az

épületeken belülre és kívülre is telepíthető. A zártláncú tévérendszer legfontosabb részei a kamerák (lehet fix, forgatható, állandó vagy állítható fókuszú), figyelő monitorok, alarmmonitorok (ezek csak abban az esetben közvetítik a kamera képét, esetleg hangjelzés kíséretében, ha mozgást érzékel) és különböző digitális, valamint mágneses rögzítők (ezek nem szükségszerű tartozékai a rendszernek).[65]

A kamerás megfigyelőrendszerek telepítésénél figyelni kell az alkotmányos korlátokra: a vagyonvédelem határainak kijelölésénél figyelembe kell venni más alapjogok korlátozhatóságát is. Ilyen alapjog az információs önrendelkezési jog, így tehát a kamerás megfigyelőrendszerek alkalmazásánál kiemelt védelemben kell részesíteni a magánszférát, annak a kamerás megfigyelés általi korlátozhatóságát. Az Alkotmánybíróság a 36/2005. (X. 5.) AB határozatában kimondta, hogy „az alkotmányosan megengedhető alapjogi korlátozás szintje nem azonos az elektronikus megfigyelőrendszer egyes elemei tekintetében". Amikor felvétel készül, de azt nem rögzítik, tehát csak megfigyelés történik, a vagyonvédelem érdekei jobban korlátozhatják az információs önrendelkezési jogot, mint abban az esetben, amikor a felvételt rögzítik is. A puszta megfigyelés esetén tehát „a személyeknek a megfigyelt helyen való jelenléte, a hely jellegének megfelelő szokásos magatartása nem esik megfigyelési korlátozás alá", azonban a bekamerázott helyek meghatározásánál figyelembe kell venni az intimszféra sérthetetlenségét. Így az AB határozat kizárja olyan helyiségek bekamerázását, amelyekben az intimszféra (mint a magánszféra legbensőbb, legszűkebb része) körébe eső cselekmények, tevékenységek folyhatnak: például mosdók, öltözők stb.

Abban az esetben azonban, ha a kamerákkal készített felvételt tárolják is, a személyes adatok kezelése valósul meg. Ilyenkor a

65 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 106. p.

vagyonvédelmi érdek kevésbé korlátozhatja a magánszférát, mert „a vagyonőrzés során óhatatlanul megfigyelt, de jogsértő magatartást el nem követő személyekről készült felvételek – mindaddig, amíg meg nem semmisítik azokat – akár szenzitív tartalommal is bírhatnak. A felvétel dokumentatív jellege miatt ugyanis különösen alkalmas arra, hogy a magánszférához való jog sérelmét eredményező módon visszaéljenek vele."[66] Ezért a rögzített adatokat az adott vagyonvédelmi helyzet által megkívánt legrövidebb ideig lehet csak tárolni. Ha ez az idő bűncselekményre utaló jel nélkül telt el, a tárolt adatokat meg kell semmisíteni, ellenkező esetben pedig meg kell tenni a szükséges intézkedéseket (szabálysértési feljelentés, rendőrségi feljelentés stb.).

Létesítmények és helyiségek biztonsága: Az informatikai rendszerek környezetét legalább a biztonsági osztálynak/zónának megfelelő fizikai, mechanikai, elektronikai és személyi védelemmel kell biztosítani (például rácsos ablakok, az áttörést megnehezítő üvegezés, acélajtók).

A következő védelmi intézkedéseket érdemes megfontolni:

a) A kulcsfontosságú eszközöket úgy ajánlatos elhelyezni, hogy elkerüljük illetéktelen személyek hozzáférését.
b) Különböző műszaki eszközök, mint a fénymásolók, szkennerek, a biztonsági zónán belül legyenek elhelyezve, hogy ezzel is elkerüljük az illetéktelen hozzáférés lehetőségét és az adatok kijutását, amely az információ veszélyeztetésével járna.
c) Az ajtók és ablakok legyenek elreteszelve, amikor nincs a közelben felügyelő személyzet, és az ablakok külső védelméről (rácsozat) is ajánlatos gondoskodni, különösen a földszinten.
d) A helyiségeket olyan behatolás-jelző rendszerrel kell védeni, amely az összes külső ajtót és hozzáférhető ablakot (nyílászárót) lefedi és védi.

66 36/2005. (X. 5.) AB határozat

e) Az adott szervezet által kezelt és menedzselt adatfeldolgozó eszközöket fizikailag is ajánlatos elválasztani azoktól, amelyekkel harmadik felek foglalkoznak.
f) A belső telefonkönyveket, címjegyzékeket, amelyek érzékeny adatfeldolgozó eszközök helyét azonosítják, nem szabad a nyilvánosság számára elérhetővé tenni.
g) Veszélyes vagy gyúlékony anyagokat ajánlatos a biztonsági zónától kellő távolságban és biztonságosan tárolni.
h) A tartalékberendezést és a tartalékolt adathordozókat ajánlatos olyan biztonságos távolságban elhelyezni, amellyel elkerülhető, hogy a központi telephely katasztrófája esetén kárt szenvedjenek.

Mechanikai védelem: A mechanikai védelem eszközei körkörösen veszik körül az adatot magában rejtő információs rendszert. Négy kört különböztetünk meg:

1. (legkülső) kör: A belépés-ellenőrzésnél is igen nagy szerepe van: ide tartoznak a kerítésvédelmi eszközök: árok, töltés, kerítés, kapu, sorompó, mechanikai akadályok.
2. kör: Az épületek felülete, felület- vagy más néven héjvédelemnek[67] is nevezik. Az ide tartozó elemek az épületek falazata, aljzata és födémje.
3. kör: Nyílászárók és az ezeket megerősítő eszközök. Ide tartoznak a különböző egyszerű és biztonsági ajtók, valamint a zárak, zárrendszerek. A záraknál általában az ún. hengerzárbetétek különböző fajtáit, illetve egyéb biztonsági zárakat alkalmaznak.
   A zárrendszerek három fajtáját szokták alkalmazni. Az első az ún. központi zárrendszer: több különböző egyedi kulcs egy vagy

67 Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2000. 176. p.

több központi hengerzárbetétet zár,[68] vagyis a központi hengerzár több különböző tollmintázatú kulccsal zárható. A központi zárrendszert gyakran alkalmazzák társasházaknál, ahol a lakások egyedi kulcsai a főbejárat hengerzárbetétjét is zárják. (Lásd: 10. ábra.)

A zárrendszerek második fajtája az ún. főkulcsos zárrendszer: egy főkulccsal a zárrendszerben lévő összes hengerzárbetétet zárni lehet, amelyeknek természetesen egyedi kulcsai is vannak.[69] (Lásd: 11. ábra.)

A harmadik fajta az ún. vezérkulcsos zárrendszer: egyfajta főkulcsos zárrendszer, azonban itt nemcsak főkulcs, hanem több hengerzárbetétet is záró csoportkulcsok is vannak.[70] (Lásd: 12. ábra.)

A biztonsági (törhetetlen, lövésálló stb.) üvegek, valamint az üvegfelületek megerősítésére szolgáló biztonsági fóliák is ebbe a körbe tartoznak. Ez utóbbi a betört, szilánkosodott üveget nem engedi széthullani, így a törött üveg ellenére az üvegfelületen nem keletkezik áthatolásra alkalmas nyílás.[71] Szintén ebbe a körbe tartoznak a nyílászárók teljes szerkezetét védő rácsok, speciális redőnyök.

4. kör: Értéktárolók, páncélszekrények, széfek és trezorhelyiségek.

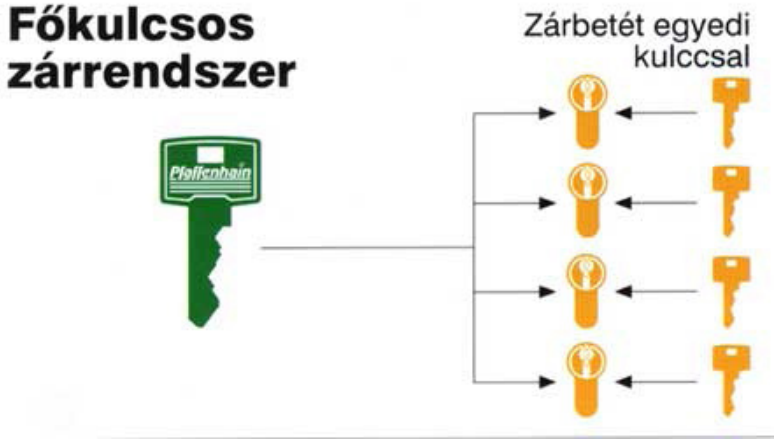
68 Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2000. 178. p.

69 Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2000. 179. p.

70 Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2000. 179. p.

71 Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2000. 181. p.

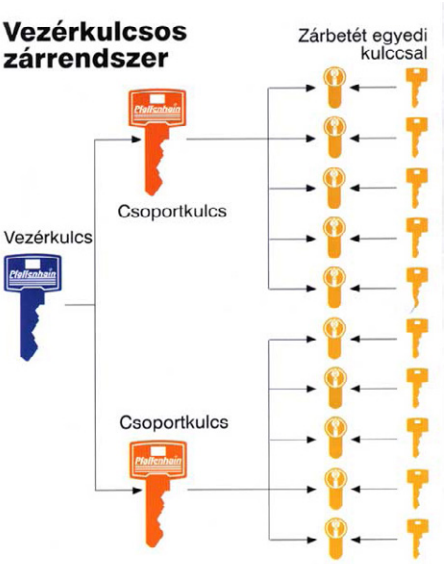
10. ábra: Központi zárrendszer[72]



11. ábra: Főkulcsos zárrendszer[73]

72 http://www.elektronsky.hu/images/zar/fogalommeg/kozpontizarasrendsz.jpg – letöltve: 2011.11.03.

73 http://www.elektronsky.hu/images/zar/fogalommeg/fokulcsoszrendsz.jpg – letöltve: 2011.11.03.



12. ábra: Vezérkulcsos zárrendszer[74]

Elektronikai védelem: Az elektronikai védelmet körkörösen felépített jelző- és érzékelő-rendszerrel valósítják meg. Az elektronikus rendszereken belül megkülönböztetjük a kül- és beltéri, héjvédelmi, térvédelmi, tárgyvédelmi és személyvédelmi elektronikákat, illetve a különböző felderítő eszközöket, detektorokat. Az idetartozó legfontosabb eszközök a következők:

- az árnyékoló rendszerek közül az akusztikai és elektromágneses árnyékoló rendszerek;
- a megfigyelő rendszerek közül a kül- és belétéri zártláncú tévérendszer;
- a héjvédelmi eszközök közül a nyitás-, feszítés-, falbontás-, üvegtörés-, rezgésérzékelők (lásd: 13-14. ábra);

74 http://www.elektronsky.hu/images/zar/fogalommeg/vezerkulcsosrendsz.jpg – letöltve: 2011.11.03.

- a térvédelmi eszközök közül a mikrohullámon, illetve infravörös fényen, ultrahangon alapuló mozgásérzékelők, valamint a nyomáskapcsolók és kábelszakadás-érzékelők (lásd: 15. ábra);
- a tárgyvédelmi eszközök közül a súlyérzékelők és fémhang-érzékelők;
- a személyvédelmi elektronikák közül az ún. pánikkapcsoló, valamint a dőlésérzékelő.[75]

Az akusztikus lehallgatás-védelem terén az ún. bizalmas tárgyalókat, valamint az ún. süketszobákat alkalmazzák. A bizalmas tárgyaló falfelületeit olyan zajjal bombázzák, amely lehetetlenné teszi a lehallgatás megvalósítását. A süketszobák általában átlátszó, jó hangszigetelésű anyagból készülnek, és nem alkalmaznak bennük fém alkatrészeket, amelyeket a lehallgatók rezonátorként használhatnának fel.[76] A lehallgató készülékek felderítésére rádiófrekvenciás detektorokat használnak. (Lásd: 16. ábra.)

13. ábra: Rádiós nyitásérzékelő[77]

14. ábra: Üvegtörés-érzékelő iránymikrofonnal[78]

75 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 77–84. p.

76 Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2000. 303–304. p.

77 http://oktel.hu/wp-content/uploads/2011/05/r_egyeb_nyitaserzekelo_ja60b_k.jpg – letöltve: 2011.11.04.

78 http://oktel.hu/wp-content/uploads/2011/05/r_egyeb_bg2000_uvegtores_pyronix.jpg – letöltve: 2011.11.04.

15. ábra: Infravörös mozgásérzékelő[79]

16. ábra: Rádiófrekvenciás detektor[80]

Élőerős védelem: Az élőerős védelem általában biztonsági őrökből és esetleg szolgálati kutyákból áll. A belépés- és mozgásellenőrzés a kerítésvédelem be- és kilépést biztosító pontjainál ún. pontőrzéssel, az objektum egyéb területein – a kerítésvédelem mentén, az épületek mentén, illetve magukban az épületekben – pedig járőrözéssel valósítható meg.

A be- és kilépés ellenőrzésekor az élőerős védelmet biztosító személyek feladata a belépni szándékozók belépési jogosultságának tisztázása, az objektumba bevihető tárgyak ellenőrzése, a kimenő forgalom biztosítása és a kivihető tárgyak ellenőrzése. E belépés-ellenőrzési pontok az objektum határvonalainál, a kerítésvédelem megfelelő pontjaiban, illetve az épületek ki- és bejáratainál is kialakíthatók.

A járőrözésnek előre meghatározott útvonalon és idő alatt kell megvalósulnia. Adatbiztonsági szempontból veszélyforrást jelent, ha a járőr nem a megadott helyről, nem a megadott időpontban jelentkezik be vagy egyáltalán nem jelentkezik be. Ugyancsak veszélyforrásként értékelendő, ha az ellenőrzési helyeken a járőr nem talál mindent rendben.

79 http://www.iparikamera.hu/product_150/dsclc100.jpg – letöltve: 2011.11.04.
80 http://nservices.com/sh055.jpg – letöltve: 2011.11.04.

Ezekben az esetekben az informatikai rendszer a fenyegetettség állapotába lép, és ez az állapot megfelelő védelmi-elhárító intézkedés megtételét teszi szükségessé.

Védelem a külső és környezeti veszélyforrások ellen: Teljesen egyértelmű, hogy kevés olyan hely létezik, ahol az adott intézmény épülete semmilyen külső veszélynek nem lenne kitéve. Így az adott helyszín kiválasztásakor elvégzett elemzéseket követően tudjuk meghatározni a védelmi módszereket, azaz, alkalmazkodni a környezethez. Fontos figyelembe venni az épület földrajzi elhelyezkedéséből fakadó veszélyeket (például árvíz, belvíz, földrengés, erdő- és bozóttűz), a klímáját (például vihartérképek beszerzése, ár- és belvízveszély felmérése). Ilyenkor érdemes szakértő segítségét kérni.

A szervezetek telephelyének közelében lévő különféle ipari létesítmények (olajfinomítók, erősáramú vezetékek) vagy tevékenységek is komoly veszélyt jelentenek. Költözéskor vagy új telephely létrehozásakor érdemes ilyen irányú környezettanulmányt, kockázatelemzést végezni.

Ilyen jellegű veszélyforrások esetén az épületet olyan módon kell megépíteni, hogy ellenálló legyen. Jó példa erre Japán, ahol olyan módszerekkel építik fel az épületeket, hogy kibírjanak egy nagyobb földrengést is.

Bevált gyakorlat a több telephellyel rendelkező szervezeteknél, hogy a tartalékeszközök, adathordozók tárolását egymással elcserélik, így biztosítva a működésfolytonosságot és az üzletmenetet bármelyik telephelyet ért katasztrófa esetére is.[81]

Berendezések fizikai védelme: Az informatikai berendezéseket, eszközöket fizikai valójukban is védeni kell a biztonságukat fenyegető veszélyektől és káros környezeti hatásoktól. Ily módon meg tudjuk őrizni az adatok sértetlenségét, bizalmasságát és rendelkezésre állását,

81 A KIB 25. számú ajánlása, 92. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

illetve magukat az adatokat tároló eszközöket tudjuk megvédeni fizikai védelmi módszerekkel.

Az informatikai rendszerek fizikai védelmének fajtái példákkal:[82]

Az extrém hőmérsékletek és a levegő meg nem engedett mértékű nedvességtartalma elleni védelem (klímatizálás): beszélhetünk a helyiség vagy a berendezés klímatizálásáról. Az előbbi esetben gondoskodnunk kell megfelelő klímaberendezésről, ami termosztát segítségével szabályozza a hőmérsékletet. Az utóbbi esetben hűtőventillátort (processzorhoz, lásd: 17. ábra), nagy teljesítményű víz- és léghűtéses rendszert alkalmazhatunk. (Lásd: 18. ábra.)

17. ábra: Processzorhűtő ventilátor[83]

18. ábra: Vízhűtéses rendszer[84]

A fémes adatvezetékek elektromágneses impulzusok elleni védelme (elektromágneses besugárzás elleni védelem): Az elektromágneses árnyékolás eszköze az ún. Faraday-szoba vagy Faraday-sátor. A monitorok videojeleinek árnyékolására szintén speciális árnyékoló eszközök használatosak, mivel a videojelek viszonylag nagyobb távolságból is érzékelhetők.[85]

82 A KIB 25. számú ajánlása, 94. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

83 http://upload.hardver-teszt.hu/imgs/news/2009/378/spire-dual-star-cpu-cooler-right-angle-big.jpg – letöltve: 2011.11.02.

84 http://www.pto.hu/gallery/1/1-514.jpg – letöltve, 2011.11.02.

85 Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2000. 301–303. p.

Külső tényezők (tűz, víz, vihar stb.) elleni védelem: különösen a tűzjelző berendezések megléte és működőképessége, illetve a vízelvezetés, továbbá tűzálló ajtók használata. Ha azonban a tűz már bekövetkezett, csak a kár minimalizálására alkalmas oltóberendezések és -rendszerek jöhetnek számításba. A tűzoltó készülékeket a helyiségeken belül a bejárat mellett, valamint a helyiség erre alkalmas, jól megközelíthető pontjain kell elhelyezni.

Áramellátó-rendszerek kiesése következményeinek elhárítása (akkumulátoros és generátoros szükség-áramellátással): Történhet olyan szünetmentes tápegységekkel (UPS – uninterruptable power supply, lásd: 19. ábra), amelyek áramkimaradás esetén a számítógépek biztonságos leállításáig (15–60 perc) képesek a megfelelő áramot betáplálni a rendszerbe, illetve a szünetmentes tápegység akkumulátorának lemerülése után a UPS szabványosan leállítja az adott informatikai rendszert. Másik lehetőség áramfejlesztő generátorok használata, amelyekkel folyamatos működést lehet biztosítani. Egyik esetben sem maradhat el azonban a veszélyforrás megfelelő jelzése – a szünetmentes tápegységek éles, sípoló hangot adnak, amikor megszűnik a központi áramellátás.

19. ábra: Szünetmentes tápegység[86]

86 http://pcu.hu/pictures/termekek/5~218.jpg, http://prohardver.hu/dl/cnt/2005-04/625/004.jpg – letöltve: 2011.11.02.

20. ábra: Elosztó túlfeszültség védelemmel[87]

Az áramellátás területén a villámcsapások elsődleges és másodlagos hatásai, illetve egyéb alacsony és túlfeszültségek elleni védelem: Az előbbi megoldására szintén alkalmasak a szünetmentes tápegységek, az utóbbi azonban villámvédelmet igényel, amelyre nem minden szünetmentes tápegység képes. A villámvédelemnél alacsonyabb erősségű, de túláramnak számító áramerősség kiküszöbölésére speciális szűrőket alkalmaznak. (Lásd: 20. ábra.)

Elektrosztatikus kisülések hatásainak elhárítása (a helyiségek és munkahelyek megfelelő kialakításával, amelyekbe az informatikai rendszereket telepítették): a padlóburkolatok, berendezési tárgyak antisztatikus kivitelűek legyenek

Berendezések karbantartása: A megbízható működés és a rendelkezésre állás érdekében a dokumentációkban, használati leírásokban leírtaknak megfelelő időközönként el kell végezni a berendezések karbantartását, szervizelését, ellenőrzését. Ezeket a műveleteket csak szakképzett emberek végezhetik. Az informatikai berendezések külső helyszínen

87 http://www.loud.hu/kepek/Elektronika/TULFESZULTSEG_VEDO_ELOSZTO-KONIG_SPB07.jpg – letöltve: 2011.11.02.

történő javítása, karbantartása esetén gondoskodni kell a berendezésen tárolt adatok végleges (visszaállíthatatlan) törléséről. A javítás során meg kell felelni a személyi, fizikai biztonsági előírásoknak.

A fizikai védelem megtervezése: Ide Mtartozik – az objektum elhelyezésén kívül – az épület informatikai rendszerének kialakítása, melynek feladata a fizikai védelem automatizált működtetése. Összetételét tekintve a fizikai védelmet végrehajtó érzékelőkből (nagyszámú érzékelő, mérőműszer, látjelző) és az azokat működtető, ellenőrző humán erőforrásokból (kevés szakember) áll.[88]

A fent vázolt rendszer összehangolt működéséhez szükséges, hogy a működés elveit deklarálják a biztonsági szabályzatokban, illetve integrálják a szervezet működési mechanizmusába, hiszen a hatékony védelmet csak akkor lehet megvalósítani, ha az a szervezet érdekeivel, a benne dolgozók egyetértésével történik, ugyanakkor nem akadályozza a működést és a hatékonyságot. E rendszer lényege, hogy minden, a fizikai védelemmel kapcsolatos információ egy központba fut össze – legyen szó akár az őrjárat által biztosított információkról, akár a látjelzők, érzékelők által közölt adatokról –, amely képes ezeket az információkat összefüggéseikben értékelni, elemezni és az elemzés alapján a szervezet működésével összehangolt döntést hozni.

Minősített adatok fizikai védelme: A minősített adatok fizikai biztonságáról a 90/2010. (III. 26.) Kormányrendelet V. fejezete rendelkezik, amely két biztonsági területet határoz meg:

- I. osztályú biztonsági területnek minősül minden olyan helyszín, ahol „Bizalmas!" vagy annál magasabb minősítési szintű minősített adatot használnak fel, vagy használnak fel és tárolnak, vagy tárolnak olyan módon, hogy a területre való belépés egyben a minősített adathoz való hozzáférést is jelenti. A terület fizikailag

88 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 63–65. p.

körülhatárolt és védett, a ki- és belépés ellenőrzött. A ki- és belépés csak beléptető rendszeren keresztül és csak azon személyek számára engedélyezhető, akik erre külön felhatalmazással és személyi biztonsági tanúsítvánnyal rendelkeznek.[89]

- II. osztályú biztonsági területnek minősül minden olyan helyszín, ahol „Bizalmas!" vagy annál magasabb minősítési szintű minősített adatot használnak fel, vagy használnak fel és tárolnak, vagy tárolnak olyan módon, hogy az illetéktelen hozzáférést belső intézkedésekkel meg lehet akadályozni. A terület fizikailag körülhatárolt és védett, a ki- és belépés ellenőrzött, a minősített adatokhoz történő illetéktelen hozzáférés megakadályozása érdekében pedig a biztonsági területre csak külön felhatalmazással lehet belépni. Személyi biztonsági tanúsítvánnyal nem rendelkező személy csak kísérettel léphet be.[90]

A Kormányrendelet 19-21. §-ai részletesen szabályozzák, hogy milyen paramétereknek kell megfelelniük azoknak a helyiségeknek és tárolóeszközöknek, amelyekben minősített adatot tárolunk nyíltan vagy zártan. A fentebb említett fizikai védelmi eszközökkel a kívánt biztonság elérhető.

Amennyiben a gazdálkodó szervezet cégellenőrzése és az érintett személyek nemzetbiztonsági ellenőrzése megtörtént, valamint nyilvántartóval, illetve rendszerengedéllyel rendelkezik, és megteremtette a minősített adatok kezelésének – adminisztratív, fizikai és elektronikus biztonsági – feltételeit, kiadható részére a Telephely Biztonsági

89 90/2010. (III. 26) Kormányrendelet 17. § (3)
90 90/2010. (III. 26) Kormányrendelet 17. § (4)

Tanúsítvány (a továbbiakban: TBT).[91] A tanúsítványt iparbiztonsági ellenőrzés alapján adják ki. Az iparbiztonsági ellenőrzés módját a 92/2010. (III. 31.), illetve a 90/2010. (III. 26.) Kormányrendelet szabályozza. Az iparbiztonsági ellenőrzés célja, hogy a nemzetbiztonsági szolgálat a gazdálkodó szervezet által kitöltött cég-adatlapban foglalt adatok valóságtartalmát ellenőrzi abból a célból, hogy a gazdálkodó szervezet minősített szerződés végrehajtásába történő jövőbeni bevonása sértheti-e Magyarország nemzetbiztonsági, továbbá a NATO vagy az EU biztonsági érdekeit. E folyamat része a vezető testületébe tartozó személyek, a kijelölésre kerülő biztonsági vezető, valamint a titkos ügykezelő és helyettese, a rendszerbiztonsági felügyelő, a rendszeradminisztrátor, továbbá a minősített szerződésben való igazolt részvétel esetén annak előkészítésében és végrehajtásában érintett személyek nemzetbiztonsági ellenőrzése. A telephely biztonsági tanúsítványa visszavonásig érvényes. Amennyiben a telephely biztonsági tanúsítványát visszavonják, a gazdálkodó szervezet a visszavonásról szóló határozat jogerőre emelkedésétől számított két éven belül nem kérelmezheti újabb iparbiztonsági ellenőrzés végrehajtását. A gazdálkodó szervezet a TBT minősítési szintjének megfelelő szintű nemzeti minősített adatot kezelhet.[92]

■ ■ ■

91 Nemzeti Biztonsági Felügyelet: Az iparbiztonsági ellenőrzés, illetve a Telephely Biztonsági Tanúsítvány kiadásának rendjét érintő legfontosabb változások http://www.nbf.hu/anyagok/iparbiztonsag/ Valtozas_iparbizt.doc – letöltve: 2012.02.23.

92 Az Alkotmányvédelmi Hivatal honlapja http://www.ah.gov.hu/html/iparbizt_ellenorzesek.html – letöltve: 2012.02.23.

8. Logikai veszélyforrások és védelmi módszerek

A logikai veszélyforrások közé a logikai eszközökkel előidézhető veszélyforrásokat sorolhatjuk. Ezek általában az informatikai biztonsági környezet logikai elemeire hatnak, azonban közvetve, a szoftvereken keresztül kihatással vannak a hardvereszközök működésére is.

Jogosulatlan logikai hozzáférés: Ez a veszélyforrás az adatot közvetlenül körülvevő két védelmi gyűrűvel kapcsolatos: a jogosultságokat és szoftvereket, valamint a kriptográfiai megoldásokat tartalmazó védelmi réteggel. A jogosultságok és a szoftverek esetében akkor beszélünk veszélyforrásról, ha a logikai rendszerekhez való belépés ellenőrzése gyenge lábakon áll. A belépés ellenőrzésének gyengeségét több tényező okozhatja:

- Gyenge jelszavak – rövid, könnyen kitalálható, a felhasználóhoz tartalmilag köthető, a magánszférájukból „származó" jelszavak: például kutya, macska, kisállat neve; feleség, férj, barát, barátnő, gyermek neve; születési dátum vagy túl primitív, egyszerű jelszó, például 1234, abc123, xxxyyy.
- Rosszabb esetben nincs is jelszó, elég csak a felhasználó nevét megadni.
- A jelszavak nem megfelelő tárolása – a korábban említett „sárga cetlik" esete.

Az értelmes szavakkal az is probléma, hogy egy úgynevezett szótár alapú támadással ki lehet találni őket. Ez úgy működik, hogy a jelszót próbálgató program egy több ezer szót tartalmazó szótárfájlból veszi végig a szavakat, és próbál meg behatolni a rendszerbe.

A rövid, egyszerű vagy primitív jelszavakat pedig egy úgynevezett brute force (magyarul: nyers erő) alapú támadással lehet könnyedén

kitalálni. Ez azt jelenti, hogy a jelszót feltörni szándékozó hacker végigpróbálja az összes lehetőséget. Például egy 6 karakterből, csak kisbetűkből álló jelszó kitalálásához maximum kb. 320 millió próbálkozást kell végrehajtani[93] (ennyi az összes lehetőség). A mai technikával ez már nem tart olyan hosszú ideig.

Vannak e-mail szolgáltatók, ahol új jelszót lehet kérni néhány személyes adat és egy titkos kérdésre (például gyerekkori szerelmünk neve, kisállatunk neve stb.) adott válasz ellenében. Ilyen esetben ezek az adatok a jelszó fontosságával érnek fel. Ha valaki megtudja ezeket az adatokat, úgy járhat, mint Sarah Palin, aki a 2008-as amerikai elnökválasztáson volt az alelnökjelölt. Az ő e-mail címét úgy törték fel, hogy megtudták a szükséges személyes adatokat, és egy korábbi beszédéből kiderült a válasz a titkos kérdésre is.[94]

Egy másik, igen tanulságos történet 2009-ből:[95] egy Hacker Croll nevű francia huszonéves feltörte a Twitter közösségi oldal egyik alapítójának a Google-fiókját. Semmilyen titkos trükköt nem alkalmazott. Miután célba vette a Twittert, elkezdett profilokat készíteni a vállalat alkalmazottaiból (név, vállalati e-mail cím, beosztás, születési dátum, kisállat neve), és ezeket az adatokat mind publikus helyen találta meg az interneten. Két dolgot használt ki ezek után: a webes alkalmazások a felhasználóktól azonosítóként e-mail címet követelnek meg, illetve jelszót kell választani; s ezzel már meg is van a kulcs, hiszen az emberek hajlamosak arra, hogy azonos adatokkal dolgozzanak. Az előző bekezdésben említettem az „elfelejtett jelszó" opciót, amely még az internet hőskorából származik.

A Twitter mint cég online üzemel, így sok adatot, dokumentumot e-mailen osztanak meg. Így a rendszer lánccá épül fel, amelynek

93 http://etikushack.info/tananyag/bruteforce.html – letöltve: 2011.11.05.
94 http://kulfold.ma.hu/tart/cikk/b/0/23940/1/kulfold/Pattogatott_kukoricaval_tortek_fel_Sarah_Palin_postafiokjat – letöltve: 2011.11.05.
95 http://www.szerver.com/index.php/2009/07/gmail-fiok-jelszo-hack – letöltve: 2011.11.05.

szilárdságát – ahogy a közhely tartja – a leggyengébb láncszem határozza meg. Hacker Croll dolga csak annyi volt, hogy megtalálja ezt a gyenge láncszemet. Próbálgatással rájött, hogy ki az, akinek az online viselkedése tipikus, azaz nem tér el a felhasználók 98%-a által produkálttól. Az egyik alkalmazott esetében küldött a Gmailnek egy üzenetet, és új jelszót szeretett volna kérni. Ezt többször megpróbálta másoknál is, ám az áttörés mégis itt következett be. A fent említett esetben a Gmail honlapja arról értesítette, hogy új jelszavát elküldték a másodlagos („secondary") e-mail címre, melyet így jelenített meg a szolgáltatás: ******@h******.com. Nem volt nehéz kitalálni, hogy ez egy hotmailes cím. A Hotmail esetében Hacker Croll újra az elfelejtett jelszó menühöz folyamodott – feltételezte, hogy az azonosító ugyanaz, amit már ismert. És ekkor borult a dominó. Az adott alkalmazott már rég nem használta ezt az e-mailt, ezért a Hotmail – szabályzatának megfelelően – törölte a fiókot. Innen már egyszerű volt. Az azonosító alapján létrehozott egy új fiókot, majd újra lekérte a Gmailtől az elfelejtett jelszót, amit szépen meg is kapott az újonnan létrehozott Hotmail-fiókba.

Ezen a ponton lebukhatott volna, hiszen ha más jelszót használ a Gmail-nél, mint az eredeti tulajdonos, kiderült volna a feltörés ténye. Azonban a levelek között kutatva ráakadt egy olyanra, melyben az alkalmazott egy másik webes szolgáltatásnál egy általa elfelejtett jelszó után érdeklődött, s kapott egy olyan levelet, amilyet már mindannyian: „Az ön azonosítója: Malacka, jelszava: Farkas1." Ezek után jött a próba: a hacker kicserélte az új Gmail jelszót erre, amelyet a felhasználó más szolgáltatásoknál használt, hogy ellenőrizze, majd figyelt, hogy működik-e még tovább a fiók – s működött, a felhasználó nem vett észre semmit, tehát ugyanazt a jelszót használta, ahogy a hacker feltételezte.

Egyértelmű, hogy a jelszavak mögött jogosultságok vannak. Ha jó is a jelszórendszer, mindenképpen a belépés ellenőrzésének hibájaként róható fel, ha a jelszavakhoz rendelt jogosultságok nem feladatfüggően vannak meghatározva. A leggyakoribb hiba – különösen a közigazgatásban

– az, hogy a hozzáférési jogosultságok rendszerével a szervezeti hierarchiát próbálják meg lefedni, és nem feladatfüggően vannak meghatározva, tehát a szervezet vezetőjének van a legtöbb jogosultsága az informatikai biztonsági környezetben: ő bármit telepíthet, törölhet, bármit olvashat, módosíthat, míg a biztonságért felelős munkatársak nem kapják meg a feladatukhoz szükséges jogosultságokat. Belátható, hogy ez az elv biztonsági kockázatok tömegét hordozza magában.[96]

Még a helyesen működő jogosultsági rendszer esetén sem feledkezhetünk el az emberi tényezőről. A kapott jogokkal lehet élni és visszaélni. Alapvető logikai veszélyforrást jelent tehát, ha a felhasználók teljesítményének követése, a számonkérés, a naplózás (ki, mikor, milyen műveletet végzett) nem biztosított. A teljesítménykövetés, naplózás azonban nem terjeszkedhet túl a munkavégzéssel szorosan összefüggő tevékenységek figyelésén.

A logikai hozzáférés szempontjából komoly veszélyforrást jelentenek a nyílt, vezeték nélküli (wifi) hálózatok. Mivel nincs jelszó a hálózaton, ezért a teljes hálózati forgalom lehallgatható, illetve veszélyforrást jelent, ha ezek a hálózatok nincsenek kellően leválasztva a bizalmas rendszerektől, azaz a belső hálózatról.

A kriptográfiai megoldásokat tartalmazó védelmi réteghez való illetéktelen hozzáférést célzó veszélyforrás a kriptográfiai támadás, a rejtjelfejtés. Ennek célja a titkos üzenet, a titkos kulcs, jelszó visszafejtése és megszerzése. A kriptográfiai támadás passzív formájában a támadó csak lehallgatja az üzenetet, és később használja fel. Aktív formájában azonban a támadó befolyásolni akarja a szervezeti működést, ezért az üzenetet lehallgatja, módosítja, és ezt a módosított üzenetet juttatja vissza a rendszerbe, így a szervezet nem az eredeti, hanem a támadó szándéka szerinti információra fog reagálni.

96 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 115. p.

Óvatosnak kell lennünk, ha számítógépünkkel, mobiltelefonunkkal nyílt wifi hálózatra csatlakozunk. Nem tudhatjuk, hogy ki és milyen szándékkal ül a gyorsétterem vagy a pláza másik sarkában. Egy konferencián vettem részt, ahol az előadó a wifi hálózatok biztonsági kérdéseit taglalta, és megosztotta, hogy az előadás előtti fél órában jó néhány személyes adatot tudott meg a webet böngésző, üzenetküldő programokon keresztül „beszélgető" résztvevőkről, mindössze azzal, hogy egy teljesen ingyenes programmal lehallgatta a hálózati forgalmat, amely a nyílt wifi hálózat miatt nem volt titkosítva. Természetesen, az előadást követően ezek az adatok törölve lettek. A vezeték nélküli hálózatok biztonsági kérdéseiről később még bővebben lesz szó.

A logikai rendelkezésre állás megszakadása: A logikai rendelkezésre állás megszakadását okozó veszélyforrások jelentkezhetnek az informatikai biztonsági környezeten belül, de nem zárhatjuk ki a külső támadás lehetőségét sem. Az egyik ilyen belső veszélyforrás a mentések rendszerének kidolgozatlansága, ugyanis a rendszer meghibásodásának esetén az eredeti állapot, az adatok visszaállítása szinte kizárt. Ugyanezzel a problémával találkozhatunk abban az esetben, ha nincs megoldva a mentett példányok megfelelő tárolása, hiszen így a rendszer visszaállításához nem áll rendelkezésre a szükséges adattár. Ki kell itt emelnem, hogy a mentett adatok tárolása is adatkezelés, tehát a nem megfelelő tárolási szabályok eredményeként személyes adatok kerülhetnek ki az informatikai biztonsági környezetből.

A mentési stratégia hiányán kívül az újraindítási stratégia hiánya is logikai veszélyforrásként értékelhető. Nem mindegy ugyanis, hogy a rendszer mely elemeit milyen sorrendben állítják helyre/indítják újra. A nem megfelelő újraindítási stratégia azt okozhatja, hogy az utolsó mentés és az újraindítás között keletkezett adatok elveszhetnek.

A logikai rendelkezésre állás megszakadhat a rosszindulatú szoftverek, vírusok, valamint a szándékos elektromágneses támadás nyomán. Az előbbi a hiányos vagy nem létező vírusvédelem következményeként

súlyos károkat (adatlopást, adatszivárgást, adatvesztést, logikai rombolást) is okozhat. Az utóbbi ugyan közvetlenül az informatikai eszközök mágneses háttértárait támadja, azonban a mágneses jelek megzavarásával, eltorzításával a háttértárakon tárolt szoftvereket, adatokat is megsemmisíti, tehát – közvetett módon – logikai veszélyforrásként is értékelhető.

A dokumentáció hiánya itt is veszélyeket hordoz magában – hasonlóan, mint a fizikai veszélyforrásoknál –, hiszen a szoftverek üzemeltetési, felhasználói és egyéb leírásainak hiánya jelentősen megnehezíti egy-egy szoftver működésének visszaállítását és sokszor – részleges mentés esetén – a mentett változatok helyreállítását, visszaállítását is.

8.1. Logikai védelmi módszerek

A hozzáférés-ellenőrzés követelményei: Fontos annak megoldása, hogy az adatokhoz csak a megfelelő személyek és a megfelelő jogosultsággal férhessenek hozzá, és ez ellenőrizhető legyen. Ehhez korlátozni kell az információkhoz, számítógépekhez, hálózatokhoz, alkalmazásokhoz, rendszererőforrásokhoz, állományokhoz és programokhoz való hozzáférést, illetve eseménynaplókban szükséges rögzíteni a hibákat és felhasználói tevékenységeket, a tárolt részleteket pedig elemezni kell a biztonsági események megfelelő módon való felderítésének és kezelésének érdekében. Ezek biztosítékai a következők:[97]

a) Hozzáférés-ellenőrzési szabályzat: világosan meg kell határozni minden felhasználó és felhasználói csoport számára. **Általánosan elfogadott elvnek kell lennie, hogy csak a szükséges jogokat szabad kiadni.**

97 A KIB 25. számú ajánlása, 151–152. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

b) Felhasználók hozzáférése a számítógépekhez: A rendszerben azonosítani kell a felhasználókat, s mind a sikeres, mind a sikertelen belépési kísérleteket naplózni kell.
c) Felhasználók hozzáférése adatokhoz, szolgáltatásokhoz és alkalmazásokhoz: Az adott munkaállomáson vagy a hálózaton hozzáférés-védelmi eljárásokat kell alkalmazni az adatok és szolgáltatások jogosulatlan elérésének kiküszöbölésére. Például külső hálózatról hozzá lehet-e férni a belső hálózat adataihoz; ha igen, kiknek lehetséges, milyen IP című[98] számítógépről; vannak-e tiltott IP címek és/vagy felhasználók stb.
d) Hozzáférési jogok felülvizsgálata és módosítása: Minden felhasználó esetében rendszeresen felül kell vizsgálni a kiosztott felhasználói jogosultságokat. A visszaélések elkerülése érdekében sokkal gyakrabban kell ellenőrizni a kiemelt jogosultságokat. A szükségtelen jogosultságokat azonnal vissza kell vonni!
e) Ellenőrzési napló: Mint minden informatikai támogatással végzett tevékenységet, a felhasználói hitelesítések folyamatát is naplózni kell.[99] Ez tartalmazza a rendszerbe történő sikeres és sikertelen belépési kísérleteket, az adatokhoz való hozzáférés naplózását, a rendszer által használt funkciókat stb.; a hibákat szintén naplózni kell. AA naplók rendszeres ellenőrzésére van szükség. A napló adatait a személyiségi jogi és adatvédelmi jogszabályoknak megfelelően kell kezelni, például csak meghatározott ideig lehet tárolni és csak biztonsági célokra lehet felhasználni.

A felhasználói hozzáférés menedzsmentje: Ahhoz, hogy meg lehessen akadályozni az információs rendszerek illetéktelen elérését, megfelelő hozzáférés-védelmi rendszert kell kiépíteni. Fontos elv, hogy hozzáférés

98 Az IP cím azonosítja a hálózati eszközt (például számítógép hálózati csatolója) a hálózaton.
99 Infotv. 7. § (5)

iránti, illetve jogosultság módosítására, hozzáférés törlésére vonatkozó igény csak írásban kérhető, s a kérelmeket nyilvántartásba kell venni. A kiadott engedélyek listáját naprakészen kell tartani. A felhasználók regisztrációjával kapcsolatban a következő elveket kell figyelembe venni:[100]

a) A felhasználó-azonosítónak minden esetben egyedinek kell lennie, azaz semmilyen körülmények között sem adható ki különböző felhasználók részére megegyező azonosító. Azonos felhasználói azonosítók lehetetlenné teszik a felelősségek szétválasztását.
b) Időszakosan meg kell vizsgálni az ismétlődő azonosítókat, és le kell tiltani őket, valamint biztosítani kell, hogy már létező felhasználói azonosítót le lehessen kiadni. (Az információs rendszer legtöbbször már rendelkezik ezzel a tulajdonsággal.)
c) A felhasználói azonosítók képzését a szervezeten belül egy helyen kell végrehajtani.
d) Új felhasználók esetén biztosítani kell, hogy a szolgáltatók, rendszergazdák ne adják meg a hozzáférést, amíg be nem fejeződnek a jogosultság-megadási eljárások.
e) Készítsenek felhasználó regisztrációs lapot minden személyről, akit bejegyeztek a szolgáltatás használatára.
f) A felhasználói azonosítók és jogosultságok rendszerében bekövetkezett mindennemű változást (az ellenőrizhetőség érdekében) naplózni kell.
g) Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör ellátásához szükséges minimális funkcióelérést biztosíthatják.
h) A felhasználói azonosítók nem örökéletűek, tehát addig léteznek, ameddig a felhasználó rendszeresen használja az informatikai rendszert.
i) A felhasználókkal alá kell íratni egy nyilatkozatot, amely dokumentálja, hogy megértették a hozzáférés feltételeit és felelősségeit.

100 A KIB 25. számú ajánlása, 151-156. oldal, www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

Jelszavas védelem: A logikai védelem egyik legfontosabb és legtöbb veszélyforrást hordozó része a jelszó-rendszer. A jelszavas hitelesítés célja, hogy a belépni szándékozó meggyőzze a rendszert, jogosult a belépésre, tehát a belépő bizonyít, a rendszer pedig ellenőriz.[101] A jelszavas védelem két részből áll. Időben az első a bejelentkezési azonosító (logon ID, felhasználónév) megadása. Ebben a fázisban a belépni szándékozó állít magáról, a saját személyéről valamit: egyrészt tudja a felhasználónevet, másrészt azt állítja, hogy ő olyan személy, aki jogosult a rendszer használatához, az adatokhoz való hozzáféréshez. Ebben a fázisban történhet meg annak a végpontnak az azonosítása is, ahonnan a bejelentkezést kezdeményezik.

A jelszavas védelem időben második része a hitelesítés. Itt a belépni szándékozónak be kell bizonyítania, hogy ő valóban az, akinek az első fázisban mondta magát. Ez többféle módon, egy vagy több különböző jelszó megadásával történhet. Ebben a fázisban a rendszer ellenőrző funkciója lép előtérbe,: a megadott jelszót összehasonlítja az adatbázisában tároltakkal. Ha a belépni szándékozó által megadott jelszó létezik az adatbázisban, akkor megtörtént a hitelesítés, hiszen a belépő olyan személynek mondta magát, aki a belépésre jogosult, és megadta a szükséges jelszót vagy jelszavakat is.[102]

A KIB 25. ajánlása szerint a következő alapelveket szükséges betartani a jelszavakkal kapcsolatban:[103]

a) A felhasználónak kötelezően alá kell írnia egy nyilatkozatot, melyben felelősséget vállal személyes (esetleg csoportos) jelszavainak bizalmas kezelésére.

101 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 93. p.

102 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 117. p.

103 A KIB 25. számú ajánlása, 161–162. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

b) A belépéskor kapott, illetve – például elfelejtés esetén – ideiglenes jelszó átadása csak biztonságos csatornán történhet, a felhasználó előzetes – például személyes – azonosítása után. Az ideiglenes jelszavak csak az adott munkanap végéig lehetnek érvényesek, megváltoztatásuk kötelező.
c) **Telefonon, illetve elektronikusan aláíratlan e-mailen történő kérésre jelszóváltoztatás nem kezdeményezhető**.
d) A felhasználónak minden esetben ellenőrizhető úton kell visszaigazolnia új jelszavának átvételét – például e-mailben vagy személyesen.
e) A jelszónak a felhasználó számára szabadon megváltoztathatónak kell lennie.
f) A felhasználói jelszavakkal kapcsolatban (amennyiben az adott rendszerben erre lehetőség van) biztosítani kell a következő követelmények teljesülését:
   - minimális jelszóhossz megadását;
   - a jelszó egyediségét (történeti tárolás), tehát jelszóváltoztatás esetén nem lehet már korábban használt jelszót felhasználni;
   - a központi jelszó megadása utáni első bejelentkezéskor a kötelező jelszó cseréjét;
   - a jelszó maximális élettartamát, tehát mennyi az a legtöbb idő, amely után már mindenképp meg kell változtatni a jelszót;
   - a jelszó minimális élettartamát;
   - a jelszó zárolását;
   - a jelszó képzési szabályainak megváltoztatását, például kell-e kisbetű, nagybetű, szám, nem alfanumerikus karakter stb.
g) A számítógépes rendszerekben a jelszavakat **tilos nyílt formában tárolni**. A jelszófájlokat megfelelő rejtjelezési védelemmel kell ellátni.
h) A jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos.

Jelszóhasználati szabályok:[104]

a) A jelszavakat bizalmasan kell kezelni
b) A jelszavakat nem szabad papíron tárolni (a biztonsági másolat kivételével, viszont azt megfelelően védett helyen, például széfben kell őrizni). Ha ez elkerülhetetlen, például a kezdeti jelszó esetén, akkor gondoskodni kell a zárt borítékban történő biztonságos tárolásról.
c) Ha a felhasználóban felmerül a gyanú, hogy jelszavát feltörték, azonnal le kell cserélnie.
d) A jelszó hossza **haladja meg a 8 karaktert**, ne tartalmazzon egymást követő azonos karaktereket vagy számokat, mert ez igencsak megkönnyíti a feltörhetőséget például a brute force támadások esetében.
e) Kívülállók ne tudják könnyen kitalálni a jelszót, ne tartalmazzon a felhasználó személyére utaló információkat (például neveket, telefonszámokat, születési dátumokat), összefüggő szövegként ne legyen olvasható, ne legyen értelmes. Az érthetőség megkönnyíti a jelszó feltörését az úgynevezett szótár alapú támadások esetén.
f) A legnagyobb biztonságot a felhasználóhoz nem köthető, kis- és nagybetűkből és számokból álló, véletlenszerűen összeállított jelszavak garantálják.
g) A felhasználói jelszavakat rendszeresen (kb. 3 havonta) cserélni kell. Előfordul, hogy a rendszer ezt automatikusan kötelezővé teszi. A korábbi jelszavak ciklikus vagy ismételt használatát kerülni kell.
h) Kiemelt jogosultságú felhasználók esetén (rendszergazda, szoftvertelepítő szakember) sokkal gyakrabban kell cserélni a jelszavakat.

104 A KIB 25. számú ajánlása, 164–165. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.

i) Első bejelentkezéskor kötelezően le kell cserélni a kezdeti jelszót.
j) Minden felhasználónak oktatni kell a biztonságos jelszóhasználat szabályait.
k) A felhasználóknak tudniuk kell, hogy minden olyan műveletet, melyet az ő azonosítójával és jelszavával mások hajtanak végre, az informatikai rendszer az ő „terhére" könyveli el, és azokért személyesen felel.

Jelszavak típusai: három típust különböztetünk meg: a többször használatos jelszót, az egyszer használatos jelszót, illetve a biometrikus jelszót.

A *többször használatos jelszó* valamilyen titkos információ tudására épül, tehát a „mit tudsz?" elven alapul.[105] Gyakorlatilag a legtöbb esetben ilyeneket használunk az e-mail fiókunkhoz, a számítógépünkbe való belépéskor stb.

Miért érdemes olyan jelszavakat használni, amelyek kis- és nagybetűkből és számokból állnak, véletlenszerűen összekeverve? Az angol abc 25 kisbetűjét, 25 nagybetűjét, valamint a tízes számrendszer számjegyeit (0-9-ig), azaz összesen 60 karaktert figyelembe véve a lehetséges változatok száma igen magas, így brute force támadással nagyon sok időbe telik feltörni a jelszót.

A brute force típusú jelszó-feltöréseket további intézkedésekkel szokták megnehezíteni. Ilyen védelmi intézkedés például az, hogy a rendszer néhány – általában 3, 4 vagy 5 – rosszul megadott jelszó után megadott időre (30 perc, 60 perc stb.) vagy végleg kitiltja a felhasználót. A másik védelmi intézkedés a jelszó hossza. Egy hosszú jelszót ugyanis aránytalanul tovább tart feltörni, mint egy rövidet.

105 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 94. p.

Az *egyszer használatos jelszó* a „mi van a birtokodban?" elvén alapul.[106] Ez a jelszó a bejelentkezés folyamatában a felhasználói azonosító – és esetleg a többször használatos jelszó – helyes megadása után keletkezik. Ekkor a felhasználó birtokában van valamilyen algoritmus, amelynek segítségével előállíthatja a jelszót. Ez az algoritmus lehet például egy matematikai művelet is. A hitelesítés úgy történik, hogy a rendszer generál egy véletlen számot, amellyel el kell végezni az algoritmust, majd a belépni szándékozó válaszként visszaadja az algoritmus megoldását. A rendszer is megoldja az algoritmust, és ha a két eredmény megegyezik, akkor a felhasználó engedélyt kap a belépésre.

A *biometrikus jelszó* a „ki vagy?" elvén alapul. Ez alatt az ember fiziológiájából következő, a tényleges személyazonosságot igazoló egyedi azonosítókat értünk. Ilyen lehet például a hanglenyomat, az ujjlenyomat, a tenyérnyomat, a retinahártya és az íriszhártya mintázata, valamint a DNS.

Azokban a rendszerekben, ahol biometrikus jelszavakat használnak, ilyen azonosításra általában csak az előző két azonosítási mód sikeressége után kerülhet sor.[107]

A rendelkezésre állás biztosítása: A logikai rendelkezésre állás biztosításának módszerei közé soroljuk a rendszer-karbantartási eszközöket, illetve az adatmentési és adattöbbszörözési technikákat.

A rendszer-karbantartási eszközök között felsorolhatjuk a munkaállomások, szerverek fájlrendszereinek szerkezeti épségét, integritását ellenőrző szoftvereket. Ezek a szoftverek általában megtalálhatók az

106 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 94. p.

107 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 95. p.

operációsrendszer eszközei között,[108] de számos ingyenes program is rendelkezésre áll.

Fontos a lemezek töredezettség-mentesítése, ugyanis a fájlok a merevlemezen általában fizikailag nem folyamatosan helyezkednek el. Így egy nagymértékben széttöredezett fájl esetében a merevlemez olvasófejének annyira hosszú utat kell bejárnia, hogy vagy nagyon meghosszabbodik a fájl beolvasási és így feldolgozási ideje, vagy a rendszer szerint „túl hosszú" időbe telne az adat elérése, azaz időtúllépés miatt hibaüzenetet kapnánk, és ilyenkor az adat elérhetetlensége miatt megszakad a logikai rendelkezésre állás.

A logikai rendelkezésre állás biztosításának másik formája a rendszeres adatmentés, a biztonsági másolatok készítése vagy biztonsági háttérrendszer üzemeltetése. Biztonsági másolat készülhet az adatról vagy az egész rendszerről. Fontos szempont a rendszeresség, ugyanis a véletlenszerűen, ad hoc időpontokban elvégzett biztonsági mentéseket gyakorlatilag veszélyforrásként kell értékelnünk. A védelmi intézkedések azonban nem szorítkozhatnak csak és kizárólag a biztonsági mentések elkészítésére: a mentett példányok is fontos adatot tartalmaznak, ezért egyaránt különös figyelmet kell fordítani az adathordozó kiválasztására és tárolására.

A biztonsági háttérrendszerek üzemeltetése tulajdonképpen a hardver- és szoftverelemek többszörözését jelenti. Két típusra oszthatjuk őket: aktív és passzív redundáns háttérrendszer. Az aktív redundáns háttérrendszert aktiválni kell az eredeti rendszer rendelkezésre állásának megszakadásakor, ami sok időbe kerül. A passzív redundáns háttérrendszert egy háttérprocesszor működteti folyamatosan, amely ugyanazokon az adatokon ugyanazokat a feladatokat hajtja végre, mint az eredeti rendszer, így a rendelkezésre állás megszakadása esetén a háttérrendszer

108 Például a Windowsban a Hibaellenőrzés, illetve a Lemeztöredezettség-mentesítő.

azonnal át tudja venni az eredeti rendszer feladatát.[109] Erre példa a háttértárak többszörözése a szervergépben a RAID (Redundant Array of Independent Disks) technológia alapján. Nézzünk erre egy egyszerű példát: két merevlemezt tükrözünk, ami azt jelenti, hogy mindkét merevlemez tartalma bitről bitre megegyezik. Ezeket összekötjük, így a számítógép logikailag egy merevlemezt lát, és amennyiben bármilyen változás áll be a tartalomban, mindkét merevlemez változik, és a bitről bitre való egyezés megmarad. Ha bármelyik merevlemez kiesik, az adatok sem vesznek el, és a rendelkezésre állás sem szakad meg.

Fontosabb hardware eszközök – például a RAM meghibásodása esetén – alapesetben le kellene állítani a szervert, kicserélni a RAM-ot, aztán újraindítani. 7/24-es rendelkezésre állás esetén el kell kerülni a szerver leállítását. Ilyen esetben léteznek úgynevezett „hot plug" eszközök, amelyeket a számítógép leállítása nélkül ki lehet cserélni, így a rendelkezésre állás nem szakad meg.

8.1.1. Vírusok, káros tartalmak, spam és az ellenük való védekezés

A rosszindulatú programok tárgyalása előtt néhány statisztikai adattal támasztom alá, hogy miért érdemes komolyan venni a logikai veszélyforrásokat és megfogadni a védelmi módszerek alkalmazását.

Több mint 1 millió magyar netező belép veszélyes weboldalakra a vírusirtója jelzése ellenére, sőt, a világhálón járók 10%-a szánt szándékkal kapcsolja ki a védelmi szoftvert. Miért? Azért, hogy

- lopott szoftvert vagy az ahhoz szükséges törést letöltse;
- véletlen ismerőstől kapott, cseppet sem vicces .ppt-fájlt nyisson meg;
- lopott vagy ingyenes pornót töltsön le;
- bármilyen illegális szoftvert vagy tartalmat szerezzen meg.

109 Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek*. BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001. 174. p.

Mindez a 18–29 éves korosztályra a legjellemzőbb, azaz az internetezők 17%-ára. Az idősebb emberek (50–69 évesek) a legóvatosabbak, és a férfiak 15%-a, a nők csupán 6%-a indít el vírusosnak jelzett fájlt.[110]

Ennek a hozzáállásnak komoly következménye van: 2011-ben Magyarország 4. helyen állt a spam küldési világranglistán, illetve az Eurostat adatai szerint a világhálóra kötött gépek 46%-a vírusos. Ez majdnem minden második, internetre kötött magyar gép.[111] Tehát helye van annak, hogy komolyan vegyük, hogyan alkalmazzuk a következőkben kifejtésre kerülő módszereket.

A rosszindulatú program, más néven malware olyan szoftver, amelyet kifejezetten abból a célból készítettek, hogy kárt okozzon a számítógépes rendszereknek, azaz, hogy ezen rendszerek bizalmasságát, sértetlenségét és rendelkezésre állását veszélyeztessék. A rosszindulatú programok körébe számos különféle rossz szándékú program tartozik: vírusok, férgek, trójai programok, illetve egyes nagyon veszélyes kém- és reklámprogramok.[112]

A malware-ek a logikai veszélyforrások legnépesebb táborát képviselik. Az ellenük való védekezésnek folyamatosnak kell lennie, de pusztán ez nem elég, folyamatosan fejleszteni is kell ezt a védelmet, mert a rosszindulatú programok fejlődése miatt a támadási módszerek folyamatosan változnak. Ahhoz, hogy hatékonyan tudjunk védekezni ellenük, érdemes közelebbről megismerkednünk velük.

A rosszindulatú programoknak fertőzési technikájukat tekintve két csoportja van: memóriarezidens programok és közvetlenül fertőző programok. A memóriarezidens vírusok a vírusprogram lefutása után

110 http://index.hu/tech/2011/04/04/minden_tizedik_magyar_netezo_idiota – letöltve: 2011.11.17.

111 http://index.hu/tech/2011/02/09/a_magyar_szamitogepek_46_-a_virusos – letöltve: 2011.11.17.

112 Andrew Conry-Murray – Vincent Weafer: *Internetes biztonság otthoni felhasználóknak*. Kiskapu Kiadó, Budapest, 2006. 43. p.

a memóriába kerülnek, és egyes részeiket itt tárolják (azaz rezidenssé válnak). Különböző rendszerhívásokhoz kapcsolódva (például írás egy állományba) töltik be a vírus többi részét a memóriába, majd megindítják a fertőzést.[113] Ha a vírus egyszer rezidenssé vált, minden olyan rendszerhívásnál fertőz, amelyre rákapcsolódott.

A közvetlenül fertőző vírusok nem a memóriában „ülnek és figyelnek" a fertőzés lehetőségére várva, hanem a számítógépbe való bejutás (e-mail, internet, egyéb fertőzött külső forrás, például pendrive stb.) után valamilyen módon lefutnak (az e-mailek mellékleteként terjedő vírusok például a felhasználók hiszékenységét kihasználva), majd végrehajtják a fertőzést. Ezek a vírusok általában minden lefutáskor meghatározott számú célpontot fertőznek meg.[114]

Minden esetben érdemes csínján bánni a rosszindulatú programokkal. Igaz, vannak veszélyesek, amelyek komoly veszélyforrást jelentenek a logikai biztonságra (adatvesztést, adatsérülést, adattörlést okozhatnak), de a kevésbé veszélyeseket sem szabad lebecsülni, amelyek például annyit tesznek, hogy „csak" a memóriát, a háttértárak szabad kapacitását csökkentik. Azonban még ezzel a „szinte ártalmatlan" működéssel is lehetetlenné teszik a memóriaigényes programok futtatását, sőt, adatvesztést is okozhatnak vagy legalább a rendelkezésre állást szakíthatják meg.[115]

Terjedési és fertőzési módjuk alapján a rosszindulatú programokat négy nagy csoportba sorolhatjuk: vírusok, férgek, trójai programok, egyéb malware.[116]

113 Dreiliger Tímea: *Vírusvédelem.* Panem Könyvkiadó, Budapest, 2004. 23. p.
114 Szappanos Gábor: *Kirándulás a számítástechnika sötét oldalára.* VirusBuster Kft., Budapest, 2003. 21–22. p.
115 Dreiliger Tímea: *Vírusvédelem.* Panem Könyvkiadó, Budapest, 2004. 24. p.
116 A Virus Bulletin nevű, független malware tanácsadó csoportosítását vettem alapul. http://www.virusbtn.com – letöltve: 2011.11.16.

Vírusok: A vírus olyan önmagát reprodukálni képes program, amely úgy fertőz meg más programokat, hogy azok tartalmazzák a vírus egy – esetleg megváltoztatott – új példányát.[117]

A vírusok fajtái:

- Bootvírusok – A rendszer boot szektorát fertőzik meg úgy, hogy a vírus a saját kódját írja be a boot szektorba annak a programnak a helyére, amely rendszerinduláskor megkapja a vezérlést. Így a számítógép elindításakor a vírus fut le az operációs rendszer betöltő rutinja helyett. 1995-ben jelent meg a Microsoft Windows 95 operációs rendszer, ami nagy csapást jelentett az addigi vírusokra, mert nak az addig legnépesebb és leggyakrabban előforduló csoportjuk, a boot vírus nem tudott szaporodni az új rendszerben. Azóta ezek a típusú vírusok nem játszanak nagy szerepet.
- Fájlvírusok – A fájlvírus más programokat úgy fertőz meg, hogy a célprogramot használja fel hordozóként: belemásolja a víruskódját vagy annak egy részletét, avagy más módon kapcsolódik a fertőzetlen fájlokhoz (például bemásolja magát különböző könyvtárakba). Ennek megfelelően a fájlvírus lehet önálló program, amely csak kapcsolódik egy nem vírus programhoz, vagy lehet nem önálló, amely beépül a megfertőzött programba.
- Makróvírusok – A makróvírus olyan rosszindulatú program, amely az adatfeldolgozó rendszer (például Office programok) valamely beépített parancsára, beépített makrójára épül rá, vagy az adatfeldolgozó rendszerben új parancsként, új funkcióként jelenik meg. A makró – így a makróvírus is – a dokumentummal, dokumentumsablonnal együtt lesz elmentve. A dokumentummal elmentett makró az adott dokumentum

117 http://www.virusbtn.com/resources/glossary/virus.xml – letöltve: 2011.11.16.

megnyitásakor vagy a dokumentumban annak a parancsnak a kiadásakor fertőz, amelyhez a makró hozzákapcsolódott. A dokumentumsablonba mentett makró minden olyan új dokumentumot megfertőz, amely az adott dokumentumsablonon alapul. A fertőzés legelső tünete általában az, hogy az adatfeldolgozó rendszer valamely parancsa (makrója) feltűnően lassan hajtódik végre, hiszen nemcsak az adott parancshoz definiált belső makró, hanem a makróvírus is lefut. Öröm az ürömben, hogy a makróvírusok terjedésének gátat vet az adatfeldolgozó rendszer nyelve, ugyanis egy makróvírus csak abban a nyelvi környezetben tud fertőzni, amelyben megírták.[118] Ennek az az oka, hogy a beépített makróknak, amelyekhez hozzákapcsolódik a makróvírus, a különböző nyelvi verziókban más és más a neve.

- Script vírusok – Nem tárgykódban (gépi kód), hanem forráskódban terjednek. Ahhoz, hogy a vírus lefusson, minden esetben futtatókörnyezetre van szüksége. Például egy honlap esetében a honlap (például egy .html fájl) a forráskód és a böngésző a futtatókörnyezet, amely megjeleníti ezt a honlapot. Ezek a vírusok elektronikus levelek megnyitásával, illetve weboldalak letöltésével futnak le, fertőznek. Sajnos, ilyen vírusokat nagyon könnyű írni, így a szerzők sokszor tinédzserek vagy fiatal felnőttek, akik nincsenek tisztában tettük következményeivel.
- Hardver vírusok – Ezek a vírusok nem túl gyakoriak, mégis, mióta lehetőség van a számítógépek BIOS-át frissíteni (ezt hívják Flash BIOS-nak), valós veszélyt jelentenek. Néhány vírus kihasználja a Flash BIOS írhatóságát és törölhetőségét, így törli azt, vagy teleírja véletlenszerű karakterláncokkal, majd tönkreteszi a BIOS író programot is. Az eredmény: a számítógép

118 Dreiliger Tímea: *Vírusvédelem*. Panem Könyvkiadó, Budapest, 2004. 22. p.

elindításakor a hardver (minden alkatrész) tökéletesen működik, viszont a képernyő sötét, ugyanis BIOS hiányában a rendszerteszt nem lesz végrehajtva, és az operációs rendszer betöltése sem tud elkezdődni. A számítógép definíciójából következően pedig szoftver nélkül a működő hardver önmagában nem számítógép…[119]

Férgek: Olyan önálló programok, amelyeket arra terveztek, hogy automatikusan terjesszék magukat (saját másolatukat) számítógépről számítógépre. Általában elektronikus levélben vagy az interneten keresztül terjednek, kihasználva a megtámadott rendszer sebezhetőségét vagy a felhasználók hiszékenységét.[120] A féreg (angolul: worm) definíciója korszakonként változott. A múlt század '80-as éveinek végén, '90-es éveinek elején a férgek célja a pusztítás, adatok megszerzése, védelmi intézkedések áttörése volt. 1991-ben a szakirodalom a férgeket a következőképpen határozta meg: „Olyan programok, amelyek nem szaporodnak, hanem egy rendszerbe belépve keresztülrágják magukat annak védelmi mechanizmusán. Feladatuk legtöbbször az, hogy behatoljanak az operációs rendszer magjába (a kernelbe), és kihozzanak onnan bizonyos információkat, például jelszótáblákat. Ennek elvégzése után általában csendesen kimúlnak. Újabban féregnek nevezik azokat a vírusokat is, amelyek pusztítása nem látványos, hanem lassan, fokozatosan munkálkodva teszik tönkre az operációs rendszert."[121] Ekkor tehát még nem volt cél a szaporodás, hanem „csak" a logikai védelmi intézkedések áttörése és adatok kijuttatása a rendszerből, majd a megsemmisülés.

119 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 132. p.

120 http://www.virusbtn.com/resources/glossary/worm.xml – letöltve: 2011.11.16.

121 Kis János – Szegedi Imre: *Új víruslélektan.* Cédrus Kiadó, Budapest, 1991. 68. p.

1995-ben már más ismérvek alapján határozták meg a férget: „A vírusoknak olyan alfaja, amely azzal okoz kárt, hogy addig másolja be magát a fertőzött állományokba, amíg azok futtathatatlanul hosszúak lesznek, illetve amíg csurig nem telik a lemez… Az interneten komoly riadalmat keltett 1988-ban az internet-worm, amely a rendszer postai szolgáltatásait kihasználva terjesztette kódját. Szerencsére ez a féreg nem tartalmazott kifejezetten romboló rutint, sőt ki is takarodott a számítógépről, ha már néhány példányban szétküldte saját másolatait. Rendkívül gyorsan végighaladt az internet hálózat gépeinek többségén, majd végül sikerült megszabadulni tőle."[122] Ezek szerint a férgek elsődleges célja az lett, hogy a rendszer erőforrásait kihasználva minél több számítógépre küldjék el saját másolatukat, amire az internet kiváló közeg.

1995 és 2003 között jelentősen átértékelték a férgek fogalmát. A férgek fő céljává a hálózaton való terjedés vált. „A férgek olyan programok vagy program-gyűjtemények, amelyek képesek más rendszerekre eljuttatni önmaguk funkcionálisan ekvivalens másolatát. Megjegyzendő, hogy a vírusokkal ellentétben ez a csoport nem szükségszerűen csatolja saját programját más hordozóprogramokhoz."[123]

Így jutunk el a férgek 2006-os definíciójáig: a férgek olyan önálló programok, amelyeket arra terveztek, hogy automatikusan terjesszék magukat (saját másolatukat) számítógépről számítógépre. Általában elektronikus levélben vagy az interneten keresztül terjednek, kihasználva a megtámadott rendszer sebezhetőségét vagy a felhasználók hiszékenységét.[124]

A férgek legnagyobb ereje valóban a gyors terjedés. Ezt a gyorsaságot a saját szememmel is lehetőségem volt megtapasztalni. Nem kellett

122 Nagy Gábor: *Vírusvédelem a PC-n.* ComputerBooks Kiadó, Budapest, 1995. 15–16. p.

123 Szappanos Gábor: *Kirándulás a számítástechnika sötét oldalára.* VirusBuster Kft., Budapest, 2003. 6. p.

124 Forrás: a Virus Bulletin nevű, független malware tanácsadó honlapja, http://www.virusbtn.com – letöltve: 2011.11.16.

tíz perc, hogy egy védelem nélkül hagyott (azaz szervizcsomag nélküli), internetre kötött Windows XP-t megfertőzzön egy féregprogram. Többek között ezért is van nagy szerepük az operációs rendszerek biztonsági frissítéseinek.

Trójai programok: Az ismert ókori csel eszközéről kapták a nevüket. Olyan rosszindulatú programok, amelyek úgy tesznek, mintha nem lennének azok. Azért „viselkednek" így, hogy valamilyen trükkel rávegyék a gyanútlan felhasználót, hogy futtassa le őket.[125]

A trójai programok családjába tartoznak a backdoor típusú programok, amelyek kiskapukat (szó szerint hátsó ajtókat) nyitnak a hálózatról érkező támadás vagy támadók számára. A clicker programok átirányítják a felhasználót az egyik weblapról a másikra, megváltoztatják a böngésző kezdőlapját, beleírnak a Kedvencek mappába. Erre példa: a Kedvencek mappában a kedvenc weboldalunk neve van, de a rámutató link már más, így juthatunk el olyan oldalakra, ahova nem kellene. A downloader programok installálásuk után megkísérlik más malware-ek észrevétlen letöltését és installálását a fertőzött gépre. A dropper programok működő programok, amelyek a működő program kódja mellett más vírusokat, malware-eket (többet is!) tartalmaznak és aktiválnak. Végül a trójai programok közé tartoznak azon különböző kémprogramok, amelyek megpróbálnak megszerezni adatokat (jelszavakat, felhasználói neveket stb.) akár a háttértárakról, akár a memóriából, és kijuttatni azokat a támadó számára (például e-mailen).[126]

Egyéb malware: Ebbe a csoportba azok a programok tartoznak, amelyek nem sorolhatók be egyértelműen az előző három kategóriába. Vannak közöttük olyanok, amelyek képesek károkozásra, mások „csak" kellemetlenkednek, de vannak olyanok is, amelyeket egyszerűen csak

125 http://www.virusbtn.com/resources/glossary/trojan.xml – letöltve: 2011.11.16.
126 Forrás: a Virus Bulletin nevű, független malware tanácsadó honlapja, http://www.virusbtn.com – letöltve: 2011.11.16.

viccnek szántak.[127] Ilyenek az adware-ek, amelyek kevésbé veszélyesek, „csak" reklámokkal zaklatják a felhasználót, azonban kémfunkcióval is rendelkezhetnek: figyelhetik a felhasználó internetes vásárlási szokásait, és továbbíthatják ezeket az adatokat. Ezek közé tartoznak a sokkal veszélyesebb billentyűzetfigyelő programok, amelyek segítségével akár jelszavakat is el lehet lopni. A hoaxok is az egyéb malware-ek csoportját „gazdagítják". Ezek azok a levelek, amelyek valamilyen valótlan hírrel, ténnyel próbálják elérni azt, hogy tovább legyenek küldve, például: „Ha nem küldöd tovább, szerencsétlen leszel." vagy „Küldd tovább az e-mailt egy x címre, és pénzt fogsz kapni." A rosszindulatú programok közé sorolhatjuk a tréfás programokat is (jockes), amelyek nem vírusok ugyan, „csak" „viccből" imitálják a vírusfertőzés tüneteit, de a felhasználó ijedtségén túl nagyobb kárt nem okoznak (hacsak a megijedt felhasználó maga nem okoz kárt).

Védekezés a malware-ek ellen: megállapíthatjuk, hogy a vírusirtók hátrányból indultak a vírusírókkal szemben, ám mára leküzdötték ezt a hátrányt újabb antivírus technikák kidolgozásával, illetve a lehetséges malware fejlődési irányok prevenciójával. Az antivírus programokkal foglalkozó cégek ma már igen rövid időn belül választ tudnak adni az egyre újabb malware-akciókra. Fontos, hogy a jogrendszer is a vírusirtók mellé állt: jogerősen kiszabott börtön- és pénzbüntetések jelzik a nagyobb malware-támadások útját. Az is az antivírus szakemberek mellett áll, hogy a vírusok fiatal írói manapság már 10–15 éves szakértelemmel találják szemben magukat.[128]

127 A Virus Bulletin nevű, független malware tanácsadó csoportosítását vettem alapul. http://www.virusbtn.com – letöltve: 2011.11.16.

128 Szappanos Gábor: *Kirándulás a számítástechnika sötét oldalára*. VirusBuster Kft., Budapest, 2003. 10. p.

Az antivírus programok három csoportra oszthatók: víruskereső (és -irtó) programokra, vírusblokkoló programokra és integritás-ellenőrző programokra.[129]

A víruskereső és -irtó programok azon az elven működnek, hogy mindegyik vírus tartalmaz egy csak rá jellemző kódrészletet, amelyet „vírusujjlenyomat"-nak neveznek. Az antivírus programok írói ezeket az ujjlenyomatokat úgynevezett vírusdefiníciós adatbázisba gyűjtik, a víruskereső program pedig ellenőrzi, hogy a számítógépen lévő programok valamelyikében szerepel-e az adatbázisban tárolt ujjlenyomat.[130] Épp emiatt fontos, hogy mindig a legfrissebb vírusdefiníciós adatbázissal rendelkezzünk, hiszen ha régi adatbázissal fut a programunk, akkor az azóta született vírusokat nem fogja felismerni.

Ezek a programok úgy működnek, hogy ha olyan kódot találnak, amely szerepel a víruskereső adatbázisában, akkor általában három dolgot tehetnek. Ha a vírus egy egyébként nem rosszindulatú program kódjába ágyazta be magát, akkor a vírus kódját eltávolíthatja, így az eredeti program működőképes és vírusmentes marad. Ha a megtalált program maga a malware, akkor azt törölheti, de ugyanígy eltávolíthatja a fertőzött fájlt is (ezt a felhasználó döntheti el). Lehetőség van arra is, hogy a víruskereső szoftver a fertőzött fájlt karanténba helyezze, amely e fájlok biztonságos tárolására szolgáló, elkülönített terület a háttértáron (hasonlóan a „normál" karanténhoz). A fertőzött fájl karanténba helyezése csökkenti az esélyét annak, hogy a vírus lemásolja önmagát, és más fájlokat megfertőzzön. Ezzel azonban a vírus nem törlődik, hanem ott marad a számítógépen, csak a terjedése lehetetlenül el. A karanténba helyezett állományok később törölhetők, újra

129 Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007. 135. p.

130 Szappanos Gábor: *Kirándulás a számítástechnika sötét oldalára.* VirusBuster Kft., Budapest, 2003. 106–108. p.

átvizsgálhatók (újabb vírusdefiníciós adatbázis alapján), vagy visszaállíthatók eredeti helyükre és állapotukba (ha kiderül, hogy valójában nem a malware kategóriájába tartoznak).

A védelem kétféle módon valósítható meg ezekkel a programokkal: vagy a felhasználó által elindított folyamatos, rendszeres időközönként visszatérő vírusellenőrzésen alapul, vagy az úgynevezett rezidens vírusvédelmen. Az utóbbi úgy valósul meg, hogy a víruskereső program automatikusan elindul az operációs rendszer elindítása után, azaz bekerül a memóriába (ettől rezidens), és ha a felhasználó műveletet végez egy fájllal (másol, áthelyez, megnyit, ment stb.), ellenőrzi, hogy az állomány vírusmentes-e.

A blokkolók is rezidens programok, azonban ezek nemcsak a vírusdefiníciós adatbázisban szereplő malware-ek ellen képesek védekezni, hanem általában minden rosszindulatú programmal szemben. Működési elvük az, hogy a legfontosabb rendszer-funkciókat figyelik (írás, olvasás, betöltés stb.), és mielőtt ezeket alkalmaznánk, előbb a blokkolóra kerül a vezérlés, amely figyelmezteti a felhasználót a veszélyre.[131] Előnyük, hogy képesek megakadályozni bármilyen vírus futtatását, képesek kiszűrni az új vírusokat is. Azonban az a hátrányuk, hogy gyakran adnak téves riasztásokat, ugyanis a vírusokon kívül más programok is használják az előbb említett rendszerfunkciókat. Itt a felhasználói gondosság, tudatosság, figyelmesség az, amely nélkül a blokkolók nem tudják kifejteni áldásos hatásukat: ha a felhasználó a gyakori figyelmeztetések miatt minden műveletet engedélyez (a folyamatos működés érdekében), anélkül, hogy meggyőződne arról, a műveletet nem malware akarja-e végezni (el sem olvassa a blokkoló által küldött üzeneteket), akkor könnyen előfordulhat, hogy saját maga engedélyezi, hogy a vírus fertőzzön, szaporodjon.

131 Szappanos Gábor: *Kirándulás a számítástechnika sötét oldalára*. VirusBuster Kft., Budapest, 2003. 108. p.

Az antivírus programok harmadik fajtáját az integritásellenőrzők képviselik, amelyek nemcsak vírusok ellen, hanem bármilyen rosszindulatú program ellen is hatékony védelmet nyújtanak. Működésük lényege, hogy telepítéskor az állományokról adatbázist készítenek, amelyben minden fájlhoz tartozik egy bejegyzés a fájl legfontosabb adataival és egy úgynevezett ellenőrző összeggel. Így az integritásellenőrző programok gyakorlatilag „fényképet" készítenek a rendszer vírusmentesnek vélt állapotáról. Tehát képesek ellenőrizni, követni, hogy az adatbázisukba bejegyzettekhez (a „fényképhez") képest történt-e változás a fájlokban. (Amint azt fentebb láttuk, a vírusfertőzés általában valamilyen fájlba való írással, illetve a fájlrendszer megváltozásával jár.) Hátrányuk, hogy csak akkor képesek reális képet alkotni az állományrendszerről, ha adatbázisuk „tiszta", vírusmentes rendszer alapján készül, tehát valóban vírusmentes rendszerről készítettek „képet". Ha fertőzött rendszerről készítik az adatbázisukat, akkor a vírusfertőzést „normálisként" tekintik, és esetleg a víruskód eltávolítása – amikor a fájl integritása sérül – lesz számukra a fenyegető tényező, veszélyforrás.[132]

A piacon sok olyan fizetős és ingyenes termék található, amely a fenti három programfajta közül legalább kettőnek – de lehet, hogy mind a háromnak – a feladatait el tudja látni. Ezek nevét és elérhetőségeit a Függelékben találja az Olvasó. Ezek alkalmasak az otthoni és irodai védelem kialakítására is.

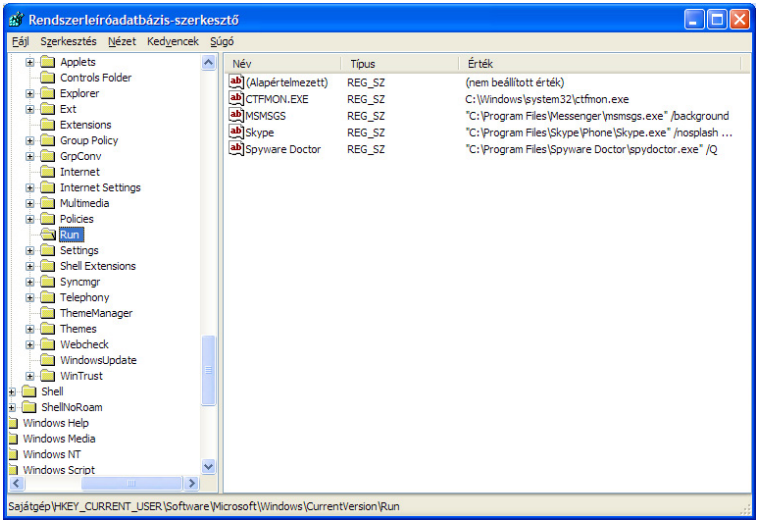
A vírusok és egyéb rosszindulatú programok forrásai a kivehető adattárolók, különösen a CD és DVD lemezek, külső winchesterek, pendrive-ok és a Flash memóriák is. A fentebb említett antivírus szoftverek ezek ellen is megfelelő eszközök, de ajánlatos gondolni egyéb eljárási szabályokra is. Például: egyáltalán rá lehet-e dugni külső adattárolót

132 Szappanos Gábor: *Kirándulás a számítástechnika sötét oldalára*. VirusBuster Kft., Budapest, 2003. 108–109. p.

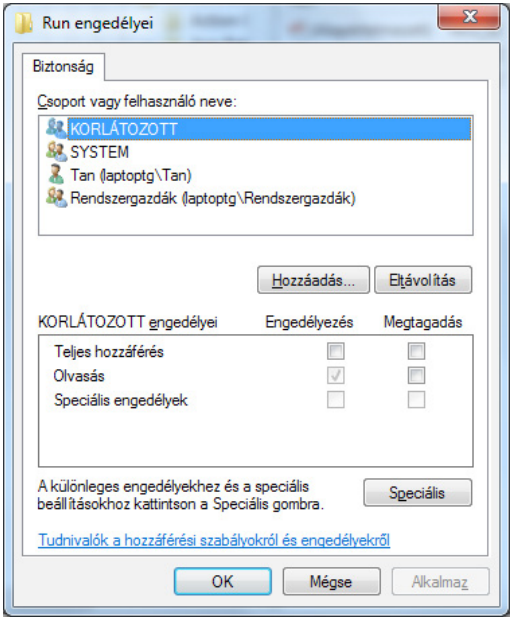
az adott intézmény számítógépeire? A felhasználók és rendszergazdák számára útmutatókat kell készíteni azoknak az eljárásoknak és gyakorlatoknak a bemutatására, amelyekkel a rosszindulatú programok behurcolásának lehetőségét minimalizálni lehet. Ezeknek az útmutatásoknak ki kell térniük a játékok és egyéb szoftverek betöltésére, a különböző internetes szolgáltatások használatára és különböző adatállományok importjára. A rosszindulatú kódok megelőzését szolgáló dokumentált eljárások és gyakorlatok be nem tartása esetén a biztonsági tudatosság fejlesztésére irányuló képzés, fegyelmet fokozó tevékenység és más kapcsolódó eljárások szükségesek.[133]

Szót kell ejteni a Windows regisztrációs adatbázisának (registry) védelméről. Ez az adatbázis a Windows „lelke", ugyanis ez tárolja az összes meghajtó-program beállításait és elérési útvonalait, az alkalmazások beállításait és elérési útvonalait, az alapértelmezett programok lelőhelyét, továbbá a menükről, opciókról, programablakokról, programtelepítésekről és egyéb programspecifikus beállításokról szóló információkat. Látható, hogy ha sérül a regisztrációs adatbázis, a Windows helyes működése, esetleg maga a rendszer elindítása kerül veszélybe. A regisztrációs adatbázisban több bejegyzés is tartalmaz automatikusan elinduló programot. Ez azért kényes pont, mert előfordulhat, hogy egy rosszindulatú program ezt a bejegyzést írja át, és a Windows indítása közben semmi lehetőségünk nem lesz arra, hogy ennek a programnak a futását megakadályozzuk. eEz ellen úgy lehet védekezni, hogy mindig rendelkezzünk „tiszta" biztonsági másolattal, illetve helyesen állítsuk be a jogosultságokat: kinek és minek van joga átírni az adatbázis automatikusan induló programokról szóló bejegyzését. (Lásd: 21-22. ábra.) A rendszerleíró adatbázist a regedit nevű programmal lehet szerkeszteni.

133 A KIB 25. számú ajánlása, 119. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.



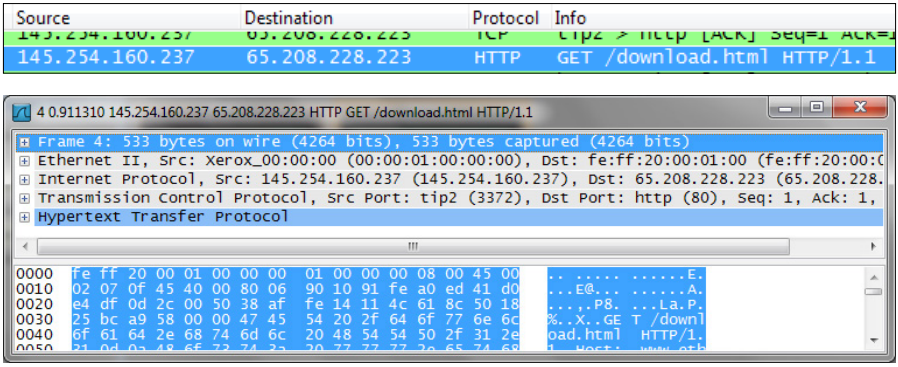
21. ábra: A registry Run bejegyzése



22. ábra: A Run bejegyzés védelme

8.1.2. Az internethez való biztonságos csatlakozás eszközei

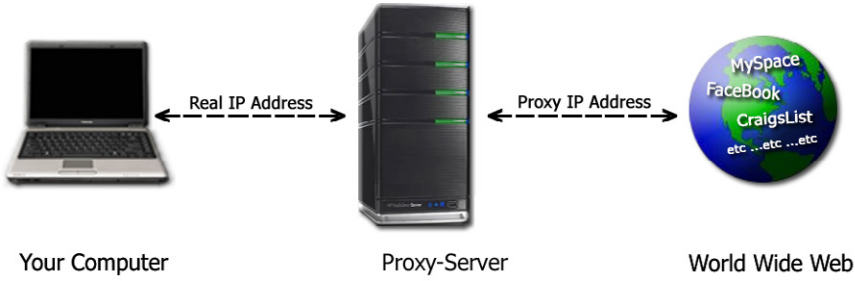
Ahhoz, hogy megértsük, hogyan is lehet biztonságosan csatlakozni a világhálóhoz, meg kell ismernünk az internetes kommunikáció alapjait. Az adatforgalom alapegysége a csomag, tehát egy letöltött fájlt így is el lehet képzelni: csomag + csomag + csomag… Az adatforgalom bizonyos szabályok szerint zajlik, melyeket a protokollok határozzák meg. Például az Internet Protocol (IP) írja le, hogyan kerülnek az egyes csomagok egyik számítógépről a másikra. Minden hálózaton levő számítógépnek van IP címe: például 192.101.32.156 (IPv4 szabvány szerint). A csomag így ezekből a részekből áll: forrás IP cím, cél IP cím, adathalmaz részlete. (Lásd: 23. ábra.) Az IP-nek az a hátránya, hogy nem jelzi vissza, hogy a csomagok rendben megérkeztek-e.



23. ábra: Példa hálózati csomagra és tartalmára

A Transmission Control Protocol (TCP) sorozatszámot ad minden csomagnak – így tudjuk, hány csomag lesz, illetve meggyőződik arról, hogy csomagok célt értek-e. Minden protokoll vagy alkalmazás úgynevezett kapukat (portokat) használ az egyes számítógépekhez való csatlakozás során, például http – 80 vagy 8080-as port, https – 443-as port.

A tűzfalak az internethez való biztonságos csatlakozás eszközei. Ezzel kapcsolatban számos védelmi feladat ellátására alkalmasak. Egyrészt elősegítik a név nélküli internet-használatot. Ugyanis az, hogy az interneten milyen lapokat milyen gyakorisággal látogatunk meg, személyes adatnak minősül, ilyen típusú érdeklődésünk a magánszféra védendő része. Az anonimitást biztosító tűzfalakat proxykiszolgálóknak (angolul proxy server) hívjuk, amelyeknek az a feladatuk, hogy a felhasználó megbízásából, őt helyettesítve végezzék az internet-kapcsolatok (TCP) fel-, illetve leépítését.[134] Ez annyit jelent, hogy a webszerver(ek) és a felhasználó közé egy harmadik fél, a proxykiszolgáló kerül. A felhasználó (böngészője) által kért weblapokat a proxykiszolgáló tölti le és továbbítja a felhasználónak. Így a felhasználó csak a proxykiszolgáló számára azonosítható (IP cím alapján), de az internet tartalmát szolgáltató webszerverek számára nem. (Lásd: 24. ábra.)



24. ábra: Proxykiszolgáló működése[135]

A tűzfalak másik feladata annak megakadályozása, hogy a számítógépről információ jusson ki az internetre, illetve, hogy onnan

134 Othmar Kyas: *Számítógépes hálózatok biztonságtechnikája.* Kossuth Kiadó, Budapest, 2000. 195. p.

135 http://www.elite-proxy-server.com/image-files/elite-proxy-server-diagram.png – letöltve: 2011.11.18.

rosszindulatú programok jussanak be a felhasználó számítógépébe.[136] A tűzfalak védelme olyan, mintha „fallal", „kerítéssel" vennénk körbe a számítógépet (személyes tűzfalak), illetve egy egész hálózati szegmenst (hardver alapú tűzfalak, amelyek útválasztókba vannak beépítve): az információs rendszer és a külvilág (internet) közötti ki- és bemenő (adat)forgalmat egyetlen (vagy néhány) jól őrizhető kapun keresztül bonyolítja. Tehát a tűzfal azt figyeli, hogy

- melyek azok az engedélyezett portok (kapuk), amelyeken keresztül kapcsolódni lehet;
- melyek azok a helyek (IP cím), ahonnan lehet vagy nem lehet csomagot (adatot) fogadni, és melyek azok a címek, ahova engedélyezett vagy tilos az adatküldés;
- melyek azok a szoftverek, amelyek kommunikálhatnak a világhálóval.

Tűzfalprogramokból is sok fajta található a piacon, ezen programok listáját a Függelékben találja meg az Olvasó.

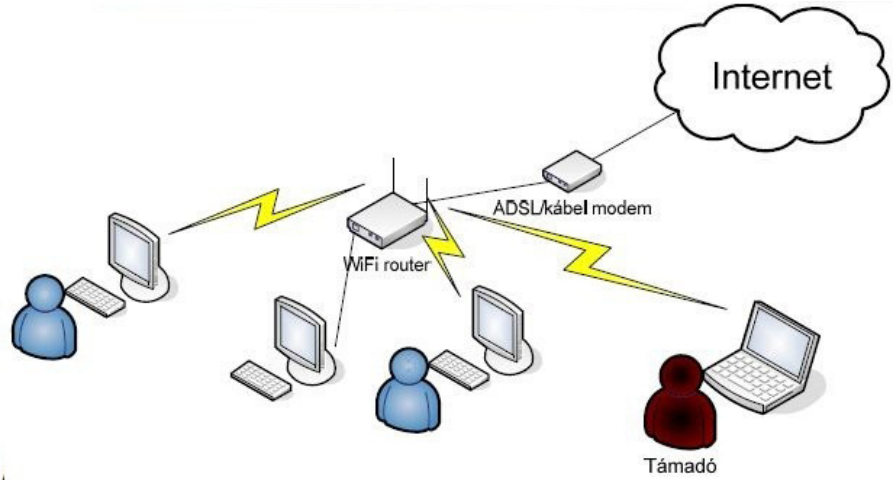
Léteznek olyan szoftverek is, amelyek komplex védelmet nyújtanak, tehát antivírus programot, kémprogram-irtót és személyes tűzfalat is tartalmaznak. Ezekről a szoftverekről is a Függelékben található forrásokból tudhat meg többet az Olvasó.

Egy személyi számítógép védelmének alappillérei tehát a következők:

- mindig friss adatbázissal futó antivírus program;
- tűzfal program;
- mindig friss adatbázissal futó kémprogram-irtó;
- legyenek fent az operációs rendszer és az alkalmazói programok frissítései;
- felhasználói tudatosság.

136 Andrew S. Tanenbaum: *Számítógép hálózatok*. PANEM Könyvkiadó, Budapest, 2004. 829. p.

Vezeték nélküli hálózatok: Az elmúlt tíz évben váltak egyre olcsóbbá és ennek okán egyre népszerűbbé a vezeték nélküli technológiák, így a vezeték nélküli hálózatok. Előnyei mellett (például nincs annyi kábel a szobában) valós veszélyeket is rejt magában ez a technológia (gondolok itt különösen a nyílt wifi hálózatokra). Egyszerű példaként nézzünk egy tipikus otthoni hálózatot! (Lásd: 25. ábra.)



25. ábra: Tipikus otthoni hálózat [137]

Az ilyen otthoni hálózatnak két gyenge pontja lehet: az egyik a felhasználó, a másik pedig a biztonsági protokollok minősége. A vezeték nélküli hálózatok természetüknél fogva kevésbé biztonságosak, mint jobban kiérlelt, nagyobb múlttal rendelkező vezetékes testvéreik. Mivel a vezeték nélküli hálózati kártyák adatközvetítő közege a levegő, így jobban ki vannak téve annak, hogy illetéktelenek is hozzáférjenek az adatokhoz. A „hálózatszaglászók" a WLAN esetében könnyebben

137 http://tszo.hte.hu/root/club_ppt/201005/eloadas_szgyi_wifi_hte.pdf – letöltve: 2011.11.18.

követhetik figyelemmel és lophatják el az adatokat, mint a vezetékeseken, hiszen a behatoláshoz nincs szükségük fizikai kapcsolatra, így könnyebb dolguk van. A leendő hackernek csak egy vezeték nélküli csatolókártyára van szüksége, valamint ismernie kell az aktuális hálózat biztonsági réseit, így akár „a ház előtt, az autóban ülve" is be tud jutni a hálózatba.

Ha a vezeték nélküli hálózaton nincs kódolás, a rajta áthaladó adatok gyakorlatilag bárki számára elérhetőek. A 26. ábrán látni lehet a csomagok forrás- és a célállomás IP címeit és a tartalmukat is.

Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port
IP/TCP	GemtekTe...	Intel:96:0...	192.168.0.4	192.168.0.1	micros...
IP/UDP	GemtekTe...	01:00:5E:...	192.168.0.4	239.255.2...	1900
IP/UDP	GemtekTe...	33:33:00:...	158.22.250.0	0.0.0.12	1900

26. ábra: Mi látszik egy nyílt, vezeték nélküli hálózaton?

A vezeték nélküli hálózati szabvány (IEEE[138] 802.11, 1997.) tervezői már a kezdettől fogva fontosnak tartották a biztonságot. Már a szabvány korai verziója is tartalmazott biztonsági mechanizmusokat, melyek célja az volt, hogy a vezeték nélküli hálózat legalább azokkal a biztonsági tulajdonságokkal rendelkezzen, mint vezetékes testvére, így ezt vezetékes ekvivalencia-protokollnak (wired equivalency protocol = WEP) nevezték el. Elméletben ez a protokoll biztosítja a hálózati adatok titkosságát, valamint másodlagos funkcióként megakadályozza, hogy illetéktelenek hozzáférhessenek magához a hálózathoz. 2001-ben számos kutató vizsgálata megmutatta, hogy a WEP nem tölti be e két funkcióját.[139] A főbb problémák: Az IEEE 802.11-es szabvány egyik hiányossága, az, hogy nem rendelkezik a megosztott kód kezeléséről. A legtöbb vezeték nélküli hálózat esetén ez mindösz-

138 Institute of Electrical and Electronic Engineers
139 http://hu.wikipedia.org/wiki/WEP – letöltve: 2011.11.18.

sze egyetlen kód, melyet kézzel állítanak be minden csomóponton és az Access Pointon (AP) is. Ha gyenge a kódolás (rövid kulcs) és túl hosszú ideig használja a hálózat, passzív lehallgatással néhány perc alatt elég csomagot lehet elfogni ahhoz, hogy azokból visszafejtsék a kulcsot.

A WEP hibáit felismerve az IEEE új biztonsági megoldást dolgozott ki, amelyet a 802.11i szabvány tartalmaz. Ennek része a WPA (Wireless Protected Access), amely a TKIP (Temporal Key Integrity Protocol) kulcskiosztást használja. A titkos kulcsot az AES (Advanced Encryption Standard) algoritmussal titkosítják. Az új módszerrel hitelesített eszközök esetében a forgalmazott adatcsomagokban dinamikusan képes váltogatni a titkosítást szolgáló kulcsokat, azaz hiába szerzi meg a támadó az éppen használt kulcsot a forgalom lehallgatásával összegyűjtött adatokból, a TKIP-nek elég 5 percenként változtatni a kulcson, a betörni szándékozó már kezdheti is elölről munkáját, sőt a TKIP adatcsomagonként is képes új kulcsot generálni.[140]

A WPA két működési módban alkalmazható. Otthoni felhasználóként a vezeték nélküli AP beállításánál a WPA-PSK (Wireless Protected Access – Preshared Key) beállítást érdemes választani. A WPA-PSK-nak jelszóra van szüksége, ebből áll elő a hozzáférési pont kódolási kulcsa.[141] Ez első látásra megegyezik a WEP módszerével, a WPA azonban a kapcsolódást követően folyamatosan változtatja a titkos kulcsot, így szinte lehetetlen megfejteni az éppen érvényben lévőt. Újabb kapcsolódás esetén ismét az eredeti kulcsot kell megadni, tehát csak arra kell figyelnünk, hogy titkos kulcsunkat senki ne ismerje meg rajtunk kívül.

A WPA másik működési módja az úgynevezett Enterprise mód, amely nagyvállalatok számára nyújt biztonságos megoldást. Otthoni

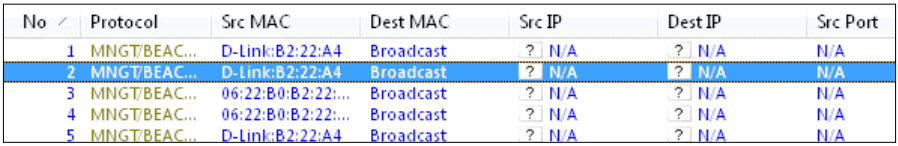
140 http://torpospapa.weboldala.net/vezetek_nelkuli_halozat_otthon_-_ii.html – letöltve: 2011.11.18.

141 Andrew Conry-Murray – Vincent Weafer: *Internetes biztonság otthoni felhasználóknak*. Kiskapu Kiadó, Budapest, 2006. 161. p.

alkalmazása körülményes. Ez a mód az EAP -ot (Extensible Authentication Protokol) használja, amellyel kiterjeszthető a hitelesítés, egy felhasználó például a vállalati azonosító adataival lép be valójában a vezeték nélküli hálózatba, így gyakorlatilag dupla hitelesítésen megy át a felhasználó. Az Enterprise mode alkalmas továbbá többszintű felhasználói jogosultság kezelésére is, azaz (egyszerűen fogalmazva) meghatározható, hogy a hálózaton ki milyen erőforrásokat érhet el, például ki férhet hozzá csak az internethez, és ki férhet hozzá egyéb információkhoz is.

A WPA2 már a 802.11i biztonsági szabvány véglegesítése után jött létre, amely annyiban különbözik a WPA-tól, hogy erősebb kódolást használ, és kötelezően az AES algoritmussal titkosít.

Amennyiben titkosítjuk vezeték nélküli hozzáférési pontunk forgalmát, a külső támadó már csak kódolt adatokat lát. (Lásd: 27. ábra.) Vessük össze az előző ábrán látottakkal!



No	Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port
1	MNGT/BEAC...	D-Link:B2:22:A4	Broadcast	? N/A	? N/A	N/A
2	MNGT/BEAC...	D-Link:B2:22:A4	Broadcast	? N/A	? N/A	N/A
3	MNGT/BEAC...	06:22:B0:B2:22:...	Broadcast	? N/A	? N/A	N/A
4	MNGT/BEAC...	06:22:B0:B2:22:...	Broadcast	? N/A	? N/A	N/A
5	MNGT/BEAC...	D-Link:B2:22:A4	Broadcast	? N/A	? N/A	N/A

27. ábra: Kódolt, vezeték nélküli hálózat „látványa”

Amikor új vezeték nélküli routert vásárolunk és beüzemeljük, érdemes néhány dolgot figyelembe venni:[142]

- a router neve gyári;
- a router jelszava gyári;
- a router IP-címe gyári;
- a router SSID[143]-ja gyári;
- a router WiFi interfésze titkosítatlan, azaz nyílt,;
- ha mégis titkosított, akkor gyári jelszóval van ellátva!

142 http://tszo.hte.hu/root/club_ppt/201005/eloadas_szgyi_wifi_hte.pdf – letöltve: 2011.11.18.

143 A vezeték nélküli hozzáférési pont neve.

A router MAC címéből ki lehet találni, hogy melyik cég gyártotta a routert, és innentől kezdve a világhálóról meg lehet tudni bármelyik router gyári adatait. Ezeket az adatokat tehát érdemes a beüzemelést követően azonnal megváltoztatni. Fontos, hogy a router biztonsági beállításainál a WPA2-PSK-t vagy a WPA2-PSK+AES-t válasszuk! (Lásd: 28. ábra.) A hozzáférési pont jelszavánál természetesen vegyük figyelembe a jelszavak biztonságáról korábban tanultakat!

28. ábra: Vezeték nélküli router helyes beállítása

Azért is érdemes a WPA2-t használni, mert 2009-ben japán tudósok feltörték a WPA-TKIP titkosítását.[144]

Vannak olyan biztonsági lehetőségek, amelyeket ma már könnyű kijátszani:

- Kiszűrjük azokat a MAC címeket, amelyek hozzáférhetnek a hálózathoz.
  - A MAC címet lehet klónozni, átállítani, illetve a hálózatot figyelve könnyű kideríteni, melyek a „legitim" MAC címek,

144 http://index.hu/tech/2009/08/28/egy_perc_alatt_feltorheto_a_wifi – letöltve: 2011.11.18.

aztán már csak meg kell várni, míg a legitim felhasználó eltűnik az éterből…
- Elrejtjük a hozzáférési pont nevét (SSID).
  - Ha valaki kommunikál, az SSID már lehallgatható.

Sok negatív következménnyel kell számolnia annak, akinek rákapcsolódnak a hálózatára:
- hozzáférnek a belső hálózathoz…
- az operációs rendszer biztonsági réseit kihasználva adatot lehet lopni;
- kéretlen leveleket (spam) küldhetnek a hálózatból, internetes bűncselekményeket hajthatnak végre, és a nyomok a feltört hálózathoz fognak vezetni;
- sávszélességet foglalnak, így lassabb lesz a hálózat;
- egyéb illegális tevékenységet végezhetnek mindenféle kockázat nélkül.
- Németországban már pénzbüntetés jár a nem védett WiFi hálózatért.[145]

Mivel az otthoni hozzáférési pontok általában nem naplóznak, jó esélyel nem lehet megtalálni azt, aki betört az otthoni hálózatunkba.

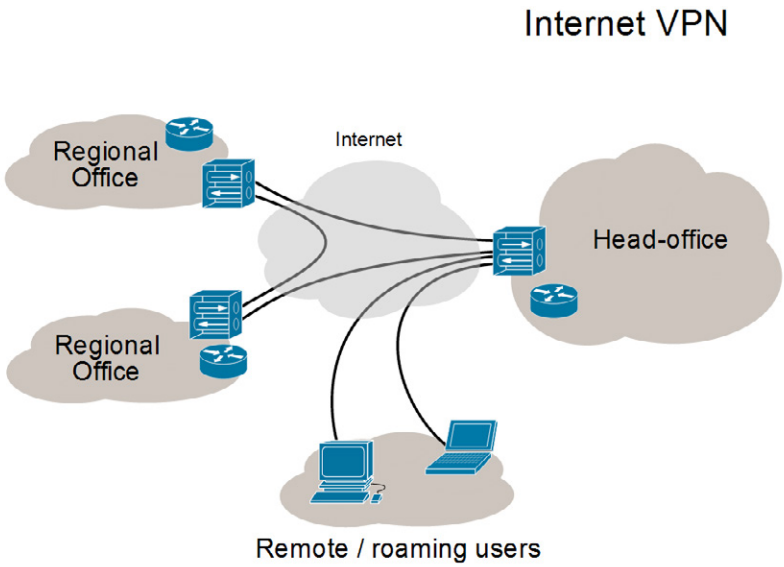
Amennyiben nincs más lehetőségünk, mint nyílt, vezeték nélküli hálózaton barangolni, vagy egyszerűen kódoltan szeretnénk az „éterbe" küldeni az adatfolyamunkat, jó megoldás a virtuális magánhálózat használata.

A virtuális magánhálózat (Virtual Private Network, VPN) egy számítógép-hálózat fölött kiépített másik hálózat. „Magán" jellegét az adja, hogy a VPN-en keresztülmenő adatok nem láthatók az eredeti

145 http://tszo.hte.hu/root/club_ppt/201005/eloadas_szgyi_wifi_hte.pdf – letöltve: 2011.11.18.

hálózaton, mivel titkosított adatcsomagokba vannak becsomagolva. A titkosítás általánosan használt szolgáltatása a VPN-nek, de titkosítás nélkül is használható a különböző adatfolyamok elkülönítésére vagy a hálózat logikai felépítésének egyszerűsítésére.[146]

A VPN-t gyakran arra használják, hogy a munkatársak távolról hozzáférjenek munkahelyük hálózatához. Az interneten keresztül biztonságos csatorna építhető ki a munkahelyen kívüli számítógép és a vállalat központjában működő VPN forgalomirányító között. Így a felhasználó bár fizikailag távol van, logikailag a vállalati hálózatban lesz benne a gépe. (Lásd: 29. ábra.)



29. ábra: Virtuális magánhálózat[147]

146 http://hu.wikipedia.org/wiki/Virtu%C3%A1lis_mag%C3%A1nh%C3%A1l%C3%B3zat – letöltve 2011.11.19.

147 http://hu.wikipedia.org/wiki/Virtu%C3%A1lis_mag%C3%A1nh%C3%A1l%C3%B3zat – letöltve 2011.11.19.

8.1.3. Adatbiztonság az internethasználat során

Még mielőtt megismernénk azt, hogy a böngészők milyen biztonsági beállításokat nyújtanak, nézzük meg mindennek az alapját, néhány kriptográfiai alapfogalmat, illetve magát a kapcsolatot, amin keresztül egy böngészőprogramhoz eljutnak az adatok.

Napjainkban kétfajta titkosítási módszert alkalmaznak: a szimmetrikus kulcsú és az aszimmetrikus kulcsú titkosítást. A titkosítás olyan matematikai eljárás, melynek során egy üzenetet akképpen változtatunk meg felismerhetetlenül, hogy abból az eredeti üzenet csak valamilyen, kizárólag a küldő és a címzett által ismert eljárás segítségével fejthető vissza.[148] (Lásd: 30. ábra.)

30. ábra: Titkosítás[149]

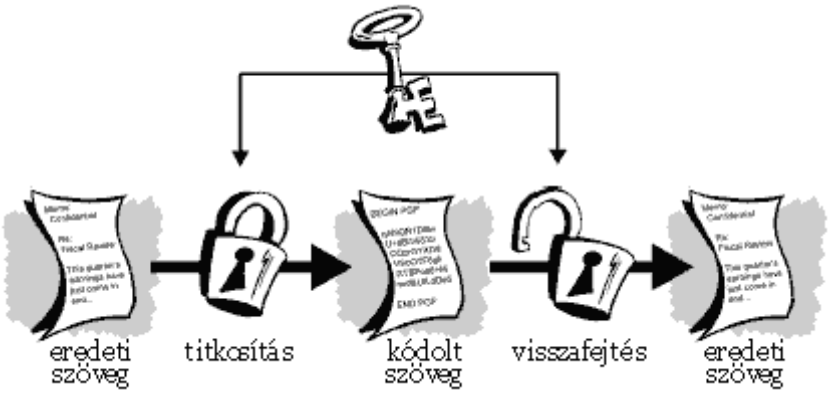
A titkosítás és visszafejtés során használt eljárás két részből áll: az egyik a titkosító/visszafejtő algoritmus (cipher), a másik pedig ennek az algoritmusnak egy vagy több paramétere, a kulcs (key). A művelet során a titkosító algoritmusnak két bemenete van: a titkosítandó adat és a kulcs, az eljárás kimenete pedig a titkosított információ. A visszafejtésnél ez utóbbi és a kulcs lesz a bemenet, a visszafejtett szöveg pedig a kimenet. Az algoritmus/kulcs

148 http://ecdlweb.hu/Elektronikus_al%C3%A1%C3%ADr%C3%A1s,_titkos%C3%ADt%C3%A1s – letöltve: 2011.11.26.

149 http://ecdlweb.hu/images/5/57/M7titk1.gif – letöltve: 2011.11.26.

jellege alapján különböztetjük meg a szimmetrikus kulcsú, illetve az aszimmetrikus vagy más néven nyilvános kulcsú (public key) titkosítási eljárásokat.

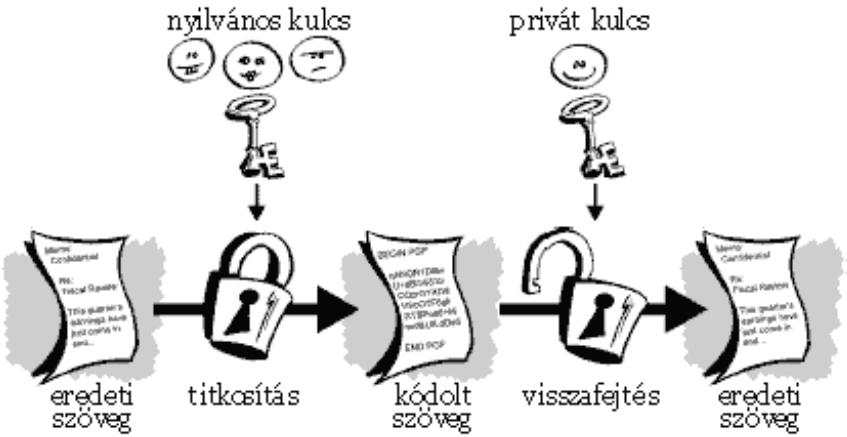
A szimmetrikus titkosításnál a kódoláshoz és a visszafejtéshez használt kulcs megegyezik, vagy egyik könnyen kiszámolható a másikból. (Lásd: 31. ábra.) Ilyen algoritmusokra példa a DES, TripleDES, AES (Rijndael), Blowfish, CAST, IDEA, Twofish, MARS.



31. ábra: Szimmetrikus titkosítás[150]

Mint láttuk, a szimmetrikus eljárás gyenge pontja a titkosítás kulcsa, amit valamilyen megbízható módon kell a címzettel tudatnunk. Ezt a problémát a nyilvános kulcsú titkosító algoritmusok oldják meg, melyek összetartozó kulcspárt használnak. Az egyik neve privát vagy más néven titkos kulcs (private key); ezt – mint a neve is mutatja – titokban tartjuk. A másikat, a nyilvános kulcsot (public key) pedig szabadon elérhetővé tesszük bárki számára. (Lásd: 32. ábra.)

150 http://ecdlweb.hu/images/d/dc/M7titk2.gif – letöltve: 2011.11.26.



32. ábra: Aszimmetrikus titkosítás[151]

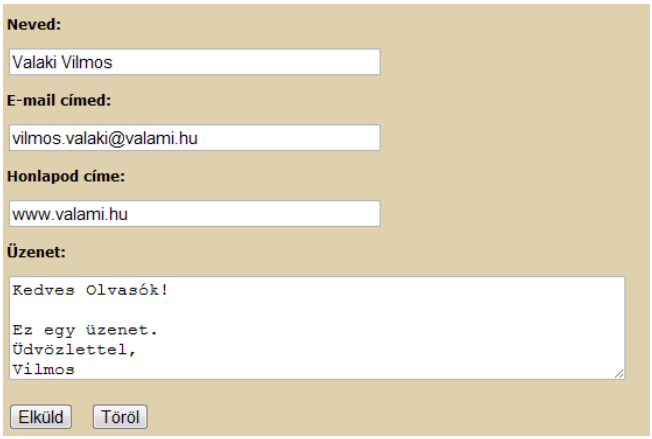
Fontos, hogy a privát kulcsból könnyen elő lehet állítani a nyilvános kulcsot, azonban fordítva már nem vagy csak nagyon nehezen lehetséges. Ez tehát azt jelenti, hogy a kellően biztonságosnak ítélt titkosítási eljárással létrehozott rejtjelezett szöveg visszafejtése a jelenleg elérhető komputeres számítási kapacitással legalább néhány emberöltőig eltartana. Legismertebb algoritmusok: Diffie-Hellmann, RSA, DSA.

A HTTP (HyperText Transfer Protocol) a világháló általános átviteli protokollja, egy kérés-válasz alapú protokoll kliensek és szerverek között.[152] A kommunikációt mindig a kliens kezdeményezi (a mi szempontunkból nézve ez általában a számítógépünk webböngészője). Amikor beírjuk a http://valami.hu címet a böngészőprogramunkba, akkor ezt a protokollt használjuk. Ezen lépés után a kapcsolat felépítése a szerverrel úgy történik, hogy egy TCP-összeköttetés (Transmission Control Protocol) jön létre a kiszolgáló gépének 80-as portjával.

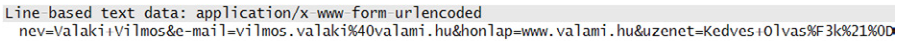
151 http://ecdlweb.hu/images/3/3c/M7titk3.gif – letöltve: 2011.11.26.
152 http://iesb.hu/logikai-biztonsag/protokollok-ftpsftp-http-https-ssl – letöltve: 2011.11.24.

A HTTP 1.0-ban az összeköttetés kiépítése után csak egyetlen kérést lehetett elküldeni, amire csak egyetlen válasz érkezhetett, ami után a felek lebontották a TCP-összeköttetést. Ez teljesen meg is felelt az akkori oldalaknál (a HTTP 1.0 1990-ben jött létre), azonban az új, több médiaadatot (például képeket) tartalmazó oldalaknál már nem volt elégséges megoldás. Ez vezetett a HTTP 1.1-hez, ami már támogatja a tartós kapcsolatokat. Ezáltal lehetővé vált, hogy egy kiépített TCP összeköttetésen belül több kérést küldjünk el egymás után, és ezekre válaszokat kapjunk. Így jelentősen csökkenteni lehet a TCP-re eső terhelést (és az oldalak betöltési idejét).

Az egyik fontos HTTP művelet a GET, amely egy weboldal letöltését kezdeményezi. Amikor a HTTP protokollt használjuk, egyáltalán nem vagyunk biztonságban, ugyanis a GET által lekért adatokat bárki elolvashatja, aki az átvitel közben hozzáfér. A 323. ábra egy adatbekérő honlap részletét tartalmazza (ez lehetne akár egy webes e-mail kliens is). A 334. ábrán látható, hogy a kommunikáció olvasható az azt lehallgatók számára, így hozzájuthatnak olyan személyes adatokhoz, mint például az e-mail cím.



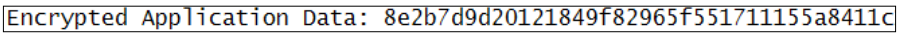
33. ábra: Adatbekérő űrlap



34. ábra: Az adatok HTTP kapcsolaton keresztül olvashatók

Ezen hiba elhárítására lett bevezetve a HTTPS (Hypertext Transfer Protocol over SSL) protokoll, ami szintaktikailag majdnem teljesen megegyezik a HTTP-vel (a 80-as port helyett a 443-ast használja), azonban jelzi a webszervernek, hogy az SSL réteget is használni kell az adatátvitel során. Ez a megoldás akkor is működik, ha csak az egyik oldal hitelesített. Így van ez a HTTP protokoll esetében is (általában csak a szerver hitelesített, a böngésző nem).

Az előbb megemlített SSL (Secure Socket Layer – biztonságos csatlakozóréteg) egy protokollréteg, amely a TCP/IP rétege és a HTTP rétege között helyezkedik el. Böngészésnél az SSL teszi lehetővé a biztonságos kommunikációt a böngésző és a webszerver között. A hitelesítéshez digitálisan aláírt tanúsítványokat használ, a kommunikáció titkosítva zajlik. Az SSL kapcsolat-felépítés során a böngésző és a szerver közösen megegyeznek egy kulcsban. Ez általában véletlenszerű számsorozat. Ebből generálják azután – az egy kapcsolat erejéig használatos – kulcsot, és ezt használják valamely szimmetrikus titkosító algoritmussal (például DES, AES).[153]



35. ábra: HTTPS kapcsolaton keresztül már kódolt az üzenet

A másik protokoll, amelyet az SSL utódjának is nevezek, a TLS (Transport Layer Security). A protokoll elsődleges célja a titkosság és az adatintegritás biztosítása a két egymással kommunikáló alkalmazás között.[154] A kapcsolódás azzal indul, hogy a kliens egy TLS-el ellátott

153 http://iesb.hu/logikai-biztonsag/protokollok-ftpsftp-http-https-ssl – letöltve: 2011.11.24.

154 http://wiki.hup.hu/index.php/TLS – letöltve: 2011.11.26.

szerverhez kérelmet küldve próbál biztonságos kapcsolatot létesíteni, és listát biztosít a szerver számára a felhasználható kriptográfiai algoritmusokkal és hash függvényekkel. Majd ebből a listából a szerver kiválasztja a legerősebbet, azaz a legnehezebben feltörhetőt. Aztán a szerver elküldi a digitális aláírását, ami a szerver nevéből, egy tanúsítványból és a szerver nyilvános kulcsából áll. A kliens ezután már képes csatlakozni, és elkészíti a munkafolyamat-azonosító kulcsot (session key). Ilyen kulcs előállításához a kliens vesz egy véletlen számot, amit titkosít a szerver nyilvános kulcsával együtt, és ennek eredményét visszaküldi a szerver számára, amit kizárólag a szerver képes dekódolni a titkos kulcsa segítségével.

A világhálón barangolva biztonságunkat böngészőnk beállításainál növelhetjük. Ez a tankönyv nem kíván állást foglalni a „böngészőháborúban". Biztos, hogy nincsen 100%-osan biztonságos böngésző.

Az Internet Explorer rossz híre az általa használt ActiveX technológia miatt van. Ezzel a technológiával a weblapok interaktívabbá tehetők (például animálás útján vagy a böngésző ablakában nyílnak meg különböző típusú fájlok). Az ezen technológiával írt programok együtt működnek az operációs rendszerrel, kvázi „beépülnek", így egy rosszindulatú ActiveX-program közvetlenül hozzáférhet az operációs rendszerhez, s ily módon komoly károkat okozhat.[155] Azt gondolom, hogy a népszerűség átka miatt is vált közkedvelt célponttá az Internet Explorer.

Ilyen módon a többi böngészőre kevesebb figyelem vetült, és az ActiveX technológia hiánya miatt kisebb a sebezhetőség. A többi böngésző (például Google Chrome, Mozilla Firefox) interaktivitását Java kisalkalmazásokkal, úgynevezett appletekkel növelhetjük. Ezek a kisalkalmazások úgynevezett „homokozóban" futnak, azaz el vannak

155 Andrew Conry-Murray, Vincent Weafer: *Internetes biztonság otthoni felhasználóknak*. Kiskapu Kiadó, Budapest, 2006. 119. p.

zárva az operációs rendszer erőforrásaitól, így közvetlen módon sokkal nehezebb megvetnie a lábát egy rosszindulatú programnak.[156]

Néhány dolgot érdemes megfogadni a böngészőnk biztonsági beállításaival kapcsolatban:

- Ne engedjük, hogy a böngésző elmentse a jelszavainkat, különösen, ha nyilvános helyen használjuk az internetet!
- „Harmadik féltől származó sütik[157] (cookie-k) elfogadása: megerősítés minden alkalommal" opció bekapcsolása.
- Adatvédelmi szempontból a Privát böngészés beállítása ajánlott.
- Érdemes mindig a böngészőnk legfrissebb verzióját használni.

A biztonságos internethasználatot elősegíti a Firefox HTTPS everywhere és Force-TLS nevű kiegészítője.

Végül, de nem utolsósorban érdemes beszélni korunk egyik legnépszerűbb böngészési célpontjáról, a közösségi oldalakról, amelyek közül a Facebookot fogom kiemelni.

A Facebooknak ma annyi felhasználója van, hogy gyakorlatilag a világ minden 13. embere rajta van. Ez körülbelül félmilliárd ember. Adatbiztonsági szempontból igen veszélyes terület, ugyanis emberi tulajdonságok előtérbe helyezésével el lehet érni, hogy önként osszunk meg olyan adatot, amit valójában nem adnánk ki. A Facebook egyik legegyszerűbb módszere, hogy ki lehet fejezni a tetszésünket többek között emberek, hozzászólások, fényképek iránt. Általában minden ember örül annak, ha valamilyen hozzá kapcsolódó dologról pozitív véleménnyel vannak az ismerősei, barátai. Ilyen módon személyes közösségi élmény-érzést (vagy ehhez hasonlót) lehet elérni, így bátran

156 Andrew Conry-Murray, Vincent Weafer: *Internetes biztonság otthoni felhasználóknak*. Kiskapu Kiadó, Budapest, 2006. 125. p.

157 Más néven HTTP-süti: egyes webszerverek által küldött kódsorozat, mely a kliens számítógépének háttértárolójára kerül, és a felhasználó későbbi azonosítására szolgál.

megosztunk magunkról olyan adatokat, amelyek ha például egy ügyintézés adatvédelmi hibája miatt kerülnének ki, perrel fenyegetnénk az adott intézményt.

Azt tapasztalom, hogy sok felhasználó nem böngészi végig az adatvédelmi beállításokat. Az egyik ilyen opció, amit érdemes beállítani, az a Biztonságos böngészés, amit a Fiókbeállítások Biztonság részénél találunk. Ezzel azt lehet elérni, hogy mindenképp HTTPS protokollt használjunk, amikor a Facebookot böngésszük.

Az Adatvédelmi beállításoknál lehet szabályozni, hogyan tartjuk a kapcsolatot ismerőseinkkel: kik láthatják az adatlapunkat név vagy kapcsolat alapján; kik küldhetnek nekünk mint ismerősnek jelölést vagy üzenetet; kik tehetnek közzé az üzenőfalunkon.

Az egyik legfontosabb adatvédelmi beállítás, hogy kik láthatják az üzenőfalunkat, a hozzászólásainkat, a képeinket és az alapadatainkat. Ezeket ma már igen jól lehet differenciálni, ugyanis lehetőségünk van csoportokat létrehozni az ismerőseink között (például barátok, család, évfolyam stb.), és külön be tudjuk állítani akár azt is, hogy az adott csoport mit láthat és mit nem az adataink közül. Ugyanez az elv igaz az alkalmazásokra is. Érdemes egyik alkalmazásnak sem engedni, hogy automatikusan hozzászólásokat tehessen az üzenőfalunkra.

Mi történhet, ha nem figyelünk oda ezekre? Megtörtént eset, hogy egy Facebook felhasználó lelkesen kiírta az üzenőfalára, hogy vett egy plazmatelevíziót, majd megosztotta országgal-világgal, hogy elmegy két hétre nyaralni külföldre, végül arra ért haza, hogy valaki feltörte a lakását és elvitt „valamit".

Mobil alkalmazásokkal és a nem rég megjelent Check in szolgáltatással minden egyes hozzászólásunkhoz meg lehet adni, hogy hol is vagyok, ily módon egy külső megfigyelő végig tudná kísérni az egész életünket, szokásainkat. Biztos, hogy megéri ennyi személyes adatot rábízni a Facebookra és közönségére?

Az elmúlt évek folyamán sokat javult a Facebook adatvédelme, de messze nem működik tökéletesen. 2011 őszén 250 gigabájtnyi személyes adatot bányásztak ki a Facebookból amerikai tudósok.[158] A vizsgálathoz a programokat, az úgynevezett socialbotokat úgy tervezték, hogy az valódi felhasználónak álcázza magát. A kísérletben 102 socialbot és 1 ember vett részt. Azt várták a kutatók, hogy a Facebook ki fogja szűrni ezeket a robotokat, azaz programokat. Nem így történt. Igazából csak húszat zárt ki a rendszerből a közösségi oldal, de azokat is csak azért, mert más felhasználók blokkolták, illetve spamnek jelölték őket.

Ezek a robotok több mint 3000, valószínűleg valódi emberi barátra tettek szert, és így az ő személyes adataikra is, illetve, mivel rengeteg felhasználó a barátaik barátaival is megosztja érzékeny adatait, így a robotoknak kb. 1 millió ember személyes adatait sikerült beszerezni. Ez olyan, mintha valaki minden második budapesti ember személyes adatait ismerné. Ezzel kapcsolatban az a rossz hír, hogy nem kell sok pénz ahhoz, hogy valaki egy ilyen robotot megvásároljon a feketepiacon.

8.1.4. Titkosítás az elektronikus levelezésben, az adatforgalomban

Az elektronikus levelezést széles körben alkalmazzák a hivatalos kommunikáció során – már csak azért is, mert ezzel sok papírt és pénzt lehet megtakarítani. Az elektronikus üzenetküldés, az e-mail, az azonnali üzenetküldés vagy az online konferenciák egyre fontosabb szerepet játszanak az üzleti információcserében. Az elektronikus üzenetküldésnek a papír alapú adatközléstől jelentősen eltérő

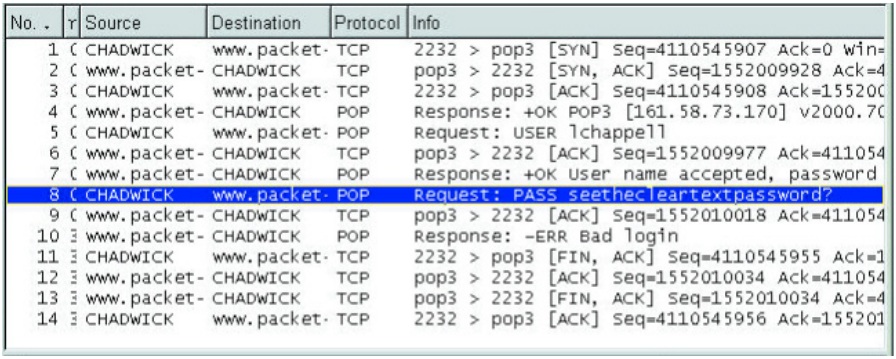
158 http://index.hu/tech/2011/11/03/kutatok_250_gigabajtnyi_szemelyes_adatot_banyasztak_ki_a_facebookbol – letöltve: 2011.11.26.

kockázatai vannak. A KIB 25. ajánlása a következő kockázatokat sorolja fel:[159]

a) Az üzenetek illetéktelen elérésének vagy módosításának, illetve a szolgáltatás megtagadásának veszélye.
b) Emberi hibákból eredő veszélyeztető tényezők, például rossz címzés vagy irányítás.
c) Bizalmas adatok továbbításának lehetősége és ennek veszélyei, például nem titkosított kapcsolat használata.
d) A feladó és a címzett hitelesítésének problémái (könnyű a feladó e-mail címét meghamisítani), illetve a levél átvételének bizonyítása.
e) A kívülről hozzáférhető címjegyzékek tartalmával való visszaélési lehetőségek.
f) Távolról bejelentkező felhasználó biztonsági problémái.
g) Rosszindulatú program forrása lehet az elektronikus üzenet: vagy az üzenet csatolmánya, vagy maga az üzenet, ha az .html-ben készült, ugyanis ilyenkor rosszindulatú kódot lehet beleírni.

A nem titkosított kapcsolat használatának veszélyeiről már szó volt a HTTP-protokoll kapcsán. A levelezés azért érzékenyebb, mert minden egyes kapcsolódáskor, azaz a levelek fogadásakor és elküldésekor hitelesítés történik, és a hitelesítés összes információja (tehát a jelszó is) – nem titkosított kapcsolat esetén – olvasható a hálózaton. (Lásd: 36. ábra.) Ilyen protokoll a POP3 (Post Office Protocol version 3), melynek segítségével az e-mail kliensek egy meglévő TCP/IP kapcsolaton keresztül letölthetik az elektronikus leveleket a kiszolgálóról.

159 A KIB 25. számú ajánlása, 135–137. p., www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf – letöltve: 2011.10.28.



No. .	Source	Destination	Protocol	Info
1	CHADWICK	www.packet-	TCP	2232 > pop3 [SYN] Seq=4110545907 Ack=0 Win=
2	www.packet-	CHADWICK	TCP	pop3 > 2232 [SYN, ACK] Seq=1552009928 Ack=4
3	CHADWICK	www.packet-	TCP	2232 > pop3 [ACK] Seq=4110545908 Ack=155200
4	www.packet-	CHADWICK	POP	Response: +OK POP3 [161.58.73.170] v2000.70
5	CHADWICK	www.packet-	POP	Request: USER lchappell
6	www.packet-	CHADWICK	TCP	pop3 > 2232 [ACK] Seq=1552009977 Ack=411054
7	www.packet-	CHADWICK	POP	Response: +OK User name accepted, password
8	CHADWICK	www.packet-	POP	Request: PASS seetheCleartextpassword?
9	www.packet-	CHADWICK	TCP	pop3 > 2232 [ACK] Seq=1552010018 Ack=411054
10	www.packet-	CHADWICK	POP	Response: -ERR Bad login
11	CHADWICK	www.packet-	TCP	2232 > pop3 [FIN, ACK] Seq=4110545955 Ack=1
12	www.packet-	CHADWICK	TCP	pop3 > 2232 [ACK] Seq=1552010034 Ack=411054
13	www.packet-	CHADWICK	TCP	pop3 > 2232 [FIN, ACK] Seq=1552010034 Ack=4
14	CHADWICK	www.packet-	TCP	2232 > pop3 [ACK] Seq=4110545956 Ack=155201

36. ábra: A jelszó a 8. csomagnál olvasható[160]

A következő védelmi módszereket alkalmazhatjuk elektronikus leveleink biztonságának megőrzése érdekében:[161]

Az egyik védekezési módszer a levelek titkosítása, rejtjelezése. Ilyenkor a lehallgatás ellen szeretnénk védekezni, tehát a levélnek már kódolva kell lennie még mielőtt a levél elhagyja a számítógépünket, ,és a fogadó félnek a saját gépén kell visszafejtenie a levelet. Az a cél, hogy a külvilág mindenképpen a kódolt levelet „lássa". Titkosítási módszerként olyan algoritmust kell használni, ami garantálja, hogy a levelet csak a címzett tudja dekódolni és elolvasni. Ezeknek előfeltétele az, hogy a küldő és a címzett számítógépe biztonságos, „tiszta" legyen. Ezt az állapotot a korábban tárgyalt antivírus és tűzfal programokkal éretjük el.

A levelek titkosítására a legegyszerűbb mód titkosított kapcsolatot használni a levél küldésénél és fogadásánál. Itt a kapcsolat a korábban említett TLS vagy SSL protokollt használja.

A másik védelmi módszer a levelek ellátása elektronikus aláírással, amellyel két veszélyforrás ellen védekezhetünk: az elektronikus levelek

160 http://support.novell.com/techcenter/articles/img/nc20042004_05tt5_01.gif – letöltve: 2011.11.26.

161 Nagy Sándor: *Elektronikus leveleink védelme.* ComputerBooks Kiadó, Budapest, 2005. 63–65. p.

illetéktelen módosítása a kézbesítés során, illetve a levelek vagy azok küldőjének hamisítása. A digitális aláírás garantálja a levél tartalmi hitelességét és a küldő fél személyazonosságát. Az elektronikus aláírástól elvárjuk, hogy legyen egyedi és személyhez köthető (hasonlóan a hagyományos aláíráshoz), ne lehessen hamisítani, szorosan kötődjön az elektronikus üzenethez, dokumentumhoz (az üzenet megváltoztatása esetén veszítse érvényét), ne lehessen hitelesen másolni (tehát egyik dokumentumról a másikra átrakni úgy, hogy a másik is hitelesen aláírt dokumentum legyen), illetve, hogy bárki ellenőrizni tudja a hitelességét.

A harmadik védelmi módszer a levelek tartalmán keresztül indított támadások (vírusok, férgek, rosszindulatú programok) ellen nyújt segítséget. Egyrészt ismét a korábban említett vírusirtó és tűzfal programok segítenek, illetve minden levelező programban és/vagy antivírus programban be lehet állítani, hogy a .html-ben kapott levelek mindig szövegesen jelenjenek meg, ugyanis így az esetleges rosszindulatú kód nem fog lefutni. Ilyenkor a .html megjelenítését kell letiltani. Ekkor a levelünk azért fog mégis helyesen megjelenni, mert a levél törzsében mindig tárolódik az üzenet szöveges változata. Ezek mellett sohase indítsunk el csatolásként kapott futtatható programot, amelynek eredetéről és ártalmatlanságáról nem győződtünk meg.

8.1.5. Mobil eszközök védelme

Napjainkban húzóágazattá vált a mobil számítástechnika, különösen az okostelefonok miatt. Az okostelefonok gyakorlatilag nem is igazán telefonok, hanem olyan tenyérgépek, amelyek többek között telefonálásra is alkalmasak. Az elmúlt években az árak annyira alacsonyak lettek, hogy már-már az alacsony kategóriás készülékek között is találunk ilyen tudású készülékeket. Ezt különösen elősegítette az Android platform megjelenése. A korábban említett közösségi hálózatok is nagyban hozzájárulnak ahhoz, hogy egyre több felhasználó vegyen

okostelefont, hiszen így napjának szinte minden percét megoszthatja ismerőseivel. Ennek veszélyeiről már korábban említést tettem.

Az egyik probléma az, hogy egy vállalati hálózaton belül kényes szereplőkké válnak ezek a készülékek, ugyanis kívülről behozott computereknek minősülnek. Tehát beengedjük-e őket a vállalati hálózatra vagy sem? Általában a top-menedzsereknek vannak ilyen készülékeik, rajtuk keresztül akarnak elérni mindent, ezeken a készülékeken tárolnak/tárolhatnak bizalmas és személyes adatokat is. Ha mindenképpen szükséges, hogy a munkatársak elérjék mobilkészüléken keresztül a vállalat hálózati erőforrásait, akkor külön biztonsági politikát kell létrehozni az ilyen készülékek számára, és a többi számítógéptől ezeket elkülönítve kell kezelni őket. Ebben a politikában érdemes letiltani a közösségi oldalak elérését.

A fenti helyzetből következik, hogy a telefon ellopása/elvesztése óriási kockázatot jelent a vállalat számára. Ilyen esetre léteznek szoftverek, amelyek lehetővé teszik, hogy egy megadott számról küldött SMS üzenettel (azaz egy jelszóval) a telefon teljes tartalma törlődjön; ezzel lehet megakadályozni, hogy illetéktelen kezekbe kerüljenek a készüléken tárolt adatok.

Az előző veszélyforrás miatt érdemes rendszeresen adatmentést végeznünk a telefonon tárolt adatokról. Sajnos a rendszeres mobil adatmentés fogalma a legtöbb helyen még ismeretlen, pedig a telefon gyártójának szoftvere általában lehetőséget ad erre, vagy be lehet szerezni külön erre a célra írt mobiltelefonos alkalmazásokat is.

A rosszindulatú programok jelenleg kisebb veszélyt jelentenek a mobiltelefonokra, mint a Windows operációs rendszert futtató számítógépekre. Viszont tudjuk, hogy a népszerűség vonzza a rosszindulatú programok íróit, így, véleményem szerint, idő kérdése, mikor fognak a hírek olyan „zombi" telefonokról szólni, amelyek felett már nem a tulajdonosuk bírja az irányítást. A nagy vírusirtó programot gyártó cégek is felismerték ezt az üzleti lehetőséget, így ma már vannak ingyenes és fizetős szoftverek, amelyekkel telefonunkat védhetjük a kívülről érkező veszélyektől. (A példákat lásd a Függelékben.)

A piacon négy nagyobb operációs rendszer (platform) verseng a vevők kegyeiért: a Blackberry, a Windows Mobile, az IOS (az Iphone rendszere) és az Android. A négy közül a legutóbbi a kakukktojás, ugyanis ez a rendszer nyílt forráskódú, nem véletlenül ez fejlődik jelenleg a legintenzívebb módon. Ám a nyílt platformnak megvannak a maga veszélyei. A zárt forráskódú rendszereknek egységesek a hardverkövetelményeik. Magyarul: például a Windows Phone 7 operációs rendszer meghatározza, hogy milyen és mekkora memória- és processzorteljesítmény mellett képes futni. Ugyanez nem igaz az Androidra. Csak a processzor órajelét tekintve a készülékek általában 600 MHz és 1,2 GHz között mozognak.

A zárt forráskód ad bizonyos szintű biztonságot, ugyanis, amikor egy fejlesztő zárt forráskódú platformra ír szoftvert, és azt publikálni akarja, akkor a szoftvernek először egy igen komoly szűrőn kell átmennie, ami a gyakorlatban egy bizottságot jelent, amely különböző és igen szigorú minőségi és biztonsági szempontok alapján értékeli a publikálni kívánt alkalmazást. Csak pozitív eredmény után jelenhet meg egy program zárt forráskódú mobil-platformon.

Sajnos, ugyanez nem igaz az androidos alkalmazásokra, bár tény, hogy akármi nem kerülhet ki a Google Play-re (korábbi nevén Android Marketre),[162] de közel sem olyan szigorú az ellenőrzés, mint a fentebb említett példánál, illetve a világháló hemzseg az olyan ellenőrizetlen androidos alkalmazásoktól, amelyeket lehetőségünk van feltelepíteni a Google Play megkerülése nélkül is. Ebben az esetben valamennyi védelmet nyújt az a beállítási lehetőség, hogy a telefonunk csak a Google Play-ről származó alkalmazásokat fogadja el.

A Symantec mobilbiztonsági felmérése szerint[163] a vállalatok utazó munkatársaik hatékonysága, valamint a kollégák mobilitása érdekében egyre inkább alkalmaznak okostelefonokat és táblagépeket. A vállala-

162 Hivatalos alkalmazásbolt androidos telefonokhoz.

163 http://index.hu/tech/2011/10/16/vedtelenek_a_vallalati_mobilok_es_tabletek – letöltve: 2011.11.27.

tok 71%-a már használ céges okostelefont, és általában a dolgozóknak is vannak ilyen készülékeik.

Annak ellenére, hogy a mobileszközök használata igen gyorsan terjed, a vizsgált vállalatok mindössze 40%-ában ellenőrzik, hogy a kollégák milyen tevékenységeket végeznek, milyen alkalmazásokat futtatnak a mobilkészülékeiken. A vizsgálat rámutatott arra is, hogy csupán a cégek húsz százalékánál dolgozik informatikai biztonsági szakértő.

A vállalatok leginkább az adatvesztéstől tartanak (69%). Megközelítően a felük az emberi tényezőt emelte ki kockázatként, beleértve a megfelelő ismeretek hiányát és a tiltott tartalmak letöltését is. A vírusfertőzés és a céges hálózat jogosulatlan használata a vállalatok 47%-ánál szerepel a legnagyobb kockázatként, miközben az informatikai biztonságért felelős vezetők többsége nem tartja reálisnak egy esetleges mobilbiztonsági támadás bekövetkeztét.

Sajnos, csak minden második vállalat alkalmaz valamilyen megoldást a mobilkészülékek védelmére, és csupán a felhasználók negyede rendelkezik valamilyen szoftveres védelemmel. A védelmi megoldások közül a legelterjedtebb a programok telepítésének tiltása, valamint a PIN-kód használata.

Ezek az egyszerű megoldások nem jelentenek teljes körű védelmet az összes vállalati mobileszközre, és nem felelnek meg a vállalatok komolyabb biztonsági előírásainak sem.

■ ■ ■

9. Adatvédelmi audit

Az Infotv. 69. §-a külön szól az adatvédelmi auditról. Az (1) bekezdés szerint „Az adatvédelmi audit a Hatóság[164] olyan szolgáltatása, amelynek célja a végzett vagy tervezett adatkezelési műveletek a Hatóság által meghatározott és közzétett szakmai szempontok szerinti értékelésén keresztül a magas szintű adatvédelem és adatbiztonság megvalósítása. Tervezett adatkezelési műveletek akkor vonhatók audit alá, ha az adatkezelésre vonatkozó koncepció kidolgozottsága ezt lehetővé teszi." Ez a paragrafus – ellentétben a törvény túlnyomó részével – csak 2013. január 1-jén fog hatályba lépni. Ennek oka, hogy Magyarországon jelenleg még nincs kialakítva egységes módszertan. Iránymutatásul szolgálhat az Európai Unió Szabványosítási Bizottsága (European Committee for Standardization, Comité Européen de Normalisation – CEN) által kiadott adatvédelmi audit keretrendszer (Personal Data Protection Audit Framework (EU Directive EC 95/46), CWA 15499-1:2006).

Dr. Péterfalvi Attila adatvédelmi biztosként 2007-ben állásfoglalást adott ki az adatvédelmi átvilágításról.[165] Ez alapján általánosságban felvázolható egy audit menete, és meghatározhatók az adatbiztonság kapcsán vizsgálandó főbb területek.

9.1. Az audit céljának meghatározása

Az audit egyik célja annak biztosítása, hogy az adatkezelés a jogszabályoknak megfeleljen, a cél meghatározása azonban ennél bonyolultabb. Ebben a szakaszban pontosan meg kell határozni az adatkezelő azon

164 Nemzeti Adatvédelmi és Információszabadság Hatóság

165 http://abiweb.obh.hu/abi/index.php?menu=Jogszabaly&dok=2585_H_2007-1 – letöltve: 2011.11.27.

tevékenységét, amelyhez szükséges az adatok kezelése, és azon jogviszonyokat, melyekhez adatkezelés kapcsolódik. Elkerülhetetlen azon érdekek nevesítése, melyeket érvényesíteni kell. Ennek tükrében határozható meg az audit általános célja: olyan adatkezelési rend kialakítása, amely a jogok gyakorlását, a kötelezettségek teljesítését, az egyes – akár egymással szemben álló – érdekeket egyaránt szolgálja. Ebben a szakaszban kell meghatározni az audit irányát, mélységét, azt, hogy csak egyes adatkezelésekre vagy a teljes adatkezelési rendszerre irányuljon; a meglévő adatkezelések jogszerűségének biztosítása legyen a középpontban vagy egy a jövőbeni céloknak is megfelelő rendszer kialakítása.

9.2. Az auditot lefolytató személy kiválasztása

Az audit lehet belső és külső. A belső audit mellett szól egyszerűsége és olcsósága, kérdéses azonban, hogy a szükséges szaktudás és tapasztalat rendelkezésre áll-e. A belső audit ellen szól az is, hogy az auditot lebonyolító személy (vagy szervezeti egység) munkáját nehezítik a szervezeten belüli függőségi viszonyok, és eredményét megkérdőjelezheti, hogy az auditot végzőnek milyen érdekei fűződnek az eredményhez, illetve, általában nehezebb észrevenni a hibákat a saját, jól megszokott környezeten belül. A külső auditot független személy végzi, akinek munkáját függőségi viszonyok nem befolyásolják, a végeredményhez pedig nem fűződik érdeke. A külső audit esetén ugyanakkor kiemelt figyelmet kell fordítani a megfelelő személy kiválasztására.

9.3. Az audit módszerének kiválasztása

Miként az fent olvasható, az auditnak többféle módszere lehet. Elterjedt a „kérdőíves” módszer, de fontos lehet az alkalmazott eljárások, technológiák, belső szabályzatok áttekintése is.

9.4. A vizsgált területek, kérdések részletes áttekintése

A szervezet által kezelt adatok közül meg kell határozni a személyes adatok körét, fel kell mérni az adatkezelések mögött álló célt. Vizsgálni kell a megfelelő jogalap létét, az érintettek jogainak érvényesülését, az erre vonatkozó eljárások szabályozottságát. A technikai-informatikai biztonság körében vizsgálni kell személyi, eljárási és technikai feltételeket. Ki kell térni arra a kérdésre, hogy az adatkezelő miképpen szabályozza a szervezeti és működési szabályzat, valamint a belső utasítások szintjén az adatbiztonság személyi, szervezeti és technikai követelményeit. Nem elhanyagolható szempont az sem, hogy a biztonságra törekvés jegyében bevezetett intézkedések hogyan hatnak az érintettek – például munkavállalók, ügyfelek – jogaira.

A gyakorlatban ilyenkor végigellenőrzik az informatikai biztonsági környezet néhány vagy összes elemét. Az auditorok

- megfigyelhetik a szervezet napi rutinját, különös tekintettel az adatkezelésre, s ezt a rutint összevethetik a hatályos szabályzatokkal;
- vizsgálhatják a szervezeten kívülről vagy belülről az informatikai rendszer sérülékeny pontjait, például
  - webes alkalmazások tesztelése külső és belső hálózatból,
  - vezeték nélküli hálózat tesztelése,
  - milyen könnyű a felhasználókat kártékony weboldalra vezetni,
  - hálózati eszközök, alkalmazások és operációs rendszerek konfigurációs beállításainak felülvizsgálata,
  - hálózati topológia vizsgálata;
- vizsgálata végrehajtásának egy speciális igénye lehet, hogy a támadást ne vagy csak nehezen lehessen észrevenni. A munkavégzés egyik célja ilyenkor – természetesen a biztonsági hibák felderítésén túl – a riasztási rendszer, az üzemeltető személyek munkájának ellenőrzése is.

9.5. Az audit eredménye

A „végeredmény" nagymértékben függ az audit céljától. Ennek tükrében az eredmény lehet egy jelentés, amely a visszásságokat feltárja, és javaslatot ad azok kiküszöbölésére. Összetettebb audit végeredménye egy átfogó adatvédelmi, adatkezelési szabályzat, amely a meglévő szervezeti és tevékenységi struktúrához, esetleg a jövőbeni célokhoz igazodva határozza meg az adatkezelés kereteit.

9.6. Nyomon követés

Az eredményes audit többnyire adott időponthoz kötődik, ehhez képest akár a jogszabályi környezet, akár az adatkezelés mögötti érdekek változhatnak. Ennek következtében elengedhetetlen a tényleges adatkezelések, a célok, illetve az esetlegesen megalkotott szabályzatok felülvizsgálata bizonyos időközönként.

Ez a folyamat azonban inkább tekinthető vázlatnak, mintsem egy audit forgatókönyvének. Ennek elsődleges oka az, hogy a keretrendszer kiindulópontja az általános európai gyakorlat, ugyanakkor a hazai adatvédelmi szabályozás speciálisnak tekinthető: az adatvédelmi törvény szigorúbb, mint az Európai Unió többi tagállamának hasonló jogszabálya. Ez az egyes területeket szabályozó, úgynevezett szektorális jogalkotásra, illetve a gyakorlatra is rányomja bélyegét. Ilyenformán egy hazai auditor szűkebb keretek között mozog, egyszersmind nehezebb is a feladata, mint külföldi kollégájának.

A másik fontos tényező, amelynek okán a fenti vázlat csak nagyvonalú iránymutatás: minden adatkezelés különbözik. Ennek okán a keretrendszer nem helyettesítheti az adatvédelemben jártas szakember közreműködését.

Míg külföldön, elsősorban Nyugat-Európában az adatvédelmi auditnak kialakult intézményei vannak: auditot végeznek szolgáltatásként gazdálkodó szervezetek, tanácsadó vállalkozások, illetve adatvédelmi hatóságok akár törvény alapján, esetleg díj ellenében, akár üzleti alapon; hazánkban ez hiányzik. Az informatikai biztonság vizsgálatával számos vállalkozás foglalkozik, többnyire csak technikai szempontból, vagyis egyfajta szemléletváltás szükséges. A jogi, szervezeti oldalról „közelítő" audit lefolytatására azonban nehezebb megfelelő személyt találni. Egyes tanácsadással foglalkozó vállalkozások már felismerték a kérdés fontosságát, így tevékenységi körüknek része az adatvédelmi szempontú átvilágítás és tanácsadás. Emellett – az adatkezelésekre vonatkozó szabályozás bonyolulttá válása és a hatékony jogérvényesítés intézményrendszerének kialakulása következtében – egyre több ügyvéd szakosodott kisebb-nagyobb mértékben adatvédelemmel kapcsolatos ügyekre.

A 2013. január 1-jétől hatályos Infotv. alapján a hatóság meghatározza az adatvédelmi audit szakmai szempontjait, illetve az adatkezelő kérelmére lefolytatja azt.[166] Így a jövőben várható egységes szempontrendszer az adatvédelmi audit tartalmával kapcsolatban. Az audit lefolytatása után a hatóság elkészíti az értékelést, melyben rögzíti az audit eredményét. Ez az eredmény nyilvános, ha csak az adatkezelő külön nem kérelmezi titkosítását.[167] Az értékelés tartalma vélhetően nem fog eltérni a fentebb olvasottaktól.

■ ■ ■

166 Infotv. 38. § (4) g)-h)
167 Infotv. 69. § (3)

Felhasznált irodalom

Könyvek, folyóiratok, jegyzetek

- Andrew Conry-Murray – Vincent Weafer: *Internetes biztonság otthoni felhasználóknak.* Kiskapu Kiadó, Budapest, 2006.
- Andrew S. Tanenbaum: *Számítógép-hálózatok.* Panem Könyvkiadó Kft., Budapest, 2004.
- Dreiliger Tímea: *Vírusvédelem.* Panem Könyvkiadó, Budapest, 2004.
- Dr. Horváth Katalin – Kohány András – dr. Orbán Anna: *7. modul. A közigazgatási informatika alapjai.* Informatikai és Közigazgatás c. tankönyvsorozat. Budapest, 2003.
- Horváth László – dr. Lukács György – dr. Tuzson Tibor – Vasvári György: *Informatikai biztonsági rendszerek.* BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001.
- Jeff Crume: *Az internetes biztonság belülről. Amit a hekkerek titkolnak.* Szak Kiadó, Budapest, 2003.
- Kazári Csaba: *Hacker, cracker, warez.* Computer Panoráma Kiadó, Budapest, 2003.
- Kis János – Szegedi Imre: *Új víruslélektan.* Cédrus Kiadó, Budapest, 1991.
- Kohány András: *Informatikai védelem. Az adatvédelem és az adatbiztonság egységes elmélete.* Elektronikus tankönyv. Budapesti Corvinus Egyetem, Budapest, 2007.
- Kovács László – Krasznay Csaba: *Digitális Mohács. Kibertámadási forgatókönyv Magyarország ellen.* Hadmérnök, IV. évf. 2009/4. sz. (december)
- Muha Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme.* (Doktori értekezés) 2007. 50. p.
- Muha Lajos: *Kiberháború az orosz–észt viszony kapcsán.* Hacktivity 2007 Konferencia, Budapest, Magyarország, 2007. 09. 22–23.

- Nagy Gábor: *Vírusvédelem a PC-n.* ComputerBooks Kiadó, Budapest, 1995.
- Nagy Sándor: *Elektronikus leveleink védelme.* ComputerBooks Kiadó, Budapest, 2005.
- Othmar Kyas: *Számítógépes hálózatok biztonságtechnikája.* Kossuth Kiadó, Budapest, 2000.
- Peter Norton – Mike Stockman: *A hálózati biztonság alapjairól.* Kiskapu Kiadó, Budapest, 2000.
- Szappanos Gábor: *Kirándulás a számítástechnika sötét oldalára.* VirusBuster Kft., Budapest, 2003.
- Dr. Szövényi György (szerk.): *Biztonságvédelmi kézikönyv.* KJK-Kerszöv Kiadó, Budapest, 2000.
- Virasztó Tamás: *Titkosítás és adatrejtés. Biztonságos kommunikáció és algoritmikus adatvédelem.* NetAcademia Kft, Budapest, 2004.

Jogszabályok

- 2080/2008. Kormányhatározat
- 90/2010. (III. 26.) Kormányrendelet
- 92/2010. (III. 31.) Kormányrendelet
- 36/2005. (X. 5.) AB határozat
- Az Európai Parlament és a Tanács 95/46/EK irányelve (Adatvédelmi Irányelv)
- Az Európai Unió Zöld Könyve a létfontosságú infrastruktúrák védelmére vonatkozó európai programról
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. Törvény
- A minősített adat védelméről szóló 2009. évi CLV. törvény
- Személyes adatok védelméről és a közérdekű adatok nyilvánosságáról 1992. évi LXIII. Törvény

Internetes anyagok

- 20 évesek a számítógépes vírusok című cikk (2003. november 11.), SG.hu Hírmagazin http://www.sg.hu/cikkek/29793 (letöltve: 2011.11.16.)

- A KIB 25. számú ajánlása www.ekk.gov.hu/hu/kib/KIB-25-1-2_IBIK_v1_0_vegl.pdf (letöltve: 011.10.28.)

- A magyar számítógépek 46%-a vírusos http://index.hu/tech/2011/02/09/a_magyar_szamitogepek_46_-a_virusos

- A személyes adatok értékét kiszámító kalkulátor http://turbulence.org/Works/swipe/swipe_data_cal.html (letöltve: 2011.11.05.)

- A Virus Bulletin, független malware tanácsadó cég honlapja http://www.virusbtn.com, http://www.virusbtn.com/resources/glossary/index

- Az adatbiztonság követelménye az új adatvédelmi törvényben http://www.adatvedelmiszakerto.hu/2011/09/az-adatbiztonsag-kovetelmenye-az-uj-adatvedelmi-torvenyben (letöltve: 2011.10.27.)

- Az Alkotmányvédelmi Hivatal honlapja http://www.ah.gov.hu/html/ iparbizt_ellenorzesek.html (letöltve: 2012.02.23.)

- Az etikus hackelés alapjai – Brute force http://etikushack.info/tananyag/bruteforce.html (letöltve: 2011.11.05.)

- Dr. Péterfalvi Attila adatvédelmi biztos állásfoglalása az adatvédelmi átvilágításról http://abiweb.obh.hu/abi/index.php?menu=Jogszabaly&dok=2585_H_2007-1 (letöltve: 2011.11.27.)

- Egy perc alatt feltörhető a wifi http://index.hu/tech/2009/08/28/egy_perc_alatt_feltorheto_a_wifi (letöltve: 2011.11.18.)

- Elektronikus aláírás, titkosítás – ECDL Web http://ecdlweb.hu/Elektronikus_al%C3%A1%C3%ADr%C3%A1s,_titkos%C3%ADt%C3%A1s (letöltve: 2011.11.26.)

- Gmail-fiók jelszó hack http://www.szerver.com/index.php/2009/07/gmail-fiok-jelszo-hack (letöltve: 2011.11.05.)

- Hungarian Unix Portal Wiki: TLS http://wiki.hup.hu/index.php/TLS (letöltve: 2011.11.26.)

- Index.hu: 250 gigabájtnyi személyes adatot bányásztak ki a Facebookból http://index.hu/tech/2011/11/03/kutatok_250_gigabajtnyi_szemelyes_adatot_banyasztak_ki_a_facebookbol (letöltve: 2011.11.26.)

- Index.hu: Védtelenek a vállalati mobilok és tabletek http://index.hu/tech/2011/10/16/vedtelenek_a_vallalati_mobilok_es_tabletek (letöltve: 2011.11.27.)

- Információ és biztonság – Protokollok (FTP/SFTP, HTTP, HTTPS, SSL) http://iesb.hu/logikai-biztonsag/protokollok-ftpsftp-http-https-ssl (letöltve: 2011.11.24.)

- Létai János: Elutasították az Anna Kurnyikova-vírus szerzőjének fellebbezését HWSW Online informatikai hírmagazin, 2002. október 29. http://www.hwsw.hu/hir.php3?id=18263 (letöltve: 2011.10.29.)

- Magyar Közlöny 2011/88. szám, 25449. p. http://kozlony.magyarorszag.hu/pdf/9906 (letöltve: 2011.10.27.)

- Mennyit érnek a személyes adatok? http://www.gportal.hu/gindex.php?pg=198341 (letöltve: 2011.10.27.)

- Mikrofonnal lehet lehallgatni a nyomtatókat http://www.adatvedelmiszakerto.hu/2010/08/adatbiztonsag-mikrofonnal-lehet-lehallgatni-a-nyomtatokat (letöltve: 2011.10.31.)

- Minden tizedik magyar netező idióta http://index.hu/tech/2011/04/04/minden_tizedik_magyar_netezo_idiota

- Nemzeti Biztonsági Felügyelet: Az iparbiztonsági ellenőrzés, illetve a Telephely Biztonsági Tanúsítvány kiadásának rendjét érintő legfontosabb változások http://www.nbf.hu/anyagok/iparbiztonsag/Valtozas_iparbizt.doc (letöltve: 2012.02.23.)

- Országos Fogyasztóvédelmi Egyesület – Fogalommagyarázat: Adathalászat http://www.ofe.hu/inet/ofe/hu/fogalmak/fogalom.html?phraseid=2173 (letöltve: 2011.10.29.)

- Pattogatott kukoricával törték fel Sarah Palin postafiókját http://kulfold.ma.hu/tart/cikk/b/0/23940/1/kulfold/Pattogatott_kukoricaval_tortek_fel_Sarah_Palin_postafiokjat (letöltve: 2011.11.05.)

- Szentgyörgyi Attila: WiFi hálózatok biztonsági kérdései http://tszo.hte.hu/root/club_ppt/201005/eloadas_szgyi_wifi_hte.pdf (letöltve: 2011.11.18.)

- Vezeték nélküli hálózat otthon II. http://torpospapa.weboldala.net/vezetek_nelkuli_halozat_otthon_-_ii.html (letöltve: 2011.11.18.)

- Wikipédia, Virtuális magánhálózat http://hu.wikipedia.org/wiki/Virtu%C3%A1lis_mag%C3%A1nh%C3%A1l%C3%B3zat (letöltve 2011.11.19.)

- Wikipédia: Cracker http://hu.wikipedia.org/wiki/Cracker (letöltve: 2011.10.29.)

- Wikipedia: Hacker http://hu.wikipedia.org/wiki/Hacker#Script_kiddie (letöltve: 2011.10.29.)

- Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról http://eur-lex.europa.eu/LexUriServ/site/hu/com/2005/com2005_0576hu01.pdf (letöltve: 2011.10.28.)

■ ■ ■

Függelék: Mailware-ek elleni védekezést segítő szoftverek[168]

Antivírus programok

- AVG (ingyenes)
  http://free.avg.com/

- Avira Antivir (ingyenes)
  http://www.avira.com/en/avira-free-antivirus

- ESET NOD32
  www.eset.hu

- F-secure
  http://www.f-secure.hu/

- Kaspersky Lab
  http://www.kaspersky.hu/
  http://www.kaspersky.com/virusscanner

- McAfee
  http://hu.mcafee.com/
  http://hu.mcafee.com/root/mfs/

168 Hivatkozások letöltve: 2011.11.07.

- Symantec Norton Antivirus
  http://www.symantec.com/hu/hu/index.jsp
  http://hu.norton.com/antivirus/

- Trend Micro
  http://emea.trendmicro.com/emea/home/
  http://www.trendsecure.com/portal/en-US/tools/security_tools/housecall

- VirusBuster
  www.virusbuster.hu

Kémprogramok elleni védelem (ingyenesek)

- Ad Aware Free
  http://www.lavasoft.com

- Microsoft Security Essentials
  http://www.microsoft.com/hu-hu/security_essentials/default.aspx

Tűzfalak

- Hardver alapú tűzfalak
  http://www.cisco.com/web/hu/index.html

- Kaspersky Internet Security
  http://www.kaspersky.hu/termekek/ kaspersky_internet_security.html

- McAfee Internet Security
  http://hu.mcafee.com/

- Norton Internet Security
  http://hu.norton.com/internet-security

- Zone Alarm (ingyenes)
  http://www.zonealarm.com/security/en-us/anti-virus-spyware-free-download.htm

Tűzfal tesztek

- Audit My Pc
  http://www.auditmypc.com

- Mc Afee MySecurityStatus
  http://us.mcafee.com/MySecurityStatus

- Norton Security Scan
  http://security.symantec.com

- Shields Up!!
  http://www.grc.com/intro.htm

Komplex védelem

- ESET Smart Security
  http://www.eset.hu/letoltes/otthoni/ess

- Kaspersky Pure
  http://www.kaspersky.hu/termekek/kaspersky_pure.html

- Mc Afee Total Protection
  http://home.mcafee.com/Store/PackageDetail.aspx?pkgid=275

- Norton 360
  http://hu.norton.com/360

Mobiltelefonok védelme

- AVG Antivirus for Android
  http://www.avg.com/us-en/antivirus-for-android

- ESET Mobile Security
  http://www.eset.hu/otthoni/mobil

- F-Secure Mobile Security
  http://www.f-secure.com/en/web/home_global/protection/mobile-security/overview

- Kaspersky Mobile Security
  http://www.kaspersky.com/kaspersky_mobile_security

- Mc Afee Mobile Security
  https://www.mcafeemobilesecurity.com/default.aspx

- Norton Mobile Security
  http://us.norton.com/mobile-security