F. Ható Katalin

ADATBIZTONSÁG, ADATVÉDELEM

SZÁMALK KIADÓ

F. Ható Katalin

ADATBIZTONSÁG, ADATVÉDELEM

4. javított, bővített kiadás

Szakmai lektor: Auer Péterné

SZÁMALK Kiadó
Budapest, 2005

Kiadja a SZÁMALK Kiadó
Felelős kiadó: Dr. Zárda Sarolta
Témafelelős: Lengyel Zsuzsánna

TARTALOMJEGYZÉK

Előszó

Az informatikusok tevékenységében az információ „nyersanyag". Munka közben az ember hajlamos elfeledkezni arról, hogy az információ valaminek a leképezése, mögötte áll az anyagi valóság, és általában maga az ember is. Nagyon fontosnak tartjuk, hogy a leendő informatikusok tisztában legyenek az információra vonatkozó törvényi előírásokkal, és azzal a szellemiséggel és elvekkel, ami ezen törvények megalkotásához vezetett.
Munkájuk során szinte biztosan kerülnek olyan helyzetbe, amikor olyan adatokat kell feldolgozniuk, amire törvényi előírások vonatkoznak. A törvények ismeretének hiánya nem mentesít azok megsértésének következményeitől.

Másrészt azzal is tisztában kell lenniük, hogy az információ mekkora értéket képvisel a mai életünkben. Az informatikai szakemberek feladata a biztonsági intézkedéseknek a megteremtése, amivel ezeket az értékeket védeni lehet.

Ahogy a könyv címe is mutatja, két nagy, egymással szorosan összefüggő témáról szól. Az **adatvédelem** meghatározza, hogy *ki, milyen adatokkal, mit* tehet. Az **adatbiztonság** azokat a technikai módszereket tárgyalja, amelyek segítségével az adatvédelemben megfogalmazott alapelvek teljesíthetők, tehát azt, hogy *hogyan* kell ezeket az adatokat kezelni.

Adatvédelem

Az **adatvédelemmel** elsősorban jogászok foglalkoznak. A témában számos nemzetközi ajánlás, egyezmény készült, amelyek alapján különböző időpontokban a legtöbb országban megszülettek a saját nemzeti jogszabályok is. A technika fejlődése azonban mindig újabb megoldandó kérdéseket vet fel, amire a jogalkotóknak válaszolni kell.

Ilyen aktuális téma az Internet, aminek szabályozása a nemzetközi szervezeteket és a nemzeti törvényhozásokat egyaránt foglalkoztatja. A könyvben ezeket a kérdéseket is érintjük.

Adatbiztonság

Az **adatbiztonság** műszaki, szervezési kérdés, napjaink egyik legizgalmasabb témája. A megfelelő biztonság megteremtésén akár emberéletek is múlhatnak (pl. egy repülésirányító rendszer meghibásodásánál), de egy számítógépes rendszer összeomlása napok alatt tönkretehet egy olyan vállalkozást, amelynek fő munkaeszköze az információ (pl. bankok, biztosítók, csomagküldő áruházak, stb.). De kisebb rendszerhibák is okozhatnak nagy bosszúságot, mint pl. ha a bankkártyánkkal hosszabb ideig nem tudunk a pénzünkhöz jutni. Az adatbiztonság mostanára már a bűnügyi híradások kedvelt témájává vált, lassan köznapi fogalmakká válnak az olyan angol szakkifejezések, mint a hackerek, a crackerek, Cypherpunk.

Természetesen a jogi és a műszaki megközelítés akkor hatékony csak, ha egységesen, egymást kiegészítve kezeli a problémákat. Erre számos gyakorlati példát látunk: a műszaki fejlődés által felvetett problémákra megoldására jogi és műszaki intézkedések is születtek egyidőben.

A könyvben röviden áttekintjük az adatbiztonság fejlődésének állomásait. Megnézzük, milyen területek befolyásolják az adatbiztonságot, honnan várható a legnagyobb fenyegetés, milyen intézkedésekkel tudjuk ezeket a támadásokat kivédeni. Néhány adatbiztonsági módszert részletesen megtárgyalunk.

A számítógépeken tárolt és feldolgozott adatoktól való függőség komoly veszélyeket hordoz magában. Foglalkozunk azzal, hogy milyen tényezők befolyásolják ezek biztonságát, honnan várható a legnagyobb fenyegetés, milyen intézkedésekkel tudjuk ezeket a támadásokat kivédeni. Átnézzük a biztonságos informatikai rendszer minősítésének folyamatát és feltételeit, nemzetközi szabványok és ajánlások alapján.

Néhány adatbiztonsági módszert részletesen is megtárgyalunk. Foglalkozunk a programozott kártevőkkel a vírusokkal. Áttekintjük a titkosítás egyre népszerűbb tudományát a kriptográfiát. Megnézzük, hogy a számítógép hálózatok védelmére milyen eszközeink vannak.

Mivel jelenleg ez a téma rendkívül népszerű, ezért naponta jelennek meg újabb adatbiztonsági módszerek és eszközök. Könyvünkkel a témában való eligazodást szeretnénk megkönnyíteni.

A fejezetek elején összefoglaljuk, hogy milyen témát tárgyalunk meg az adott részben. A tananyag elsajátítását és a vizsgára való felkészülést a fejezetek végén ellenőrző kérdések segítik.

Végül köszönetemet szeretném kifejezni Auer Péternének, Faragó Eszternek és Szabó Andrásnénak, akik hasznos tanácsaikkal segítették munkámat.

Budapest, 2005. január

a Szerző

1. Történeti fejlődés

Ebben a fejezetben átnézzük az adatkezelés fejlődésének különböző szakaszait. Megvizsgáljuk, hogy az adott fejlődési szakaszban milyen hangsúlyt kapott az adatok védelme és milyen kihívásokkal kellett megküzdeni a szakembereknek.

Ahogy az ember lerögzítette az addig szóban terjedő információt, vagyis feltalálta az írást, rögtön megjelent az igény, hogy megvédje az „adathordozóit". Az ókori kőtáblák anyaga eléggé masszív volt, nehéz volt őket tönkretenni. A középkorban a papírra írt anyakönyvek és krónikák már nagyobb védelmet igényeltek, ezért általában a biztonságos templomokban és kolostorokban helyezték el őket. Az információ tömege nőtt, az élet ritmusa felgyorsult. Már nem volt elég az anyakönyv és a golyós számológép. Az emberiség új eszköz után áhítozott, és feltalálta a számítógépet.

1.1 Kezdeti lépések

Babbage

Az ipari forradalom a XIX. század Angliájában sok olyan változást hozott (Watt gőzgépe, Stephenson gőzmozdonya, stb.), ami azt igazolta, hogy az emberi erőt, a kézi munkát gépekkel kívánják helyettesíteni. *Charles Babbage* angol matematikus 1820-ban megbízást kapott az angol kormánytól egy differenciagép megalkotására. Hosszas kísérletezés és sok kudarc után 1840-ben kidolgozta az általános célú, analitikus számítógép elvét. A kor szakmai színvonala még nem tette lehetővé a gép megépítését. A kor fejlettségét megelőző gondolatait kortársai őrültségnek tartották, ma azonban határozott vélemény, hogy Babbage-től származik a számítógép alapgondolata.

Hollerith

Az első igazi számítógép az USA-ban 1880-ban végzett nagy népszámlálás adatainak feldolgozásakor debütált, amit *Hermann Hollerith*, német származású amerikai mérnök épített. Az adatokat 80 oszlopot és 10 sort tartalmazó, az egydolláros bankjegy nagyságának megfelelő kártyára lyukasztották. Ezeket a lyukkártyákat elektro-mechanikus szortírozó gépekkel

rendezték, és az adatokat táblázó gépekkel összesítették. A programozásuk a régi telefonközpontok kapcsoló rendszeréhez hasonlóan folyt. Ezek a berendezések az *1970*-es évek közepéig üzemszerűen működtek, a hetvenes évek elején ezt a technikát még tanították.

Zuse

Az elektronika fejlődése más irányokat hozott a számítástechnikában. Az 1930-as években *Konrad Zuse* kifejleszti a digitális programvezérelt számítógépet, amely már digitális számrendszerben dolgozik és a programot lyukszalagon fogadja. A II. világháború felgyorsuló eseményei sürgették a fejlesztést, egyre több bonyolultabb és gyorsabb számításra volt szükség. Ez jelentősen ösztönözte a kutatásokat.

Neumann elv

A modern számítógép elvét *Neumann János* magyar születésű, Németországban, majd az USA-ban dolgozó matematikus alkotja meg. Ez az elv a következőkön alapul: a gép felépítése független a megoldandó feladatoktól, a programokat, adatokat, a számítási eredményeket ugyanabban a tárolóban helyezi el, a tárolót egyforma cellákra osztják, amelyeknek címe van és tartalma lehívható és minden adat binárisan kódolt.
Ez az elv teremti meg a számítógépek ipari gyártásának alapjait. A mai számítógépek ezen elvek alapján működnek.[14]

Hőskor

Ez a szakasz a számítástechnika hőskora. A gépek egyedi építésűek, általában valamilyen kutató laborban működnek, főként tudományos számításokra használják őket. Szinte kizárólag csak a tudósok kerülnek vele kapcsolatba. A nagyközönségnek csak a tudományok iránt érdeklődő vékonyka rétege hallott a létezésükről. Elsősorban a gépek műszaki adatait védik.

1.2 Az ipari gyártás megindulása

Az IBM színre lép

A második szakasz 1950-1965 közé esik, amelynek legfőbb jellemzője a számítógépek ipari gyártásának megindulása. 1956-ban az USA-ban hivatalosan már 44 gyártót jegyeztek, amelyből 17 egyetemi intézmény és 27 ipari laboratórium. Neves fejlesztők az *UNIVAC*, a *Sperry Rand,* de már akkor is az

IBM volt a legerősebb, ami hamarosan a legnagyobb számítógép-gyártó lett nemcsak az USA-ban, hanem az egész világon.

Tudományos számítások

Az ipari gyártás ellenére a számítógép alkalmazása ekkor még nagyon szűk területet ölelt fel. Még mindig elsősorban tudományos számításokra használták, az egyéb jellegű feldolgozások épphogy megindultak. A géptermek misztikus, elzárt helyiségek voltak, ahol valami érthetetlen dolog folyt, és oda belépni csak keveseknek adatott meg. Ekkor a biztonság még mindig elsősorban a gépek műszaki védelmét, a megfelelő környezet kialakítását jelenti.

1.3 Számítóközpontok kora

Tömeges adat-feldolgozások

1965-től kezdődően Magyarországon minden ágazati minisztérium létrehozza a saját számítóközpontját (pl. a Kohó-és Gépipari a KGMISZI-t, a Nehézipari a NIMIGÜSZI-t, a Kereskedelmi a KERSZI-t, a Magyar Posta a PSZSZI-t, stb.). Az első kötegelt feldolgozások általában a könyvelés, bérszámfejtés, később a termelésirányítás, a logisztikai tervezés területét érintik. Az adatrögzítés előbb lyukszalagra, lyukkártyára, később mágnesszalagra történik. Ezt általában a gépekkel egy épületben elhelyezett, nagy létszámú adatrögzítő stáb végzi.

Nagyüzemi számítás-technika

Egy ilyen nagy számítóközpontban több száz képzett szakember (szervezők, programozót, hardveresek, operátorok, adatrögzítők, táblaellenőrök, stb.) dolgozik. Bonyolult, sokféle feldolgozás, fejlesztés folyik, több száz mágnesszalaggal, lemezzel dolgoznak, több mázsa leporellót gyártanak naponta. Ezeket különböző helyekre szállítják, selejtezik, a bizalmas adatokat tartalmazókat megsemmisítik. Bár nem ment minden zökkenőmentesen! A nyolcvanas évek elejének egyik elhíresült esete volt, amikor bankszámla-kivonatot tartalmazó leporellóba csomagolva lehetett a piacon epret kapni.

Adatvédelmi szabályzatok, felelősök

Ezt már szabályozni kell: ki mikor, hova léphet be, hol tartózkodhat, hogyan kell azonosítani a különböző adathordozókat, mi a teendő rendszerleállás esetén, mit kell tenni az elrongyolódott mágnesszalaggal, stb. Megjelennek az első *adatvédelmi*

szabályzatok, minden számítóközpontban *adatvédelmi felelősöket* neveznek ki, akiknek a fő feladatuk biztonsági kérdések képviselete a fejlesztésnél és az üzemeltetésnél.

1.4 A PC és az Internet korszaka

Az IBM PC

A szakma által kezdetben életképtelennek tartott IBM PC működéséhez szükséges operációs rendszer elkészítését egyetlen nagyobb szoftverkészítő cég sem akarta elvállalni. Az akkortájt induló Microsoft nevű cég William Gates vezetésével 1981-ben ***6 hónapos*** határidőre végül elvállalta. A program, mivel külön lemezen adták a géphez, a DOS (Disk Operating System) nevet kapta. A nehéz indulás után a PC alapjaiban változtatta meg a számítástechnika alkalmazását.

Háztartási eszköz

Ezzel megkezdődött a számítástechnika popularizációjának is nevezett korszak, amely gyökeres változást hozott az alkalmazásokban. Ma már a számítástechnika kikerült a szakemberek felügyelete alól, a mindennapi élet részévé vált. Az irodákból kiszorította az író- és számológépeket. Mára már a háztartások egy részében is besorolt a porszívó és a videomagnó mögé.
Az élet végletesen felgyorsult. Az Interneten keresztül szinte a keletkezés pillanatában hozzájuthatunk az információhoz. Az információ áru lett.

Információ = hatalom

Az Internet hatalmas kihívást jelent a biztonsági szakembereknek. Óriási mennyiségű, sokszor nem törvényes úton megszerzett információ van rajta, amelyek érdekeket, törvényeket sérthetnek. Másrészt az Interneten nem csak kifelé lehet menni a világba, hanem befelé is bejárat a lokális hálózatokba a nem óhajtott látogatók számára.
Sok új fogalommal ismerkedtünk meg az elmúlt években: vírusok, hackerek, információs szupersztráda, fehérgalléros bűnözés, számítógépes terrorizmus, számítógépes hadviselés és még sorolhatnánk.
Babbage óta a világ nagyon megváltozott. Az adatbiztonsági szakemberek előtt hatalmas feladatok állnak, a versenyfutás a számítógépes bűnözőkkel naponta ismétlődik.

A témában az Európa Tanács mellett más nemzetközi szervezetek működnek, amelyek munkája a magyar jogszabályokra és a mindennapi gyakorlatra is kihat. Az információk kezelésének szabályozása az államigazgatás, a politika, a jog számos területét érinti. Összefügg a tájékoztatással, az emberi jogok kérdésével egyaránt, amit az Európai Unióban súlyponti kérdésként kezelnek.

95/46 EK irányelvek

Az Európai Parlament és a Tanács 1990-ben kidolgozta az *egyénnek a személyes adatok feldolgozásával kapcsolatos védelméről és ezeknek az adatoknak a szabad áramlásáról szóló* irányelveket, amelyet 1995-ben hirdettek ki. Ez az irányelv a *95/46 EK irányelv* néven vonult be az európai törvényalkotásba és lett az európai adatvédelem alapdokumentuma.

Az irányelv leszögezi, hogy az adatfeldolgozó rendszerek az emberiséget szolgálják azzal, hogy e rendszereknek – függetlenül a természetes személyek állampolgárságától és lakóhelyétől – tiszteletben kell tartaniuk a személyek alapvető jogait és szabadságait, nevezetesen a magánélet védelméhez fűződő jogot és elő kell segíteniük a gazdasági és társadalmi haladást, a kereskedelem bővülését és az egyéni jólétet. [30]

Az irányelv célja

Az európai adatvédelmi irányelv **célja:**

- egyensúly biztosítása a személyes adatok védelme és az információ szabad áramlása között,
- a nemzeti törvényhozásokban az irányelv érvényesítése,
- azonos adatvédelmi normák érvényesítése mind az állami, mind a magánszektorban.

Alapelvek

Az Irányelvben a következő **alapelveket** fogalmazták meg:

1. Meg kell határozni az adatgyűjtés célját, és azt ismertetni kell az adatszolgáltatóval.
2. Korlátozni kell az adatgyűjtés körét, pontosan meghatározva azt, hogy milyen adatokra terjedhet ki.
3. Az adatokat csoportosítani kell, és ezekhez a csoportokhoz kell meghatározni, hogy milyen szabályok vonatkoznak rájuk.

4. Meg kell határozni azokat az adatcsoportokat, amelyek csak az érintett külön engedélyével tárolhatók.
5. Az állampolgárral ismertetni kell, hogy kik jutnak hozzá az adataihoz.
6. Biztosítani kell, hogy mindenki hozzáférhessen a róla szóló adatokhoz, és az esetleges hibák kijavítása megtörténjék.
7. Az adatkezelő köteles az általa tárolt adatok védelmét biztosítani.
8. Gondoskodni kell az adatvédelemre vonatkozó előírások betartásának intézményesített ellenőrzéséről.

Az irányelv két testület létrehozását írja elő: az egyik az Adatvédelmi Bizottság, amely véleményezi a meghozandó intézkedések tervezetét. A másik szerv a 29-es Adatvédelmi Munkacsoport, amely az EU tagállamainak adatvédelmi biztosaiból álló független tanácsadó testület. A két szervezet együtt felügyeli az európai adatvédelem helyzetét. [30]
A Bizottság nagy hangsúlyt fekete a közösség adatvédelmi jogának továbbfejlesztésre és az egységes joggyakorlat kialakítására. Az irányelv viszonylag kevés lehetőséget ad a tagállamoknak a rendelkezésektől való eltérésre, illetve önálló szabályozásra.

Kiemelt témaként kezeli az. ún. harmadik országba történő adattovábbítás egységes gyakorlatának kialakítását. Egyik nehezen megoldható feladat volt az Amerikai Egyesült Államokkal megkötendő megállapodás. Az USA-ban nincs az európai értelemben vett adatvédelmi törvény, és jelenleg is folyik a vita arról, vajon megteremthetők-e a magánszféra védelmének feltételei az egyes, adatkezeléseket tömegesen végző szervezetek (direkt marketing cégek, stb.) önszabályozásával, vagy esetleg az amerikai hagyományokhoz kevésbé illeszkedő állami beavatkozásra, törvény alkotására van szükség. Bár a szeptember 11-ei terrortámadás után az USA hozzáállása is sokat változott, az adatvédelmi felfogás a gyakorlat közötti különbségek nehezen oldhatók fel. [24, 30]

2.2 Az Internet jogi szabályozása

Az Internet megjelenése alapjaiban változtatta meg az információ nyilvánosságra hozatalának, és a legszélesebb körben való terjesztésének módszereit. Ez jelentős hatással van az adatvédelem érvényesítésre is.
A hagyományos médiában közzétett információt lokalizálni lehet, mivel egyértelmű, hogy ki közölte le az adott hírt. Az Interneten ez már sokszor követhetetlenné válik.
A másik nagy veszélye az Internetnek az „adatbányászat", vagy az ún. „fisching" (adathalászat). Az Interneten rengeteg olyan információ található, amelyet összegyűjtve és elemezve az emberek érdeklődési köre, politikai nézetei kiderülhetnek. Elegendő megvizsgálni azt, hogy milyen WEB oldalakat keres fel rendszeresen. Ezt a közhatalom nemzetbiztonsági, bűnüldözési szervei is felhasználhatják. Kedvenc vadászterülete ez a marketingnek is, de ártó szándékú csoportok is gyűjthetnek innen információt. Mára már önálló üzletággá nőtte ki magát az e-mail címek kereskedelme.

Cypherpunk mozgalmak

A kilencvenes évek közepétől újabb polgárjogi mozgalmak indultak el, amelyek az Internet keltette veszélyekre hívják fel a figyelmet A cypherpunk mozgalomban olyan emberek vesznek részt, akiket a hálózatok szakmai problematikáján túl elsősorban az Internet szociológiai következményei foglalkoztatnak. Ezen mozgalmak célkitűzését jól illusztrálja egy osztrák szervezet, az ARGE DATEN felhívásából való idézet:

Figyelő szemek

"A globális kommunikáció korszakában a magánszféra biztosítása a leglényegesebb demokratikus kihívások egyikévé válik. Az információ továbbításának, összegyűjtésének és kiértékelésének (adatbányászat, információ-halászat) technikai lehetőségei egyre több szervezetet csábítanak arra, hogy ezekkel az új eszközökkel visszaéljenek. A bűnözés elleni harc és az állambiztonság megőrzése mögé bújva a polgári jogokat korlátozzák. Ez egy átfogó, mindenkire kiterjedő magatartási kontrollhoz vezet - végső soron pedig a polgár viselkedésének irányításához. A mindent lefedő információs rendszerek (GSM, GPS, bank-automaták, elektronikus csomópontok) révén a polgár minden mozdulata feljegyezhető, összekapcsolható s más személyekkel összefüggésbe hozható lesz. A szabad egyénből bioló-

giai mozgásjelző válik, ami állandó megfigyelését teszi lehetővé. Az információhoz jutás és a kiértékelés lehetőségei a harmadik évezred fontos stratégiai eszközeivé válnak." [26]

Az adatvédelem nemzetközi alapelvei az Internetre is vonatkoznak. Az Internet azonban több szempontból is problémát jelent:

- Az előbb már említett személyes adatok sokasága jelenik meg rajta, amelyek védelmét itt sokkal nehezebb biztosítani, mint a hagyományos adathordozókon vagy a lokális számítógépeken.
- Az Internetre feltett anyagok tartalma sok esetben törvénybe vagy a jóízlésbe ütközik.
- A hálón lévő anyagokat nagyon egyszerű módszerekkel lehet lemásolni és sokszorozni a szerző tudta nélkül, megsértve ezzel a szerzői jogokat.

Mivel az Internet alapjaiban tér el az eddig megszokott kommunikációs csatornáktól, nehéz rá alkalmazni a korábban megszokott szabályozási formákat. Mik azok a jellemzők, amelyek megnehezítik a jogalkalmazást?

- **Decentralizált** – tehát nincs egyetlen központi irányító egysége, amelytől technikailag függne. Nincs egyetlen olyan csúcsszerv, amely befolyással lenne az összes vonalra, lehetősége lenne azt ellenőrizni.
- **Nyitott** – bárki, minimális technikai igények kielégítése után rákapcsolódhat. Nem lehet senkit sem „kitiltani", mert számtalan másik elérési útvonalon csatlakozhat.
- **Csomagkapcsolt** – vagyis az információ csak a küldő és a fogadó gépén áll össze tényleges formájában.

Kezdetben az Internet használatának általánosan elfogadott erkölcseit a Netikett (Netiquette) rögzítette, amely a hálózati viselkedés alapelveinek egy minimális halmazát határozta meg. Eredetije az IETF Felelős Hálózati Használat csoportjának munkája. A magyar fordítás az Interneten több helyen is megtalálható.

Netikett

A teljesség igénye nélkül, néhány alapelv:

- Ha nem egy Internet Szolgáltatón keresztül kerülsz kapcsolatba az Internettel, akkor fontos ismerned a munkáltatód szabályait az elektronikus levelek tulajdonjogáról; ezek mindenütt mások.
- Fel kell tételezned hogy az Interneten történő levelezés nem biztonságos, kivéve ha valamilyen rejtjelező eszközt (akár szoftvert, akár hardvert) használsz. Ne írjál semmi olyasmit egy elektronikus levélbe, amit nem küldenél el levelezőlapon.
- Tiszteld a szerző jogait avval az anyaggal kapcsolatban, amit másolsz. Majdnem minden országban vannak a szerzők jogait védő törvények.
- Ha továbbküldesz (forward) vagy újrapostázol egy üzenetet, akkor ne változtasd meg annak a szóhasználatát. Ha ez egy neked írt személyes üzenet volt, és egy csoportnak kívánod továbbadni, akkor kérjél először engedélyt a feladótól, ...

A kezdeti időszakban, ami az egyetemi számítógépes hálózatok összekapcsolását jelentette, az önszabályozásnak ez a módja teljesen kielégítően működött, mivel a tudományos életben megszokott etikát tükrözte. Mára azonban jelentősen megváltozott az Internet felhasználók összetétele. Az e-bussines beindulásával már olyan információk találhatók az Interneten, amelyek megszerzése jelentős anyagi haszonnal járhat.

A téma hazai jogi szakértőinek - többek között - Verebics Jánosnak és Jóri Andrásnak sok érdekes írása foglalkozik a témával [24, 26].
Nézzük meg, hogy a felsorolt problémának milyen megoldásaival találkozhatunk a különböző országokban:

Személyiségi jogok

A személyiségi jogok védelme

Általánosságban elmondható, hogy az Interneten ugyanazok az alapelvek érvényesülnek, mint más adatkezelés esetében. Fő elv az, hogy az érintett hozzájárulását meg kell kérni ahhoz, hogy a személyes adatait kezeljék. Az Internet speciális tulajdonságaira tekintettel nemcsak a tiltás az egyetlen eszköz, hanem a felhasználónak olyan módszereket kell biztosítani, amelyek segítik a védekezésben.

Németországban 1997-ben lépett hatályba a világ első, kifejezetten az Internet-felhasználók jogait védő adatvédelmi törvénye. Számos új elemet tartalmaz, amely példaként szolgálhat más államok törvénykezésének is. A törvény előírja azt, hogy az ügyfélt ne lehessen arra *kényszeríteni*, hogy a szolgáltatás biztosítása fejében adja meg a beleegyezését abba, hogy az adatait *más célokra is felhasználják*. Szintén új elem, hogy a szolgáltatónak *már az általa használt technológia kiválasztásánál* figyelemmel kell lennie az adatvédelmi követelményekre: olyan technológiát kell választania, amely csak a minimális személyes adatokat kezeli.
A felhasználó tevékenységére utaló forgalmi adatokat a szolgáltató csak akkor rögzítheti, ha a használathoz feltétlenül szükséges, ill. a számlázhoz kell, és ha már nincs rá szükség azonnal meg kell semmisítenie.

Anonim internetezés

A jogalkotók megfogalmazták, hogy a szolgáltatónak a "technikailag lehetséges és elvárható" mértékig anonim módon vagy álnév használatának lehetőségével kell szolgáltatásait elérhetővé tennie a felhasználók számára. A törvény teret enged a hatékony online marketingnek: rendelkezései szerint szabad a felhasználó használati szokásairól szóló adatokat gyűjteni, s ez alapján róla profilt alkotni, ám csak abban az esetben, ha ezek *nem a felhasználó valódi nevéhez, hanem álnevéhez kötöttek*; a profilok *nem köthetők össze* az álnevet használó valós személy adataival.

Tartalom szabályozás

Tartalom szabályozás

Európában az Emberi Jogok Egyezménye teljes védelmet biztosít az összes Internet felhasználó számára, hogy szabadon kifejezhessék magukat, terjeszthessenek és kaphassanak információt. Az európai, az amerikai és a kanadai jogrendszer ugyanakkor tiltja a rágalmazást, az illegális tevékenységre való felhívást valamint pornografikus, pedofil anyagok terjesztését. Bonyolult jogi helyzetet teremt az Interneten található káros tartalmú anyagok terjesztőinek felelősségre vonása.

A jogi eszközök korlátozottak, de itt is új technikai lehetőségek is segítenek ennek a problémának a megoldásában. Ezek megteremtik annak lehetőségét, hogy a felhasználó vagy a szolgáltató dönthesse el, hogy milyen anyagokat kíván beengedni a saját gépére vagy a hálózatára.

PICS

A World Wide Web Consortium kidolgozta *Platform for Internet Content Selection* (PICS - Internetes Tartalomszűrő Felület) szabványt. Ez lehetőséget ad arra, hogy a felhasználó által az Internet eléréséhez használt, a PICS szabványnak megfelelő szoftverek képesek legyenek a felhasználó által meghatározott szempontok szerint szűrni a hálózaton elérhető anyagokat, és megakadályozni azok elérését, amelyeket a felhasználó nemkívánatos kategóriába sorolt.

Előzetesen természetesen el kell végezni a kérdéses tartalom minősítését. A minősítés bármilyen, eltérő szempontokat ill. értékrendeket tükröző minősítési rendszer szerint történhet, s azt maga az adott állomány megalkotója ill. valamilyen minősítő szolgálat is elvégezheti.

Ha a címke alapján az anyag nem felel meg a felhasználó előzetesen megadott kívánalmainak, akkor a hozzáférést nem engedélyezi. A PICS-kompatibilis szoftverekkel elérhető, hogy a gyermek úgy legyen elzárva az „illetlen" anyagoktól, hogy szülei megtekinthessék azokat; lehetővé válik az is, hogy a munkáltatók csak meghatározott anyagok elérését tegyék lehetővé az alkalmazottak számára. A PICS kidolgozói szerint célszerű a rendszerrel a végfelhasználók kontrollját erősíteni a tartalomelérés fölött, ám akár valamely internet-szolgáltató, akár egy ország telepítheti azt saját rendszerére, ha létezik egy olyan kitüntetett pont, ahol az adott szolgáltató/ország internetes forgalmának túlnyomó része áthalad. [24]

Szerzői jogok

A szerzői jogok

A szerzői jogok valamely mű szerzőjének azon jogát jelenti, hogy műve felhasználásának bizonyos módját engedélyezze vagy megtiltsa.

Minden mű (írott, zenei, audovizuális, szoftver, adatbázisok, Web-oldalak, stb.) szerzői jogi oltalom alatt áll, amennyiben eredeti alkotásnak minősíthető, továbbá, amennyiben meghatározott formába öntötték vagy megfogható anyagi hordozón rögzítették.
A szerzőnek vagyoni és személyhez fűződő jogai vannak. A műve megváltoztatásához, másolásához, vagy nyilvánosságra hozatalához a szerző engedélye szükséges. Az amerikai jogban a felhasználóknak nem szükséges engedélyt kérniük a szerzőtől a mű „tisztességes" felhasználásához. A felhasználók letölthetnek fájlokat, feltéve, ha betartják a szerző által kikötött feltételeket.

Ellenőrző kérdések

1. Melyek az európai adatvédelmi irányelvek célja és alapelvei?
2. Milyen európai szervezetek foglakoznak az adatvédelemmel?
3. Hogyan érvényesülnek a személyiségi jogok az Interneten?
4. Milyen szabályok érvényesek az Interneten megjelenő anyagok tartalmára?
5. Hogyan érvényesülnek a szerzői jogok az Interneten?

3. Az adatvédelem hazai szabályozása

Ebben a fejezetben áttekintjük a magyar adatvédelemi törvényt. Megnézzük azokat az intézkedéseket, amelyek megelőzték a törvény megjelenését. A törvény teljes szövegének feldolgozása során megismerkedünk az adatvédelem alapfogalmaival és alapelveivel.

Bár szakmai körökben a mai napig is folyik a terminológiai vita az adatvédelem és adatbiztonság fogalma körül, definiáljuk, hogy mit is értünk adatvédelem alatt. Az Informatikai Tárcaközi Bizottság ajánlásában a következő definíció áll az adatvédelem címszó alatt:
„Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik."
Egyszerűbben fogalmazva:

Adatvédelem

Az adatvédelem adatok meghatározott csoportjára vonatkozó jogszabályi előírások érvényesítése az adatok kezelése során.

A nemzetközi ajánlásokban megfogalmazott alapelvek a magyar jogrendszerben is érvényesültek. Nézzük meg, mi a helyzet itthon, milyen lépéseken keresztül jutottunk el abba az állapotba, amikor is az Európai Bizottság Kanada és Svájc mellett Magyarországot jelölte meg olyan országnak, amely megfelelő védelmet nyújt az információk továbbítására.

3.1 Előzmények

I/1981.BM rendelet

Először a Belügyminisztérium szabályozta ezt a területet: 1981-ben jelent meg a *számítástechnikai rendszerek titok-, vagyon-, és tűzvédelméről szóló I/1981.(I.27.) BM sz. rendelet*. Ez előírta kötelező jelleggel az intézmények számára a Számítástechnikai

Védelmi Szabályzat (SzVSz) elkészítését és az adatvédelmi felelősök megbízását. A törvényi szintű szabályozás azonban még néhány évig váratott magára.

Alkotmány, XII. fejezet, 59. §

Az adatvédelem alapjait a Magyar Köztársaság Alkotmánya teremti meg. Az Alkotmány XII. fejezet, 59. § értelmében kimondja, hogy:

(1) A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.

(2) A személyes adatok védelméről szóló törvény elfogadásához a jelenlévő országgyűlési képviselők kétharmadának szavazata szükséges.

Az 1989. október 23-án kihirdetett alkotmánymódosítással létrejött a köztársasági alkotmány, mely Kelet-Közép-Európában elsőként alkotmányos szintre emelte a személyes adatok védelmét és az információszabadságot. Az adatvédelmi törvényt azonban csak 1992-ben terjesztették be a parlament elé. A késlekedés miatt az Alkotmánybíróság is foglalkozott a témával.

15/1991. AB határozat

Az Alkotmánybíróság (AB) 1991. április 13-án kihirdette a 15/1991 AB határozatát, mely a személyi szám alkotmányellenes használatáról szólt, ám ezen túlmenően a népességnyilvántartás egész jogi rendszerét hatályon kívül helyezte.
A jogállamiság megteremtésének mérföldkövei voltak a személyiségi jogok és az információs önrendelkezés védelmére született törvények. Nem véletlen, hogy az AB ezen határozata nagy vitát váltott ki, amely kimondta:
„... hogy személyes adatok meghatározott cél nélküli, tetszőleges jövőbeni felhasználásra való gyűjtése és feldolgozása alkotmányellenes.
..., hogy a korlátozás nélkül használható, általános és egységes személyazonosító jel (személyi szám) alkotmányellenes. „

Az AB a határozatait azzal indokolta, hogy a nem pontosan meghatározott adatgyűjtésből természetszerűen adódik, hogy az egyes személyekre vonatkozó adatokat összefüggésükben meg-

ismeri az adatfeldolgozó. Ez teljesen kiszolgáltatja az adatalanyokat, átvilágíthatóvá teszi magánszférájukat is. Egyenlőtlen helyzetet eredményez, amelyben az érintett nem tudja, hogy az adatfeldolgozó mit tud róla.
A 70-es években Európa legtöbb országában elvetették a személyi szám általános használatát, hasonló indokok alapján.

A rendelkezés az informatikusok között különösen nagy vitát váltott ki, néhányan a mai napig elhibázott lépésnek tartják. Ezt azzal indokolják, hogy a személyi szám rendkívül kényelmes megoldás volt a személyek egyértelmű azonosításra. Az új azonosítók és az osztott nyilvántartások megteremtése jelentős anyagi ráfordítást igényelt.

A mostani helyzetet dr. Jóri András így foglalja össze:
„A korai törvények beváltották a hozzájuk fűzött reményeket: a hierarchikus, szigorú szabályok alapján működő szervezetek által végzett adatkezelések jogszabályokkal valóban keretek közé szoríthatók. A helyzet azonban napjainkra alapvetően megváltozott: a nemzetközi számítógépes hálózatok közegébe egyre több személyes adat kerül, s ezeket az adatokat igen széles személyi kör érheti el, kapcsolhatja össze.
A hagyományos kommunikációs csatornákon továbbított üzenetek széles körű lehallgatása és feldolgozása nem volt automatizált és csak igen nagy ráfordítással volt megoldható, az ilyen csatornákról történő totális adatgyűjtést minden államban akadályozták a magas költségek, demokratikus államokban pedig az is, hogy széleskörű adatgyűjtés aligha képzelhető el nyom nélkül. A számítógépes hálózatokon azonban igen nehéz ellenőrizni az adatgyűjtés törvényességét, s annak költségei is jóval alacsonyabbak.
A másik lényeges változás, hogy az adatok összekapcsolásának és a személyiségprofil felállításának immár csak egyik célja az, hogy az állam hatékonyabban ellenőrizhesse saját vagy más államok polgárait. A napjainkban felvett profilok többségének a célja nem a politikai ellenőrzés, hanem a hatékony marketing; a magánszférát az állam (a nagy testvér) mellett egyre nagyobb mértékben fenyegeti az üzleti szféra (a kis testvér).” [24]

A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény rendelkezik az adóazonosító jelről és a TAJ számról. Itt az új kódok használatát és képzési módját is leírják. Ugyancsak ez a törvény szól arról, hogy mely nyilvántartásokban használható továbbra is a személyi azonosító/szám.

A személyi számot most is használjuk!

A közhiedelemmel ellentétben még mindig sokféle nyilvántartás használja a személyi számot: többek között a lakcím-, az ingatlan-, a katonai, a választási és a lőfegyver nyilvántartás. Az AB határozat csak a személyi szám ***korlátozás nélküli*** használatát tiltotta be. Ez a rendelkezés később az adatvédelmi törvénybe is bekerült.

Az államnak általában fontos érdeke fűződik ahhoz, hogy ha már nagy költségek árán kialakítanak és naprakész állapotban tartanak információrendszereket, akkor azok adattartalma minél szélesebb körben felhasználható legyen a legkülönbözőbb célokra. Ezzel ellentétben áll az adatalanyoknak (az állampolgároknak és szervezeteknek) az az érdeke, hogy a magánélet szűkebb szférájába vagy az üzleti titok körébe tartozó adataik vagy egyáltalán ne kerülhessenek be a külső szervek nyilvántartásaiba, vagy ha ez elkerülhetetlen, legyen garancia arra, hogy az adatok nem jutnak illetéktelenek tudomására. Ugyancsak alapvető érdeke az adatalanyoknak, hogy a rájuk vonatkozó információkat még az állam illetékes szervei is csupán meghatározott és általuk ismert célra használhassák fel. Ezek között az ellentétes érdekek között teremt egyensúlyt az adatvédelmi törvény.

1992. XI. 17-én - hosszas vita után - kihirdették az 1992. évi LXIII. törvényt, amely a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szól. Mivel a törvény a magyar adatvédelem alapvető szabályozó dokumentuma, ezért fontosnak tartjuk, hogy a hallgatók a törvény eredeti szövegét ismerjék meg.

3.2 Az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

Az 1992. évi LXIII. törvény

Az Országgyűlés - a Magyar Köztársaság Alkotmányában foglaltakkal összhangban - a személyes adatok védelmét, valamint a közérdekű adatok megismeréséhez való jog érvényesülését szolgáló alapvető szabályokról a következő törvényt alkotja:

I. fejezet
Általános rendelkezések
A törvény célja

1.§ (1) E törvény célja annak biztosítása, hogy - ha e törvényben meghatározott jogszabály kivételt nem tesz - személyes adatával mindenki maga rendelkezzen, és a közérdekű adatokat mindenki megismerhesse.

(2) E törvényben foglaltaktól eltérni csak akkor lehet, ha azt e törvény kifejezetten megengedni.

(3) E törvény szerint megengedett kivételt csak meghatározott adatfajtára és adatkezelőre együttesen lehet megállapítani.

A törvény hatálya

1/A. § (1) E törvény hatálya a Magyar Köztársaság területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz.

(2) E törvényt a teljesen vagy részben automatizált eszközzel, valamint a manuális módon végzett adatkezelésre és adatfeldolgozásra egyaránt alkalmazni kell.

(3) Nem kell alkalmaznia e törvény rendelkezéseit a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire.

Értelmező rendelkezések

2.§ E törvény alkalmazása során

Személyes adat

1. *személyes adat: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt -*

közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet;

Különleges adat

2. *különleges adat:*
   a) *a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra,*
   b) *az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a valamint a bűnügyi személyes adat; vonatkozó személyes adatok; .*

Bűnügyi személyes adat

3. *bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;*

Közérdekű adat

4. *közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső adat;*

Közérdekből nyilvános adat

5. *közérdekből nyilvános adat: minden olyan, természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet kezelésében lévő vagy rá vonatkozó, a közérdekű adat fogalma alá nem tartozó adat, amelynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli;*

hozzájárulás

6. *hozzájárulás: az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;*

tiltakozás

7. *tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;*

adatkezelő

8. *adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely a személyes adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;*

adatkezelés

9. *adatkezelés: az alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása,*

megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is;

továbbítás

10. adattovábbítás: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik;

nyilvánosságra hozatal

11. nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

törlés

12. adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

zárolás

13. adatzárolás: az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele;

megsemmisítés

14. adatmegsemmisítés: az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése;

15. adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől;

adatfeldolgozó

16. adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából - beleértve a jogszabály rendelkezése alapján történő megbízást is - személyes adatok feldolgozását végzi;

17. személyesadat-nyilvántartó rendszer (nyilvántartó rendszer): személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető;

18. adatállomány: az egy nyilvántartó rendszerben kezelt adatok összessége;

19. harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely vagy aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

20. harmadik ország: minden olyan ország, amely nem tagja az Európai Uniónak.

II. fejezet
A személyes adatok védelme
Adatkezelés

3.§

Az érintett hozzájárul, vagy a törvény elrendeli

(1) Személyes adat akkor kezelhető, ha
- *a) ahhoz az érintett hozzájárul, vagy*
- *b) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete elrendeli.*

(2) *Különleges adat akkor kezelhető, ha*
- *a) az adatkezeléshez az érintett írásban hozzájárul, vagy*
- *b) a 2.§ 2. a) pontjában foglalt adatok esetében, az nemzetközi egyezményen alapul, vagy Alkotmányban biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekében törvény elrendeli;*
- *c) egyéb esetekben azt törvény elrendeli.*

(3) Kötelező adatkezelés esetén az adatkezelés célját és feltételeit, a kezelendő adatok körét és megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg.

Nyilvánosságra hozatal

(4) Törvény közérdekből - az adatok körének kifejezett megjelölésével - elrendelheti a személyes adat nyilvánosságra hozatalát. Minden egyéb esetben a nyilvánosságra hozatalhoz az érintett hozzájárulása, különleges adat esetében írásbeli hozzájárulása szükséges. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

A hozzájárulás formái

(5) Az érintett hozzájárulását megadottnak kell tekinteni az érintett közszereplése során általa közölt vagy a nyilvánosságra hozatal céljából általa átadott adatok tekintetében.

(6) Az érintett kérelmére indult eljárásban a szükséges adatainak kezeléséhez való hozzájárulását vélelmezni kell. Erre a tényre az érintett figyelmét fel kell hívni.

(7) Az érintett a hozzájárulását az adatkezelővel írásban kötött szerződés keretében is megadhatja a szerződésben foglaltak teljesítése céljából. Ebben az esetben a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából - e törvény alapján - az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbítását, adatfeldolgozó igénybevételét. A szerződésnek félreérthetetlen módon

tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.

(8) Ha az érintett fizikai cselekvőképtelensége folytán nem képes hozzájárulását adni adatai kezeléséhez, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint katasztrófa- vagy szükséghelyzet elhárításához vagy megelőzéséhez szükséges mértékben sor kerülhet személyes adatainak, beleértve különleges adatait is, kezelésére.

***4.§** A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait - ha törvény kivételt nem tesz - az adatkezeléshez fűződő más érdekek, ideértve a közérdekű adatok nyilvánosságát (19.§) is, nem sérthetik.*

Adatfeldolgozás

***4/A.** § (1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel.*

(2) Az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért. Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót nem vehet igénybe.

(3) Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

(4) Az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni. Az adatfeldolgozásra nem adható megbízás olyan vállalkozásnak, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

(5)

(6) E törvényben foglaltakat kell alkalmazni, ha az Európai Unió területén kívül személyes adatok kezelését folytató adatkezelő az adatfeldolgozással a Magyar Köztársaság területén székhellyel, telephellyel (fiókteleppel) vagy lakóhellyel (tartózkodási hellyel) rendelkező adatfeldolgozót bíz meg, vagy itt lévő eszközt használ fel. Az ilyen adatkezelőnek ki kell jelölnie egy képviselőt a Magyar Köztársaság területén.

Az adatkezelés célhoz kötöttsége

5.§

(1) Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak.

Határozott cél

(2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.

(3) Kötelező adatszolgáltatáson alapuló adatkezelést közérdekből lehet elrendelni.

(4) A személyes adatot - akár az érintett hozzájárulásával, akár jogszabály alapján - különösen akkor lehet kezelni, ha ez közérdekű feladat vagy az adatkezelő törvényi kötelezettségének teljesítéséhez, az adatkezelő vagy az adatátvevő harmadik személy hivatalos feladatának gyakorlásához, az érintett létfontosságú érdekeinek védelméhez, az érintett és az adatkezelő között létrejött szerződés teljesítéséhez, az adatkezelő vagy harmadik személy jogos érdekének érvényesítéséhez, társadalmi szervezetek jogszerű működéséhez szükséges.

(5) Kizárólag állami vagy önkormányzati szerv kezelheti az állam bűnüldözési és bűnmegelőzési, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása céljából kezelt bűnügyi személyes adatokat, illetve a szabálysértési, a polgári peres és nemperes ügyekre vonatkozó adatokat tartalmazó adatállományokat.

6.§

Tájékoztatás

(1) Az érintettel az adat felvétele előtt közölni kell, hogy az adatszolgáltatás önkéntes vagy kötelező. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályt is.

(2) Az érintettet tájékoztatni kell az adatkezelés céljáról, és arról, hogy az adatot kik fogják kezelni. A tájékoztatás megtörténik azzal is, hogy jogszabály rendelkezik a már létező adatkezelésből továbbítással vagy összekapcsolással az adat felvételéről.

(3) Az adatkezelésről való tájékoztatás megtörténik azzal is, hogy jogszabály rendelkezik a már létező adatkezelésből továbbítással vagy összekapcsolással az adat felvételéről.

(4) A tájékoztatás - különösen statisztikai vagy tudományos (ideértve a történelmi kutatásokat is) célú adatkezelés esetén - megtörténhet az adatgyűjtés tényének, az érintettek körének, az adatgyűjtés céljának, az adatkezelés időtartamának és az adatok megismerhetőségének mindenki számára hozzáférhető módon történő nyilvá-

nosságra hozatalával, ha az egyénre szóló tájékoztatás lehetetlen vagy aránytalan költséggel járna.

Az adatok minősége

7.§ (1) A kezelt személyes adatoknak meg kell felelniük az alábbi követelményeknek:

a) felvételük és kezelésük tisztességes és törvényes;

b) pontosak, teljesek és ha szükséges időszerűek;

c) tárolásuk módja alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.

(2) Korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos.

Adattovábbítás, az adatkezelések összekapcsolása

8.§

Hozzájárult, vagy törvény megengedi

(1) Az adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.

(2) Az (1) bekezdést kell alkalmazni az ugyanazon adatkezelő, valamint az állami és az önkormányzati szervek által kezelt adatok összekapcsolására is.

Adattovábbítás külföldre

9.§ (1) Személyes adat (beleértve a különleges adatot is) az országból - az adathordozótól vagy az adatátvitel módjától függetlenül - harmadik országban lévő adatkezelő vagy adatfeldolgozó részére csak akkor továbbítható, ha ahhoz az érintett hozzájárul, ha azt törvény lehetővé teszi, vagy ha arról nemzetközi szerződés rendelkezik, feltéve, hogy a harmadik ország joga - az Európai Unió által meghatározott - megfelelő védelmet biztosít az átadott adatok kezelése során.

Automatizált egyedi döntés

az érintett személyes jellemzőinek értékelésére

9/A. § (1) Kizárólag számítástechnikai eszközzel végrehajtott automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésére csak akkor kerülhet sor, ha ahhoz kifejezetten hozzájárult, vagy azt törvény lehetővé teszi. Az érintettnek álláspontja kifejtésére lehetőséget kell biztosítani.

(2) Az automatizált adatfeldolgozás esetén az érintettet - kérelmére - tájékoztatni kell az alkalmazott matematikai módszerről és annak lényegéről.

Adatbiztonság

10. § — Adatkezelő köteles

(1) Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(2Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.

Az érintettek jogai és érvényesítésük

11.§ (1) Az érintett — Betekintés, helyesbítés

a) tájékoztatást kérhet személyes adatai kezeléséről (12. és 13.§), valamint

b) kérheti személyes adatainak helyesbítését,. illetve - a jogszabályban elrendelt adatkezelések kivételével - törlését (14-16.§).

(2) Az adatvédelmi nyilvántartásba [28.§ (1) bek.] bárki betekinthet, az abban foglaltakról feljegyzést készíthet és kivonatot kérhet. A kivonatért díjat kell fizetni.

12.§ — Tájékoztatás

(1) Az érintett kérelmére az adatkezelő tájékoztatást ad az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat. Az adattovábbításra vonatkozó nyilvántartás és ennek alapján a tájékoztatási kötelezettség időtartamát az adatkezelést szabályozó jogszabály korlátozhatja. A korlátozás időtartama személyes adatok esetében öt évnél, különleges adatok esetében pedig húsz évnél rövidebb nem lehet.

(2) Az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban, közérthető formában megadni a tájékoztatást.

(3) A (2) bekezdésben foglalt tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos területre vonatkozó tájékoztatási kérelmet az adatkezelőhöz még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

Tájékoztatás megtagadása

13.§

(1) Az érintett tájékoztatását az adatkezelő csak akkor tagadhatja meg, ha azt a 16.§-ban meghatározott esetekben a törvény lehetővé teszi.

(2) Az adatkezelő köteles az érintettel a felvilágosítás megtagadásának indokát közölni.

(3) Az elutasított kérelmekről az adatkezelő az adatvédelmi biztost évente értesíti.

Helyesbítés, törlés

14.§

(1) A valósággnak meg nem felelő adatot az adatkezelő helyesbíteni köteles.

(2) A személyes adatot törölni kell, ha

a) kezelése jogellenes;

b) az érintett - a 11.§ (1) bekezdésének b) pontjában foglaltak szerint - kéri;

c) az hiányos vagy téves - és ez az állapot jogszerűen nem korrigálható -, feltéve, hogy a törlést törvény nem zárja ki;

d) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt;

e) azt a bíróság vagy az adatvédelmi biztos elrendelte.

(3) A törlési kötelezettség - jogellenes adatkezelés kivételével - nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

15.§

A helyesbítésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

16.§

Korlátozások

Az érintett jogait (11-15.§) törvény az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűnmegelőzés vagy bűn-

üldözés érdekében, továbbá állami vagy helyi önkormányzati pénzügyi érdekből, valamint az érintett vagy mások jogainak védelme érdekében korlátozhatja.

Tiltakozási jog

Tiltakozás

16/A. §

(1) Az érintett tiltakozhat személyes adatának kezelése ellen, ha

a) a személyes adatok kezelése (továbbítása) kizárólag az adatkezelő vagy az adatátvevő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést törvény rendelte el;

b) a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik;

c) a tiltakozás jogának gyakorlását egyébként törvény lehetővé teszi.

(2) Az adatkezelő - az adatkezelés egyidejű felfüggesztésével - a tiltakozást köteles a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 nap alatt megvizsgálni, és annak eredményéről a kérelmezőt írásban tájékoztatni. Amennyiben a tiltakozás indokolt, az adatkezelő köteles az adatkezelést - beleértve a további adatfelvételt és adattovábbítást is - megszüntetni és az adatokat zárolni, valamint a tiltakozásról, illetőleg az annak alapján tett intézkedésekről értesíteni mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

(3) Amennyiben az érintett az adatkezelőnek a (2) bekezdés alapján meghozott döntésével nem ért egyet, az ellen - annak közlésétől számított 30 napon belül - e törvény szerint bírósághoz fordulhat.

(4) Ha az adatátvevő törvényes jogának érvényesítéséhez szükséges adatokat az érintett tiltakozása miatt nem kapja meg, a (2) bekezdés alapján történő értesítés közlésétől számított 15 napon belül, az adatokhoz való hozzájutás érdekében - e törvény szerint - bírósághoz fordulhat az adatkezelő ellen. Az adatkezelő az érintettet is perbe hívhatja.

(5) Ha a bíróság az adatátvevő kérelmét elutasítja, az adatkezelő köteles az érintett személyes adatát az ítélet közlésétől számított 3 napon belül törölni. Az adatkezelő köteles az adatokat akkor is törölni, ha az adatátvevő a (4) bekezdésben meghatározott határidőn belül nem fordul bírósághoz.

(6) Az adatkezelő az érintett adatát nem törölheti, ha az adatkezelést törvény rendelte el. Az adat azonban nem továbbítható az adatátvevő részére, ha az adatkezelő egyetértett a tiltakozással, illetőleg a bíróság a tiltakozás jogosságát megállapította.

Bírósági jogérvényesítés

17.§

(1) Az érintett, jogainak megsértése esetén, az adatkezelő ellen a bírósághoz fordulhat.

(2) Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az adatkezelő köteles bizonyítani.

(3) A perre az a bíróság illetékes, amelynek területén az adatkezelő székhelye van. A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége.

(4) Ha a bíróság a kérelemnek helyt ad, az adatkezelőt a tájékoztatás megadására, az adat helyesbítésére, törlésére kötelezi, illetőleg az adatvédelmi biztost arra kötelezi, hogy az adatvédelmi nyilvántartásba való betekintést tegye lehetővé.

(5) A bíróság elrendelheti ítéletének az adatvédelmi nyilvántartásba történő bejegyzését, ha azt az adatvédelem érdekei és nagyobb számú érintett, e törvényben védett jogai megkövetelik.

Kártérítés

18.§

(1) Az adatkezelő az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével másnak okozott kárt köteles megtéríteni. Az adatkezelő mentesül a felelősség alól, ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.

(2) Nem kell megtéríteni a kárt annyiban, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

III. fejezet

A közérdekű adatok nyilvánossága

Közérdekű adatok

19.§

(1) Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv és személy (a továbbiakban együtt: szerv) a feladatkörébe tartozó ügyekben - ideértve a gazdálkodásával kapcsolatos ügyeket is - köteles elősegíteni a közvélemény pontos és gyors tájékoztatását.

(2) Az (1) bekezdésben említett szervek rendszeresen közzé vagy más módon hozzáférhetővé teszik a tevékenységükkel kapcsolatos legfontosabb - így különösen a hatáskörükre, illetékességükre, szervezeti felépítésükre, a birtokukban lévő adatfajtákra és a működésükről szóló jogszabályokra vonatkozó - adatokat. E szervek hatáskörében eljáró személyek neve és beosztása - ha törvény másként nem rendelkezik - bárki számára hozzáférhető, nyilvános adat.

Kivételek

(3) Az (1) bekezdésben említetteknek lehetővé kell tenniük, hogy a kezelésükben lévő közérdekű adatot bárki megismerhesse, kivéve, ha az adott törvény alapján az arra jogosult szerv állam- vagy szolgálati titokká nyilvánította, továbbá, ha a közérdekű adatok nyilvánosságához való jogot - az adatfajták meghatározásával - törvény

a) honvédelmi;
b) nemzetbiztonsági;
c) bűnüldözési vagy bűnmegelőzési;
d) központi pénzügyi vagy devizapolitikai érdekből;
e) külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra;
f) bírósági eljárásra tekintettel
korlátozza.

(4) Az (1) bekezdésben említett szervek hatáskörében eljáró személynek a feladatkörével összefüggő személyes adata a közérdekű adat megismerését nem korlátozza.

(5) Ha törvény másként nem rendelkezik, a belső használatra készült, valamint a döntés-előkészítéssel összefüggő adat a keletkezését követő harminc éven belül nem nyilvános. Kérelemre az adatok megismerését a szerv vezetője e határidőn belül is engedélyezheti.

20.§

Közérdekű adatok közlése

(1) A közérdekű adat megismerésére irányuló kérelemnek az adatot kezelő szerv a kérelem tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül, közérthető formában tesz eleget. Az adatokat tartalmazó dokumentumról vagy dokumentumrészről annak tárolási módjától függetlenül - költségtérítés ellenében - a kérelmező másolatot kérhet.

(2) A kérelem megtagadásáról - annak indokaival együtt - 8 napon belül írásban értesíteni kell a kérelmezőt.

(3) A közérdekű adat közléséért az adatkezelő szerv vezetője - legfeljebb a közléssel kapcsolatban felmerült költség mértékéig - költ-

ségtérítést állapíthat meg. A kérelmező kérésére a költség összegét előre közölni kell.

(4) A 19.§ (1) bekezdésében említett szervek évente értesítik az adatvédelmi biztost az elutasított kérelmekről, valamint az elutasítások indokairól.

Peres eljárás

21.§

(1) Ha a közérdekű adatra vonatkozó kérését nem teljesítik, a kérelmező a bírósághoz fordulhat.

(2) A megtagadás jogszerűségét és megalapozottságát az adatot kezelő szerv köteles bizonyítani.

(3) A pert a megtagadás közlésétől számított 30 napon belül az ellen a szerv ellen kell megindítani, amely a kért felvilágosítást megtagadta.

(4) A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége. .

(5) Az egész országra kiterjedő hatáskörű szerv ellen indult per a megyei (fővárosi) bíróság hatáskörébe tartozik. A helyi bíróság hatáskörébe tartozó ügyekben a megyei bíróság székhelyén lévő helyi bíróság, Budapesten a Pesti Központi Kerületi Bíróság jár el. A bíróság illetékességét az adatközlést nem teljesítő szerv székhelye (működési helye) állapítja meg.

(6) A bíróság soron kívül jár el.

(7) Ha a bíróság a kérelemnek helyt ad, határozatában az adatkezelő szervet a kért közérdekű adat közlésére kötelezi.

***22.§** E fejezet rendelkezései nem alkalmazhatók a közhitelű nyilvántartásból történő - külön törvényben szabályozott - adatszolgáltatásra.*

IV. fejezet
Az adatvédelmi biztos és az adatvédelmi nyilvántartás
Adatvédelmi biztos

23.§

Választás

(1) A személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való alkotmányos jog védelme érdekében az Országgyűlés adatvédelmi biztost választ azok közül az egyetemi végzettségű, büntetlen előéletű, kiemelkedő tudású elméleti vagy legalább 10 évi szakmai gyakorlattal rendelkező magyar állampolgárok közül, akik az adatvédelmet érintő eljárások lefolytatásában, felügyeletében vagy tudományos elméletében jelentős tapasztalatokkal rendelkeznek és köztiszteletnek örvendenek.

(2) Az adatvédelmi biztosra - e törvényben foglalt eltérésekkel - az állampolgári jogok országgyűlési biztosáról szóló törvény rendelkezéseit kell alkalmazni.

24.§ Az adatvédelmi biztos

Feladatai

a) ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabály megtartását;
b) kivizsgálja a hozzá érkezett bejelentéseket;
c) gondoskodik az adatvédelmi nyilvántartás vezetéséről.

25.§

(1) Az adatvédelmi biztos figyelemmel kíséri a személyes adatok védelmének és a közérdekű adatok nyilvánossága érvényesülésének feltételeit. Javaslatot tesz az adatkezelést és a közérdekű adatok nyilvánosságát érintő jogszabályok megalkotására, illetve módosítására, véleményezi az ilyen jogszabályok tervezetét. Kezdeményezheti az államtitokkörben, valamint a szolgálati titokkörben meghatározott adatfajták szűkítését vagy bővítését.

(2) Az adatvédelmi biztos a jogellenes adatkezelés észlelése esetén az adatkezelőt az adatkezelés megszüntetésére szólítja fel. Az adatkezelő haladéktalanul köteles megtenni a szükséges intézkedéseket, és erről 30 napon belül írásban tájékoztatni az adatvédelmi biztost.

(3) Ha az adatkezelő a jogellenes adatkezelést nem szünteti meg az adatvédelmi biztos tájékoztatja a nyilvánosságot az adatkezelés tényéről, a kezelő személyéről és a kezelt adatok köréről.

26.§

(1) Az adatvédelmi biztos a feladatai ellátása során az adatkezelőtől minden olyan kérdésben felvilágosítást kérhet, és az összes olyan iratba betekinthet, adatkezelést megismerhet, amely személyes vagy közérdekű adatokkal összefügghet.

Jogosítványai

(2) Az adatvédelmi biztos minden olyan helyiségbe beléphet, ahol adatkezelés folyik.

(3) Az államtitok és szolgálati titok az adatvédelmi biztost e §-ban szabályozott jogainak gyakorlásában nem akadályozhatja, de a titok megtartására vonatkozó rendelkezések rá nézve is kötelezőek. Az államtitkot vagy szolgálati titkot érintő adatkezelés esetén a fegyveres erőknél, a rendőrségnél és a nemzetbiztonsági szerveknél az adatvédelmi biztos a jogait csak személyesen gyakorolhatja.

(4) Ha az adatvédelmi biztos eljárása során az adat minősítését indokolatlannak tartja, a minősítőt annak megváltoztatására vagy a minősítés megszüntetésére szólítja fel. A felszólítás megalapozatlanságának megállapítása iránt a minősítő 30 napon belül a Fővárosi Bírósághoz fordulhat. A bíróság az ügyben zárt tárgyaláson soron kívül jár el.

Bejelentések

27.§

(1) Bárki az adatvédelmi biztoshoz fordulhat, ha véleménye szerint személyes adatainak kezelésével vagy a közérdekű adatok megismeréséhez fűződő jogainak gyakorlásával kapcsolatban jogsérelem érte, vagy annak közvetlen veszélye fennáll, kivéve ha az adott ügyben bírósági eljárás van folyamatban.

(2) Az adatvédelmi biztoshoz tett bejelentése miatt senkit sem érhet hátrány. A bejelentőt a közérdekű bejelentővel azonos védelem illeti meg.

Adatvédelmi nyilvántartás

28.§

A nyilvántartás tartalma

(1) Az adatkezelő köteles e tevékenysége megkezdése előtt az adatvédelmi biztosnak nyilvántartásba vétel végett bejelenteni

a) az adatkezelés célját;

b) az adatok fajtáját és kezelésük jogalapját;

c) az érintettek körét;

d) az adatok forrását;

e) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját;

f) az egyes adatfajták törlési határidejét;

g) az adatkezelő nevét és címét (székhelyét), valamint a tényleges adatkezelés helyét.

h) a belső adatvédelmi felelős nevét és elérhetőségi adatait.

(2) A jogszabályban elrendelt adatkezelést a szabályozás tárgya szerint illetékes miniszter, országos hatáskörű szerv vezetője, illetőleg a polgármester, főpolgármester, a megyei közgyűlés elnöke köteles bejelenteni a jogszabály hatálybalépését követő 15 napon belül.

(3) A nemzetbiztonsági szervek az adatkezelésük célját és jogalapját jelentik be.

29.§

(1) Az adatkezelő az első nyilvántartásba vételkor nyilvántartási számot kap. A nyilvántartási számot az adatok minden továbbítá-

sánál, nyilvánosságra hozásánál és az érintettnek való kiadásakor fel kell tüntetni.

(2) A 28.§ (1) bekezdésében felsorolt adatok megváltozását 8 napon belül be kell jelenteni az adatvédelmi biztosnak, és a nyilvántartást megfelelően módosítani kell.

30.§ Nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely

Nem kell bejelenteni +

a) az adatkezelővel munkaviszonyban, tagsági, tanulói viszonyban, ügyfélkapcsolatban álló személyek adatait tartalmazza;

b) egyház, vallásfelekezet, vallási közösség belső szabályai szerint történik;

c) az egészségügyi ellátásban kezelt személy betegségére, egészségi állapotára vonatkozó személyes adatokat tartalmaz, gyógykezelés vagy az egészség megőrzése, társadalombiztosítási igény érvényesítése céljából;

d) az érintett anyagi és egyéb szociális támogatását célzó és nyilvántartó adatokat tartalmaz;

e) a hatósági, az ügyészségi és a bírósági eljárás által érintett személyeknek az eljárás lefolytatásával kapcsolatos személyes adatait tartalmazza;

f) a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve hogy - külön törvényben meghatározottak szerint - az adatok személlyel való kapcsolatának megállapítását véglegesen lehetetlenné teszik;

g) a sajtótörvény hatálya alá tartozó társaságok és szervek olyan adatait tartalmazza, amelyek kizárólag saját tájékoztatási tevékenységüket szolgálják;

h) a tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra;

i) az adatkezelőtől levéltári kezelésbe került át;

j) a természetes személy saját célját szolgálja.

Előzetes ellenőrzés

31. § (1) Az adatvédelmi biztos a nyilvántartásba vételt megelőzően előzetes ellenőrzést végezhet.

(2) Új adatállomány feldolgozását vagy új adatfeldolgozási technológia alkalmazását megelőzően az adatvédelmi biztos előzetes ellenőrzést végezhet a következő adatkezeléseket végző adatkezelőknél:

a) országos hatósági, munkaügyi és bűnügyi adatállományok;

b) pénzügyi szervezetek és közüzemi szolgáltatók ügyfelekre vonatkozó adatkezelései;

c) távközlési szolgáltatóknak a szolgáltatást igénybe vevőkre vonatkozó adatkezelései;

d) külön törvényben meghatározott egyedi statisztikai adatokat tartalmazó adatállományok.

(3) Az adatkezelőnek az új adatállomány feldolgozására vagy az új adatfeldolgozási technológia alkalmazására irányuló szándékát a tevékenység megkezdését megelőzően 30 nappal be kell jelentenie az adatvédelmi biztosnak. Az adatvédelmi biztos az előzetes ellenőrzésre vonatkozó igényét a bejelentéstől számított 8 napon belül köteles jelezni az adatkezelőnek, és az ellenőrzést 30 napon belül köteles elvégezni. Az adatkezelő a feldolgozást csak az adatvédelmi biztos előzetes ellenőrzésének befejezése után kezdheti meg.

(4) Az ellenőrzés alapján az adatvédelmi biztos a kezelendő adatok körének, illetőleg az adatfeldolgozás módszerének megváltoztatására hívhatja fel az adatkezelőt. Ha az adatvédelmi biztos az adatkezelést elrendelő jogszabályt kifogásolja, ajánlást tehet a jogszabály módosítására.

Belső adatvédelmi felelős és adatvédelmi szabályzat

Belső adatvédelmi felelős és adatvédelmi szabályzat

31/A. § (1) Az adatkezelő, illetőleg az adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó - jogi, közigazgatási, számítástechnikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező - belső adatvédelmi felelőst kell kinevezni vagy megbízni:

a) az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetőleg feldolgozó adatkezelőnél és adatfeldolgozónál;

b) a pénzügyi szervezetnél;

c) a távközlési és közüzemi szolgáltatónál.

(2) A belső adatvédelmi felelős:

a) közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

b) ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;

c) kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;
e) vezeti a belső adatvédelmi nyilvántartást;
f) gondoskodik az adatvédelmi ismeretek oktatásáról.

(3) Az (1) bekezdésben meghatározott adatkezelőknek, valamint - az adatvédelmi nyilvántartásba bejelentési kötelezettség alá nem eső adatkezelők kivételével - egyéb állami és önkormányzati adatkezelőknek, e törvény végrehajtása érdekében, adatvédelmi és adatbiztonsági szabályzatot kell készíteniük.

V. fejezet
Különleges rendelkezések
Személyes adatok feldolgozása és felhasználása kutatóintézetben

32.§

Kutatásban felhasznált személyes adatok

(1) Tudományos kutatás céljára felvett vagy tárolt személyes adat csak tudományos kutatás céljára használható fel.

(2) A személyes adatot - mihelyt a kutatási cél megengedi - anonimizálni kell. Addig is külön kell tárolni azokat az adatokat, amelyek meghatározott vagy meghatározható természetes személy azonosítására alkalmasak. Ezek az adatok egyéb adatokkal csak akkor kapcsolhatók össze, ha az kutatás céljára szükséges.

(3) A tudományos kutatást végző szerv vagy személy személyes adatot csak akkor hozhat nyilvánosságra, ha
a) az érintett abba beleegyezett, vagy
b) az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges.

Személyes adatok felhasználása statisztikai célra

32/A. § (1) A statisztikai célra felvett, átvett vagy feldolgozott személyes adatok csak statisztikai célra használhatók fel. A külön törvény szerinti egyedi statisztikai adatok - beleértve a személyes adatokat is - a statisztikai céltól eltérő célra semmilyen módon vagy jogcímen nem adhatók és vehetők át, nem dolgozhatók fel és nem hozhatók nyilvánosságra.

(2) A személyes adatok statisztikai célra történő kezelésének részletes szabályait külön törvény határozza meg.

Az adatvédelmi szabályozás hazai történetének legjelentősebb alkotása az 1992. évi LXIII. törvény. Az Európai Unió 2000. júliusi döntésében adatvédelmi szempontból megfelelő országnak ismerte el Magyarországot. Ezt a minősítést a tagjelölt or-

országok közül elsőként kapta meg hazánk. A magyar adatvédelmi jogrend nem szorul alapvető változtatásokra, csupán annak finomítása szükségeses: 1992. óta sok körülmény megváltozott, ami más igényeket támaszt az adatvédelemmel szemben. Ezek a finomítások folyamatosan épülnek be a törvénybe.
Az aktuális jogszabályi változások, az adatvédelmi nyilvántartás és az adatvédelmi biztos állásfoglalásai megtalálhatók az adatvédelmi biztos WEB oldalán [ ]

Ellenőrző kérdések

1. Mi az adatvédelem fogalma?
2. Miben áll az Alkotmánybíróság döntése a személyi számmal és a népességnyilvántartó rendszerrel kapcsolatban?
3. Mi az alkotmányban megfogalmazott adatvédelmet érintő alapelv?
4. Mi az 1992. évi LXIII. törvény célja?
5. Mit értünk a következő fogalmak alatt?
   - személyes adat,
   - különleges adat,
   - bűnügyi személyes adat
   - közérdekű adat,
   - közérdekből nyilvános adat,
   - adatkezelés,
   - nyilvánosságra hozatal,
   - adattörlés,
   - adatkezelő
6. Mit jelent az adatkezelés célhoz kötöttsége?
7. Milyen tájékoztatási kötelezettsége van az adatkezelőnek?
8. Mit ért a törvény az adatok minősége alatt?
9. Milyen esetben kezelhető ill. hozható nyilvánosságra személyes, ill. különleges adat?
10. Milyen jogosítványokkal rendelkezik az érintett saját adataival kapcsolatban?
11. Milyes esetekben kell törölni a személyes adatokat?

12. Mi a bírósági jogérvényesítés és kártérítési kötelezettség lényege?
13. Milyen adatok megismerését korlátozza a törvény?
14. Hogyan érvényesíthető a közérdekű adatok megismerése?
15. Melyek az adatvédelmi biztos feladatai?
16. Milyen jogosítványokkal rendelkezik az adatvédelmi biztos?
17. Milyen adatokat tartalmaz az adatvédelmi nyilvántartás?
18. Mely nyilvántartásoknak nincs bejelentési kötelezettsége?
19. Milyen szervezetek kötelesek belső adatvédelmi felelőst kinevezni?
20. Milyen feladatokat lát el a belső adatvédelmi felelős?
21. Hogyan rendelkezik a törvény a személyes adatok kutatási és statisztikai célra történő felhasználásáról?

Jegyzetek:

4. Más törvények adatvédelmi vonatkozásai

Az előző fejezetben megismerkedtünk a személyes adatok, illetve azok kezelésének alapfogalmaival. A személyes adatok kezelésének vannak még további, törvény által szabályozott esetei is. A személyes adatokon kívül más adatcsoportok is kiemelt kezelést igényelnek, külön törvények vonatkoznak rájuk. Ezek az állam-, szolgálati, üzleti és banktitkok. Mi történik akkor, ha valaki megszegi az adatok kezelésére vonatkozó törvényeket. Milyen büntetésre számíthat? Ebben a fejezetben ezeket a kérdéseket tárgyaljuk.

4.1 Személyes adatok kezelése kutatási és üzletszerzési céllal

A kutatási célú személyes adatkezeléssel az adatvédelmi törvény is fogalakozik. Az utóbbi időszakban azonban sokkal gyakrabban találkozunk a személyes adatok üzleti célú felhasználásával. Nézzük meg, hogyan szabályozta ezt a Törvényhozás.

Bizonyára már mindenki kapott névre szólóan címzett ajánlatot valamilyen csomagküldő cégtől, amiben különböző termékek vásárlására ösztönzik, vagy boldogan közlik vele, hogy értékes nyereménnyel lett gazdagabb. Ilyenkor felvetődik a kérdés, hogyan jutottak ezek a cégek az ő személyes adataihoz, és menynyire törvényes ez az egész? Ugyanakkor a marketing egyik leghatékonyabb módszerének tekintett direkt megkereséshez nélkülözhetetlenek a személyes adatok. A piac- és közvélemény kutatók szintén csak ilyen adatok felhasználásával tudnak dolgozni.

Ezen a területen az Európa Tanács 108-as ajánlásának és az adatvédelmi törvény szellemének megfelelően kellet az intézkedéseket meghozni. Így szültetett meg az *1995. évi CXIX. törvény a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről.*

Honnét lehet adatokat átvenni?

A törvény szabályozza ezen adatok átvételének módját. Erre az alábbi lehetőségek vannak:

- saját korábbi ügyfelek adatai,
- nyilvánosságra hozatal céljából készített adatállományok (szaknévsor, telefonkönyv, névjegyzék, stb.)
- más hasonló tevékenységet végző szerv adatállományának átvétele,
- a központi személyi adat és lakcímnyilvántartóból.

Az adatok felhasználásnak feltételei:

- az illetőt a nyilvántartás létrehozásakor tájékoztatták arról, hogy adatait más is felhasználhatja,
- a válogatási szempont nem lehet olyan, amelyből különleges adatokra lehet következtetni (pl. valamilyen betegségben szenvedők).

Az adatvédelmet az adatkezelőnek kell biztosítani a következő módon:

- a kapcsolatfelvételkor az érintettet írásban kell tájékoztatni arról, hogy a megkereső az adatokat milyen forrásból szerezte,
- biztosítani kell a jogot, hogy az illető bármikor letilthassa az adatainak további használatát,
- tilalmi listát kell összeállítani azokról az állampolgárokról, akik megtiltották adataik felhasználását, hogy ez a továbbiakban sem történhessen meg.

Az informatika fejlődésével a reklám célú megkeresések újabb területre terjedtek ki. Ezeket összefoglaló néven *„az információs társadalommal összefüggő szolgáltatásoknak"* szokás nevezni. Ide tarozik pl. az e-mail, a telefonnal kapcsolatos üzenetek, SMS, stb. Ezt a *2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről c.* törvény

szabályozza. A törvény 14. bekezdése foglalkozik a reklámokkal:

„Az információs társadalommal összefüggő szolgáltatás felhasználásával küldött reklámokra vonatkozó különös szabályok

14. *§ (1) Az információs társadalommal összefüggő szolgáltatás felhasználásával küldött reklámnak világosan és egyértelműen azonosíthatónak kell lennie, amint az hozzáférhetővé válik az igénybe vevő számára. Kizárólag az igénybe vevő egyértelmű, előzetes hozzájárulásával küldhető elektronikus úton, levelezés során reklám.*

(2) Az információs társadalommal összefüggő szolgáltatás felhasználásával küldött reklámhoz kapcsolódóan tájékoztatni kell a címzettet arról az elektronikus levelezési címről és egyéb elérhetőségről, ahol a reklámok információs társadalommal összefüggő szolgáltatás felhasználásával történő küldésének megtiltása iránti igényét bejelentheti.

(3) A reklámozó, a reklámszolgáltató és a reklám közzétevője köteles nyilvántartást vezetni azokról, akik részükre írásban bejelentették, hogy kívánnak információs társadalommal összefüggő szolgáltatás felhasználásával reklámot kapni. A nyilvántartás harmadik fél számára kizárólag az igénybe vevő előzetes hozzájárulásával adható át.

(4) A reklámozó, a reklámszolgáltató és a reklám közzétevője nem küldhet információs társadalommal összefüggő szolgáltatás felhasználásával reklámot azoknak, akik a (3) bekezdésben meghatározott nyilvántartásban nem szerepelnek. A küldés tilalma a reklámozó, a reklámszolgáltató, illetve a reklám közzétevője által küldendő összes reklámra vonatkozik."

SPAM

A törvény tehát egyértelműen leszögezi, hogy kéretlen reklámlevél, az un. „spam" –ok küldése csak abban az esetben engedélyezett, ha az illető ezt kérte. Más küldő részére a címet csak az érintett előzetes engedélyével lehet átadni. Az adatvédelem rendelkezéseinek megsértésén túl a spam más területeken is gondot okoz. A rengeteg üzenet lefoglalja a szolgáltatók infrastruktúráját, és a megcélzottak számára is terhet jelent, növeli

költségeit. A spam-áradat már-már az elektronikus levelezés megbénításával fenyeget. Természetesen ebben az esetben is megjelent a technikai segítség: különböző ún. anti-spam rendszereket kínálnak a szoftverfejlesztők, amelyek – részben - kiszűrik a kéretlen leveleket.

4.2 Államtitok, szolgálati titok

Az államtitokról és a szolgálati titokról szóló, 1995. évi LXV. törvény szabályozza a minősített adatok fajtáit, a minősítést végző szervek körét, a minősített adatokkal való rendelkezések módját. A minősített adatok két nagy csoportját különböztetjük meg:

Államtitok

Államtitok az az adat, amely:

- a törvény által *meghatározott adatkörbe* tartozik,
- ezt a *minősítési eljárásban* a minősítő kétséget kizáróan megállapította,
- *az érvényességi idő* lejárta előtti *nyilvánosságra hozatala*, jogosulatlan *megszerzése* vagy felhasználása, illetéktelen személy tudomására hozása,
- továbbá az arra jogosult részére *hozzáférhetetlenné* tétele
- sérti vagy veszélyezteti a *Magyar Köztársaság* honvédelmi, nemzetbiztonsági, bűnüldözési vagy bűnmegelőzési, központi pénzügyi vagy devizapolitikai, külügyi vagy nemzetközi kapcsolataival összefüggő, valamint igazságszolgáltatási érdekeit.

Szolgálati titok

Szolgálati titok

- a minősítésre *felhatalmazott* által meghatározott *adatkörbe* tartozó adat, amelynek az érvényességi idő lejárta előtti
- *nyilvánosságra* hozatala, jogosulatlan *megszerzése* és felhasználása, illetéktelen személy részére hozzáférhetővé tétele

- sérti az állami vagy *közfeladatot ellátó szerv* működésének rendjét, akadályozza a feladat- és hatáskörének illetéktelen befolyástól mentes gyakorlását.

Minősítés

Azt, hogy melyik adatkört ki minősíthet, a törvény 5. bekezdése határozza meg. Ez úgy rendelkezik, hogy az országos hatáskörű szervek vezetői saját hatáskörükben jogosultak az adatok minősítésre. A törvény melléklete részletesen tartalmazza az egyes intézményekhez tartozó titokfajtákat és azok érvényességi idejét. A minősítési kérelmet indokolni kell, megjelölve a konkrét titokkört és érvényességi időt. Csak a titokkörben szereplő adatokat lehet állam- vagy szolgálati titoknak minősíteni.

Szigorúan titkos
Titkos

Amennyiben a javaslatot elfogadják, akkor fel kell tüntetni az *államtitkot* képező adat hordozóján *a "Szigorúan titkos!"*, a *szolgálati titkot* képező adat hordozóján a *"Titkos!"* jelölést, az érvényességi időt, a minősítő nevét és beosztását.
A minősítést 3 évenként felül kell vizsgálni, és megfelelő indokkal a minősítés megváltoztatható.

4.3 Üzleti és banktitok

Az üzleti titok fogalmát a tisztességtelen piaci magatartás tilalmáról szóló 1990. évi LXXXVI. törvény határozza meg.

Üzleti titok

Üzleti titok a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldási mód vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik.

Tilos üzleti titkot tisztességtelen módon megszerezni vagy felhasználni, valamint jogosulatlanul mással közölni illetve nyilvánosságra hozni. Üzleti titok tisztességtelen módon való megszerzésének minősül az is, ha azt a jogosult hozzájárulása nélkül, a vele bizalmi viszonyban vagy üzleti kapcsolatban álló személy közreműködésével szerezték meg.

A banktitokkal a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény foglalkozik

Banktitok

Banktitok az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldási mód vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.

A hitelintézeti törvény három esetben teszi lehetővé a banktitoknak harmadik személy részéről való kiszolgáltatását:

1. Amikor a pénzügyi intézmény ügyfele vagy annak törvényes képviselője kéri a banktitok kiadását, vagy arra felhatalmazást ad.
2. Magának a pénzügyi intézménynek az érdeke szükségessé teszi ezt abból a célból, hogy az ügyféllel szemben fennálló követelését érvényesíthesse
3. Maga a törvény ad lehetőséget a banktitok megtartásának kötelezettsége alóli felmentésre. A hitelintézeti törvény 51. §-ának (2) bekezdése részletesen felsorolja ezeket. Így a banktitok megtartásának kötelezettsége nem áll fenn:
   - az Országos Betétbiztosítási Alap,
   - a Magyar Nemzeti Bank,
   - az Állami Számvevőszék,
   - a feladatkörében eljáró felügyelet,
   - az intézményvédelmi és betétbiztosítási alapok,
   - a versenyfelügyeleti eljárásban eljáró Gazdasági Versenyhivatal,
   - a Kormányzati Ellenőrzési Iroda,
   - a hagyatéki ügyben eljáró közjegyző,
   - a feladatkörében eljáró gyámhatóság,

- a csődeljárást, felszámolási eljárást és bírósági eljárást végző vagyonfelügyelő, felszámoló és bírósági végrehajtó,
- a folyamatban lévő büntetőeljárás keretében eljáró, valamint a feljelentés kiegészítését végző nyomozó hatóság, ügyészség,
- a büntető-, a hagyatéki, valamint csőd- és felszámolási ügyekben eljáró bíróság,
- a titkosszolgálati eszközök alkalmazására felhatalmazott szervek, a nemzetbiztonsági szolgálatok,
- az adó- és vámhatóság, valamint a társadalombiztosítási szervek,

Nemzetközi szerződések

A banktitok *megtartásának kötelezettsége nem áll fenn* abban az esetben sem, ha az adóhatóság nemzetközi szerződés alapján, külföldi hatóság írásbeli megkeresésének teljesítése érdekében írásban kér adatot a pénzügyi intézménytől.

Nyomozó hatóság

A pénzügyi intézmény a nyomozó hatóság, a nemzetbiztonsági szolgálat és az ügyészség írásbeli megkeresésére *haladéktalanul kiszolgáltatja* a kért adatot a nála vezetett bankszámláról és az általa lebonyolított ügyletről, ha gyanú merül fel arra, hogy a bankszámla vagy az ügylet

a) kábítószer-kereskedelemmel,
b) terrorizmussal,
c) illegális fegyverkereskedelemmel,
d) pénzmosással,
e) szervezett bűnözéssel van összefüggésben.

Központi hitelinformációs rendszer

A rendszer a hitelintézetek és a befektetési társaságok közötti adatcserét teszi lehetővé egymás adósairól.

A központi hitelinformációs rendszer a természetes személy hiteladósokra vonatkozóan a hitel- vagy hiteljellegű szerződés megkötéséhez vagy módosításához szükséges azonosító adatot,

valamint az érintett szerződésre vonatkozó lényeges adatot kezelhet és tarthat nyilván, ha az adós a szerződésben vállalt kötelezettségeinek *90 napot meghaladóan, összegben pedig a minimálbért meghaladóan nem tesz eleget.*

Az adatszolgáltatás lehetőségéről, céljáról, a közlendő adatok körének megjelölésével – a hitelszerződés megkötésével egyidejűleg – köteles az érintettet írásban tájékoztatni. Amennyiben egy másik pénzintézet adatot kér, az adósra vonatkozó adatokon kívül egyéb adat nem szolgáltatható ki.

A központi hitelinformációs rendszer a természetes személyekre vonatkozó azonosító adatokat az adós tartozásának megszűnését követő legfeljebb 5 évig tarthatja nyilván és kezelheti azzal, hogy az adós a vele szerződő hiteladat-szolgáltató közvetítésével tekinthet bele a róla nyilvántartott adatokba.

4.4 Büntető Törvénykönyv

Nézzük meg, milyen büntetőjogi következményei vannak a jogosulatlan adatkezelésnek, a számítógépes rendszer és adatok ellen elkövetett bűncselekménynek, ill. a szerzői jog megsértésének. *Btk.*

Jogosulatlan adatkezelés

177/A.§ Az az adatkezelő, aki

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel,
b) személyes adatot jogellenesen továbbít, vagy nyilvánosságra hoz,
c) személyes adatok kezelésére vonatkozó bejelentési kötelezettségét nem teljesíti,
d) személyes adatot az arra jogosult elől eltitkol,
e) kezelt személyes adatot meghamisít,
f) közérdekű adatot eltitkol vagy meghamisít,

vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

177/B. § (1) Aki a személyes adatok védelmére vonatkozó jogszabályban meghatározott adatkezelése során tudomására jutott különleges adatot

a) jogellenesen nyilvánosságra hozza;

b) jogosulatlanul felhasználja, vagy illetéktelen személy részére hozzáférhetővé teszi

bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.

(2) Aki különleges adatot maga vagy más részére jogosulatlanul megszerez, vétséget követ el, és két évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő.

Számítástechnikai rendszer és adatok elleni bűncselekmény

300/C. § (1) Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Aki

a) számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz,

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(3) Aki jogtalan haszonszerzés végett

a) a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl vagy hozzáférhetetlenné tesz, vagy

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza,

és ezzel kárt okoz, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.

(4) A (3) bekezdésben meghatározott bűncselekmény büntetése

a) egy évtől öt évig terjedő szabadságvesztés, ha a bűncselekmény jelentős kárt okoz,

b) két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény különösen nagy kárt okoz,
c) öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekmény különösen jelentős kárt okoz."

Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása

300/E. § (1) Aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot
a) készít,
b) megszerez,
c) forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz,
vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő, számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit másnak a rendelkezésére bocsátja.

(3) Nem büntethető az (1) bekezdés a) pontja esetén, aki - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adat készítése a hatóság tudomására jutott volna - tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását."

Szerzői és a szomszédos jogok megsértése

329/A.§ (1)Aki irodalmi, tudományos vagy művészeti alkotás szerzőjének művén, előadóművésznek előadói teljesítményén, hangfelvétel előállítójának hangfelvételén, rádiónak vagy televíziónak a műsorán fennálló jog megsértésével vagyoni hátrányt okoz,

vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.
(2)A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a szerzői és szomszédos jogok megsértését
a) jelentős vagyoni hátrányt okozva;
b) üzletszerűen követik el.
(3)A büntetés öt évig terjedő szabadságvesztés, ha a szerzői és szomszédos jogok megsértését különösen nagy vagyoni hátrányt okozva követik el.

Ellenőrző kérdések

1. Milyen módon lehet üzleti és kutatási célra átvenni személyes adatokat?
2. Milyen kötelezettségei vannak a személyes adatokat felhasználónak?
3. Milyen szabályok vonatkoznak az elektronikus úton küldött reklámokra?
4. Mi a különbség az állam- és szolgálati titok között.
5. Hogyan zajlik az adatok minősítése?
6. Mi az üzleti titok?
7. Mi a banktitok?
8. Kik és milyen esetben kaphatnak felmentést a banktitok hatálya alól?
9. Milyen büntetőjogi következményei vannak a jogosulatlan adatkezelésnek?
10. Milyen büntetőjogi következményei vannak a számítástechnikai rendszer ill. az adatok elleni támadásoknak?
11. Milyen büntetőjogi következményei vannak a szerzői jogok megsértésének?

Jegyzetek:

5. Az adatbiztonság

Az előző fejezetekben az adatvédelemmel foglalkoztunk. Megnéztük, hogy milyen ajánlások és törvények vonatkoznak az adatkezelésre hazánkban és nemzetközi szinten. Ezek előírják, hogy az adatkezelő feladata megteremteni az adatok biztonságos kezelésének feltételeit. A következő fejezetekben azzal foglalkozunk, hogyan kell megteremteni ezt a biztonságos környezetet. Megismerkedünk az adatbiztonság alapfogalmaival, a különböző hazai és nemzetközi biztonsági szabványokkal és ajánlásokkal, a biztonsági osztályokkal.

Az adatbiztonság - az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.[1]

Adat-biztonság

Az intézkedések és eljárások célja annak biztosítása:

- hogy az adatok a megfelelő helyen és időben *rendelkezésre álljanak* az arra jogosultak számára,
- csak a tulajdonos engedélyével lehessen megváltoztatni, vagyis *sértetlenek* legyenek,
- amennyiben szükséges, *bizalmasan* kezeljék őket,
- el legyenek látva egyértelmű azonosítókkal, vagyis *hitelesek* legyenek, valamint
- feldolgozásuk zavartalan legyen, vagyis a teljes informatikai, illetve információs rendszer *működőképes* állapotának megőrzése.

[1] A terminológia a szakmában nem egységes. Különböző megközelítési módok léteznek egymás mellett és mindenki a sajátjára esküszik. Ez egyrészt abból adódik, hogy még a nemzetközi terminológia sem teljesen egyértelmű, ráadásul a már eleve létező különbségeket a fordítások tovább torzítják. A másik ok az, hogy biztonsággal foglakozó szakemberek különböző szakmai „előélettel", abból adódóan különböző nézőponttal rendelkeznek, és ezt érvényesítik az általuk megfogalmazott anyagokban. A tankönyvben az Informatikai Tárcaközi Bizottság ajánlásait vettük alapul, és az ott használt terminológia szerint értelmezzük az adatbiztonság, ill. adatvédelem fogalmát. [29]

vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.
(2)A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a szerzői és szomszédos jogok megsértését
a) jelentős vagyoni hátrányt okozva;
b) üzletszerűen követik el.
(3)A büntetés öt évig terjedő szabadságvesztés, ha a szerzői és szomszédos jogok megsértését különösen nagy vagyoni hátrányt okozva követik el.

Ellenőrző kérdések

1. Milyen módon lehet üzleti és kutatási célra átvenni személyes adatokat?
2. Milyen kötelezettségei vannak a személyes adatokat felhasználónak?
3. Milyen szabályok vonatkoznak az elektronikus úton küldött reklámokra?
4. Mi a különbség az állam- és szolgálati titok között.
5. Hogyan zajlik az adatok minősítése?
6. Mi az üzleti titok?
7. Mi a banktitok?
8. Kik és milyen esetben kaphatnak felmentést a banktitok hatálya alól?
9. Milyen büntetőjogi következményei vannak a jogosulatlan adatkezelésnek?
10. Milyen büntetőjogi következményei vannak a számítástechnikai rendszer ill. az adatok elleni támadásoknak?
11. Milyen büntetőjogi következményei vannak a szerzői jogok megsértésének?

Jegyzetek:

5. Az adatbiztonság

Az előző fejezetekben az adatvédelemmel foglalkoztunk. Megnéztük, hogy milyen ajánlások és törvények vonatkoznak az adatkezelésre hazánkban és nemzetközi szinten. Ezek előírják, hogy az adatkezelő feladata megteremteni az adatok biztonságos kezelésének feltételeit. A következő fejezetekben azzal foglalkozunk, hogyan kell megteremteni ezt a biztonságos környezetet. Megismerkedünk az adatbiztonság alapfogalmaival, a különböző hazai és nemzetközi biztonsági szabványokkal és ajánlásokkal, a biztonsági osztályokkal.

Az adatbiztonság - az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.[1]

Az intézkedések és eljárások célja annak biztosítása:

- hogy az adatok a megfelelő helyen és időben *rendelkezésre álljanak* az arra jogosultak számára,
- csak a tulajdonos engedélyével lehessen megváltoztatni, vagyis *sértetlenek* legyenek,
- amennyiben szükséges, *bizalmasan* kezeljék őket,
- el legyenek látva egyértelmű azonosítókkal, vagyis *hitelesek* legyenek, valamint
- feldolgozásuk zavartalan legyen, vagyis a teljes informatikai, illetve információs rendszer *működőképes* állapotának megőrzése.

[1] A terminológia a szakmában nem egységes. Különböző megközelítési módok léteznek egymás mellett és mindenki a sajátjára esküszik. Ez egyrészt abból adódik, hogy még a nemzetközi terminológia sem teljesen egyértelmű, ráadásul a már eleve létező különbségeket a fordítások tovább torzítják. A másik ok az, hogy biztonsággal foglakozó szakemberek különböző szakmai „előélettel", abból adódóan különböző nézőponttal rendelkeznek, és ezt érvényesítik az általuk megfogalmazott anyagokban. A tankönyvben az Informatikai Tárcaközi Bizottság ajánlásait vettük alapul, és az ott használt terminológia szerint értelmezzük az adatbiztonság, ill. adatvédelem fogalmát. [29]

5.1 Nemzetközi és hazai ajánlások

Amíg izolált számítógépeken folytak a feldolgozások, addig mindenki csak a saját rendszere biztonságáért felelt. Amikor azonban ezeket a gépeket összekapcsolták, a fenyegetettség is megnőtt, mivel újabb „ajtók" nyíltak meg, amelyeken be lehetett jutni. Egy rosszul védett rendszer már nem csak saját magát, hanem a vele összekapcsolt gépeket is veszélybe sodorhatja. Szükségessé vált tehát egységes elvek és eljárások kidolgozása, amelyek garantálják az összekapcsolt rendszerek biztonsági „egyenszilárdságát".

Ezek az elvek szabványok és ajánlások formájában jelentek meg. Nagy előnyük, hogy egységes nyelvet teremtettek az informatikai biztonsági kérdésekben, jelentősen megkönnyítve ezzel a felhasználók és a gyártók közötti kommunikációt. A rendszerekkel szembeni biztonsági követelményeket osztályokba sorolták, így a rendszer biztonsági szintjének meghatározására elegendő az osztályt megnevezni, és nem szükséges részletes és bonyolult specifikációt adni.

TCSEC

Mint általában, ebben is a hadsereg járt az élen: 1985-ben az Egyesült Államok Védelmi Minisztériuma (Department of Defense – DoD) kidolgozta a **TCSEC** -Trusted Computer System Evaluation Criteria (Biztonságos Számítógépes Rendszerek Értékelési Kritériumai) dokumentumot vagy más néven a "Narancs Könyvet" (Orange Book of DoD).

ITSEC

Ezt követően több országban, (pl. Anglia, Németország, Franciaország) dolgoztak ki hasonló dokumentumokat. A '80-as évek vége felé a személyi számítógépek, a helyi és a nagy területeket átfogó hálózatok elterjedésével, erősödött az igény egy nemzetközi téren egyeztetett dokumentum létrehozására. Európában az első ilyen erőfeszítés eredménye volt az **ITSEC** - Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) dokumentum 1. változata, amelyet Anglia, Franciaország, Hollandia és Németország közösen dolgozott ki. Az ITSEC 1.2 változatát az Európai Közösség részére kísérleti célból 1991-ben adták ki.

Ezt a dokumentumot másképpen Fehér könyvnek „White Book" is nevezik.

CTCPEC
FC

Kanadában 1993-ban dolgozták ki a **CTCPEC** - Canadian Trusted Computer Product Evaluation Criteria (A Biztonságos Számítástechnikai Termékek Értékelési Kritériumai Kanadában) dokumentumot. Az Egyesült Államokban szintén az évben elkészült az **FC** - Federal Criteria for Information Technology Security (Az Információtechnológia Biztonságára vonatkozó Szövetségi Kritériumok).

ISO

1993-ban az Európai Közösség illetékes bizottságában az a határozat született, hogy az ITSEC, a CTCPEC és az FC szerzői dolgozzanak ki egy olyan követelményrendszert, amely nemzetközileg elfogadható lesz és az ISO - International Organization for Standardization (Nemzetközi Szabványügyi Szervezet) számára ajánlani lehet a szabványosítási munka alapjául.

CC

Ennek a munkának az eredménye lett a **CC** - Common Criteria (Közös Követelmények) dokumentumtervezet, amely megpróbálja a korábbi ajánlások tartalmi és technikai eltéréseit összhangba hozni.

X 800

Ezzel párhuzamosan az ISO már több informatikai szabványt kidolgozott. Ezek közül az 1992-ben kiadott **ISO OSI 7498**-2 (OSI - Open System Interkonnection – Nyílt Hálózatok Összekapcsolása) jelű szabvány, más jelölés szerint az **X.800**-as, ami az adatbiztonsággal foglalkozik. Ez a szabvány a nyílt hálózatok felépítésénél szükséges biztonsági feltételeket és az ezt megvalósító módszereket írja le.

Míg az TCSEC, az ITSEC és a CC főleg az informatikai rendszer operációs rendszerére írja le biztonsági funkcióit, addig az X.800 a hálózatba (nyílt rendszerbe) kapcsolhatóság biztonsági jellemzőit határozza meg. Így ezek a módszertani anyagok jól kiegészítik egymást és megteremtik az alapját a nyílt rendszerekben a biztonsági követelmények érvényre juttatásának.

ITB

Magyarországon a Miniszterelnöki Hivatal Információs Koordinációs Irodája tette közzé az *Információs Tárcaközi Bizottság* (ITB) ajánlásait. Az ITB ajánlások módszertani segítséget nyújtanak – elsősorban az állam- és közigazgatás területén – működő informatikai rendszerek kidolgozóinak és üzemeltetőinek. Ezek a módszertani anyagok azonban csak akkor alkalmazhatók, ha minden esetben adaptálják őket a helyi sajátosságokra. Az ITB ajánlások adaptálják az előzőekben említett nemzetközi ajánlásokat a magyar viszonyokra, és jól használhatók az üzleti területen működő szervezeteknél is.

Az ajánlások közül több foglakozik az adatbiztonság témakörével:

8. számú	Informatikai biztonsági módszertani kézikönyv
12. számú	Az informatikai rendszerek biztonsági követelményei
16. számú	Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana [29]

5.2 Az adatbiztonság alapfogalmai

Az előbb említett dokumentumokban a fogalmak használata nem mindig azonos. Az alábbi meghatározásoknál általában az ITB meghatározásaihoz tartottuk magunkat. Ahol ettől eltérünk, azt külön jelezzük.

Alapkövetelmények

A biztonsági *alapkövetelmények* a következők:

- rendelkezésre állás
- sértetlenség
- bizalmasság
- hitelesség
- működőképesség

Az ITSEC csak az első három alapkövetelményt definiálja, a hitelességet és a működőképességet beleérti a többibe.

Rendelkezésre állás

Üzemképes

Egy informatikai rendszer különböző szolgáltatásai és az abban feldolgozásra kerülő adatok állandóan, illetve egy meghatározott időben rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

Sértetlenség

Nem módosulhat

A sértetlenséget általában az információkra, adatokra, illetve a programokra értelmezik. Az információk sértetlensége alatt azt a fogalmat értjük, hogy azt csak az arra jogosultak változtathatják meg és azok véletlenül sem módosulnak. Ez a programokat is érinti, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani.

Bizalmasság

Hozzáférés

Az információk vagy adatok esetében a bizalmasság azt jelenti, hogy azokhoz csak az arra jogosítottak csak az előírt módokon férhetnek hozzá és nem fordulhat elő úgynevezett jogosulatlan információszerzés.

Hitelesség

Azonosított

Olyan eljárás, amely segítségével egy informatikai rendszeren belüli kapcsolatban a partnerek kölcsönösen és kétségtelenül felismerhetik egymást, és ez az állapot a kapcsolat egész idejére változatlanul fennmarad.

Működőképesség

Üzembiztos

A rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való tartása. A működőképesség fogalom sok esetben azonos az üzembiztonság fogalommal. Ezen állapot fenntartásának alapfeladatait a rendszergazda (rendszeradminisztrátor) látja el.

Fenyegető tényezők

Támadások, véletlenek

A fenyegető tényezők a biztonsági alapkövetelmények teljesítését zavaró körülmények vagy események. Ide soroljuk a *személyektől* eredő informatikai rendszer elleni *támadásokat,* és valamennyi szélesebb értelemben vett fenyegetést, mint például a *véletlen események* (a tűz, az áramkimaradás, stb.), a külső tényezők általi *behatások* (pl. elektromágneses sugárzás) és olyan körülmények, amelyek általában magának az informatikának a *sajátosságaiból adódnak* (pl. adatbeviteli hiba, hibás kezelés, hardver tönkremenetele, számítógépes vírusok és programhibák).

Az alapfenyegetettség

A fenyegető tényezők csoportja

Az alapfenyegetettség a fenyegető tényezők olyan csoportosítása, amely a biztonsági alapkövetelmények valamelyikének teljesíthetetlenségét okozza. A fenyegetés az alapkövetelmények valamelyike ellen irányul, de egyszerre többet is sérthet. Olyan intézkedésekre van szükség, amelyek a fenti követelményeket a *lehető legkisebb kockázattal* és *egyenlő szinten* biztosítják.

Védelmi mechanizmusok

Eljárások, módszerek

Ezek olyan eljárási módszerek vagy megoldási elvek, amik azt a célt szolgálják, hogy egy vagy több biztonsági követelményt teljesítsenek. A védelmi intézkedések sorát biztonsági szabványok határozzák meg. Ezeket az eljárásokat a gyártó cégek beépítik a hardver és szoftver termékeikbe és így szolgáltatják a felhasználók részére.

5.3 A TCSEC és az ITSEC

Az informatikai rendszerek biztonsági minősítésének alapjait a TCSEC-ben rakták le, amely az összes többi ajánlás alapját képezi. A dokumentumok segítséget nyújtanak a rendszerek illetve azok komponensei besorolásához és értékeléséhez, valamint biztonsági osztályokat, azok védelmi követelményeit, az azokat teljesítő védelmi mechanizmusokat és a teljesítés mértékétől függő, minősítési fokozatokat határoznak meg.

5.3.1 A megbízható informatikai rendszerek alapfunkciói

Az ITSEC nyolc biztonsági alapfunkciót ír le, amelyek a három alapkövetelmény, a bizalmasság, a sértetlenség és a rendelkezésre állás megvalósítását biztosítják.

Alapfunkciók

Ezek a következők:

- azonosítás
- hitelesítés
- jogosultság kiosztás
- jogosultság ellenőrzés
- bizonyíték biztosítás
- újraindítási képesség
- hibaáthidalás, a rendeltetésszerű működés biztosítása
- átviteli biztonság

Azonosítás és hitelesítés

Megkülönböztethetőek

Azt biztosítják, hogy az informatikai rendszer felhasználói, folyamatai, erőforrásai és adatcsoportjai egyértelműen megkülönböztethetőek legyenek, és az azonosítást valamely eszközzel ellenőrizni lehessen.

Jogosultság kiosztás és ellenőrzése

Hozzáférés

A felhasználók sokféle tevékenységet végezhetnek, és különböző erőforrásokhoz férhetnek hozzá az informatikai rendszerben. Az eljárás célja annak biztosítása, hogy a felhasználók ne férhessenek hozzá olyan információkhoz vagy eszközökhöz, amelyekhez hozzáférési jogosultsággal nem rendelkeznek. Ugyanígy meggátolandó az információ engedélyezetlen létrehozása vagy módosítása (beleértve azok törlését is). Ide tartoznak azok az eljárások is, amelyek az információáramlást, illetve az eszközfelhasználást szabályozzák felhasználók, folyamatok és tárgyak között. Ezen belül a hozzáférési jogosultság adminisztrálása (például: a jogosultság adása és visszavonása), valamint az ezekhez fűződő hitelesítés.

Bizonyíték biztosítás

Kimutathatóság

Ez az alapfunkció arra szolgál, hogy a ráruházott jogokkal való visszaélést ki lehessen mutatni, vagy a nem megengedett jogok alkalmazásának kísérletét fel lehessen tárni.

Újraindítási képesség

Folytatás

Megakadályozza a meg nem engedett információáramlást az újrafelhasználható üzemi eszközöknél, mint a főtároló vagy a perifériás tárolók, és lehetőséget biztosít egy rendszerleállás után a feldolgozások zavartalan folytatására.

A hibaáthidalás és a rendeltetésszerű működés biztosítása

Tartalék

Biztosítania kell olyan megoldásokat, amelyek valamilyen hiba fellépésekor automatikusan átadják a vezérlést a tartalék eszközöknek, garantálva a folyamatos működést. Olyan rendszerek esetében van nagy jelentősége, amelyeknél a hibás funkció vagy a kimaradás emberéleteket fenyegethet, vagy magas dologi károk keletkezhetnek, mint például erőművek, vagy a légiforgalom irányításában résztvevő informatika rendszerek esetében.

Átviteli biztonság

Olyan módszerek alkalmazása szükséges, amelyek biztosítják az adatátvitel sértetlenségét. Ebben az esetben különösen fontos követelményeket támaszthatunk a kommunikációs partnerekkel, az átvitel útjával és az átvitel menetével kapcsolatban.

5.3.2 Biztonsági osztályok, biztonsági szintek

Felesleges túlbiztosítani

A különböző informatikai rendszereknek más-más szinten kell megfelelni a biztonsági követelményeknek. Könnyen belátható, hogy nem ugyanaz a követelmény pl. egy videotéka kazetta nyilvántartásával szemben, mint a titkos rakétabázisok adatnyilvántartásánál. Felesleges lenne mindkét rendszert azonos szinten biztosítani. Az adatbiztonság egyik legfontosabb alapelve, hogy mindig csak a szükséges biztonsági szintet valósítsuk meg, a túlbiztosítás felesleges és igen sokba kerül.

Biztonsági osztályok

A TCSEC biztonsági osztályokat állít fel, amelyeknél egyre magasabbak a biztonsági követelmények. Az osztályokat azért hozták létre, hogy figyelembe lehessen venni az informatikai rendszerek különböző típusait, mint a termelésirányító rendszerek, az adatbank-rendszerek vagy hálózatok, valamint hogy a különböző szabványok összehasonlíthatóak legyenek.

A TCSEC alapvetően négy csoportra osztja a biztonsági osztályokat:

D – minimális védelem
C – szelektív és ellenőrzött védelem
B – kötelező és ellenőrzött védelem
A – bizonyított védelem

A B és C csoportok több osztályt is tartalmaznak, így az TCSEC összesen 7 osztályt különböztet meg:

D – minimális védelem

Bármit tehet

Egy ilyen rendszerben bárki elérhet, módosíthat és törölhet bármilyen adatot és módosíthatja a rendszer erőforrásait. Ide sorolható pl. az *MS-DOS*.

C1 – megkülönböztetéses védelem

Azonosított

Minden felhasználó névvel és jelszóval azonosítja magát, amivel kétséget kizárólag meg lehet őket különböztetni. A felhasználó csak a jogosultsági köréhez tartozó műveleteket végezhet. Ilyen pl. a *UNIX*.

C2 – ellenőrzött hozzáférésű védelem

Hozzáférés

A felhasználó azonosításhoz egy fokozott ellenőrzés társul. Lényeges eleme a részletekbe menő rendszer-adminisztráció és a pontos személyazonosítás. A hozzáférési jogok odaítélése az egyes felhasználók vagy felhasználói csoportok számára lehetséges. Ide tartozik az *MS Windows NT 4.x* és a *Novell NetWare 4.x* rendszerek.

B1 – címkézett biztonságú védelem

Címkék

Itt már az is követelmény, hogy a rendszer objektumai olyan címkét kaphassanak, amelyek szabályozhatják a hozzáférési mechanizmusokat. Ilyen pl. a *System V/MLS* és a *Unisys OS 1100.*

B2 – strukturált védelem

Referencia monitor

Itt a strukturált hozzáférés-védelem eszközeit alkalmazzák, vagyis az objektumok azonosítása és hozzáférés ellenőrzése szigorúan elkülönített referenciamonitor használatával történik. Ide sorolható a *Honeywell Multics* rendszer.

B3 – biztosított védelmi területek

Elkülönítve

Az ide tartozó rendszerek az egyes védelmi területeket elkülönítve kezelik, vagyis fizikailag és logikailag is elválasztják egymástól. A biztonsági felügyelő, a rendszeradminisztrátor és a felhasználók biztonsági funkciói és jogosultságai is elkülönítettek. Ide sorolható a *Honeywell XTS-200* rendszere.

A1 – ellenőrzött tervezés

Matematikai bizonyítás

Ez az osztály az előzőn túl megköveteli a biztonsági rendszer eredményes működésének matematikai úton való bizonyítását. A rendszer biztonsági vizsgálatát a tervezésnél kezdi, és az ellenőrzés végigköveti a bevezetés és az üzemeltetés összes lépését. Ebbe az osztályba tartozik a *Honeywell SCOMP* és a *Boeing Aerospace SNS* rendszer.

Az ITSEC tíz osztályt ajánl. Az első öt megegyezik a TCSEC C1-A1 osztályaival, csak az ITSEC-ben a B3 és az A1 osztályt összevonták. Az ITSEC szerinti jelölés még egy F betűt hozzátesz a TCSEC jelöléséhez, így az ITSEC esetében F-C1...F-B3 osztályokról beszélhetünk.

Az ITSEC meghatároz még további öt biztonsági osztályt, amelyeknek követelményeit az amerikai kritériumokban nem vették figyelembe, hanem pótlólagosan fogalmazódtak meg. Ezen osztályoknál az informatikai biztonság más vonatkozásai állnak az előtérben.

F-IN osztály

Adatbázisok

Az azonosítás és a hitelesítés, a jogkezelés, a jogellenőrzés és a bizonyítás-biztonság követelményeit állítja fel, amely különösen az adatbankoknál vagy a szoftver-fejlesztési környezetekben szükséges. Az ajánlást olyan informatikai rendszerekhez dolgozták ki, amelyek adatainál és programjainál magas sértetlenségi követelmények érvényesülnek. Ilyen követelményeknek való megfelelés szükséges például az adatbázis jellegű informatikai rendszereknél.

F-AV osztály

Gyártási folyamatok

A hibaáthidalás és a funkcionalitás biztosítása alapfunkciókkal szemben támaszt követelményeket, amelyek valamely rendszer hozzáférhetőségét célozzák meg. Az ajánlás magas követelményeket támaszt egy teljes informatikai rendszer vagy különleges rendeltetésű informatikai rendszer biztonsága iránt. Az ilyen követelmények fontosak olyan informatikai rendszerek esetében, amelyek például gyártási folyamatokat szabályoznak.

F-DI osztály

Integritás

Az adatok integritását célozza az átvitel során, amely az azonosítás, a hitelesítés, az átvitelbiztosítás és a bizonyítás-biztonság alapfunkciók által elérendő. Az ajánlás magas követelményeket támaszt az adattovábbításkor érvényesülő adatsértetlenség védelme tekintetében.

F-DC osztály

Rejtjelzés

Az adatok átvitel során történő titokban tartását tartalmazza, amelynek az átvitelbiztonság alapfunkciójával szemben támasztott követelményekből kell következnie. Az ajánlást olyan informatikai rendszerekhez alakították ki, amelyek az adattovábbítás során magasfokú adatvédelmet, rejtjelzést igényelnek. (Például rejtjelező berendezések.)

F-DX osztály

Védett információ nyílt hálózaton

Az adatok hálózati rendszerekben való titokban tartásával és sértetlenségével foglalkozik, melynek érdekében az azonosítás és hitelesítés az átvitelbiztonság és a bizonyítás-biztonság alapfunkciókkal szemben támaszt követelményeket. Az ajánlás olyan hálózatoknál használatos, amelyeknél magas az igény a továbbított információ bizalmasságának (titkosságának) és sértetlenségének biztosítására. Példa lehet erre az az eset, amikor érzékeny információ kerül továbbításra nem védett (például nyilvános) hálózatokon.

5.3.3 Védelmi mechanizmusok, védelmi eljárások

A védelmi alapfunkciókat különböző védelmi eljárásokkal lehet biztosítani. Ezek olyan módszerek, eszközök vagy algoritmusok, amelyek beiktatásával a biztonsági funkciókkal szemben támasztott igények teljesíthetők.

Felhasználó-azonosítási és hitelesítési eljárás

Azonosság

Az eljárás keretében nemcsak a felhasználó igazolt személyazonosságát kell megállapítani, de hitelesíteni kell, hogy azzal azonos-e, akinek állítja magát. Erre szolgál a *felhasználónév* és a *jelszó*, amihez különböző szoftverekben még többféle kiegészítő információ társulhat.

Magában foglal olyan eljárást is, amely generálás, megváltoztatás vagy engedélyezés révén lehetővé teszi, hogy a jogosultsággal rendelkező felhasználó (rendszergazda, rendszeradminisztrátor) megvizsgálja azt a hitelesítési információt, mely az adott felhasználó személyazonosságának igazolásához szükséges.

Tartalmaz továbbá olyan eljárásokat, amelyek megakadályozzák, hogy illetéktelen felhasználó hitelesítési információhoz juthasson, valamint olyan eljárást is, amely korlátot szab a hamis azonossággal való kísérletek megismétlésének. Biztosítani kell új felhasználók beléptetését, illetve a régiek törlését.

Hozzáférés-jogosultság ellenőrzési eljárás

Az eljárás célja az, hogy a felhasználó ne férhessen hozzá olyan információkhoz vagy eszközökhöz, amelyekre nem jogosult. Új információt ne hozhasson létre, ne módosíthasson, ne törölhessen, ne változtathassa meg a kiadott jogosultságokat.

Felelősségre vonhatósági eljárás

Az informatikai rendszerek legtöbbje esetében fontos, hogy a felhasználók által végrehajtott műveletekre vonatkozó fontosabb információk rögzítésre kerüljenek abból a célból, hogy a felhasználók a műveletért felelőssé tehetők legyenek.

Könyvvizsgálati eljárás

Naplózás

Mind a rutinszerű feladatokról, mind a rendkívüli eseményekről megfelelő információ kerüljön rögzítésre, miáltal későbbi vizsgálatok során megállapítható, hogy a védettséget, biztonságot érte-e valós sérelem és ha igen, ez mely információkat, vagy eszközöket érintett.

Eszköz-újrafelhasználási eljárás

Általában szükséges annak biztosítása, hogy bizonyos eszközök (mint például a fő memória, vagy a lemeztároló területei) újra felhasználhatók legyenek a védelem károsodása nélkül. Ide sorolandó valamennyi olyan funkció, amely az adatokat tartalmazó eszközök újrafelhasználásának vezérlését, szabályozását szolgálja valamint azon funkciók, amelyek rendeltetése ki nem jelölt, vagy újra kijelölt adathordozók címzése, vagy megtisztítása.

Pontossági eljárás

Megfelelő forma

Az informatikai rendszerek legtöbbje esetében követelményként jelentkezik annak biztosítása, hogy a feldolgozás során az adatok megfelelő formában rögzüljenek, illetve, hogy a folyamatok közötti mozgás során az adatok ne változzanak meg. Tartalmaz továbbá olyan funkciókat, amelyek biztosítják, hogy amikor folyamatok, felhasználók és tárgyak között adatátvitelre kerül sor, a veszteség, hozzátétel, vagy módosítás felfedhető vagy megakadályozható legyen, illetve

lehetetlenné teszik, hogy az igénybe venni kívánt vagy éppen használt forrást, vagy az adatátvitel célállomását megváltoztassák.

A szolgáltatások megbízhatósága eljárás

Időérzékenység

Az időérzékeny feladatokat akkor hajtsák végre, amikor azokra szükség van, nem pedig korábban, vagy később és, hogy a nem időérzékeny feladatok ne válhassanak időérzékenyekké. Ehhez hasonlóan, hogy az eszközökhöz való hozzáférés is akkor történjék, amikor arra szükség van és azokat ne igényeljék vagy tartsák fel szükségtelenül.

Adatok cseréje eljárás

Az eljárás lényege az adatok kommunikációs csatornákon történő átvitelének védelme.

5.3.4 Minősítés

Az ITSEC mértéket ad az informatikai rendszerek és egyes részegységeik minőségének értékeléséhez, a minősítéséhez. A minősítés a következő tényezőktől függ:

- milyen biztonsági követelményeket állítottak fel,
- a biztonsági szempontból lényegtelen funkciók elhatárolása,
- a védelmi mechanizmusok milyen mértékben, milyen erősséggel valósulnak meg,
- az alkalmazott eljárások az előállítás során,
- az alkalmazott eljárások a működéskor,
- mennyire jól használhatók a biztonsági funkciókat leíró dokumentumok.

5.3.5 A biztonsági minősítési fokozatok

Az ITSEC nyolc biztonságminősítési fokozatot definiál Q0-tól Q7-ig, amelyekben egyre erősebb követelményeket támaszt az egyes minősítési aspektusok iránt. Egy magasabb minősítési fokozat az üzemeltető számára magasabb mértékű biztonságot jelent arra nézve, hogy az informatika rendszer megfelel a követelményeknek.

A definiált minősítési fokozatokat nagy vonalakban három kategóriába lehet sorolni:

I. olyan rendszerek, amelyek *nem vagy csak kevés védelmet* nyújtanak a külső támadások ellen, de a hibáktól védenek,
II. olyan rendszerek, amelyek a *jónak minősíthetőtől a kiválóig terjedő* védelmet nyújtanak a támadások ellen,
III. olyan védelemmel rendelkező rendszer, amely *nem leküzdhetőnek* minősíthető.

Q0 minősítési fokozat

Olyan rendszerek számára előirányzott, amelyek egy magasabb fokozat követelményeit nem elégítik ki.

Q1 minősítési fokozat

Szándéktalan fellépések

A minősítési követelmények elleni szándéktalan fellépések, tettek kivédésére alkalmas (pl. az adatok véletlen átírásának megakadályozására). Nem alkalmas a biztonsági szempontból kritikus területekre, amelyeken a biztonsági követelményekkel szembeni szándékos fellépéssel lehet számolni.

Q2 minősítési fokozat

Már egy csekély védelem van a szándékos károkozások ellen, ami azonban jó rendszerismeretekkel leküzdhető. Nagy minőségi értéke van annak, hogy a biztonsági követelményeket véletlen hibával nem lehet megsérteni vagy hatályon kívül helyezni.

Q3-Q5 minősítési fokozatok

Szándékos támadások

Jó védelem áll fenn a biztonsági követelmények szándékos megsértésével szemben. A minősítés során itt már költséges elemzéseket folytatnak, hogy a biztonsági követelmények teljesítését bizonyítsák. A Q3-rendszerek az egyszerű áthatolásokkal szemben nagymértékben védettek, a Q4 esetében pedig még nehezebb a védelmet áttörni. A Q5 fokozattól kezdődően már a tervezési folyamatban egy félformális eljárási módot kell leírni. Egy ilyen rendszernél már számolhatunk azzal, hogy nagymértékben ellenáll a támadásoknak.

Q6 és Q7 - minősítési fokozatok

Kiemelt

Ezek a rendszerek fokozottan ellenállnak a behatolási kísérleteknek. Ez azonban igen magas ráfordítást igényel mind a gyártásban, mind a minősítésben. A Q7 fokozatnál pótlólag még egy formális bizonyítást is be kell vezetni. Egy ilyen rendszer előállításának és minősítésének ráfordításai oly nagyok, hogy - a technika mai állása mellett - ez a minősítési fokozat csupán korlátozott funkcionalitású kis rendszerek számára elérhető. Magasabb minősítési fokozatot alapvetően csak magasabb előállítási és minősítés ráfordítással érhetünk el.

Minősítők

A minősítés folyamatát az Informatikai biztonsági minősítési kézikönyv szabályozza. Egy minősítés eredményét minősítési tanúsítványban rögzítik. Ilyen tanúsítványt csak az arra jogosult szervezet állíthat ki. A tanúsítvány kiadására jogosult hatóság például Németországban a Szövetségi Informatika Biztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik).

Megjegyezzük, hogy az ITSEC követelményrendszer alkalmazhatóságának feltételei Magyarországon nem adottak. Nincsenek meg azok a hatóságok, intézmények, amelyek ellenőrzik a biztonsági előírások meglétét és jóváhagyják, igazolják azok teljesülését. Mégis célszerű megismerkedni ezen követelményrendszerrel, mert a rendszertervezők, beszerzők, üzemeltetők, felügyelők átfogó képet kaphatnak a biztonsági csoportosításokról, a biztonsági eljárások érvényre juttatásáról és így fokozatosan, a módszertani lépéseket felhasználva, kiépíthetővé válnak a biztonságos informatikai rendszerek. Az EU csatlakozással pedig ezek az előírások ránk is kötelezővé válnak.

5.4 Common Criteria (CC)

Ismert, hogy a1993-ban a TCSEC, ITSEC, CTCPEC és az FC szerzői létrehoztak közös projektet a Közös Követelmények – Common Criteria (CC) kidolgozására.
A munka célja az előző dokumentumokban lévő ellentmondások feloldása az új informatikai elvárásoknak jobban megfelelő rugalmasabb értékelési rendszer létrehozása.
A dokumentum magyar nyelven is hozzáférhető az ITB 16. számú ajánlásában. Ez nem csak egyszerű fordítás, hanem fogalommagyarázatokkal, kiegészítésekkel ellátott feldolgozás, amely 1.0 verzió alapján készült. Jelenleg a 2.0 változatnál tart a fejlesztés. Nézzük meg, milyen alapfogalmakkal dolgozik a CC.

Az értékelés tárgya

Termék vagy rendszer

Az információ-technológia biztonsági értékelésénél a tárgy mindig egy számítástechnikai termék vagy rendszer. Az értékelés pedig az értékelés tárgyára vonatkozó módszeres vizsgálat, amely eredményeként meghatározzák az adott rendszer biztonsági szintjét.

Védelmi profil

Követelmény csoport

A védelmi profil a CC segítségével előre megadott követelményekből felépített, egy adott védelmi feladatot lefedő követelményrendszer. Egy feladatra több védelmi profil is készíthető. A védelmi profil termék-független, és a tipikus informatikai alkalmazások tulajdonságait veszi alapul.

A védelmi profilok hasznosak a felhasználóknak és a fejlesztőknek egyaránt. A felhasználók megvizsgálhatják, hogy a profilban leírtak tényleg megfelelnek-e biztonsági elvárásaiknak. Ezt a vizsgálatot lényegesen könnyebb lefolytatni, mint az összes biztonsági követelményt kitalálni. A fejlesztőknek azért jó, mert a védelmi profiloknak megfelelő funkciókat beépíthetik a fejlesztett eszközökbe.
A védelmi profilban leírt elvekre konkrét megoldást a Biztonsági rendszerterv tartalmaz.

A CC a követelményeket funkcionális osztályokba, azon belül pedig családokba sorolja.

Funkcionális osztályok, családok, komponensek

Nézzünk egy példát:

- *FAU osztály - biztonsági naplózás:*
  - biztonsági riasztás, automatikus válasz,
  - biztonsági napló adatainak generálása,
  - biztonsági napló kezelése,
  - biztonsági napló védelmi profil szerinti ellentmondásának észlelése
  - áthatolást azonosító eszközök,
  - biztonsági napló tárolás utáni feldolgozása,
  - biztonsági napló tartalmának védelme,
  - biztonsági napló tartalmának tárolás előtti feldolgozása,
  - biztonsági napló vizsgálata,
  - biztonsági napló áttekintése
  - biztonsági naplóesemények kiválogatása,
  - biztonsági naplóesemények tárolása.

Tehát, a biztonsági naplózás osztályát felbontják 12 családra, azokat pedig komponensekre, amelyek már művelet szintűek.

A további osztályok:

- FCO osztály – kommunikáció, letagadhatatlanság,
- FDP osztály – felhasználó adatok védelme,
- FIA osztály – azonosítás és hitelesítés,
- FPR osztály – magántitok,
- FPT osztály – biztonsági funkciók megbízható védelme,
- FRU osztály – erőforrás hasznosítás,
- FTA osztály – az értékelés tárgyához való hozzáférés,
- FTP osztály – megbízható út és csatorna.

Az ITB 16-os ajánlásában megtalálhatók az osztályokhoz tartozó családok és a családokhoz tartozó komponensek felsorolása.

Garanciális követelmények

A garancia a termék olyan tulajdonsága, amely a felhasználót meggyőzi arról, hogy a termék teljesíti az ígért biztonsági szintet. A CC csak a hatékony bevizsgálással alátámasztott garanci-

át fogadja el. A bevizsgálás a következő lépéseket foglalja magába:

Bevizsgálás

- folyamatok és eljárások elemzése,
- azok tényleges alkalmazásának ellenőrzése,
- a kapcsolatok elemzése,
- a tervek és a követelmények összevetése,
- matematikai bizonyítások,
- a kezelési dokumentáció elemzése,
- működési tesztek lefolytatása, kiértékelése,
- a sebezhetőség elemzése,
- szándékos támadással az áthatolhatóság megállapítása.

A garanciális osztályok:

- APE osztály – a védelmi profil kiértékelése,
- ACM osztály – konfiguráció kezelés,
- ADV osztály – fejlesztés,
- AGD osztály – útmutató dokumentumok,
- ALC osztály – életciklus támogatás,
- ATE osztály – tesztek
- AVA osztály – a sebezhetőség felmérése,

A garanciális osztályokat is tovább lehet bontani családokra és azokat komponensekre.

A CC hét minősítési, vagy értékelési garanciaszintet (ÉGSZ) állapít meg. A garanciaszintek azt fejezik ki, hogy a vizsgálatot milyen mélységben, milyen erőforrás-ráfordítással végezték. Nagyobb a garanciaszint, ha az informatikai rendszer értékelésénél a rendszer minél nagyobb részét, minél nagyobb mélységben és minél több eszköz felhasználásával végzik.

A CC a következő garanciaszinteket definiálja:

Garanciaszintek

ÉGSZ-1 – funcionálisan tesztelt,
ÉGSZ-2 – strukturáltan tesztelt,
ÉGSZ-3 – módszeresen tesztelt és ellenőrzött,
ÉGSZ-4 – tervszerűen tervezett, tesztelt és áttekintett,
ÉGSZ-5 – félformálisan tervezett és tesztelt,
ÉGSZ-6 – félformálisan igazoltan tervezett és tesztelt,
ÉGSZ-7 – formálisan igazoltan tervezett és tesztelt,

A CC szigorú terminológiája, módszertana, merev szerkezete és követelményei azt szolgálják, hogy az értékelés független és megismételhető legyen. Az értékelés megvalósítható a fejlesztéssel párhuzamosan vagy utána. Az értékelés eredménye egy tanúsítvány, amelyben kifejtik, hogy elvégzett vizsgálatok alapján a termék melyik védelmi profilnak vagy garanciaszintnek felel meg.

5.5 Nyílt hálózatok biztonsági szabványa ISO OSI 7498-2 (X.800)

Nyílt rendszerek

Ez a szabvány a nyílt hálózatok felépítésénél szükséges *biztonsági szolgálatokat* és az azokat megvalósító *mechanizmusokat* írja le. Biztonsági szolgálat (security service) az egymással kommunikáló nyílt rendszerek egyik rétege által nyújtott szolgálat, amely megfelelő biztonságot nyújt a rendszereknek és az adattovábbításnak.

5.5.1 Biztonsági szolgálatok az X.800-ban

Hitelesítés

Ellenőrző összeg

A tárolt adatok vagy kommunikációs üzenetek tartalmára vonatkozó védelmi eljárás. Az adatokat védi a hamisítás, a manipulálás, az üzenetkivonás vagy a járulékos üzenet beiktatása ellen. A hitelesítés olyan ellenőrző összeget (4-8 Byte-os karaktersorozat) generál, amely csak az adott titkosító rendszerben készíthető és ellenőrizhető. Előállításához általában felhasználják azokat a kulcselemeket, amelyeket a rejtjelező algoritmusok is használnak.

Hozzáférés ellenőrzése

Jogosult használat

Ez a szolgálat látja el a nyílt hálózaton keresztül elérhető erőforrások jogosulatlan használata elleni védelmet. Ez a védelmi szolgálat alkalmazható az erőforráshoz való valamennyi hozzáférés ellenőrzésére (kommunikációs, információs erőforrás olvasása, írása vagy törlése).

Adattitkosság

Ez a szolgálat látja el az adatok jogosulatlan nyilvánosságra hozatal elleni védelmét.

Adatsértetlenség

Sértetlen összeköttetés

Ez a szolgálat észleli és kivédi az adatmódosítást, beiktatást, törlést vagy visszajátszást. Az összeköttetés sértetlen, ha az összeköttetésen minden felhasználónál biztosítva van az adatok módosításának, beszúrásának, törlésének vagy újrajátszásának észlelése és rögzítése az átküldött adatok teljes terjedelmére. Kiegészülhet még olyan eljárásokkal is, amelyek megkísérlik az összeköttetési szekvencia helyreállítását.

Letagadhatatlanság

Bizonyíték

Az adat vevőjét ellátja az adat származásáról szóló bizonyítvánnyal. Ez az ellen véd, hogy az adó megkísérelje az adat vagy tartalma adásának letagadását. Ugyanez történik a másik oldalon is: az adat adóját ellátja az adat kézbesítéséről szóló bizonyítvánnyal. Ez az ellen véd, hogy a vevő megkísérelje az adat vagy tartalma vételének letagadását.

5.5.2 A biztonsági mechanizmusok az X-800-ban

Rejtjelezés

Kriptográfia

A rejtjelezés, titkosítás vagy kriptográfia az adatok transzformációját jelenti, amely biztosítja, hogy az adatok vagy az adatforgalomra vonatkozó információ csak azok számára legyen érthető, akik ismerik az adatok átalakításának aktuálisan használt módszerét. A rejtjelezés része lehet számos más biztonsági mechanizmusnak is.

Digitális aláírás, időpecsét

Hitelesítő karakterek

Az aláírás általában tartalmazza az "aláírandó" adatállomány megnevezését, az állományból készített hitelesítő kivonatot, az aláírás idejét, és helyét. Ezt a karaktersorozatot rejtlezelik. A rejtjelezés abban különleges, hogy az aláírás megfejtése csak az aláírót egyértelműen azonosító kulcs felhasználásával lehetséges.

Hozzáférést ellenőrző mechanizmusok

Naplózás

Ha valaki megkísérel olyan erőforrást használni, amelyre nincs jogosítványa, vagy nem megfelelő típusú hozzáféréssel fordul a számára jogosult erőforráshoz, akkor a hozzáférést ellenőrző funkció elutasítja ezt a kísérletet. Ezen felül még jelentést is adhat az eseményről riasztás és/vagy biztonsági átvilágítási naplóba történő feljegyzés készítése céljából.

A hozzáférést ellenőrző mechanizmus a következő egy vagy több eszköz felhasználásával működhet:

- A hozzáférést ellenőrző információbázis, amelyben a hozzáférési jogokat tartják nyilván.
- Hitelesítő információ, pl. jelszó, amelynek birtoklása és ezt követő felmutatása a bizonyíték a hozzáférés jogosságára.
- Biztonsági címkék.
- A hozzáférési kísérlet időpontja.
- A megkísérelt hozzáférés útvonala.
- A hozzáférés időtartama.

Adatsértetlenségi mechanizmusok

Kísérő információk

A továbbított adattal együtt elküldésre kerül egy olyan kiegészítő információ, amelyet az adatelemből hoztak létre valamilyen algoritmus alapján. Ez az információ csak erre az adatelemre jellemző, és a fogadás helyén újra előállítható. Amennyiben a két információ nem egyezik, akkor valószínű, hogy az adatelem a továbbítás során módosítva lett.

Hitelességcsere mechanizmusok

A két partner olyan információkat cserél, amelyekkel kölcsönösen biztosíthatják egymást a küldött és a fogadott információk hitelességéről. Több módszere lehetséges.

Forgalom helykitöltési mechanizmusok

Hamis csomagok

Az „éles" adatcsomagok között hamis adatcsomagokat küldenek, amellyel megakadályozzák, hogy a forgalom elemezhető legyen. Ez a módszer csak akkor lehet hatásos, ha a

forgalom helykitöltő adatokat nem lehet a valós adatoktól kívülről megkülönböztetni.

Forgalomirányítás ellenőrzési mechanizmusok

Útválasztás

Ezeknek egyik módja az, hogy az útvonalak megválasztása úgy történik, hogy csak fizikailag biztonságos részhálózatok, közvetítők vagy összekapcsolók legyenek használatban. Mindez történhet dinamikusan vagy előzetes megszervezéssel. Ezekben a mechanizmusokban lehetőséget kell biztosítani arra, hogy tartós manipulációs támadások detektálása esetén a végrendszerek utasíthassák a hálózati szolgáltatást nyújtót egy másik útvonalon keresztüli összekapcsolás létrehozására.

Hasonlóképpen a biztonsági irányelvekben elő lehet írni, hogy bizonyos biztonsági címkéket hordozó adatok ne haladhassanak át bizonyos részhálózatokon, közvetítőkön vagy összekapcsolókon.

Egy másik lehetőség, hogy az összekapcsolás kezdeményezője (vagy az összekapcsolás nélküli adatelem küldője) megszabhassa, hogy melyik részhálózatok, közvetítők vagy összekapcsolók ne kerüljenek bele az összeköttetésbe.

Közjegyzői hitelesítési mechanizmus

A biztosítékot egy olyan külső közjegyző (személy vagy szervezet) nyújtja, akiben a kommunikáló felek megbíznak és aki birtokában van a kívánt biztosítékok tanúsítható módon történő adásához szükséges információknak.

5.6 Az Informatikai Tárcaközi Bizottság ajánlásai

ITB

Magyarországon a Miniszterelnöki Hivatal Informatikai Koordinációs Irodája tette közzé az Informatikai Tárcaközi Bizottság (ITB) ajánlásait. Ezek az ajánlások adaptálják a nemzetközi ajánlásokat a magyar viszonyokra.

A továbbiakban a 12. számú, *Az informatikai rendszerek biztonsági követelményei* ajánlással foglakozunk.

5.6.1 AZ ITB 12 számú ajánlása

A 12. ajánlást az Informatikai Tárcaközi Bizottság 1996. április 2-ai ülésén fogadták el. Tájékoztatást ad az intézmény vezetésének az informatikai biztonsággal kapcsolatos követelményekről és célja a szervezetek egységes elveken nyugvó, az európai ajánlásokhoz igazodó informatikai biztonságának megteremtéséhez a hazai előírások biztosítása.

Szerkezet

Az I. fejezet a követelményrendszer helyét írja le az informatikai biztonságpolitika, stratégia, a biztonsági vizsgálatok és a védelmi intézkedések között. Az informatikai biztonság fogalmának definiálása és egy rövid biztonsági modell leírás mutatja be azt az alapvető szemléletet, amelyet a dokumentum a későbbiekben követ a követelményrendszer kialakításánál. A modell "középpontjában" a védendő alapérték, vagyis az adatok által hordozott információ áll, amelyet az érték környezetét alkotó rendszerelemek vesznek körül. Általában a támadások a rendszerelemekre hatnak közvetlenül és azok védelmi képességétől függően veszélyetetett a védendő érték.

A megvalósított védelemnek zártnak, teljes körűnek, a kockázatokkal arányosnak és időben folyamatosan biztosítottnak kell lennie.

Ha különböző szervezetek biztonságát vizsgáljuk, az alapkérdés mindig az, hogy az adott célok eléréséhez milyen biztonsági rendszert kell megtervezni és kialakítani. A 12-es ajánlás a biztonsági osztályokat három szempontból határozza meg:

- az információvédelem
- a kárérték
- és a megbízható működés szerint

5.6.2 Besorolások az információvédelem területén

Egy adatot, illetve az azokat kezelő alkalmazásokat és rendszerelemeket mennyire kell védeni, az határozza meg, hogy az adatra milyen előírások (jogszabályok, szabványok, ajánlások és belső utasítások) vonatkoznak. Az ezekben előírt védelmi követelmények meghatározóak. Ezek alapján a védendő adatoknak alapvetően négy csoportját különíthetjük el:

- *nyílt,* szabályozók által nem védett adat,
- *érzékeny (védendő), de nem minősített adat,*
  Ide tartoznak a jogszabályok által védendő adatok (személyes, illetve különleges adatok, az üzleti titkot, a banktitkot képező adatok, az orvosi, az ügyvédi és egyéb szakmai titkok, a posta és a távközlési törvény által védett adatok stb.) és az egyes szervezetek, intézmények illetékesei által, belső szabályozás alapján védendő adatok.
- *szolgálati titok,*
- *államtitok.*

Nyílt, Érzékenyt

Minősített

Minősített adatnak csak az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény 2. § (1) bekezdésében felsorolt adatokat nevezzük.

Az adatminősítés jelenlegi rendjét figyelembe véve az *információ-védelem szempontjából* a következő biztonsági osztályokat kell kialakítani:

Alapbiztonsági osztály

Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

Fokozott biztonsági osztály

A szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.

Kiemelt biztonsági osztály

Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

Az elemzések azt mutatták, hogy a nyílt adatok kezelésével kapcsolatosan is vannak meghatározott információvédelemi és megbízható működési követelmények. Ezen adattípushoz általában jól meghatározott szolgáltatási kötelezettség társul, amely egy bizonyos szintű megbízható működést tételez fel. E megfontolások alapján a nyílt adatokat is az alapbiztonság szintjén kezelendő kategóriaként vették figyelembe.

5.6.3 Besorolások a kárérték szerint

Az adat a fenyegetés alapvető célpontja. Sérülése vagy megsemmisülése eltérő nagyságú kárt okoz. A kár értéke arányos az információ, illetve az informatikai rendszer vagy annak a káreseménye által érintett része funkcionális, eszmei vagy anyagi értékével. A kár jellege lehet:

A kár jellege

- *közvetlen anyagi* (pl. a mindenkori amortizált értékkel vagy az elmaradt haszonnal arányos),
- *közvetett anyagi* (pl. a helyreállítási költségekkel, perköltségekkel arányos),
- *társadalmi-politikai, humán,* (pl.: bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben)
- *személyi sérülés, haláleset,*
- jogszabály által védett adatokkal történő *visszaélés* vagy azok sérülése (jogsértés: állam- vagy szolgálati titok, személyiséghez fűződő jogok megsértése, bizalmas vagy hamis adatok nyilvánosságra hozatala, közérdekű adatok titokban tartása,).

A kártípusokhoz mennyiségi jellemzők tartományait rendelve kialakítható egy kárérték osztályozás, amelyek segítségével az informatikai rendszerek biztonsági osztályokba sorolhatók. A biztonság értékeléséhez a következő kárérték szinteket definiálták:

"0": jelentéktelen kár

A közvetlen anyagi kár nem jelentős, 1 embernappal helyreállítható; nincs bizalomvesztés; a probléma a szervezeti egységen belül marad; testi épség jelentéktelen sérülése

egy-két személynél; nem védett adat bizalmassága vagy hitelessége sérül.

"1": csekély kár

A közvetett anyagi kár 1 emberhónappal állítható helyre; társadalmi-politikai hatás: kínos helyzet a szervezeten belül; könnyű személyi sérülés egy-két személynél; hivatali, belső (intézményi) szabályozóval védett adat bizalmassága vagy hitelessége sérül.

"2": közepes kár

A közvetett anyagi kár 1 emberévvel állítható helyre; társadalmi-politikai hatás: bizalomvesztés a tárca középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel; több könnyű vagy egy-két súlyos személyi sérülés; személyes adatok bizalmassága vagy hitelessége sérül; egyéb jogszabállyal védett (pl. üzleti, orvosi) titok bizalmassága vagy hitelessége sérül.

"3": nagy kár

A közvetett anyagi kár 1-10 emberévvel állítható helyre; társadalmi-politikai hatás: bizalomvesztés a tárca felső vezetésében, a középvezetésen belül személyi konzekvenciák; több súlyos személyi sérülés vagy tömeges könnyű sérülés; szolgálati titok bizalmassága vagy hitelessége sérül; szenzitív személyes adatok, nagy tömegű személyes adat bizalmassága vagy hitelessége sérül; banktitok, közepes értékű üzleti titok bizalmassága vagy hitelessége sérül.

"4": kiemelkedően nagy kár

- A közvetett anyagi kár 10-100 emberévvel állítható helyre; katonai szolgálati titok bizalmassága vagy hitelessége sérül; társadalmi-politikai hatás: súlyos bizalomvesztés, a tárca felső vezetésén belül személyi konzekvenciák; egy-két személy halála vagy tömeges sérülések; államtitok, vagy nagy tömegű szenzitív személyes adat, vagy nagy értékű üzleti titok bizalmassága vagy hitelessége sérül.

"4+": katasztrofális kár

A közvetett anyagi kár több mint 100 emberévvel állítható helyre; társadalmi-politikai hatás: súlyos bizalomvesztés, a kormányon belül személyi konzekvenciák; tömeges halálesetek; különösen fontos (nagy jelentőségű) államtitok bizalmassága vagy hitelessége sérül.

Az informatikai rendszerek biztonsági osztályait a kárérték szintek szerint az alábbi csoportokba soroljuk:

Osztályok kialakítása

- **Alapbiztonsági** követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben maximum "2", azaz legfeljebb közepes kárértékű esemény bekövetkezése fenyeget.
- **Fokozott** biztonsági követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben maximum "3", azaz legfeljebb nagy kárértékű esemény bekövetkezése fenyeget.
- **Kiemelt** biztonsági követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben a "4+", azaz a katasztrofális kárértékig terjedő esemény bekövetkezése fenyeget.

5.6.4 Információbiztonsági osztályozás a megbízható működés szempontjából

Az informatikai rendszerek megbízható működése alatt azt értjük, hogy a jól megtervezett alkalmazói rendszerek (felhasználói programok és adatok) egy megbízható informatikai alaprendszeren (hardver és alapszoftver) működnek csak megfelelően.

A megbízható működés szempontjából értelmezett biztonsági osztályokra jellemző paraméterként a rendelkezésre állást, a kiesési időt és az ezen belül egy alkalomra megengedett maximális kiesési időt adjuk meg a következő táblázatban. A paraméterek számításánál napi 24 órás üzemet és 1 hónapos üzemidőt tételeztünk fel. ($T_{ÜZ}$ - az üzemidő periódus)

$T_{ÜZ}$ = 1 hónap	Rendelkezésre állás (R)	Megengedett kiesési idő	Megengedett legnagyobb kiesési idő egy alkalomra
Alapbiztonsági	95,5 %	23,8 óra	-
Fokozott biztonsági	99,5 %	2,6 óra	30 perc
Kiemelt biztonsági	99,95 %	16 perc	1 perc

A hiba bekövetkezésétől számított kiesési időt a rendszeren belüli megoldásokkal és a rendszeren kívül foganatosított intézkedésekkel állíthatjuk be az adott biztonsági osztály követelményeinek megfelelő értékre.

Kiesési idő

A kiesési időt befolyásolják:

- *az újraindítási képesség,* vagyis milyen gyorsan tudják újra működésbe helyezni a leállt rendszert,
- *a hibaáthidalás folyamatának kialakítása,* vagyis milyen tartalék eszközök állnak rendelkezésre, mennyire jól konfigurált a rendszer,
- *a rendszerkonfiguráció hatékony menedzselése,* az átállítási folyamat mennyire megy zökkenőmentesen.

Meleg és hideg tartalék

A tartalékoknál megkülönböztetünk meleg és hideg tartalékot. A meleg tartalék folyamatosan, az éles rendszerrel párhuzamosan működik, ugyanazokat az információkat tartalmazza, mint az éles rendszer. Az átállást a felhasználók általában észre sem veszik. A hideg tartalék üzemen kívül lévő berendezés, amit a használat előtt üzembe kell helyezni.

Nincs tartalék, hibajavítás

Alapbiztonsági osztály

A rendszer - néhány rendszerelem (pl. lemezegység) kivételével - általában nem tartalmaz redundanciát. Azt, hogy milyen gyorsan tudják újraindítani a rendszert, attól függ, hogy milyen a hiba természete, mennyire pontos a hiba leírása és behatárolása, a szerviz milyen gyorsan reagál, és mennyire hatékonyan dolgozik. A rendszerben általában nem alkalmaznak hiba áthidalási és az ehhez szükséges rendszer me-

nedzselési megoldásokat. Menedzselést a tartalék alkatrész és szerviz biztosítás igényel.

Fokozott biztonsági osztály

Tartalék + hibajavítás

Már megjelenik egy bizonyos szintű redundancia, amely a legfontosabb rendszerelemeknek pl. hálózaton keresztül történő meleg tartalékolásával vagy hideg tartalék biztosításával oldható meg. A meleg tartalékra történő átkapcsolás már igényel áttérés-menedzsmentet, amely alapvetően automatikusan vagy manuálisan vezérelt áttérést jelent. A melegtartalék megoldás vezérlési és adatállomány aktualizálási eljárásait már a rendszertervezés idején ki kell alakítani, a konfiguráció erőforrásait is ennek megfelelően kell méretezni. A fokozott biztonsági osztályban még nem minden elemnek van biztonsági tartaléka, azokat javítani kell. Erre biztosítani kell olyan szervizt, amely a megfelelő idő alatt megkezdi és elvégzi a hiba kijavítását. A saját üzemeltető személyzettel szemben már komolyabb szakmai követelményeket támaszt a tartalékolási folyamat irányítása.

Kiemelt biztonsági osztály

Melegtartalék

Kizárólag a szorosan csatolt melegtartalékkal megvalósított hibaáthidalás jöhet szóba, amely komoly áttérés-menedzsmentet igényel. A kiesési idő itt gyakorlatilag az átkapcsolási idővel azonos. A szó eredeti értelmében vett rendszerindításra nincs szükség. Ebben az osztályban a legmagasabb az üzemeltető személyzettel szembeni szakmai követelmény, mert az esetlegesen szükséges beavatkozás reakcióideje olyan rövid, hogy azt külső szervizzel biztosítani nagyon drága megoldás lenne. A szerviz feladata elsősorban a meghibásodott egység kijavítása.

5.6.5 A különböző dokumentumok biztonsági osztályai közötti megfeleltetés

A nemzetközi és a hazai informatikai biztonsági osztályok máshogy fogalmazzák meg ugyanazokat a követelményeket, de az átjárhatóságot a következő táblázat mutatja:

TCSEC	ITSEC	12. sz. ajánlás
B3-A1	F-B3	
B2	F-B2	KIEMELT
B1	F-B1	FOKOZOTT
C2	F-C2	ALAP
C1	F-C1	

Az ITB 12. ajánlás kiemelt biztonsági osztálya tartalmazza a TCSEC B3 osztály néhány követelményét is. A magyar biztonsági osztályok követik az első besorolást, amit a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről szóló I/1981.(I.27.) BM sz. rendeletben határoztak meg.

A CC értékelési rendszere nem hasonlítható össze a táblázatban lévő többi rendszer osztályaival, mivel más típusú szemlélete, eltérő célrendszere és új fogalmai nem egyeznek meg a többi követelményeivel.

5.7 A COBIT

Az elmúlt években hazánkban is egyre több intézménynél alkalmazták a COBIT (Control Objectives for Information and related Technology – Informatikai és Kapcsolódó Technológiák Ellenőrzési Célkitűzése) néven ismert nyílt szabványt.
A szabvány kidolgozója az IT Governance Institute-ot (Információ Technológia Irányítási Intézet), amit az ISACA (Information Systems Audit and Control Association – Információrendszer Ellenőrök Nemzetközi Szövetsége és az ISACF (Információs Rendszer Auditorok Nemzetközi Alapítványa) együttes támogatásával hoztak létre. A cél az volt, hogy a különböző vezetőknek és szakembereknek támogatást nyújtsanak ahhoz, hogy az informatikát sikeresen használják fel az intézmények, vállalkozások küldetésének teljesítésében és üzleti céljaik elérésében.
A COBIT kiindulási alapelve az, hogy az informatikai rendszerek kialakítása és működtetése különböző – logikailag jól elkülöníthető – szakaszokra bontható. Ezek a szakaszok átfogják az igény-meghatározási, szabályozási, tervezési, beszerzési, kivi-

telezési, megvalósítási, folyamatos működtetési és ellenőrzési feladatokat.
Az üzleti élet, és az azt befolyásoló környezet, a működéssel összefüggő veszélyforrások folyamatosan változnak. A változások hatására az intézmények céljai, működési folyamatai, termékei, szolgáltatásai, informatikai rendszerei, kockázatai átalakulnak. Így a folyamatos változások követése, értékelése és az intézmény működésébe, kockázat kezelésébe történő beépítése a vezetés egyik legfontosabb feladatává vált.

A COBIT alapelve

A COBIT legfontosabb alapelve, hogy az **információtechnológiát az üzleti célok és követelmények megvalósítása érdekében alkalmazzuk.** A COBIT összegyűjtötte azokat az ellenőrzési pontokat, amelyek segítségével az informatika alkalmazásával összefüggő kockázatok csökkenthetők, valamint egy adott informatikai alkalmazás megfelelősége vizsgálható.

A COBIT fejlesztése során felhasználták a korábbi biztonsági minősítést támogató eszközök tapasztalatait. A COBIT alapvetően az informatikai szabványok, módszerek, élenjáró gyakorlatok egységes rendszerbe foglalt módszertani eszköze, az általa alkalmazott módszer a tevékenységek és a feladatok vagy funkciók kritikai elemzésén alapul.

A gyakorlati felhasználás során alkalmazható a hagyományos papír alapú változata, de a fejlesztéssel párhuzamosan kialakításra kerültek a tudásbázist, döntést és értékelést, valamint a jelentést támogató számítógépes szakértői rendszerek változata is.

A COBIT négy fő területet ölel fel:

- Tervezés és szervezet,
- Beszerzés, fejlesztés és implementálás,
- Üzemeltetés, szolgáltatások, biztonság,
- Monitorozás, független ellenőrzés.

A COBIT struktúra a fő területekben leírt folyamatokra meghatározza, hogy milyen üzleti követelmények kielégítésére milyen

ellenőrzési célkitűzésekre van szükség és ezt milyen eszközökkel, tevékenységekkel, feltételekkel látja biztosítottnak elérni. [31]

Ellenőrző kérdések

1. Mi az adatbiztonság meghatározása?
2. Milyen nemzetközi ajánlások születtek az adatbiztonság területén?
3. Milyen hazai ajánlásokat ismer?
4. Milyen alapkövetelményei vannak az adatbiztonságnak?
5. Mit nevezünk fenyegető tényezőnek, alapfenyegettségnek, védelmi mechanizmusnak?
6. Milyen alapfunkciókat határoz meg az ITSEC?
7. Milyen biztonsági osztályok vannak az TCSEC-ben?
8. Milyen speciális biztonsági osztályokat határoz meg az ITSEC?
9. Milyen védelmi mechanizmusokat ír le az ITSEC?
10. Milyen szempontok szerint minősítenek egy informatikai rendszert vagy terméket a biztonság szemszögéből?
11. Milyen biztonsági minősítési fokozatok vannak az ITSEC-ben?
12. Miben tér el a CC az előző ajánlásoktól?
13. Mit és hogyan szabályoz az ISO OSI 7498-2?
14. Milyen biztonsági szolgálatokat határoz meg az X 800?
15. Milyen biztonsági mechanizmusok vannak az X 800-ban?
16. Milyen szempontok alapján alakították ki a biztonsági osztályokat az ITB 12-ben?
17. Mik tartoznak a különböző osztályokba?
18. Hogyan felelnek meg a különböző ajánlások biztonsági osztályai egymásnak?
19. Mivel foglalkozik a COBIT?

6. Az informatikai biztonsági rendszer tervezése

Az előző fejezetben az informatikai rendszerek biztonsági jellemzőivel, besorolásával és minősítésével foglalkoztunk. Ebben a fejezetben megnézzük, hogyan kell a biztonsági elemeket beépíteni a rendszerekbe.

6.1 Az informatikai biztonság helye

Szervezeti stratégia

Minden szervezetnek vannak céljai amelyek elérésének módját a *szervezeti stratégiában* fogalmazzák meg. Az *informatikai stratégia* a szervezeti célok eléréséhez szükséges informatikaalkalmazásoknak áttekintése. A szervezet informatikai stratégiája a szervezeti stratégia része.

Biztonsági stratégia

Szintén fontos eleme a szervezeti stratégiának a *biztonsági stratégia.* A biztonság alatt azt az állapotot értjük, amiben a tevékenységek zavartalanul végezhetők. A szervezeti tevékenységek biztonságát szavatoló rendszernek le kell fedni minden olyan tevékenységet, amelyet a szervezeti stratégia érint. Ez garantálja a biztonság teljeskörűségét és egységes szintjét.
Tehát az informatikai biztonság szerves része az informatikai rendszernek valamint a szervezeti szintű biztonsági rendszernek is.

Informatikai biztonság

Az informatikai biztonság alatt a szervezeti tevékenységek informatikai összetevőinek a célok eléréséhez szükséges megfelelő állapotban tartását értjük. [29]

Olyan megoldásokra van szükség, amelyek a biztonsági követelményeket a *lehető legkisebb kockázattal* és *egyenlő szinten* elégítik ki. Ezek az intézkedések egy összefüggő, egységes rendszert alkotnak, amely az informatikai rendszer különböző életszakaszaiban más-más feladatot jelentenek:

- Az informatikai rendszer tervezésénél már feltétlenül be kell építeni a biztonságot megteremtő módszereket.

- A számítástechnikai eszközök (hardver és szoftver) beszerzésénél, elhelyezésénél, és az üzemeltetési rend kialakításánál az egyik fő szempont a biztonság megteremtése.
- Nem elég ezeket az intézkedéseket meghozni, hanem betartásukat folyamatosan ellenőrizni kell.

Különböző tervezési módszerek

A biztonságos informatikai rendszerek létrehozásánál többféle módszert lehet alkalmazni, amelyek a vizsgált folyamatok, illetve az eljárás lépéseinek tagolásában különböznek egymástól. Ezek a módszerek hasonlóak, de általában versenyeznek egymással. Nem szabad megfeledkezni arról sem, hogy az adatbiztonsági elvek, modellek, módszerek, technikák, árucikkek is egyben, amelyeket tanácsadók, biztonsági cégek a szó szoros értelmében megvételre kínálnak gyakorló vezetőknek. Megfelelő propagandával, kampányokkal, sajtóval, rendezvényekkel egy-egy módszer köré „sztárkultuszt" lehet kialakítani. A módszerek és gazdáik versenyeznek is egymással, és ez a verseny nem mindig sportszerű. Mi most az ITB ajánlásokban lévő módszert ismertetjük.

Egy informatikai biztonsági rendszer – mint minden rendszer - tervezése sok lépésből álló, sokféle szaktudást igénylő, bonyolult feladat.

6.2 A tervezés szakaszai

Az informatikai biztonság tervezésénél és megteremtésénél - hasonlóan más biztonsági feladatok megoldásához - a következő kérdések merülnek fel:

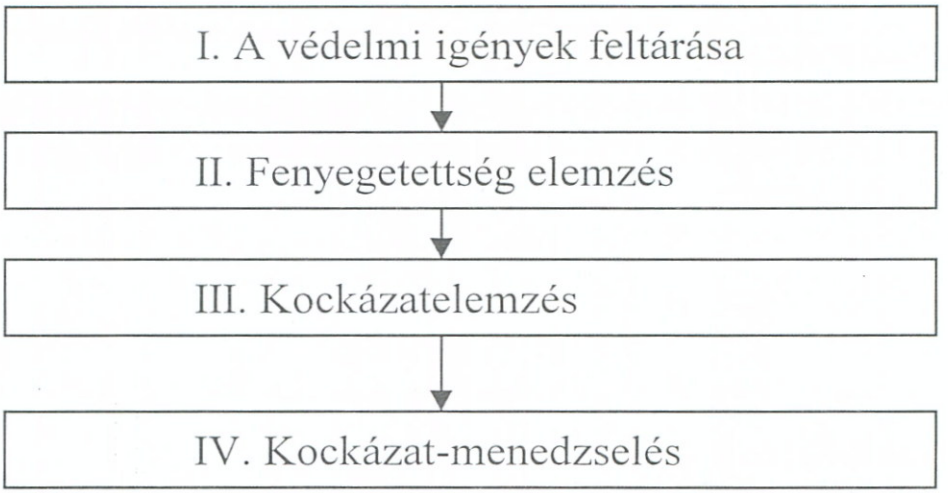
Kérdések

- Milyen információk szükségesek a szervezeti célok eléréséhez?
- Adott információkat milyen fenyegetések érhetik?
- Hol jelennek meg az információk a rendszerben?
- Adott helyen milyen okok válthatják ki a kárt okozó esemény bekövetkeztét?
- Mi a kockázata a fenyegetéseknek?
- Milyen intézkedések tehetők a kockázat csökkentésére?

- Gyakorlatilag lehetséges-e, illetve megéri-e az adott intézkedés?
- Milyen konkrét feladatok adódnak az elhatározott intézkedésekből?

Az informatikai biztonsági rendszer tervezését – a feltett kérdéseknek megfelelően - a következő szakaszokra lehet felbontani:

Szakaszok



I. A védelmi igények feltárása

Ebben a szakaszban kiválasztjuk azokat az informatikai alkalmazásokat, amelyek a szervezet szempontjából a legfontosabbak, és később már csak ezekkel foglalkozunk.

II. Fenyegetettség elemzés

Megkeressük az informatikai rendszer gyenge pontjait és azokat a fenyegetéseket, amelyek a kiválasztott alkalmazásokra veszélyt jelenthetnek.

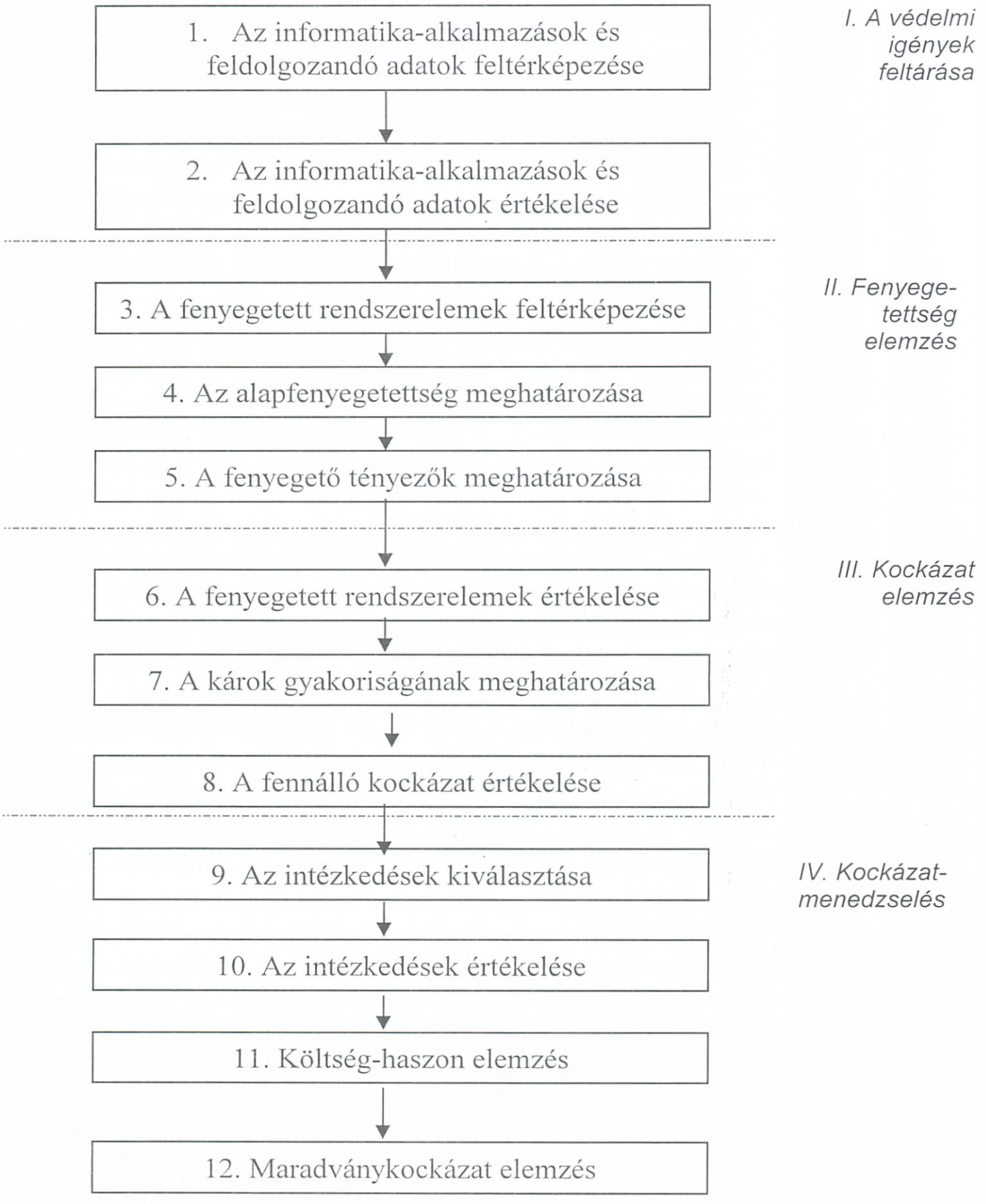
III. Kockázatelemzés

Itt azt vizsgáljuk meg, hogy az informatikai rendszerre milyen káros hatása lehet a fenyegető tényezőknek. Meghatározzuk a lehetséges kár gyakoriságát és a kárértéket.

IV. Kockázat- menedzselés

Kiválasztjuk a fenyegető tényezők elleni intézkedéseket és azok hatását értékeljük. Megnézzük, hogy az egyes intézkedések milyen költségekkel járnak és milyen hasznot hoznak.

Tovább bontva a szakaszokat, a lépések a következők:



6.3 A védelmi igények feltárása

Az informatikai-alkalmazások és a feldolgozandó adatok feltérképezése

Helyzetfelmérés

Az első lépés a helyzetfelmérés és célmeghatározás. Ennek a szakasznak az a célja, hogy reális és teljes képet kapjunk a védendő rendszer felépítéséről, tartalmáról. Csak akkor tudjuk meghatározni azt, hogy hogyan védjük meg a rendszert, ha pontosan tudjuk, hogy mit kell védeni.

E szakaszban valamennyi adott informatika-alkalmazás és feldolgozandó adat közül ki kell választani azokat, amelyek az adott szervezet számára jelentőséggel bírnak, így védelmet igényelnek. Ehhez az alkalmazónak kell megállapítania, milyen védelmi célokat tűz maga elé az öt alapkövetelmény vonatkozásában. Sorra kell venni és részeire bontani az adott intézménynél működő rendszereket. Ha szükséges egészen adatmélységig le kell menni. Ez a felmérés különböző módszerekkel folyhat.

Az informatikai-alkalmazások és a feldolgozandó adatok értékelése

Értékelés

A lépés megvalósítása a következő feladatokra bontható:

a. *A felhasználó védelmi céljainak leírása*;
   Pl. egy konkrét feldolgozás mennyi időre eshet ki; melyik adatcsoportokhoz ki férhet hozzá.

b. *A hatrészes értékskála rögzítése;*
   A következő feladat egy értékskála kialakítása, amely alapján a meglévő, illetve a megvalósítandó informatikai rendszer jelentősége, értéke meghatározható. (lásd 5.6.3.)
   A károknak a jelentéktelentől a katasztrofálisig terjedő nagysága általában hat érték-kategóriában fejezhető ki. A 6-részes skála általános beosztása a következő:
   "0": jelentéktelen, elhanyagolható kár
   "1": csekély,
   "2": közepes,
   "3": nagy,
   "4": kiemelkedő,
   "4+": katasztrofális.

A "4+" különérték olyan katasztrofális káresetekre vonatkozik, amelyek akár a legkisebb bekövetkezési gyakoriság esetén is elviselhetetlen és minden körülmények között meg kell akadályozni azokat.

Különérték

c. *Az értékek hozzárendelése az informatika-alkalmazásokhoz és az adatokhoz.*
Értékelni kell minden kárt, és ennek eredményeként mindegyikükhöz hozzá kell rendelni egy skálaértéket. Nincs jelentősége, hogy milyen pénzbeli vagy egyéb kárfajtáról van szó. Az ugyanolyan értékelésű károknak hasonló jelentőségűeknek kell lenniük.

6.4 Fenyegetettség elemzés

Ebben a lépésben meghatározzuk a rendszer gyenge pontjait és valamennyi elképzelhető fenyegető tényezőt, amelyek kárt okozhatnak az informatikai rendszerben. Különösen ügyelni kell arra, hogy egyetlen fontosabb fenyegetettséget se hagyjunk ki, miután a kockázatelemzés ennek eredményeire épül. Ha ez nem teljeskörű, az a biztonsági rendszer súlyos hiányához vezethet, (Pl. megfeledkezünk arról, hogy az épület ártéri területen épült, és nincsenek megfelelő védőgátak körülötte).

Gyenge pontok, fenyegető tényezők

A fenyegetett rendszerelemek feltérképezése

A fenyegető tényezők az informatikai rendszer valamely elemén keresztül támadnak. Az ITB 8. ajánlása az informatikai rendszert nyolc rendszerelemre bontja, amelyek a teljes rendszert és annak környezetét lefedik. Ezek a következők:

Rendszerelemek

- környezeti infrastruktúra
- hardver
- adathordozó
- dokumentumok
- szoftver
- adatok
- kommunikáció
- személyek

Védelmi eszközök

A rendszerelemek különleges osztályaként kell feltérképezni mindent, ami valamely védelmi intézkedés részének tekinthető: például olyan berendezéseket, amelyek a számítógépes helyiségekbe a belépést ellenőrzik, a biztonsági hardvereket és szoftvereket, dokumentumokat és a szükséghelyzet esetére készült szabályozásokat.

Az alapfenyegetettség meghatározása

Az előző lépésben meghatározott rendszerelemekhez hozzá kell rendelni azt az alapfunkciót, ami a nem rendeltetésszerű működés során sérül.
Például:

- Az egész hardver nem *áll rendelkezésre*, ha az áramellátás megszűnik.
- A szoftver nem lesz *működőképes*, ha vírusos lesz.
- Az adathordozó nem lesz *hiteles,* ha eltávolítják róla a jelzéseket.

Az olyan rendszerelemek esetében, amelyek a védelmi intézkedések része, a rendelkezésre állás vagy a sértetlenség elvesztése általában a védelmi funkciók teljes kieséséhez vezet.

A fenyegető tényezők meghatározása

Ebben a lépésben meghatározzuk rendszerelemenként a gyenge pontokat és fenyegető tényezőket.

Környezeti infrastruktúra

A környezeti infrastruktúra

Ide tartozik a számítóközpont épületének területe, maga az épület, az épületben lévő helyiségek, átviteli vezetékek, áramellátás, klíma, víz, világítás, telefon, és a különböző rendeltetésű védelmi berendezések (belépés-ellenőrző, tűzvédelmi, vízvédelmi, betörésvédelmi, stb.).

Gyenge pontok

- Nem védett átviteli vezetékek, kábelek, informatikai berendezések.

- Illetéktelen személyek felügyelet nélküli jelenléte, vagyis a belépési biztonság hanyag kezelése.
- A védelmi berendezések működési módjának vagy gyengeségeinek jogosulatlanok általi megismerése.

Fenyegető tényezők:

- **"Vis major":** földrengés, árvíz, szélvihar, villámcsapás, robbanás, repülőgép lezuhanása, sztrájk, háborús cselekmény.
- **Személyek által kifejtett erőszak:** robbantásos merénylet, fegyveres behatolás, gyújtogatás, savazás, vandalizmus, betörés.
- **Jogosulatlan személyek** ellenőrizetlen belépése az épületekbe, helyiségekbe, ellátó és védelmi berendezésekhez, vezetékekhez. A szervezeten kívüli személyek által végzett, nem felügyelt munkálatok.
- **Közműellátás** (áram, víz és telefon) és védelmi berendezések zavara vagy kiesése.

A hardver

Ide tartoznak a számítástechnikai eszközök (pl. központi egység, tárolók, terminálok, plotter, scanner, nyomtatók) a hálózati csatoló eszközök (pl. modem, ethernet controller); a hálózatépítő eszközök (például: gateway-számítógép, router, repeater); speciális biztonsági berendezések (pl. rejtjelzőkészülékek, végpont védelmi eszközök, chipkártya-olvasó).

Gyenge pontok

- **Eltulajdonítás:** a készülékek csekély mérete, súlya miatt a lopás könnyen lehetséges.
- **Külső behatások miatti meghibásodás:** hőhatás, vízzel való elárasztás, érzékenység az elektromágneses sugárzásra , mechanikai behatásokra.
- **Tartozékok utánpótlásának szervezetlensége**: pótalkatrészek, nyomtatópapír, festékszalagok, tonerek, stb.

Fenyegető tényezők

- **Műszaki jellegű hibák:** elöregedés, kopás, mechanikai zavarok, tervezési és kivitelezési hiányosságok,
- **Környezeti hatások:** feszültségingadozás, nedvességtartalom ingadozás, piszkolódás, zavaró sugárzás, elektrosztatikus feltöltődés.
- **A szoftver által kiváltott hibák a hardverben**: pl. olyan vírus, amely a merevlemezen az olvasó területen kívülre viszi a fejet.
- **Személyekkel összefüggő fenyegetés:** készülékek károsítása vagy roncsolása, ellopása, jogosulatlan szerelés és alkatrészcsere.

Adathordozók

Az adathordozók

Ebbe a csoportba tartoznak a raktározott állapotú szoftverek, a biztonsági másolatokat, munkakópiákat, archív adatokat, jegyzőkönyvi adatokat tartalmazó adathordozók, valamint az újonnan beszerzett és még használatba nem vett, illetve a felszabadított adathordozók melyek tartalmára a továbbiakban nincs szükség.

Gyenge pontok

- **Fizikai instabilitás**: érzékenység a mágneses térre, hőhatásra és nedvességre, elöregedés folytán szakaszos demagnetizálódás,
- Tartalmuk emberek számára **technikai segédeszközök** nélkül nem hozzáférhető,
- Kikapcsolható írásvédelem,
- Könnyen **szállíthatóak,** a szállítás nehezen ellenőrizhető.

Fenyegető tényezők

- Hiányzó vagy nem kielégítő jelölés, ami miatt a tartalmuk ránézésre nem állapítható meg.
- Az adathordozók újrafelhasználásra vagy megsemmisítésre történő kiadása előzetes törlésük vagy átírásuk nélkül.

- Ellenőrizetlen másolás illetve hozzájutás az adathordozókhoz,
- Gyári hibás adathordozók, inkompatibilis formátum, hiányzó kezelő berendezések.
- A szervezet tulajdonát képező adathordozók privát célú használata és privát adathordozók szolgálati használata (illegális másolatok, vírusok behatolása).

Dokumentumok

A dokumentumok

Dokumentum mindenfajta olyan információ, amely papíron vagy mikrofilmen van rögzítve és amelynek köze van az informatikai rendszer használatához és üzemeléséhez.

Gyenge pontok

- A dokumentumok hiányzó adminisztrációja,
- Nincsenek átvezetve a változások,
- Nem védett, ellenőrizetlen sokszorosítás

Fenyegető tényezők

- Dokumentumok, kézikönyvek teljes hiánya (nincs megírva, nem vették meg, ellopták, elvesztették vagy kikölcsönözték)
- Olvashatatlanság (kézirat, kifakult másolatok), hiányos példányok, hibák a leírásokban, nem aktualizált változatok, jogosulatlan változtatások.

A szoftver

A szoftver

Ebbe a kategóriába csak a használatban lévő szoftverek tartoznak, a raktározott állapotú szoftvereket az adathordozóknál tárgyaltuk.

Gyenge pontok

- Specifikációs hiba, programok ellenőrzésének és átvételének hiánya.
- Bonyolult felhasználói felület, felhasználó hitelesítés hiánya.

- Az események hiányzó jegyzőkönyvezése (például belépés, CPU-használat, fájlok megváltoztatása).
- A rendszer védelmi eszközeinek könnyű kiismerhetősége.
- A hozzáférési jogok helytelen odaítélése.
- Más felhasználók ismeretlen programjainak használata (vírusfertőzés).

Fenyegető tényezők

- Szoftverhiba, nem kellően kitesztelt szoftverek, megsérült fájlok miatt.
- Jogosulatlan bejutás az informatikai rendszerbe a kezelői helyről vagy a hálózatról.
- Kezelési hiba vagy visszaélés a kezelési funkciókkal.
- Szoftver ellenőrizetlen bevitele, vírusveszély.
- Karbantartási hiba vagy visszaélés a karbantartási funkciókkal, helytelen karbantartási funkciók (távoli karbantartás a hálózaton keresztül)
- A szoftver sérülése, károsodása vagy használhatatlansága hardver hibák alapján

Adatok

Az adatok

Ebben a pontban a feldolgozás különböző lépéseiben (bevitel, feldolgozás, tárolás és kivitel) lévő adatokat vizsgáljuk.

Gyenge pontok

- Az adatbevitel hiányzó vagy nem kielégítő ellenőrzése.
- Szoftverhiba, hiányzó hibakezelő eljárás, hiányzó újraindítás-előkészítés a feldolgozásban.
- Az adatterületek törlésének hiánya az újrafelhasználás előtt.
- Adathordozóra írás ellenőrző olvasás nélkül.

Fenyegető tényezők

- Hardver vagy szoftver hibák által keletkező adatvesztések, károsodások, eltérések.
- Adathordozók által okozott adatvesztések, károsodások, eltérések.

- Emberek által okozott véletlen vagy akaratlagos adattörlések, felülírások.

A kommunikáció

Ezen elemcsoport tárgya valamennyi adat a továbbítás ideje alatt, amelyeket valamely szolgáltatás realizálása érdekében hálózaton továbbítanak. Hálózatok lehetnek az üzemi területen belül (például LAN-ok) vagy azon kívül (például közüzemi hálózatok), illetve e kettő kombinációja. A kommunikációhoz szükséges hardvert mindaddig, amíg az informatikai rendszer üzemeltetőjének felelősségi körén belül van, a hardver elemcsoportban, a vezetékeket pedig, amennyiben az üzem területén belül vannak, a környezeti infrastruktúra elemcsoportban szerepeltetjük.

Gyenge pontok

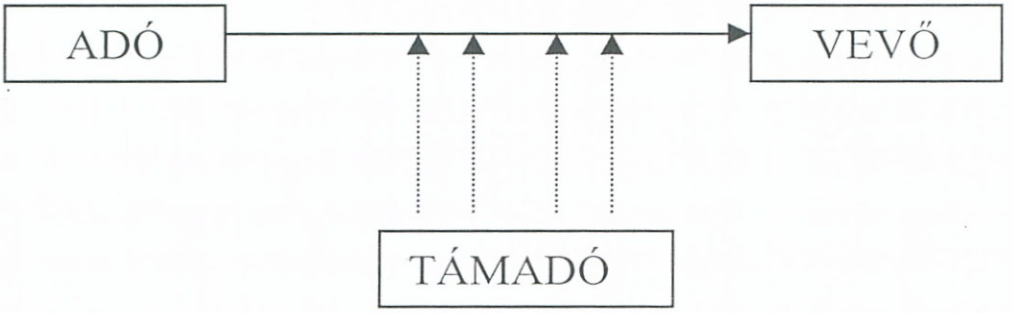
- Átviteli vonal károsodása, megszakadása.
- A hálózati szoftver és hardver hibái, azok manipulálhatósága.
- Üzenetek lehallgatása, meghamisítása, az adó és fogadó hiányzó azonosítása.
- A jelszavak vagy titkos kulcsok nyílt szövegben való továbbítása.
- Függés az átvitel sorrendjétől.
- Lehetőség az üzenetek ismételt lejátszására.
- Valamely üzenet elküldésének, kézhezvételének hiányzó bizonyítása.

Fenyegető tényezők

- Jogosulatlanok bejutása a hálózatba nem ellenőrizhető csatlakozások révén.
- A közvetítő-berendezések hibás viselkedése vagy kiesése műszaki hibák vagy hibás hálózati szoftverek miatt.
- Hálózati hardverek/szoftverek manipulálása, átviteli hibák.
- A fájl-szerver kiesése vagy hibája helyi hálózatban.

- Nem várt forgalmazási csúcsok, célzott terhelési támadások.
- Az üzenetek lehallgatása, megváltoztatása, elvesztése, ismételt lejátszása.
- A vezetékek kompromittáló sugárzásának kihasználása.
- A kapcsolat felépítésének lehallgatása (2. ábra)

Lehallgatás



2. ábra

A lehallgatásnál támadó illetéktelenül rákapcsolódik az átviteli vonalra, az ott folyó adat- és kulcs-forgalmat figyeli. Az üzenetek gyűjtésével, különleges helyzetek észlelésével támadhat.

- A kommunikációs kapcsolatok kikutatása (forgalmazáselemzés), a kommunikációs partnerek névtelenségének veszélyeztetése.

- A kapcsolat felépítése meghamisított azonossággal, megszemélyesítéssel (3. ábra)

Megszemélyesítés

3. ábra

A megszemélyesítés esetén a támadó beépül a kommunikációs összeköttetésbe, az üzeneteket elnyeli, és az ellenállomások helyett válaszol mindkét irányba. Különös veszélyforrás lehet, ha a támadó az egymással kommunikáló állomásokat sorozatos ismétlésre kényszeríti, esetleg ugyanazon üzenet két különböző rejtjelezett variációját szerzi meg, vagy valamelyik állomásról ismert választ kényszerít ki, amellyel megszerzi annak rejtjelezett változatát.

Személyek

Személyek

E csoportban csak olyan személyek szerepelnek, akikre közvetlenül vagy közvetve szükség van az informatikai rendszer használatához, ezáltal hozzáférhetnek a másik hét csoport elemeihez. Külön neve is van annak a módszernek, amely az emberek természetes, bizalomra való hajlamát használja ki az informatikai rendszerek elleni támadásokra. Ez az ún. „social engineering", magyarul: *társadalommérnökség, társas kapcsolatok manipulálása.* Ez a módszer nagy szerepet játszik abban, hogy a támadó megkerülhesse a biztonsági korlátokat (pl. a tűzfalakat vagy behatolás-érzékelő rendszereket). A számítógép-használók hiszékenysége vagy az éberség hiánya olyan információkat juttathat el a támadóhoz, amely könnyű behatolást tesz lehetővé egy védett rendszerbe.

Social engineering

Gyenge pontok

- A munkából való kiesés, hiányos kiképzés, a veszélyforrások ismeretének hiánya, a fenyegetettségi helyzet lebecsülése,
- Kényelmesség, eltérő reakciók.
- Hiányzó vagy hiányos ellenőrzés.

Fenyegető tényezők

- Munkából való kiesések miatt a munkavégzés elmaradása.
- **Szándéktalan hibás viselkedés:** stresszhelyzet, fáradság, hiányos ismeretek, hibás szabályozás, az előírások ismeretének hiánya, az információk gyanútlan kiadása.
- **Szándékos hibás viselkedés:** az előírások megsértése, fenyegetés, zsarolás, megvesztegetés, haszonszerzési célból, bosszú, frusztráció miatt.

Egy felmérés szerint a saját alkalmazottak okozzák a károk 82%-át, a külső személyek csak a többi 18 %-ot.

6.5 Kockázatelemzés

Ebben a szakaszban is szubjektív módszerekkel lehet dolgozni, mint a biztonsági igényeknél. A károk gyakoriságának meghatározása is elsősorban a tapasztalatokon alapszik.

A fenyegetett rendszerelemek értékelése

A 6. lépés megvalósítása a következő feladatokra bontható:

- Az értékek átvitele a rendszerelemekre;
- A károk áttekintő ábrázolása.

Értékek átvitele

Az értékek átvitelét befolyásolják a feltérképezett gyenge pontok és védelmi intézkedések is. Ezek hathatnak csökkentő módon, amennyiben a kárt csökkentik vagy korlátozzák. Azokat a tényezőket és megfontolásokat, amelyek egy érték megváltoztatásához vezettek, feltétlenül dokumentálni kell.
Amennyiben egy rendszerelemtől több informatikai alkalmazás vagy információ függ, akkor az adott rendszerelemnek a legmagasabb előforduló értéket kapja. Például, ha egy lemezes tároló különböző adatokat tárol, akkor a legfontosabb információnak az értékét adjuk neki. Azok a rendszerelemek, amelyek más rendszerelemek védelmére szolgálnak - azaz valamely védelmi intézkedés részei - azon rendszerelemek értékét kapják meg, amelyeket védeniük kell.

A károk gyakoriságának meghatározása

Károk gyakorisága

A lépés során annak becslése történik meg, hogy milyen gyakran következik be valamely fenyegető tényező hatása és okoz kárt valamely rendszerelemben. Ajánlatos a gyakoriság értékelését követően a rendszerelemek listáját átvizsgálni. Így a védelmi intézkedéseket szem előtt tartva ésszerűnek tűnhet, hogy egy-egy rendszerelemet több rész-rendszerelemre osszunk fel, amennyiben a fenyegető tényezők csak egyes részegységekre tudnak hatni. Több rendszerelemet összevonhatunk ún. közös rendszerelemmé is, ha ugyanazok a fenyegető tényezők lehetnek hatással rájuk. De törekedni kell arra, hogy az egyes rendszerelemek felismerhetők maradjanak, miután egyes finomításokra később is szükség lehet.

Az informatikai rendszert fenyegető veszélyek gyakorisága 0, 1, 2, 3, 4 értékekkel és - szükség esetén - a 0- szélsőértékkel rendelkező skála segítségével határozható meg. A skála szakaszainak általános értéke a következő:

Gyakoriság értékek

"4": nagyon gyakori,
"3": gyakori,
"2": közepes,
"1": ritka,
"0": nagyon ritka,
"0-": emberi számítás szerint kizárva.

A "0" érték általános jelentése "nagyon ritka, valószínűtlen, elhanyagolható gyakoriságú". A "4" felső érték általános jelentése: "nagyon gyakori, bármikor előfordulhat, beláthatatlan gyakoriságú". A "0-" különértéknek kell állnia az olyan esetekben, amelyekre azt állítjuk, hogy "az esemény emberi számítások szerint egyáltalán nem következik be".

Statisztikai becslések

A befolyásolhatatlan külső tényezők (vis major), valamint a bűncselekmény eredetű események vonatkozásában kiinduló értékeket adhatnak a biztosítási és bűnügyi statisztikák, a gyakorlati szakemberek és a biztonsági szakértők tapasztalatai.
Különösen nehéz a külső támadók vagy a belső tettesek általi támadások megbecsülése a cselekmények csekély száma és természete miatt. Az ilyen becslések kiindulópontjaként azon személyek száma szolgálhat, akiknek bejutási lehetőségük van az informatikai rendszerbe, és akik kielégítő ismeretekkel és képességekkel rendelkeznek egy támadáshoz. Általában az okok elemzése is kiindulópontokat adhat a gyakoriság becsléséhez.

Szándékos támadás

Személyek szándékos támadásaival összefüggő fenyegető tényezőknél a gyakorisági értéket egy vagy akár két nagyságrenddel is növelni kell, ugyanis egy támadás annál valószínűbb, minél nagyobb a kár, amelyet valamely tettes okozhat, vagy saját előnyére változtathat át.

A gyakoriság becslése nélkül a kockázat, amelyet valamely fenyegető tényező okoz, nem becsülhető. Ezen számok ismeretében csökkenthető az a bizonytalanság, amely a becslés folyamatában rejlik. A csökkentést folyamatos és periodikus átvizsgálással és korrigálással érhetjük el. Az ismételt vizsgálatoktól jelentős tapasztalatszerzés várható.

A fennálló kockázat értékelése

Az eljárás ezen lépése a kockázatbecslési mátrix meghatározása. Az értékskála és a gyakoriságskála alapján érték-gyakoriság párokat hozunk létre. Ezek közül meghatározunk egy határértéket, amelytől a kockázat már nem elviselhető. A lépés tartalma tehát ez a döntés, ennek háttere, elemzése és dokumentálása.

Értékpár

Minden egyes feltárt fenyegető tényezőhöz minden érintett rendszerelem és valamennyi vonatkoztatható alapfenyegetettség vonatkozásában egy értékpárt kell hozzárendelni, amely a kárértékből (első szám) és a gyakorisági értékből (második szám) áll. Ez az értékpár jelöli a kockázatot. A kockázat nagysága a két értékből együttesen adódik. A kockázatokat úgy kell ábrázolni, hogy a nagyobb kockázatok könnyen azonosíthatók legyenek és felismerhető legyen, hogyan alakultak ki ezek a kockázatok.

Az elviselhető és az elviselhetetlen kockázatok rögzítése

Meg kell állapítani a döntési tábla alapján, mely kárnagyságból és gyakoriságból összetevődő értékpárok jelentenek elviselhető kockázatot és melyek nem.

Elviselhető és elviselhetetlen kockázat

A kockázati mátrixban valamennyi értékkombinációt meg kell jelölni egy "E" betűvel, ha elviselhető kockázatokat jelentenek, és egy "N" betűvel, ha nem elviselhető kockázatokat jelentenek. Mindehhez elsőként a táblázatban meg kell vonni a határt az elviselhetetlen és az elviselhető kockázatok között. Mindazok az értékpárok, amelyek ezen határtól felfelé és jobbra helyezkednek el, az N jelölést kapják. Mindazok az értékpárok, amelyek ettől a határtól lejjebb és balra helyezkednek el, az E jelölést kapják. Azokat az okokat, amelyek ezen határ rögzítéséhez vezettek, dokumentálni kell.

A 4+ (katasztrofális kár) és 0- (emberi számítás szerint kizárva) szélsőértékeket tartalmazó kombinációkat elkülönítve kell figyelembe venni.

Függetlenül a gyakorisági értéktől valamennyi olyan kombinációnak elviselhető a kockázata, amelyben nincs kárérték.

Kockázati mátrix a kockázatok jelölésére:

K	4+						
Á	4						
R	3						
É	2						
R	1						
T	0						
É	-						
K		0-	0	1	2	3	4
		GYAKORISÁGI ÉRTÉK					

Kockázati mátrix

Végül az eredményeket, a kárnagyság, a kárgyakoriság értékeit és a kockázatok leírását a résztvevők, a felelősök és a vezetők tudomására kell hozni, felül kell velük vizsgáltatni és ítéletet kell mondatni velük ezekről.
Csak az elfogadott eredményekkel lehet rátérni a munka következő szakaszára.

6.6 Kockázat-menedzselés

Az előző szakaszokban meghatároztuk és értékeltük az egyes rendszerelemeket fenyegető veszélyeket. Most meg kell határozni azoknak az intézkedéseknek a körét, amelyeket védelmükre hozunk. Utána az intézkedések hatékonyságát értékeljük, majd elemezzük, hogy milyen költségekkel járnak és milyen hasznot hoznak. Végül a maradványkockázat elemzésével zárul a szakasz.

Az intézkedések kiválasztása

Az intézkedéseket rendszerelemenként tekintjük át.

Infrastruktúra

Biztonsági intézkedések az infrastruktúra területén:

- **Védett elhelyezés:** az épület és azon belül a számítóközponté; villámhárító, informatikai készülékek védelme az indukált túlfeszültségekkel szemben.

- **Tűzvédelem:** a tűz keletkezésének megakadályozása, a kiterjedésének gátlása, a tűzjelzés megszervezése, tűzoltási eszközök beállítása.
- **Vízvédelem**: a helyiségek kijelölése a pinceszint fölött, vízlevezetők, szivattyúk beépítése.
- **Áram biztosítása:** áramingadozás, feszültségkiesés elhárítása, pl. szünetmentes tápegységek alkalmazásával.
- **Betörésvédelmi berendezések:** rácsos ablakok, speciális üvegezés, speciális zárak, behatolás érzékelők, stb. felszerelése.
- **Sugárzásvédelem**: teljes leárnyékolással, vezetékek vascsövekben történő elhelyezésével, optikai kábelek alkalmazásával.
- **Belépés ellenőrzés:** belépés és benntartózkodás szabályozása és ellenőrzése az üzem területére, az épületekbe a helyiségekbe, a belépés és ott-tartózkodás jegyzőkönyvezése; fizikai azonosítási eszközök (pl. kulcsok, chipkártyák, kitűzők, jelszavak) kiadása, regisztrálása és visszavétele, bejelentkezés lehetőségének zárolása hibás kísérletek után.
- **Hozzáférés-védelem:** a hálózatba való bejutás, valamint az adatokhoz, alkalmazói programokhoz, rendszerprogramokhoz való hozzáférés jogának (olvasás, írás) személyekhez való hozzárendelése; a jogok odaítélése, felépítése, a továbbadás szabályozása, ennek adminisztrációja,
- **Védelmi eszközök:** használatának szabályozása (pl. a rejtjelezés kulcsainak előállítása, átadása, cseréje), a védelmi berendezések működőképességének biztosítása; eljárás előírása katasztrófák esetére; az informatikai alkalmazások prioritásainak kijelölése.
- **Háttérkapacitás:** belső vagy külső háttér, illetve tartalék számítógép-kapacitás előkészítése szükségüzem esetére a szükséges hardver és szoftver konfiguráció rögzítésével.
- **Naplózás:** a rendszer eseményeinek, (pl. hardverhibák, automatikus újraindítás, hamis jelszóval való bejutási kísérletek) és a felhasználói tevékenységeknek jegyzőkönyvezése (például felhasználási idő, eszközök használata,

fájlokhoz való hozzáférés, adatátvitel); a jegyzőkönyv adatainak védelme illetéktelen hozzájutástól, utólagos módosítástól.

- **Ellenőrzés:** a biztonsági intézkedések betartásának ellenőrzési rendszere, kötelező reakciók előírása a szabályok megsértése esetén.

Biztonsági intézkedések a hardver védelmében

Hardver

- **Beszerzések:** elzárkózás a legújabb, még nem kipróbált termékektől, redundáns, hibatűrő konfigurációk; az ergonómiai szempontok figyelembevétele a hardverválasztásnál és - kiépítésnél (a képernyő villódzása, zaj elkerülése stb.).
- **Elhelyezés:** az informatikai készülékek koncentrált elhelyezése révén a belépés ellenőrzésének megkönnyítése (például valamennyi készülék egy biztonságos, feltétlenül kulccsal zárható helyiségben); csak centralizált beviteli/kiviteli eszközök alkalmazása a külső adathordozók számára; zárható házban elhelyezett, manipulációbiztos készülékek beszerzése, a készülékek rendszeres felügyelete biztonsági szempontokból.
- **Javítás:** Megállapodás a hardver-szállítókkal a garantált javítási, illetve cserélési feltételekről és határidőkről; rendszeres megelőző karbantartás, a különösen érzékeny komponensek megelőző cseréje, a pótalkatrészek készletezése
- **Üzemeltetés:** a hardver eszközök, illetve szolgáltatásaik igénybevétele csak a felhasználó azonosítását és hitelesítését követően legyen lehetséges; a magukra hagyott, bekapcsolt készülékeknél kényszerített kijelentkezés vagy a berendezés "blokkolása" (például képernyőzárolás); a fejlesztő és a végrehajtó számítógépek szigorú elhatárolása (felhasználói gépen nem folyhat szoftverfejlesztés).
- **Nyilvántartás:** az alkalmazott rendszer valamennyi készülékéről, azok műszaki állapotváltozásairól és konfigurálásáról folyamatos nyilvántartás (műszaki törzslap) vezetése.

Adathordozó

Biztonsági intézkedések az adathordozók védelmében

- **Adathordozó-adminisztráció kialakítása:** beszerzés, gazdálkodás, készlet- és használat nyilvántartás, selejtezési eljárás, az utánpótlás megszervezése stb.
- **Tárolás:** külön, belépés-ellenőrzéssel ellátott, megfelelő hőmérsékletű és páratartalmú adathordozó tároló helyiség kialakítása; katasztrófa-megelőzés céljából a másodpéldányok kiemelten biztonságos (más telephelyen történő) raktározása.
- **Mentések:** megelőző intézkedés az elöregedett és a már nem használt formátumok átmásolására; törlés a felszabadítás, kiselejtezés előtt.
- **Ellenőrzések:** a beszerzett adathordozók ellenőrzése az alkalmazásra való kiadásuk előtt; az előállított adathordozók ellenőrzése (újraolvashatóság); azok ellenőrzött kiselejtezése.
- **Előírások** az adathordozók felhasználói számára (védelem rongálódás ellen, külső jelölés, védelem jogosulatlan használattól stb.); privát adathordozók szolgálati célokra vagy fordítva történő igénybevételének tilalma; a kölcsönzés, a regisztrálás, a visszaadás eljárásának rögzítése.
- **Az adathordozók tartalmának védelme**: kódolás, rejtjelezés, olyan jelölés, amely nem tartalmaz közvetlen utalást a tartalomra, kódoló, dekódoló eszközök használata stb.

Dokumentumok

Biztonsági intézkedések a dokumentumok védelmében

- **Szabályozás:** a hardver és szoftver dokumentációk, kezelői utasítások beszerzésének, aktualizálásának, tárolásának, rendelkezésre állásának előírása, az eljárás szabályozása az informatikai dokumentumok másolása, kölcsönzése esetére; a dokumentumok sértetlenségének biztosítása, a selejtezési eljárás rögzítése.
- **Nyilvántartás:** a szükséges dokumentációk, szoftverek és hardverek nyilvántartása valamennyi informatikai alkalmazás esetére (programok, adatállományok, pótlóla-

gos szoftverek, beviteli és kiadási készülékek, tároló- és időigény stb.).

Szoftver

Biztonsági intézkedések a szoftver védelmében

- **Beszerzés:** elfogadható biztonsági osztályú rendszer kiválasztása minőségtanúsítványa alapján; új, instabil szoftver verziók bevezetésének késleltetése a megfelelő minőségellenőrzési eredmények megszületéséig; ismert hibájú szoftver használatának elkerülése, illetve - szükséghelyzetben - gondosan ellenőrzött használata.
- **Ellenőrzés:** a teljes szoftver sértetlenségének rendszeres ellenőrzése; szoftver minőségellenőrzés különálló számítógépen lefuttatott teszt segítségével; a hardver és a szoftver funkcionális tesztprogramjainak rendszeres használata (például a fájlrendszer konzisztenciájának rendszeres ellenőrzése); a rendszer- és alkalmazói programok sértetlenségének védelme helyi hálózatokban központi szerverről történő programindítás segítségével.
- Rendszeres vírusellenőrzés.
- Idegen szoftverek ellenőrizetlen bevitelének tilalma.
- Privát szoftverek szolgálati célokra, illetve a szolgálatiak privát célokra való alkalmazásának tilalma.
- Többszintű hozzáférési rendszer használata (például külön jogosultság az adatbázis-rendszerben, levelező rendszerben stb.).
- Rendszer-adatállományok és parancsok használatának korlátozása.
- Intézkedések a karbantartási munkálatok előtti és utáni tevékenységekre (pl. az üzemi rendszer betöltése külső adathordozóról) a szoftver sértetlenségének és bizalmasságának biztosítása érdekében.
- A felhasználó általi szoftverfejlesztés megakadályozása.
- A felhasználói és rendszerszoftverek törzspéldányainak biztonságát szolgáló tárolási, kezelési előírások.

Biztonsági intézkedések az adatok védelmében

Adatok

- **Üzemviteli előírások:** az adatmentésre, helyreállításra, őrzési időtartamra, az adatbeviteli, kiadási műveletekre, adatállományok tárolása kódolással, ellenőrzőösszeg alkalmazásával, digitális aláírással, redundáns tárolással, stb.
- **Tranzakció-kezelés** alkalmazása, adatvesztés elleni biztosítás fájl-szerverrel osztott rendszerekben.
- **Az adatbevitel ellenőrzése**: az alkalmazói programokban szereplő formátum, valamint konzisztencia ellenőrzésekkel, kétszeri adatrögzítéssel, hibajavító kódok alkalmazásával, stb.
- **Hozzáférés-jogosultságok** ellenőrzése input/output műveleteknél, többlépcsős ellenőrzési lehetőségek kihasználására.
- Rejtjelezés alkalmazása.

Kommunikáció

Biztonsági intézkedések a kommunikáció védelmében

- **Az adatátviteli vezetékek** és a kommunikációs kapcsolatok védelme észrevétlen bejutástól (például nehezen hozzáférhető kábelcsatornák, ellenőrizhető nyíltszíni vezetések révén).
- **A kábelkoncentráció kerülésével** védekezés tűz- és vízkárok kihatásai ellen.
- **Azonosítás és hitelesítés** a kommunikáló feleknél és egy-egy üzenet küldőjénél.
- Erőforrások hálózaton keresztül való hozzáférésének ellenőrzése.
- Az adatforgalom jellemzői, valamint az adattartalom, vagy annak részei bizalmasságának védelme.
- Üzenet, illetve üzenetfolyam sértetlenségének védelme.
- Az üzenet forrásának és az üzenet kézbesülésének bizonyítható igazolása.
- Védelmi eljárások kommunikációs hálózatba való csatlakozásnál, például tűzfal alkalmazása.

- Biztonsági intézkedések beépítése helyi hálózatokban a topológia (például gyűrű, busz, csillag), az átviteli eszközök (például rézkábel, koaxiális kábel, optikai kábel), valamint az eljárások kiválasztásánál (védelem új állomások észrevétlen csatlakozása, az átvitt adatok lehallgatása, stb. ellen).
- A hálózati rendszerszoftver védelme manipulációk ellen (például a központi szerverről történő letöltéssel).
- A helyi és külső hálózat közötti átmenet logikai kontrollja, például az üzenetek szűrésével a kapcsolódó számítógépnél ("gateway").

Személyek

Biztonsági intézkedések a személyek védelmében

- Ergonómiailag korrekt munkahelyek kialakítása (például a zajt, a világítást, az ülőhelyeket illetően).
- A motiváció fenntartása erkölcsi és anyagi oldalról.
- Olyan munkahelyi szervezet, amely stresszmentes munkavégzést tesz lehetővé.
- Az illetékességek rögzítése különféle szabályok kiadására, aktualizálására, betartásuk ellenőrzésére és az érintettek körének kijelölésére vonatkozóan.
- Informatikai alapkiképzés (elméleti és gyakorlati) valamennyi felhasználó számára folyamatos szakmai továbbképzés.
- A biztonságtudat kialakítása és megtartása.
- Személyre szabott képzés a biztonsági kérdésekről, a jogi helyzetről, az érvényes szabályozásokról.
- Kezelési utasítások kiadása az informatikai alkalmazásokhoz (például bevitel formái, paraméterek általi vezérlés, reakciók a hibajelekre, a használandó adathordozók, startidőpontok stb.).
- A rendszerkezelésre vonatkozó előírások, (például manuális naplóvezetés, felügyeleti feladatok stb.).
- Eljárási utasítások, előírások valamilyen hiba vagy támadás felfedezése esetén.
- A személyek és személyek csoportjainak hozzárendelése a számítógépekhez és hálózatokhoz szerepeik alapján.

(pl. csak a Gazdasági osztály dolgozói indíthatják el a könyvelési programot.)

- Távozó (kilépő, más munkakörbe kerülő) személyektől a jogosultságok, jelszavak visszavonása, az általa ismertek megváltoztatása, a dokumentumok visszavétele, az ismeretei átadásának (utódlásának) megszervezése.

A költség/haszon arány elemzése

Az eljárásnak ebben a lépésében történik meg az intézkedések költségének meghatározása, valamint az intézkedések elfogadhatóságának vizsgálata.

Ráfordítások, hatás

Egyenként meg kell állapítani a hozott biztonsági intézkedések költségeit. Ehhez hozzátartozik a teljes ráfordítás, amely az adott intézkedés bevezetésével és megvalósításával keletkezik, (pl. beszerzési költségek a személyzet iskolázása, a munkafolyamatok megváltozása miatt fellépő költségek).

Ezután minden egyes intézkedés költségeit össze kell mérni azok hatásosságával. Amennyiben a költségek és a hatások pénzösszegekben megadhatók, akkor a megtakarításokból, azaz a csekélyebb kár elvárhatóságából adódó haszon nagyobb kell hogy legyen, mint a ráfordított költség.

A maradványkockázat elemzése

A lépés tartalma az elfogadható költségű intézkedésekkel nem csökkenthető mértékű kockázatok kezeléséről hozott döntéseknek, azok hátterének elemzése, dokumentálása. A lépés célja az, hogy a kockázatokat elviselhető mértékűre korlátozzuk és egyetlen elviselhetetlenül magas értékű kockázatot se fogadjunk el.

Amennyiben még egy vagy több kockázat elviselhetetlen, szükség van arra, hogy hatékonyabb intézkedéseket vagy több intézkedést válasszunk ki. Olyan maradványkockázat, amely elviselhetetlen, e lépés lezárását követően nem maradhat. Az is elképzelhető viszont, hogy az előirányzott védelem túlzott, azaz a kockázatot jóval az elviselhetőségi határ alatt tartja. Ilyenkor meg kell fontolnunk, hogy egyszerűbb vagy kevesebb intézkedéssel elérhető-e egy elfogadható maradványkockázat.

Ennek során figyelembe kell vennünk az intézkedések közötti függőségeket.
A maradványkockázat elemzésének a célja nem az, hogy valamennyi kockázatot amennyire csak lehetséges csökkentsük és kapcsoljuk ki, hanem az, hogy a kockázatokat elviselhető mértékűre korlátozzuk és egyetlen elviselhetetlenül magas értékű kockázatot se fogadjunk el.
Amennyiben még egy vagy több kockázat elviselhetetlen, visszatérünk az intézkedések kiválasztásához, hogy hatékonyabb intézkedéseket vagy több intézkedést válasszunk ki. Olyan maradványkockázat, amely elviselhetetlen, e lépés lezárását követően nem maradhat. Az is elképzelhető viszont, hogy az előirányzott védelem túlzott, azaz a kockázatot jóval az elviselhetőségi határ alatt tartja. Ilyenkor meg kell fontolnunk, hogy egyszerűbb vagy kevesebb intézkedéssel elérhető-e egy elfogadható maradványkockázat. Ennek során figyelembe kell vennünk az intézkedések közötti függőségeket.

6.7 Befejező szakasz

Az informatikai biztonsági tervezésnek befejezésekor célszerű az elvégzett munkát egy dokumentumban összefoglalni, és ezt a vezetőséggel jóváhagyatni.
A terv elkészülte és jóváhagyása nem jelenti egyben az informatikai biztonság megteremtését. Mint ahogy korábban már kifejtettük, az informatikai biztonság megteremtésének ez csak alapvető, de korántsem kizárólagos teendője. A későbbiekben gondoskodni kell a tervben leírtak megvalósításáról, folyamatos érvényesítéséről, felülvizsgálatáról és aktualizálásáról. A szervezet tevékenységi körétől és nagyságától függően különböző mélységekben lehet a tervet elkészíteni. Az alábbiakban közlünk egy lehetséges felépítést, amit az ITB 8-as ajánlása javasol:

Az informatikai biztonsági terv tartalmi felépítése

A szervezet informatikai stratégiájának biztonsági vonatkozásai
A védelmi igény leírása
Az alkalmazó biztonsági követelményei.

Az érték/kár skálaértékek jelentése.
Az informatikai alkalmazások és adatok értékeikkel.

A fenyegetettség-elemzés eredményei

A rendszerelemek listája a használatbavétel céljának leírásával.
A gyenge pontok és a releváns fenyegető tényezők listája.
Az adott intézkedések és azok kölcsönhatásai.

A kockázatelemzés eredményei

A rendszerelemek listája alap-fenyegetettségenként egy kárértékkel.
A fenyegető tényezők listája kárértékekkel.
A skálaértékek jelentése a gyakoriságra nézve.
A fenyegető tényezők listája gyakorisági értékekkel.
A fenyegető tényezők és a rendszerelemek listája kockázatértékekkel.
Kockázat-áttekintés.
Döntési tábla a kockázatok jelöléséhez megalapozással.

Az intézkedések kiválasztása

Az elviselhetetlen kockázatok listája a "hol vagyunk" állapotban.
A kiválasztott intézkedések listája, azok kölcsönhatásai.
Kihatások az informatikai rendszer üzemelésére.
Összeegyeztethetőség törvényes és üzemi előírásokkal.
A kiválasztott intézkedések hatékonysága.
A kiválasztott intézkedések költségei.
A kiválasztott intézkedések elfogadhatósága.
A kockázatok listája "szükséglet" állapotban.

A tervezés részletes ismertetése az ITB 8. számú ajánlásában található.

Ellenőrző kérdések

1. Az informatikai biztonság tervezése milyen szakaszokból áll?

2. Milyen tevékenységeket kell elvégezni a védelmi igények feltárásánál?

3. Mit jelent a fenyegetettség elemzés?
4. Milyen rendszerelemeket különböztetünk meg?
5. Az informatikai rendszer mely részei tartoznak az egyes rendszerelemekhez?
6. Milyen gyenge pontjai és fenyegető tényezői vannak az egyes rendszerelemeknek?
7. Mi a kockázatelemzés?
8. Milyen lépésekből áll a kockázat menedzselés?
9. Milyen intézkedések hozhatók az egyes rendszerelemek védelmére?
10. Mit értünk költség-haszon elemzésen?
11. Mit jelent a maradványkockázat elemzése?

Jegyzetek:

7. Programozott kártevők

Amikor adatbiztonságról beszélünk, a legtöbb embernek a vírusok jutnak az eszébe. Nem véletlen, hiszen ezek az ártó szándékú programok rengeteg kárt és bosszúságot okoznak. Eleve azzal a szándékkal íródtak, hogy mások munkáját vagy eszközét tönkretegyék. A vírus nem más, mint programsorokba öntött rosszindulat.

Általában minden programozott kártevőt vírusnak neveznek, de viselkedésük alapján több csoportba oszthatók. A területtel foglalkozó szakemberek többféle tipológiát dolgoztak ki, több szempont szerint osztályozták a programkártevőket. Az egyik ilyen osztályozás a következő:

Osztályozás

- vírusprogramok
- vírusgenerátorok
- trójai programok
- programférgek
- logikai bombák
- hátsó ajtók, kiskapuk és csapdák,
- baktériumok és nyulak

Ezeknek a programoknak egy része hasznos segédprogram is lehetne. (Például a kiskapuk jól használhatók nyomkövetésre, a programférgek alkalmasak lehetnek számítások megosztására.) Ami miatt mégis a kártevők között említjük őket, az azért van, mert rombolási céllal hozták létre őket.

7.1 Típusok

Nézzük meg az egyes csoportokat részletesen:

Vírusok

A számítógépvírus olyan program, amely képes önmagát reprodukálni, úgy, hogy más programokhoz valamilyen módon hozzáépül, anélkül, hogy ezt a felhasználó ellenőrizni tudná.

A vírus olyan programrészeket tartalmaz, amely más programokhoz kapcsolja a saját futtatható kódját. A vírus önmagában életképtelen, működését csak a megfelelő hardver-, és szoftverkörnyezetben, más programokba beépülve képes biztosítani. A számítógépvírusok rendkívül gyorsan képesek terjedni. Számítógép-hálózatokon, vagy floppy lemezeken keresztül átkerülhetnek más számítógépekre, ahonnan szintén tovább terjedhetnek. Az "eredményesebb" terjedés érdekében a vírust programozója úgy készíti el, hogy egy ideig "lappang", és csak akkor „aktivizálódik", vagyis támad, amikor már több helyen előfordul.

Vírus-kritériumok

A víruskritériumok, a vírusok főbb jellemzőit határozzák meg. Több feltétel együttes teljesülése esetén minősíthető egy program vírusnak. Ezek a következők:

- a saját kód sokszorozásának képessége,
- a rejtőzködés alkalmazása,
- adott feltételek teljesülésére való figyelés,
- különböző mellékhatások megjelenése.

Nem tekinthetünk vírusnak néhány olyan speciális programtípust, melyek a víruskritériumok közül egy vagy több pontnak nem tesznek eleget.

Platform-függőség

A vírusok, mint minden számítógépes program, csak adott környezetben működőképesek. A PC-ken futó programokat megfelelő emulátor nélkül hiába indítanak el más típusú számítógépen, így a PC-re fejlesztett vírusok is csak PC-ken fertőznek. Az ugyan nem zárható ki, hogy más platformokra is átkerülhessenek PC-s víruskódot tartalmazó programfájlok, de ahogy a gazdaprogramok sem futtathatók más rendszerű gépeken változatlan formában, úgy a vírusoknak sincs esélyük erre. Az operációs rendszerek nagy különbséget jelentenek a vírusok számára. A platformfüggőség alól kivételt képeznek az 1995 őszétől megjelenő makrovírusok.

Makrovírusok

A Word makrovírusok megjelenése egy új fejezetet nyitott a vírusok terjedésében. Addig csak a futtatható fájlokat támadták a vírusok. Szövegszerkesztővel szinte minden felhasználó dolgozik. A dokumentum fájlokat többször továbbítják, mint a futtatható fájlokat. Elég egy lokális hálózatban működő levelezési rendszerben egy mindenkinek szóló levelet fájlban szétküldeni, már mindenki meg is kapta a vírust. A Word makrovírus a *normal.dot*-ot fertőzi meg, és a fertőzés időpontja után minden új dokumentum, és megnyitott régi dokumentum is vírusos lesz. Az új fájlokat a Word dot-ként akarja elmenteni, és több üzenete küld, hogy a mentés nem lehetséges. A Word menüjéből eltünteti az Eszközök/Makro alparancsot. Az újabb generációk más hibajelzéseket is produkálnak.

Vírusgenerátorok

Vírusgyártó automaták

A vírusok mellett egyre többet hallani a vírusgyártó automatákról. Ezek olyan programok, programcsomagok, amelyek segítségével több-kevesebb programozói tudással ezerszámra lehet új vírusokat létrehozni. A vírusírás automatizálása nem rég kezdődött. A legelső próbálkozás a VCS (Virus Construction Set) volt, amely olyan vírusokat készített, melyek kódjaikban nem különböztek jelentősen egymástól, csak eltérő dátumokon a felhasználó által megadott szövegeket, üzeneteket írták ki a képernyőre és a *config.sys*-t, valamint az *autoexec.bat*-ot tették tönkre. A későbbiek során már jóval komolyabb vírusíró automaták is születtek.

Trójai programok

A trójai programok nevüket a görög mondában szereplő Trójai falóról kapták, olyan programok, melyek járulékos funkciókat fűznek egy programhoz, maguk csak álcázásra szolgálnak.
Esetenként igen nehéz felismerni őket, mivel gyakran egy közismert program mögé rejtik el, és rendszerint installáláskor jutnak a rendszerbe. A trójai programok abban különböznek a vírusoktól, hogy nem tartalmaznak szaporító rutint a kódjukban.

Másolásvédelem

Ezt a típust gyakran védelmi célból hozzák létre az időnként elkeseredett szoftverfejlesztők. Az illegálisan másolt, jogosu-

latlanul használt szoftverek eléggé gyakori jelenségnek számítanak nem csak Magyarországon. Ez a tevékenység a fejlesztőket jelentős bevételtől fosztja meg, ezért minden eszközt megpróbálnak bevetni az illegális használat megakadályozására.

A másolásvédelemmel ellátott szoftver csak valamilyen meghatározott feltételek között hajlandó működni (például: csak egy adott kártyával együtt, az eredeti programot tartalmazó lemeznek benn kell lennie a meghajtóban, stb.). Ha a program nem a neki megfelelő, és "előírt" környezetet érzékeli, vagy nincs meg valamilyen a program futtatásához szükséges feltétel, akkor aktivizálódik a romboló rutinja és tönkreteheti a lemezen tárolt adatokat, és programokat. A másolásvédelemnek van egy szelídebb fajtája, amikor is ha az eredeti program nem a neki megfelelő környezetet ismeri fel, akkor engedi hogy elinduljon.

Ezek a módszerek, bár alkalmazásuk indítéka érthető, nem szerencsések. Egyrészt az ilyen jellegű védelem feltörése szakmai kihívást jelent a programozóknak, a magas szintű szakmai tudás bizonyítékaként kezelik. Másrészt ez a módszer elriasztja a vevőket a szoftver megvásárlásától. A másolásvédelem nagy szoftverfejlesztőknél már nem szokásos védekezési forma, egyéb marketing fogásokkal helyettesítik (pl. viszonylag alacsony ár, részletes dokumentáció, tutorial programok, a regisztrált vevőknek széleskörű support, hot line segítség, az újabb verziók töredék áron való értékesítése a régebbi verziókkal rendelkezők számára, oktatási intézmények részére kedvezmény, stb.). Léteznek nem károkozó, tisztességes lopásvédelmi eljárások is. Ilyen például, hogy a programot egy "beégetett" sorszámmal, vagy a felhasználó nevére szóló dedikációval látják el, és így nyomon követhető az illegálisan forgalmazott példányok eredete

Hálózat-felderítő

Egy másik típusa a trójai programoknak a hálózatot felderítő programok: Ha nincs semmiféle, vagy elegendő joga a felhasználónak egy hálózathoz, akkor beépíthet olyan rutint a számítógépébe, amely figyeli hogy milyen jelszóval jelentkezik be valaki, majd egy számára elérhető állományba ezt a jelszót letá-

rolja. Ezek után már hozzáférhetővé válnak az előzőleg említett bejelentkezett felhasználó adatai.

Programférgek (Worms)

A programférgek olyan programok, amelyek önmagukban is futóképesek, és gépről gépre vándorolnak egy számítógép hálózaton keresztül

Hálózati kártevők

Lehet hogy több részből állnak, amelyek teljesen különböző számítógépeken futnak. A programférgek nem változtatnak meg más programokat, viszont tartalmazhatnak olyan programokat, melyek képesek erre. Programférget meglehetősen nehéz írni, viszont rengeteg kárt tud okozni jelenlétével. Az ilyen jellegű programok kifejlesztése nem csak hálózatos körülményeket igényel, hanem olyan programozót is, aki a hálózati szolgáltatásokon, és eszközökön felül pontosan ismeri az operációs rendszereket is, melyeket majd programja a terjedése során elérhet, hiszen csak így biztosíthatja életképességét minden környezetben.

Lebénítja a hálózatot

Az első generációs férgek hatása egyszerű fájlbővülés volt, ami drasztikusan csökkentette a szabad tárolókapacitást. Ennek következtében lebénult a számítógép vagy a hálózat. A férgek nem ellenőrizték, hogy fertőzendő fájl tartalmaz-e már fertőzést, így a programféreg többször is rákerülhetett a gazdaprogramra. Nem volt ritka, hogy egyetlen .EXE fájlban száznál is több példányban megbúvó férget találtak. A programférgek nem tekinthetők vírusnak, mivel önálló programok, és nincs szükségük arra, hogy más programokba beépülhessenek.

Híres elsőgenerációs féreg volt a *Cristmas Tree*, amely az IBM saját hálózatán terjedt el. A nevében is szereplő karácsonyfa, a féreg felbukkanásakor megjelt a felhasználó képernyőjén egy olyan javaslattal, hogy küldjék tovább.

„I Love You"

Az új generációs programférgek már romboló rutinokat is tartalmazhatnak. Jó példa erre a 2000. május 3-án elszabadult, az „I Love You" névre hallgató levélféreg. Előző évben volt már egy hasonló, ami „Melissa" néven hiresült el. Az „I Love You"

a Fülöp szigetekről indult, a Microsoft Outlook levelező rendszer gépeit támadta. A levélféreg lebénította az angol parlament, a BBC, az USA szenátusa, a CNN hírtelevízió levelezési rendszerét. Magyarországon több minisztérium és állami hivatal rendszerét le kellett állítani.

Mutációk

2001-ben megjelent az *Kurnyikova*, a *Naked Wife*, majd júliusban a *W32.Sircam* nevű levélféreg. Ezeket követték a *Blue Code*, az *Aliz*, a *NIMDA*, valamint a nagyon sok kárt okozó *Code Red*, a *KLEZ.E* és a *KLEZ.H*.
2002-ben kicsit kevesebb új féreg jelent meg: a *Bridex*, *Worm.Roron*, *Winevar*, a *KilOnce*, a *Galil*, a *P2P.Lolol*.
2003. elején hatalmas robajjal tűnt fel a *Slammer* féreg, mely a Microsoft SQL 2000 szervereinek sebezhetőségét kihasználva bénította meg az Internetet. Szintén januárban jelent meg a később hírhedtté váló *Sobig* első variánsa, februárban pedig a *Lovgate* mutatta meg, milyen is egy féreg és egy trójai program kombinációja. A soron következő hónapokban a "leleményes" férgeké volt a főszerep: a *Ganda* az iraki háborút és az emberi hiszékenységet (social engineering) használta ki céljaira, míg a *Fizzer* e-mailek mellékleteként és a KaZaa P2P hálózatán is terjedt. Augusztusban vitték véghez a legnagyobb pusztítást: a *Sobig.F*, *Blaster*, *Welchi* és *Mimail* férgek sebesen terjedtek, és hatalmas károkat okoztak.
Az új hálózati féregre jellemző, hogy a felhasználó beavatkozása nélkül képesek megfertőzni a gépeket, ezen tulajdonságuk pedig különösen szaporává és rejtőzködővé teszi őket. A felhasználók számára nincs egyértelmű vizuális jele annak, hogy hálózati féreggel fertőződött a rendszerük. Ez az egyik legveszedelmesebb jellegzetességük.
Idén nagy találgatások folytak a spamek és vírusok kapcsolatáról. Például a Sobig egy olyan komponenst is telepített, melyet elképzelhető, hogy spammerek használtak fel idegesítő leveleik küldözgetésére.

A legjelentősebb vírusforrások Kína, Tajvan és Dél-Korea. 2001 szeptembere óta Észak-Amerikában alig íródott vírus: a társadalom kevésbé elnéző hozzáállása a bűnözéshez lényege-

sen csökkentette az Egyesült Államokból származó vírusok számát. [1]

Hogyan védekezzünk ?

Hogyan védekezzünk a levélférgek ellen?

- Ne nyissuk meg olyan levelek mellékleteit, amelynek ismeretlen a feladója. A legkisebb gyanú esetén inkább töröljük ki a levelet!
- Ha már megtörtént a baj, azaz megnyitottuk a mellékletet, a gépünk fertőzött lett. Ilyenkor a gépet ne indítsuk újra és ne kapcsoljuk ki, hívjunk specialistát!
- Ne vegyük komolyan a vírusra figyelmeztető leveleket és ne küldjük tovább. Egyáltalán: ne hallgassunk az olyan levelekre, amelyek - általában karitatív felhívás kapcsán - arra ösztönöznek, hogy minél több helyre küldjük őket tovább. Az esetek döntő részében jóakaratunk áldozatai leszünk, és éppen az ártó szándékú programozott kártevőket terjesztjük.

Logikai bombák

A logikai bombák olyan programok, amelyek egy bizonyos ideig megbújnak az általunk használt szoftverekben, és egy adott feltétel teljesülésére elszabadulnak. Ekkor végrehajtanak valamilyen eljárást, ami voltaképpen nem feladata annak az általában hasznos segédprogramnak (pl. tömörítők), amibe gondos kezek elrejtették.

Logikai bombákat általában szoftverfejlesztők (akiknek már néhányszor nem fizették ki a munkáját, jogosulatlanul lemásolták a programját) ágyaznak be a programokba. Ezzel azt akarják elkerülni, hogy a szerződésben meghatározott fizetési vagy egyéb feltételek nem teljesítése esetén csak hosszas huzavona után, vagy sohasem juthassanak a pénzükhöz. A feltétel teljesülésekor a szoftver üzenetet küld a felhasználónak, hogy vegye fel a kapcsolatot a fejlesztőkkel, különben nem biztosított a szoftver további működése, és esetleg adatvesztés állhat be.

[1] Elhangzott az F-Secure sajtókonferenciáján, Budapest, 2003. január. 28.

Aktivizáló feltételek

A logikai bombát aktivizáló feltételek igen sokfélék lehetnek. Megkövetelhetik adott állományok létezését, vagy azok hiányát, egy adott időpont elérését, vagy azt, hogy egy meghatározott felhasználó futtassa a programot. Egy logikai bomba ellenőrizheti például, hogy kik vannak bejelentkezve, mely programok futnak pillanatnyilag a rendszeren.
A logikai bombák ellen úgy tudunk a leghatásosabban védekezni, ha nem telepítünk tesztelés, és ellenőrzés nélkül szoftvereket a számítógépünkre (és időben kifizetjük a szoftverfejlesztő számláit).

Hátsóajtók, kiskapuk és csapdák

Bennfelejtett egérutak

A hátsóajtók, kiskapuk vagy csapdák olyan kódrészletek, melyeket azért építenek bele egyes alkalmazásokba, vagy operációs rendszerekbe, hogy biztosítsák a programozók számára ezen rendszerek elérését, anélkül, hogy végig kellene járniuk az egyébként normális hozzáférési utat. Ezeket a programrészleteket főleg alkalmazásfejlesztő programozók írják, akiknek szükségük van a kód nyomkövetésére, működésének figyelésére a fejlesztés közben. A legtöbb hátsó bejáratot olyan programokban helyezik el, amelyek egyébként normális körülmények között csak hosszadalmas eljárások, beállítások, különböző értékek beírása után hajlandóak csak elindulni.
A program nyomkövetésekor a fejlesztőknek minden speciális privilégiummal rendelkezniük kell. A programozók ezzel azt is biztosítják, hogy van egy módszer a rendszerbe való bejutásra akkor is, ha a normális indítás valamilyen hiba fellépése miatt egyébként lehetetlen. Ezeknek a bejáratoknak a kódjai vagy bizonyos karaktersorozatokat ismernek fel, vagy pedig egy adott felhasználói azonosítóra lépnek működésbe. Ezek után pedig speciális jogokat biztosítanak a felhasználónak. A kiskapuk csak akkor válnak veszélyesekké, fenyegetésekké, ha jogosulatlan felhasználók, programozók arra használják fel őket, hogy engedély nélkül férjenek hozzá rendszerekhez, kódrészletekhez. A hátsó ajtók elleni védelem nagyon bonyolult, azonban ha csak megbízható forrásból származó szoftvereket használunk kevésbé vagyunk kitéve a veszélynek.

Baktériumok és nyulak

Erőforrás lefoglalása

A baktériumok, vagy más néven nyulak olyan programok, amelyek csak önmagukról készítenek másolatot. Nem kifejezett céljuk a számítógépes állományok rongálása. Egy tipikus baktérium (multitaszkos környezetben) általában elindítja magát két példányban, vagy létrehoz önmagáról két újabb másolatot. Ezután mindkét másolat reprodukálja önmagát két-két példányban, és így tovább. Így ezek a programok exponenciálisan szaporodva lefoglalják a gép processzor idejének, memóriájának és lemezkapacitásának jelentős hányadát, ezáltal lehetetlenné teszik, hogy a felhasználó az erőforrásokat hatékonyan kihasználhassa. A támadásoknak ez az egyik legrégebbi módszere. Az erőforrás nélküli számítógépek különösen ki vannak téve az ilyen jellegű támadásoknak.

7.2 Hogyan keletkeznek a számítógépvírusok?

A számítógépvírusok tervszerű fejlesztés eredményeként jönnek létre. Vannak olyan elgondolások, hogy egyszerű programtöredékek lehetnének, melyek véletlenül keletkeznek és szabadulnak el egy program sérülésekor, de ez nem valószínű. A vírusok nem is elsősorban műszaki, programozás-technikai, inkább társadalmi-szociológiai és etikai probléma. Leginkább az ember az, aki közvetve vagy közvetlenül fenyegeti a számítógépek adatbiztonságát. A témában két kérdés izgalmas:

- Kik és milyen okból fejlesztenek vírusokat?
- Milyen csatornákon keresztül juttatják el programjaikat a kiszemelt célpontokhoz?

Nem mind zseni

A köztudatban az a tévhit él, hogy a vírusokat nagy tudású szakemberek, majdhogynem zsenik írják. Romboló céljaik mögött pedig bűnöző, esetleg terrorista szervezetek állnak. A valóság azonban az, hogy az első vírusok létrehozása még valóban ötletes szakemberekhez köthető, azonban ma már nem kell olyan nagy szaktudás egy vírus létrehozásához, illetve ez a tudás már sokkal könnyebben megszerezhető, mint régebben.

Manapság bárki hozzájuthat (ha akar, ha nem) egy-két vírushoz, és működésük megértéséhez is minden információ rendelkezésre áll. Ha pedig már adott egy példa, sokkal könnyebb újabb vírusokat elkészíteni az adott minta alapján. Ezt bizonyítja az is, hogy egy eredeti vírusnak több változata, úgynevezett mutánsa létezik. Ezek a mutánsok úgy keletkeznek, hogy egy vírust valaki visszafejt, majd kis változtatásokkal a saját elképzeléseihez igazítja és újra lefordítja. Néhány ismertebb vírusnak több ilyen leszármazottja is van (például a *Péntek 13*-nak a szombat 14-én, és csütörtök 12-én aktivizálódó változata).
A gyakorlatban a vírusok többségét programozni tanuló diákok, egyetemisták, esetleg munkahelyi alkalmazottak készítik. Ők azok, akik akár otthonukban programozva rengeteg szabadidővel, ötlettel rendelkeznek. A vírusokon keresztül mutatják meg a nagyvilágnak, hogy már mire képesek. Általában a legtöbbjük terméke nem tartalmaz romboló funkciókat, kártevésük legtöbbször abból adódik, hogy a készítő csak most tanult meg programozni, és így a vírus tele van hibákkal.
Arra is van példa, hogy a vírusokat ugyanazok írják akik az antivírus programokat.
Nézzünk néhány példát, hol vannak a vírusforrások:

Egyetemi kutatólaborok

Kutatás

Az első vírusokat az egyetemeken dolgozó programfejlesztők dolgozták ki abból a célból, hogy bebizonyítsák lehetséges olyan számítógépes programot alkotni, amely képes a saját kódját manipulálni és más programok futtatható kódjába beépülni. Ezek a vírusok csupán csak kutatási célból készültek. Ma is működnek egyetemeken kutatólaboratóriumok, ahol a vírusok terjedési, fertőzési mechanizmusait analizálják, azonban az ilyen laboratóriumok száma igen kevés és teljesen izoláltan működnek. Eredményeiket csak kutatási célokra használják fel.

Katonai kutatólaboratóriumok

Hadviselés

Már régen tudunk hadviselési vagy éppen technológiaellenőrzési céllal folyó víruskutatásokról. E téren persze csak nyomokból, utalásokból lehet információhoz jutni. Az USA-

ban már az ötvenes évek végén, később Németországban is foglalkoztak olyan vírusok előállításával, amelyek megbéníthatják az ellenség vezérlőrendszerét. Ezeknek a vírusoknak a fejlesztői a nagygépes rendszerek, illetve a bonyolult vezérlőrendszerek ellophatatlanságát tűzték ki célul. Az arab-öböl háború is megélénkítette a számítógépes vírusok piacát. Ekkor jelent meg például a *Szaddam* vírussorozat, és az *Israeli defence* nevű, kifejezetten hadműveleti célra kifejlesztett vírus. Az öbölháborút követően több forrás is megerősítette, hogy az iraki légvédelem működésképtelensége többek között egy speciálisan ellenük fejlesztett vírusnak volt köszönhető. A *Fish6* és a *Whale* vírusokat folyamatos beépített mutációs lehetőségeikkel ideális hadviselési vírusokká lehet fejleszteni. Mindenesetre a katonai laborok rendkívül zártan működnek, onnan nem kerülhet ki véletlenül vírus.

Terrorista szervezetek programfejlesztői

Terrorizmus

A fegyverrendszereket világszerte egységes irányítási rendszerbe kötött számítógépek vezérlik. Kisebb méretekben ugyan, de ugyanezt a technikát alkalmazzák a terroristák is. Ebben az esetben a cél az, hogy az ellenség kommunikációs rendszerébe bekapcsolódva az adatátviteli vonalakon (rádiós, műholdas) keresztül csempésszék be akár egyetlen helyre is a vírust, amely ott könnyen elszaporodhat és tönkreteheti a számítógépes rendszert. Ha már előre beépítették a vírust a rendszerbe, akkor hasonló módon az adatátviteli csatornán keresztül lehet aktivizálni. Az egyik ilyen híres hadviselési vírus a *Jeruzsálem* volt, mely egy palesztin ellenőrzés alatt álló titkos laboratóriumban készült az izraeli állami számítógéprendszerek megbénítására. Sajnos az ilyen titkos laborokból már számtalan vírus kiszabadult a BBS-ekre és az Internetre is.

Munkahelyi alkalmazottak

Bosszú, zsarolás

A munkahelyi alkalmazottak elsősorban az általuk már jól ismert rendszerek gyengeségeit kihasználva okozhatnak károkat a munkahelyükön. Mivel mindenképpen igyekeznek biztosítani védett státuszukat, néhányan már a felmondási idő alatt vírusfejlesztéssel és telepítéssel igyekeznek megkeseríteni egykori

munkáltatójuk életét. Nem egy olyan eset ismeretes, amikor a korábban elbocsátott programozót csak azért fogadták vissza, mert egyedül ő tudta megszabadítani a rendszert az általa elhelyezett időzített bombáktól. Éppen ezért a munkahelyen főként a saját alkalmazottakra kell odafigyelni. A hálózatból kívülről behatolók és vírusterjesztők, nagyobb publicitást kapnak, és jobban felhívják a figyelmet a gyenge pontokra, de az igazi veszély az intézményen belül van.

Számítógépüzlet tulajdonosok, szervizelők

Munkaszerzés

A számítógépek szervizelésével foglalkozó szakemberek is érdekeltek lehetnek egy-egy vírus terjesztésében, így tevékenységük folytán a javításra szoruló gépek száma mesterségesen is növelhető. Például Magyarországon az első vírusprogramot egy számítógépek javításával foglalkozó szakember terjesztette, aki ezzel a trükkel ért el magának nagyobb forgalmat, könnyű kereseti lehetőséget. Programvírusa ugyanis olyan külső pályára vitte a lemezolvasó fejet, ahonnan csak kézzel, a lemezegység szétszedésével lehetett visszahozni.

Számítógépes klubok

Hobby

A klubok gyakran osztanak meg egymás között ötleteket, információkat vírusokkal kapcsolatban. Az egyik legismertebb vírusokkal foglalkozó klub a *Chaos Computer Club* Hamburgban, mely létrehozott egy vírusgyártó automatát Atari típusú számítógépre. Ez a program lehetővé teszi, hogy segítségével menüből irányítva beállíthassa a felhasználó a létrehozandó vírus tulajdonságait.
Magyarországon is működtettek ilyen jellegű cserefórumot, és néhány számítógépes klubban még szaktanácsadás is folyt ifjú vírusprogramozók számára. A következmény egy sor olyan vírusátirat, amit csak azért hoztak létre, hogy a vírusadatbázisból a darabot darabért elven cserélő, új vírusokat adhassanak a bejelentkező érdeklődők.

Felelőtlen programozók, amatőrök

Felelőtlenség, amatőrizmus

Sok programozó a vírusokat kísérleti célból maga is átírja és nem gondol arra, hogy azok könnyen kiszabadulhatnak az el-

lenőrzés alól. Gyakran továbbadják a vírust, vagy a visszafejtett víruskódot, melynek így hamarosan különböző átiratai jelenhetnek meg. Ha az átiratok mérete különbözik egymástól, akkor nagy valószínűséggel megnehezíti, vagy egyenesen lehetetlenné teszi a vírus megbízható eltávolítását a rendszerből. Így könnyen előfordulhat, hogy az adott alappéldány írója a saját kifejlesztett vírusát olyan formában kapja vissza, melyet már maga sem ismer fel.

Az amatőrök azzal jelenthetnek veszélyt, hogy nem képesek megakadályozni, hogy a vírus kiszabaduljon a kezük közül. Mire észbe kapnának, addigra már egy csomó vírusmutánst szabadítottak a világra. Az amatőr víruskészítők és terjesztők működését emellett egy sor hibás vírusátirat is jelzi, melyek úgy fertőzik meg a fájlokat, hogy azok helyrehozhatatlan károkat szenvednek. Az is előfordulhat, hogy egyes átvariált vírusfunkciók sose kapnak vezérlést.

Jogi szankciók a vírusgyártók ellen

Jogi szankciók

A vírusprogramok ellen a világ minden jogszerűségre törekvő országában hivatalosan fellépnek. A vírusok íróit és tudatos terjesztőit, vagy az adatvédelmi törvény keretében (mint az USA-ban), vagy a polgári törvénykönyvben a károkozással kapcsolatban (mint Németországban), vagy pedig a terrorizmus elleni harccal és az állambiztonsággal kapcsolatban (mint például Izraelben) büntetik. Az Amerikai Egyesült Államokban az államigazgatásban és a hadseregben nem alkalmazható egyetlen olyan program sem, amely bármiféle másolásvédelemmel van ellátva. Sőt az USA majdnem minden tagállamában tilos az ilyen programok kereskedelmi forgalomba bocsátása is. Magyarországon a Btk. foglakozik a kérdéssel (lásd. 4.4. pont)

Megválaszolásra váró kérdés továbbá, hogy létezhet-e bármilyen módszer, amellyel meg lehet állítani a vírusírókat. A 2. fejezetben szóltunk az Internet használatánál ajánlott etikai kódexről, a Netikettről. Ott és itt is csak az önkorlátozásra és az emberi jóérzésre lehet apellálni. Nehéz ellenőrizni kívülről, hogy valaki mit művel kettesben a számítógépével. A másik

megoldás az lenne, ha megszületnének azok a törvények, melyek súlyuknak megfelelően büntetnék a károkozó programok készítését (még ha csak kísérleti céllal írják is azokat) és szándékos terjesztését. Megváltást azonban egyiktől sem várhatunk, hiszen a jogi megtorlás visszarettenthet sokakat, ám a bűnözést nem szünteti meg, akárcsak a mindennapi életben.

7.3 Vírusmegelőzés a gyakorlatban

Ahogy az igaziak ellen is, a számítógépvírusok elleni védekezés leghatékonyabb módja a megelőzés.

Vírusforrások

Honnét kapjuk?

Vírus akkor kerülhet a számítógépbe, ha fertőzött programot indítunk el rajta vagy fertőzött lemezről boot-olunk. A számítógépvírus szaporítható hajlékony lemezről, újonnan telepített merevlemezről, hálózatról, cserélhető merevlemezről, sőt CD-ről is (mint történt ez egyik számítástechnikai folyóirat lemezmellékletével). Vírus érkezhet modemen, soros- és párhuzamos adatkábelen, vagy bármilyen hozzáférhető adathordozón keresztül. Újabban a leggyakoribb és leggyorsabban terjedő vírusok e-mail mellékletként érkeznek.

Honnét kerülhet vírus a gépre:

- munkatársak ellenőrizetlen adathordozóiról,
- szoftverkereskedőtől vásárolt programokon keresztül,
- ellenőrizetlen hálózati információforrásokról letöltött állományokból,
- meghajtóban felejtett lemezek révén,
- állásából eltávolított, bosszúálló munkatársak révén,
- szervizelést végző személyzet által,
- e-mail-ben, csatolt fájlként.

Vírusra utaló jelenségek

Miből tudjuk?

A számítógép időnként furcsán viselkedik. Az estek döntő részében mi csináltunk valamit rosszul, de néha ezek a jelenségek szoftverhibákra, vagy esetleg vírus(ok) jelenlétére utalhatnak.

Felsorolunk néhány (közel sem az összes) olyan jelenség, amely fertőzésre utalhat:

- a programok hossza, dátuma és a könyvtárbejegyzések megváltoznak,
- szokatlan kiterjesztésű, rejtélyes állományok jelennek meg,
- lassabban indulnak, hosszabb ideig futnak a programok,
- a programok írásvédett lemezre akarnak írni,
- szokatlan dolgok jelennek meg a képernyőn,
- memória mérete lecsökken, a hibás lemezfelületek száma nő,
- a rendszer automatikusan újraindul,
- hálózati rendellenességek lépnek fel,
- eddigi hibátlan programjaink lemerevednek,
- egyre több lesz az olvasási hiba,
- a floppy formázásakor probléma lép fel a rendszerben,
- végrehajtható állományaink hirtelen eltűnnek,
- lemezeink címkéje megváltozik, vagy akár az egész lemez és fájltartalom elveszik
- a program szokatlan üzeneteket küld, stb.

E jelenségek többségének észlelése önmagában még nem feltétlen és egyértelmű bizonyítéka a fertőzésnek. Ha több tünet egyszerre jelentkezik a felsorolt listából, az már arra utal, hogy baj van. Az egyik vírusdetektáló program szellemes üzenete ilyenkor így szól: „Egy combos virnyákot fogtam."

Mit tehetünk?

Néhány óvintézkedéssel csökkenthetjük a fertőzésveszélyt:

- eredeti szoftver biztos forrásból való beszerzése,
- írásvédett lemezek használata,
- tesztrendszer kialakítása,
- biztonsági másolat készítése,
- megfelelő hardver- és szoftvervédelem használata,
- egyszer írható optikai lemez alkalmazása,
- munkatársak betanítása, oktatása, szakértői ügyelet,
- floppymeghajtó nélküli telepítés,

- másolásvédelemmel ellátott programok használaton kívüli helyezése,
- hálózati kapcsolatfelvétel forrásának ellenőrzése,
- hozzáférés-védelem alkalmazása,
- rezidens vírusdetektorok használata
- ismeretlen feladótól érkezett e-mail törlése.

7.4 Védelmi rendszerek

Hardveres védelem

Nagyon jó hatásfokot lehet elérni az úgynevezett vírusvédelmi kártyák alkalmazásával. Segítségével egyrészt korlátozni lehet a hozzáférést az adott számítógéphez, másrészt állandó vírusfigyelést végez, így már a fertőzés gyanúja esetén is figyelmezteti a felhasználót, lehetőséget biztosítva az ellenlépésekre.

Szoftveres védelem

Sokféle ellenőrzési technikát dolgoztak ki a fejlesztők, de egyik sem nyújthat 100%-os védelmet, mivel a védekezés mindig lépéshátrányban van a vírusok fejlesztőivel szemben. Nézzük meg a különböző vírusvédelmi technikákat:

Szekvencia kereső rendszerek - egy vírus felismeréséhez elegendő ezt a rövidebb részletet megtalálni. Ha ez a szekvencia egy adott vírusra jellemző, akkor ez alapján a vírust meg lehet keresni.

Változásdetektorok - nem vírusspecifikusak, azaz csak a változás tényére hívhatják fel a figyelmünket. Arról már nem szolgálnak információval hogy valójában mi is okozta a változást, ennek eldöntését a felhasználóra bízzák.

Ellenőrző összeges védelem - számolás alapján tudja eldönteni egy program fertőzöttségét. Erre azért van szükség, mert a vírusok általában a fontos változtatásokat eltüntetik a felhasználók elől, nehogy hamar észrevegyék jelenlétüket.

Heurisztikus keresőrendszerek - vírusfunkciókra jellemző utasítássorozatokat, műveleteket keresnek, és ezek alapján döntenek az állomány állapotáról. Ha ezekből elegendő számút talál, akkor az adott fájlt fertőzöttnek minősíti, ha csak kevés szokatlan jelet, akkor gyanúsnak érzékeli.

Memóriarezidens vírusellenőrző programok - figyelik az elindított programok működését, tipikusan a vírusra utaló jelenségeket, például az illegális memória és lemezkezelés, vírusok által rendszeresen használt megszakítások gyakori hívása stb. Ha gyanúsnak minősítenek egy programot, akkor azt azonnal jelzik a felhasználónak, majd rá bízzák a döntés jogát.

Viselkedésblokkolók - az ismeretlen vírusok elleni védelemre specializálódott eljárás. Először ellenőriznie és analizálnia kell, hogy melyek azok az utasítások, "akciók", amelyek csak vírusprogramokra jellemzőek. Ha ezeket az utasításokat, funkciókat sikerül leblokkolni, akkor akár kellő vírusismeret nélkül is biztosítható a védelem.

Immunizálás - ha a vírus minden fertőzés előtt a saját azonosítókódját ellenőrzi hogy megtalálható-e az adott állományban, akkor elegendő ha elhitetjük a vírussal hogy már bele került az állományba, úgy, hogy az adott állományokba beleágyazzuk azt az azonosító kódsorozatot, melyet a vírus használ.

Egyedi killerek - általában egy bizonyos, éppen felbukkanó vírus eltávolításának érdekében gyorssegélyként hozzák létre a fejlesztők, melyet később beépítenek a komplex antivírus programjaikba.

Antivírus-szoftverek

Antivírus-szoftverek

A vírusok számának robbanásszerű emelkedésével sorra alakultak meg a kutatóközpontok, melyek köré sok tehetséges programozó gyűlt össze. Számos cég foglalkozik ilyen szoftverek gyártásával. A legismertebbek, ábécé sorrendben a következők:

- F-Secure,
- McAfee Antivirus

- Norton Antivirus
- Panda
- RAV Antivirus
- Virus Buster,

Bővebb és aktuális információ található az Interneten pl. a *www.virus.lap.hu* linkgyüjteményben.

Hazai fejlesztésű antivírus-szoftverek

A vírusok nagy része „nemzetközi", de vannak „nemzeti specialitások" is, pl. magyar vírusok a *Turbó Kukac, Kukac, Monxla, Polimer, Phantom,* és még sok más, új és mutáció. A hazai fejlesztésű antivírus-szoftverek előnye. hogy a hazai vírusokat is képesek felismerni és irtani. Magyar antivirus szoftverek széles választéka volt: Virus Killer, PRGDOKI, VirusBuster, a Sysdoki, a Pasteur, és a Virkill, VirSec, ChkVir.

Példák sora bizonyítja: a vírusgyártás és a vírusirtás folyamatosan „üzemel", és sorra jelennek meg az új generációk. Az itt felsorolt vírusirtókon kívül számos, ma már fejlettebb termék is van a piacon. Egy rendszergazdának alapvető feladata, hogy naprakész legyen ezekben a témákban. Az összes jelentős vírusirtót gyártó cégnek van honlapja az Interneten, ahonnét friss információkat lehet szerezni a legújabb termékekről.

Ellenőrző kérdések

1. Milyen programozott kártevőket ismerünk?
2. Milyen programokat nevezünk vírusoknak?
3. Mi a vírusgenerátor?
4. Mi jellemzi a trójai programokat?
5. Mik azok a programférgek?
6. Melyek a logikai bombák sajátosságai?
7. Hogyan keletkeznek a hátsóajtók, kiskapuk és csapdák?
8. Mi jellemző a nyulakra vagy baktériumokra?
9. Hogyan keletkeznek a számítógépvírusok?
10. Mondjon példákat a keletkezési helyekre!

11. Milyen jogi szankciókat lehet alkalmazni a vírusgyártók ellen?
12. Honnan kerülhetnek vírusok a számítógépre?
13. Milyen jelenségek utalnak vírusokra?
14. Milyen óvintézkedéseket tehetünk a vírusok ellen?

Jegyzetek:

8. Hálózatok védelme

Ebben a fejezetben áttekintjük az informatikai hálózatok védelmének néhány klasszikus módszerét. Elsősorban azokat választottuk ki, amelyek a számítógép hálózatok védelmében a leggyakrabban használatosak és függetlenek az alkalmazott informatikai eszközöktől. Megismerkedünk a jelszavakkal, a tűzfalakkal és a Kerberos nevű programmal.

A legbiztonságosabb számítógép az, amelyik ki van kapcsolva. Ha már mindenképpen be kell kapcsolni, akkor úgy növelhetjük a biztonságát, hogy minden perifériát eltávolítunk róla. Ez természetesen nem megvalósítható, de jól érzékelteti, hogy minél többféle hozzáférés van a számítógéphez, annál több oldalról érkezhet a támadás. Még különösebb szakmai felkészültség sem kell: az Internetről számtalan olyan program letölthető, amelyekkel be lehet jutni valaki gépére.
Ezért jól meg kell gondolni, hogy feltétlenül indokolt-e az adott gépet és a rajta futó alkalmazást rákötni a hálózatra. Gyakori megoldás, hogy külön hálózaton vagy szóló gépen futnak az érzékeny adatokat tartalmazó feldolgozások és egy másik, független hálózaton lehet elérni a külvilágot.

ISO OSI 7498-2 (X.800)

Amennyiben az adott gép csatlakozik a hálózathoz, mindent meg kell tenni a biztonsága érdekében. Az 5.5. pontban ismertettük az ISO OSI 7498-2 (X.800) szabványát, amely a nyílt hálózatok biztonságával foglalkozik. A szabványban meghatározzák a biztonsági mechanizmusokat, amelyekkel védeni lehet a hálózati adatforgalmat.
Emlékeztetőül néhány:

- hozzáférés ellenőrzése
- adatsértetlenség ellenőrzése
- hitelességcsere
- kriptográfia
- digitális aláírás és időpecsét

8.1 Jelszavak

A hozzáférés ellenőrzés egyik legfontosabb része a felhasználó azonosítása. Ezt általában a felhasználónévhez kapcsolt jelszóval oldják meg. Az egyszerű azonosító-jelszó párossal az a fő probléma, hogy könnyen ellopható. Akár úgy, hogy a begépelésnél megfigyeli a tolvaj, akár úgy, hogy ellopja a szükséges jelszavakat tartalmazó csomagokat a hálózatról. A jelszavas hitelesítés azonban nagyon kényelmes, és máig a legelterjedtebb hitelesítési forma. A kapcsolat kezdeményezéséhez a felhasználónak csak nevét és jelszavát kell megadni, semmiféle kiegészítő eszközre vagy programra nincs szükségük.

A különböző rendszerek titkosított formában tárolják a jelszavakat, amelyek ilyen formában használhatatlanok. A titkosított jelszó nem visszafejthető, még az algoritmus ismeretében sem. A titkosító eljárás széles körben használt hálózati szolgáltatás, így lehet próbálkozni a jelszó feltörésével. Sokféle jelszótörésre alkalmas módszer létezik. A leggyakrabban használtak: a szótártámadás és a nyers erőn alapuló támadás.

Szótár-támadás

Szótártámadás

Ez a támadástípus abból indul ki, hogy a felhasználók nagy része saját nyelvének valamelyik szavát használja jelszóként. A támadáskor egy szólistából indulnak ki, és ugyanazzal a titkosítási eljárással dolgoznak, amelyikkel a jelszót kódolták. A program veszi a listában szereplő szavakat, titkosítja, majd összehasonlítja a az eredményt az ellopott jelszóval. Ha egyezik, megvan a jelszó.

Nyers erő támadás

Nyers erő támadás

Számtalan ilyen elven működő, ingyenesen hozzáférhető jelszótörő program létezik. A program veszi az összes létező alfanumerikus karaktert, előállítja azok összes lehetséges kombinációját, titkosítja, majd összehasonlítja azt a megfejtendő jelszóval. Az eljárás vége a szerencsétől függ: befejeződhet gyorsan, de akár a végtelenségig is eltarthat. Ez a módszer hatékony, de nagyon időigényes is lehet.

Minél hosszabb egy jelszó, annál több időt vesz igénybe a feltörése. Jelszónak általában kisbetűket, számokat és néhány írásjelet szokás használni.
Tegyük fel, hogy ez 40 karakter. Ha ebből a 40 karakterből egyjegyű jelszót képzünk, 40 félét állíthatunk elő. Kétjegyű jelszó 40x40, vagyis 40^2 lesz. Ha „n" jegyű a jelszó, a lehetséges variáció 40^n.

Ha eggyel növeljük a jelszó hosszát, a lehetőség mindig 40-szeresére növekszik:

Jelszó hossza	Lehetséges jelszavak száma
1	40
2	1 600
3	64 000
4	2 560 000
5	102 400 000
6	4 096 000 000
7	163 840 000 000
8	6 553 600 000 000
9	262 144 000 000 000
10	10 485 760 000 000 000
11	419 430 400 000 000 000
12	16 777 216 000 000 000 000

Láthatjuk, hogy a jelszóhossz növekedésével exponenciálisan nő a lehetséges jelszavak száma. Hosszabb jelszavak megfejtéséhez az idő már csak években mérhető.

A jelszavak megadásánál a következő alapszabályok betartása célszerű:

- minimum 6 karakter hosszúak, de hosszabbak is lehetnek,
- betűket és számokat egyaránt tartalmaznak,

- nincs bennük olyan szó, ami az illetőre vagy családtagjaira utal,
- könnyen megjegyezhetők,
- gyakran cserélik őket.

Minél hosszabb egy jelszó, annál nehezebb kitalálni, de annál nehezebb megjegyezni is. Egy jelszó csak akkor biztonságos, ha a fejünkben van, és nem írjuk le valahová: pl. a monitorra ragasztott cédulára, hogy kéznél legyen. Ez még a lábtörlő alatt lévő kulcsnál is kevesebbet ér, mert még lehajolni sem kell érte.

Nézzünk néhány példát a jó jelszavakra [13]:

- Összekapcsolhatunk két értelmes szót egy írásjellel pl. *nedves&medve*, vagy számmal: *piros234kakukk.*
- Használjuk egy hosszabb, de megjegyezhető szöveg szavainak első betűit: pl. *Délután 6-tól 9-ig tilos a parkolás = d69tap,* vagy *Két szál pünkösdrózsa kihajlott az útra = 2sprkau.*
- Használjuk egy utca vagy üzlet nevét és rejtsük el benne a házszámot: pl. *bastya77setany.*
- Hagyjuk el egy könnyen megjegyezhető szöveg magánhangzóit: *mcmck&rbtgd (Mici Mackó és Róbert Gida),* vagy mássalhangzóit: *iiao&oeia.*
- Néhány betűt cseréljünk hasonló kinézetű számra: *m1ndenk0r, t0rnac1p0,*

A jelszavak elleni támadás kivédésére hardveres eszközök is vannak: ezek az egyszerhasználatos jelszavakat generáló tokenek és az intelligens kártyák.

Biztonsági eszközök

Tokenek

Ez egy kisméretű eszköz, amelynek LCD kijelzőjén percenként újabb jelszó jelenik meg.

A számítógép hálózatban lévő hitelesítő kiszolgáló ezekkel a tokenekkel szinkronban működik. Amikor a felhasználó be akar lépni a hálózatba, előveszi a tokent, ha kell beírja a PIN kódot. Az LCD kijelzőn megjelenik a jelszó, amelynek begépelésével jelentkezik be a hálózatba. A token program formájában is elképzelhető. Ilyenkor a felhasználó számára a saját számítógépén futó program állítja elő a jelszót.

Intelligens kártyák

Intelligens kártyák

Ezeken a kártyákon biztonsági adatokat tárolhatunk: jelszavakat, nyilvános és titkos kulcsokat, hitelesítő információkat. A felhasználónak ezeket az adatait nem kell a PC merevlemezén tárolni, elegendő megjegyeznie csak a kártya kódját.

Az Interneten küldött e-mailes vásárlási vagy banki tranzakció meghatározhatatlan számú számítógépen halad át, mielőtt célba ér, és minden egyes szerveren nyomot hagy. Egy vérbeli hackernek szinte rutinfeladat megfejteni az üzenetekben található személyre utaló biztonsági adatokat. Ezek birtokában aztán a meglopott nevében vásárolhat, banki műveleteket végezhet. Ezek ellen véd az intelligens kártya, amely egy bankkártya méretű eszköz mikroprocesszorokkal és memóriával. Hátrányuk, hogy speciális olvasó egység kell a használatukhoz.

USB tokenek

A két eszköz előnyeit egyesíti USB (Universal Serial Bus) token. Ebben is microchip van beépítve, ezért mind felhasználás, mind pedig műszaki működés szempontjából elmondható, hogy az USB token "ugyanazt tudja", mint az intelligens vagy chipkártyák. Az USB token előnye a chipkártyával szemben az, hogy nem szükséges külön olvasóegységet vásárolni; a token a számítógép USB portjára közvetlenül csatlakoztatható. Többféle biztonsági műveletet is elvégezhet.

8.2 A tűzfal (firewall)

A fejezet elején említettük, hogy a hálózatra kapcsolt számítógép számos ponton támadható. Manapság, amikor cégek, intézmények nagy számban csatlakoztatják hálózataikat az Internetre, a védelem egyik fontos eleme a tűzfal.

Tűzfal

A számítógépes hálózatokban a tűzfal egy olyan kiszolgáló számítógép vagy program, amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, hogy az illetéktelen behatolásoknak elejét vegyék és egyúttal lehetővé tegyék a kifelé irányuló forgalom ellenőrzését is.

A tűzfal egyik típusa az ún. „külső tűzfal", ami a teljes helyi hálózatot izolálja az Internettől, míg az ún. „belső tűzfal" a helyi hálózat különösen védendő részét zárja el annak többi részétől, így az Internettől is. A tűzfal használata titkos, érzékeny adatok védelme, vagy nagy üzembiztonságot kívánó hálózatok esetén elengedhetetlen. A tűzfal akkor alkalmazható hatékonyan, ha a teljes forgalom ezen keresztül zajlik le. A tűzfal nem a védelem alapeszköze, inkább fontos kiegészítője.

A tűzfalak rendszerint folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek, felhasználók azonosítóit, rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak. Azonban nemcsak a hálózat üzemeltetőinek kell tudniuk a tűzfalakról, hanem a felhasználóknak is, akik a tűzfal mögül érik el az Internetet. Ugyanis a tűzfal korlátozásokat jelent a felhasználók számára, amivel tisztában kell lenniük.

Le lehet tiltani vagy jelszóhoz kötni bizonyos internetoldalak böngészését, különböző szolgáltatások használatát (pl. áramló audió és videó, IRC, stb.), korlátozhatjuk veszélyes fájlok vagy levélmellékletek letöltését, stb.

A tűzfalak típusai

Csomagszűrők (Packet Filters)

Csomag-szűrők

A tűzfalak első, legegyszerűbb generációja. A beállított szűrési szabályok alapján egyes csomagokat továbbítanak, másokat eldobnak. Meghatározható, hogy milyen címtartományból fogadunk el csomagokat, azaz alhálózatonként vagy akár gépenként szabályozhatjuk a szolgáltatások használatát. Ugyancsak megoldható, hogy a belső felhasználók számára korlátozzuk a külső hálózati szolgáltatásokhoz való hozzáférést.

Megadható, hogy bizonyos események/csomagok előfordulását naplózzák, e-mail-t küldjenek a rendszergazdának, adjanak hangjelzést vagy indítsanak el valamilyen programot. A csomagszűrők fizikai és protokoll szinten (IP, UDP, TCP) működnek. Alkalmazói programok szintjén (ftp parancsok, fájl műveletek) már nem képesek védelmet nyújtani.

Előnyei: minden kimenő és bejövő csomagot külön ellenőriz, mivel a két hálózat kizárólagos kapcsolódási pontja, nagyon nehéz kijátszani.

Hátrányai: mivel a tűzfal beállítása igen bonyolult lehet, biztonsági hézagok maradhatnak, nem képes részletes biztonsági naplófile-ok írására.

Proxytűzfalak

Proxytűzfalak

Nem szűrőként, hanem közvetítőként viselkednek a védett hálózat és a külvilág között. Kívülről a tűzfal mögötti számítógépek teljesen láthatatlanok. Ez a megoldás teljesen elfedi a belső hálózati struktúrát, a gépek címeit és neveit. Egyetlen regisztrált IP címmel az egész hálózat működtethető. A regisztrált címet a tűzfal használja, a mögötte lévő gépek regisztrálatlan címet kapnak. Két kommunikálni kívánó gép között a proxy-n keresztül épül fel a kapcsolat, nem pedig közvetlenül .

Előnyei: a hálózati forgalom ellenőrzése, az illetéktelen behatolási kísérletek regisztrálhatók, pontosan – IP címre -

szabályozhatók a kapcsolatok, nagyobb biztonságot nyújtanak, mint a csomagszűrők.

Hátrányai: működési elvük alapján a proxy alapú tűzfalak áteresztőképessége kisebb, mint a csomagszűrőké,

A tűzfalakat akkor tudjuk leghatékonyabban üzemeltetni, ha a belső és külső hálózat között helyezzük el őket. Fontos, hogy a két hálózat egyetlen kapcsolata a tűzfalon menjen keresztül.

Szabad zóna

Szabad zóna

Sok esetben egy harmadik, a belső és külső hálózattól egyaránt eltérő hálózatra is szükség van, amit *szabad vagy demilitarizált zónának* neveznek

Ezt akkor használjuk, ha a nyilvános hálózatok számára elérhetővé akarunk tenni bizonyos kiszolgálókat pl. web-kiszolgálót, FTP-t, stb. Ennek az az előnye, hogy pontosan tudjuk szabályozni a zóna hálózati forgalmát. Ezzel a kalóztámadások egy részét is ki lehet védeni, mivel azok gyakran használják kiindulási pontként ezeket a kiszolgálókat, de ha azok külön hálózaton vannak, nem tudnak onnét betörni a védett belső hálózatra.

8.3 Kerberos

Illegális kliensek kiszűréses

A Kerberos egy nyitott forráskódú hitelesítő rendszer, amelyet a MIT (Massachusetts Istitute of Technology) azzal a céllal fejlesztett ki, hogy egy nem biztosított hálózatban – mint például az Internet – biztonságosan hitelesíteni lehessen a felhasználókat. Az első változatot 1988-ban mutatták be, most az 5. verziónál tartanak.

A rendszer saját szerverén kívül a hálózatban működő egységek egyikétől sem követel biztonságot. Egy speciális azonosító rendszerrel meg tudja különböztetni a bejegyzett felhasználókat az illegális kliensektől.

A rendszer működésének legfontosabb jellemzői:

- A felhasználónak csak egyszer kell azonosítani magát.
- Titkosítás nélkül a jelszavak sohasem kerülnek a hálózati adatforgalomba, sőt a felhasználói számítógépek memóriájába sem.
- Minden felhasználó és szolgáltatás rendelkezik névvel és jelszóval.
- Kizárólag a Kerberos szerver ismeri az összes jelszót.
- A Kerberos szerver maximális fizikai védelme biztosított.

Egyszeri kommunikációs kulcs

A felhasználó rendszere kapcsolatba lép a Kerberos szerverrel és a két rendszer titkosított és hitelesített adatokat cserél a felhasználó azonosítására. Ezek után a Kerberos a felhasználó rendelkezésére bocsát egy ún. jegyet. Ez tartalmazza a szolgáltatásokat nyújtó szerver nevét, a felhasználó nevét, hálózati címét, a jegy érvényességi idejét, a felhasználó és a kiszolgáló közötti egyszeri kommunikációs kulcsot. Ezek az adatok a szerver titkos kulcsával vannak titkosítva. A jegy szokásos lejárati ideje 8 óra, és ezen belül korlátlan alkalommal használható. A felhasználó ezzel a jeggyel tudja igazolni magát a többi kiszolgáló előtt. A Kerberos kizárólag hitelesítésre alkalmas, engedélyezésre nem.

A módszer előnye, hogy a hitelesítéshez használt adatokat mindössze egyszer kell elküldenünk a hálózaton keresztül a Kerberos kiszolgálóhoz. Innen kezdve a jelszavunk többé nem kerül elő. Mivel a hitelesítési folyamat titkosítva zajlik, a felhasználó jelszavát nem lehet ellopni. Ráadásul a hitelesítéshez több adat szükséges egyidőben, ezért nehéz eljátszani a hitelesített felhasználó szerepét.

A Kerberos biztonsági rendszere kizárólag a Kerberos szerver feltörésével támadható meg, ezért nagyon szigorú hozzáférési jogosultságokat kell beállítani, és nem célszerű más szolgáltatásokat is futtatni ott. A Kerberost csak olyan alkalmazásoknál lehet használni, ahol mind a szerver, mind az összes felhasználó felismeri és használja a Kerberos funkcióit. Ez a rendszer

egyetlen hátránya. Amennyiben egy hálózati rendszer tervezésnél lehetővé teszik a Kerberos funkciók beépítését, akkor minimális ráfordítással megoldható, hogy a rendszer magas szintű védelmet élvezzen.

Ellenőrző kérdések

1. Milyen támadások érhetik a jelszavakat?
2. Milyen egy jó jelszó?
3. Mi a token?
4. Mit tud az intelligens kártya?
5. Mire való a tűzfal?
6. Mi a különbség a csomagszűrő és proxy tűzfal között?
7. Mire használják a Kerberost?

Jegyzetek:

9. A kriptográfia és az elektronikus aláírás

„Ahogy az információ egyre értékesebb árucikké válik, s ahogy a kommunikációs forradalom átformálja a társadalmat, úgy játszanak mind nagyobb és nagyobb szerepet mindennapi életünkben a titkosított üzenetek és adatok. Telefonhívásaink ma már műholdakról verődnek vissza, e-mailjaink számos komputeren haladnak keresztül. Mindkettő könnyűszerrel lehallgatható, elfogható, s ilyen formán veszélyezteti érdekeinket és személyiségi jogainkat. Ahogy mind több üzleti vállalkozást működtetnek Interneten, úgy kell egyre inkább védeni a cégek és ügyfelek érdekeit. Ennek a kódolás az egyetlen módja. Az információs kor lakatját és kulcsát a titkos kommunikáció, a kriptográfia fogja biztosítani."[15]

9.1. A kriptográfia története

Ókor

Az emberi társadalmakkal egyidős a titkolózás. Az uralkodók és hadvezérek évezredeken keresztül támaszkodtak a hírközlő hálózatokra annak tudatában, hogy ha üzeneteik az ellenfél kezébe kerülnek, akkor végzetes következményekkel kell számolniuk. Igyekeztek olyan módszereket kitalálni, hogy üzeneteiket csak a címzett tudja elolvasni. Rejtjelezőket foglalkoztattak, akik a lehető legmegbízhatóbb kódokat próbálták kitalálni. Természetesen az ellenség próbálta megfejteni a titkos üzeneteket, ezért kódfeltörőket alkalmazott. Ez az intellektuális hadviselés nagyon nagy hatást gyakorolt a történelemre, csaták és háborúk sorsát döntötte el.

Nézzünk meg néhány módszert a régi időkből:

Polübiosz

Ezt az egyszerű módszert Polübiosz (i.e.200-i.e.120) alkotta meg. Az abc 25 betűjét egy táblázatba foglalta.

A rejtjelezett betűk a mátrix elemeinek feleltek meg: a sorok és oszlopok sorszáma adta a kétjegyű kódot.

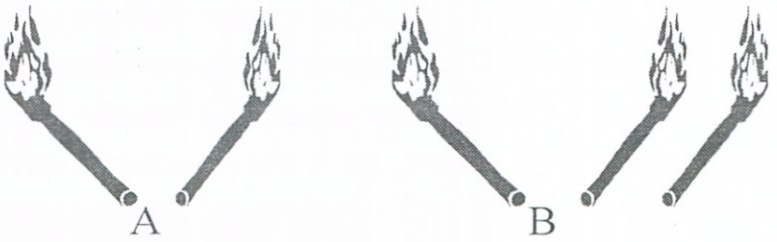
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

4. ábra: Polübiosz tábla

Ezzel a módszerrel a „titkos" szó a következőképpen néz ki:

T	I	T	K	O	S
4-4	2-4	4-4	2-5	3-4	4-3

A rejtjelezett üzenet továbbítása fáklyákkal történt. Jobb és bal kézben a számoknak megfelelő számú (1-5 db) fáklyát kellett tartani minden betű továbbításához. A kommunikáció csak sötétedés után indulhatott. Távolról is jól látható magaslatra kellett állni, és betűnként lehetett az üzenetet elküldeni.



Természetesen a görögök még számos más módszert is használtak.

Ceasar-féle helyettesítés

A rómaiak leghíresebb módszere volt a Ceasar-féle helyettesítés. A behelyettesítő kódtáblát az ábécé adott számú jobbratolásával állította elő. Azaz minden betűt behelyettesítünk az ábécében azt ciklikusan követő n-edik betűvel. Nézzünk példát rá. Minden egyes betűt megfeleltetünk egy másiknak, amely 5 hellyel van elcsúsztatva:

A → F B → G C → H D → I E → K F → L G → M
H → N I → O K → P L → Q M → R N → S O → T
P → U Q → V R → W S → X T → Y U → Z V → A
W → B X → C Y → D Z → E

A „titkos" szó rejtjelezve: **YOYPTX**

Ha nem öttel, hanem csak hárommal toljuk odébb a betűket, más lesz a kódtábla:

A → D B → E C → F D → G E → H F → I G → K ...
S → V T → W U → X W → Y X → Z Y → A Z → B

A „titkos" szóra egészen más megoldást kapunk: **WMWNRV.**

Fésűs módszer

Egy másik, szintén már a görögök által is használt módszer a szöveg átrendezése. Ennek egyik legegyszerűbb módja az ún. **fésűs módszer**. Ez azt jelenti, hogy az üzenetek betűjét váltakozva írják az alsó illetve felső sorba. Például így:

Az üzenet: *Az ellenség a tengerről támad.*

Kódolás:
a e l n é a e g r ő t m d
z l e s g t n e r l á a

A kódolt szöveg:
aelnéaegrőtmdzlesgtnerláa

Ha három sorba írjuk az üzenetet, akkor a megoldás a következő lesz:

alngeeőádzlsanrlmeeétgrta

9.2. A kriptográfia alapfogalmai

Az első két módszernél minden karakternek megfeleltettünk egy másikat. A fésűs módszernél a karakterek értékét meghagytuk, de a sorrendjüket megváltoztattuk.
Ezzel el is jutottunk a kriptográfia két alapmódszeréhez: ezek a behelyettesítés és a keverés. Előbb azonban nézzük meg, milyen alapfogalmakkal dolgozunk:

Nyílt szöveg (plaintext)

Az eredeti, kódolatlan, bárki által értelmezhető üzenetet.

Rejtjeles szöveg, kriptoszöveg (ciphertext)

A rejtjelezés eredménye, a védett, olvashatatlanná tett információ.

Rejtjelezés, titkosítás, kódolás (encryption)

Az a konverzió, amely során a nyílt információból rejtjeles lesz.

Megoldás, megfejtés, dekódolás (decryption)

Az előbbi fordítottja, amikor is egy kódolt információhalmazból nyílt információt állítunk elő.

Rejtjelező algoritmus

Olyan matematikai apparátus, amely egy tetszőleges, nyílt információhalmazból úgy állít elő egy kódoltat, hogy abból az eredeti nyílt adathalmaz visszanyerhető.

Kulcs

Az az érték, amelyet az adott kódoláshoz kiválasztunk azok közül az értékek közül, amelyekkel az adott algoritmus működhet. Például a Ceasar féle módszernél az algoritmus a betűk jobbra tolása, az az. érték, amennyivel jobbra toljuk, pedig a kulcs (tehát 5 vagy 3).

Most már megnézhetjük a két alapmódszer definícióját:

Kriptográfiai alapmódszerek

Behelyettesítés

A nyílt szöveg minden karakteréhez valamilyen algoritmus szerint hozzárendelünk egy vagy több másik karaktert.

Keverés

A nyílt szöveg karakterei változatlanok maradnak, de a sorrendjüket megváltoztatjuk.

Kriptográfia feladata

A kriptográfia alapvető feladata, hogy algoritmikus eszközökkel biztosítsa, hogy a védett adatok csak az azok felhasználására kijelölt körben legyenek elérhetők.

9.3. A kódfejtés tudománya, a kriptoanalízis

Az egyszerű helyettesítéssel rejtjelezett szöveget aránylag könnyű megfejteni. Ez azért van, mert az átalakítások száma kicsi és megőrzi az eredeti szöveg statisztikai tulajdonságait, vagyis a kódolatlan szövegben azonos karakterek a rejtjelezett szövegben is egyformák lesznek, így a megfejtéshez sok támpontot adnak. Minden nyelvnél megállapítható, hogy egy adott nyelvben az egyes betűk mekkora gyakorisággal fordulnak elő. Ha ismerjük az üzenet rendeltetését, akkor a használt szavak gyakoriságára is következtethetünk, ami még jobban megkönnyítheti a rejtjelfejtők munkáját.

Az angol ábécé betűinek gyakoriságát az alábbi táblázat mutatja [15]:

Betű	%	Betű	%	Betű	%	Betű	%
a	8,2	**h**	6,1	**o**	7,5	**v**	1,0
b	1,5	**i**	7,0	**p**	1,9	**w**	2,4
c	2,8	**j**	0,2	**q**	0,1	**x**	0,2
d	4,3	**k**	0,8	**r**	6,0	**y**	2,0
e	12,7	**l**	4,0	**s**	6,3	**z**	0,1
f	2,2	**m**	2,4	**t**	9,1		
g	2,0	**n**	6,7	**u**	2,8		

Mono-alfabetikus kód

Azokat a behelyettesítéses módszereket, amelyek betűket és/vagy szimbólumokat használnak *monoalfabetikus* kódnak nevezzük.

Iszhák al-Kindi

A IX. századi arab közigazgatásban rendszeresen használták a rejtjelezést és a kódok megfejtését is. 1987-ben találták meg azt a kéziratot, amelyet a IX. században *Iszhák al-Kindi* írt *Titkos üzenetek megfejtése* címmel. Ebben kifejti, hogy minden nyelvnek vannak gyakrabban és ritkábban használt betűi. Az egyszerű helyettesítéssel készült rejtjelezett szöveg is magánviseli ezeket a tulajdonságokat: amelyik jel legtöbbször szerepel benne nagy valószínűséggel az felel meg a leggyakoribb betűnek.
E művet ugyan hosszú ideig a feledés homálya fedte, de a későbbi korok kódfejtői is rájöttek erre a törvényszerűségre és fel is használták.

A XV. századi Európában indult újra virágzásnak a rejtjelezés használata. A monoalfabetikus kódokat viszonylag könnyen megfejtették a gyakoriságelemzés módszerével, ezért a rejtjelezők új kódok után kutattak.

Vigenere rejtjelezés

Polialfabetikus

A francia diplomata Blaise de Vigenere a XVI. században készítette azt a titkosítási rendszert, amely kivédte a monoalfabetikus kódok hiányosságait. Az általa kidolgozott módszer 26 kódábécét használ, tehát *polialfabetikus*. Ennek a lényege, hogy a Ceasar féle titkosítás továbbfejlesztéseként az eltolás betűről betűre változik. Módszerének az alapja az 5. számú ábrán lévő tábla.

Az első sor a nyílt (kódolandó) szöveg betűinek felel meg, míg az első oszlop betűi a kulcsbetűk. A rejtjelezés igen egyszerű. Nézzük meg egyetlen karakterre: Vegyük a nyílt üzenet betűjét (pl. **G**), és megkeressük a nyílt betűk között. Ezzel megkapjuk, hogy melyik oszlopban lesz a kód. A kulcsszó betűjét pedig kikeressük a kulcsbetűk közül (pl. **F**), ami kijelöli, hogy

melyik sorban lesz a kód. A rejtett üzenet betűje a kiválasztott sor és oszlop találkozásánál lesz (**I**).

									N	Y	Í	L	T		B	E	T	Ű	K							
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
	C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
	D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
	E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
K	F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
U	G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
L	H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
C	I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
S	J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
	K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
B	L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
E	M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
T	N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
Ű	O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
K	P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
	Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
	R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
	T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
	V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
	W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
	Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
	Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

5. ábra
Vigenere táblája

Nézzünk egy hosszabb példát:

Nyílt üzenet:	v	i	g	e	n	e	r	e	r	e	j	t	j	e	l	e	z	e	s
Kulcsszöveg:	e	g	y	k	u	l	c	s	e	g	y	k	u	l	c	s	e	g	y
Rejtett üzenet:	z	o	e	o	h	p	t	w	v	k	h	d	d	p	n	w	d	k	q

Az előbbiekben bemutatott példában egy kulcsszót ismételünk annyiszor, hogy olyan hosszú kulcsszöveget kapjunk, mint a nyílt szöveg. A kulcskialakításra azonban vannak más módszerek is. A kulcsszót képezhetjük a nyílt szövegből is a következők szerint. Egyszerű önkulcsoló rejtjelezés esetén választunk egy kezdeti kulcsbetűt, majd a kulcsszó többi része a nyílt üzenet lesz.

Nyílt üzenet:	e	g	y	s	z	e	r	u	o	n	k	u	l	c	s	o	l	o
Kulcsszöveg:	K	e	g	y	s	z	e	r	u	o	n	k	u	l	c	s	o	l
Rejtett üzenet:	o	k	e	q	r	d	v	l	i	b	x	e	f	n	u	g	z	z

Kezdeti kulcs

A bemutatott példa nagyon könnyen feltörhető ha ismert az eljárás, hiszen csak a kezdeti kulcsot kell megtalálni. Az eltérő kezdeti kulcsok száma annyi, ahány karaktert tartalmaz a kódtábla (jelen esetben 26), tehát a legrosszabb esetben 26 próbálkozás szükséges a kód megfejtéséhez. Nehezebb a megfejtés, ha a kulcsszót a már rejtjelezett üzenet egy részéből képezzük.

Homofónikus kód

Vigenere kódja nagyon erős volt, de bonyolultsága miatt kevésbé terjedt el. A gyorsaság és az egyszerűség miatt továbbra is inkább a *monoalfabetikus* kódokat használták, vagy a két rendszer közötti átmenetet az ún. *homofónikus* kódot. Ennek az a lényege, hogy a gyakoribb betűk több kódot kapnak, elfedve ezzel a szöveg statisztikai tulajdonságait.

Egyszeri szalag

Tökéletes, megfejthetetlen rejtjelezés akkor keletkezik, ha az ábécé betűiből egy valódi véletlen sorozatot generálunk és azt adják hozzá a kódolandó szöveghez.
Nézzünk erre egy példát: minden karakterhez egy számot rendelünk 1-64-ig: a-0, b-1, c-2, ... A-26, B-27, D-28...Z-51, 1-52, 2-53, 3-54, stb.
A nyílt szöveghez generálunk egy azonos hosszúságú, véletlen karaktersorozatot. Ez lesz a kulcs. A nyílt szöveg és a kulcs számát összeadjuk, és az összeadott érték lesz a rejtett szöveg. Ha az összeg nagyobb, mint 64, akkor kivonjuk belőle a 64-et és a maradék lesz a kód (XOR művelet).

Nyílt szöveg:

A	l	g	o	r	i	t	m	u	s
26	11	6	14	17	8	19	12	20	18

Kulcs: (véletlen karaktersorozat)

o	k	G	b	l	C	i	A	a	Z
14	10	32	1	11	28	8	26	0	51

Kódolás:

26	11	6	14	17	8	19	12	20	18
14	10	32	1	11	28	8	26	0	51
40	21	38	15	28	36	27	38	20	5

Rejtett szöveg: (a kapott számértékeket visszaírjuk a karakterekbe)

O	v	M	p	C	K	B	M	u	f

Ezt a fajta módszert nevezik *egyszeri szalagnak*, *egyszeri takarónak*, vagy *véletlen átkulcsolásnak* is. Az angol szakkifejezés: *one time pad.* Ezt a kódolási eljárást bizonyítottan lehetetlen megfejteni. Gyakorlatban azonban nehezen használható, mivel a kulcsok előállítása és azok kezelése rendkívül bonyolult feladat.
A fentieken kívül számos klasszikus módszer ismert még. [15]

9.4. Modern titkosítási módszerek

Egészen a huszadik századig futárok és postagalambok szállították az információt. Az üzenet megszerzéséhez előbb el kellett fogni a hordozót, aztán jöhetett a megfejtés. Nem kellett vele nagyon sietni, lévén, hogy egy üzenet-válasz ciklus ideje akár hónapokra is rúghatott. Az üzenet küldője egészen addig nem is gyanakodott, míg hónapokkal az üzenet elküldése után el nem jöttek a fejét venni. Ezek a ráérős módszerek voltak jellemzők a távíró és a rádióhullámú kommunikáció feltalálásáig, amely új korszakot nyitott titkosítók és a megfejtők párharcába.

Enigma

A kriptográfia történetének egyik legérdekesebb fejezete az Enigma története. A német hírszerzés a húszas évek végén állította hadrendbe ezt a táskaírógéphez hasonlító szerkezetet. A kapcsolótáblák és keverőtárcsák különböző beállításait felhasználva először sikerült gépesíteni a rejtjelezést. A rendkívül sok beállítási lehetőség miatt a kód megfejthetetlennek tűnt. A kódfejtésbe első ízben vetettek be matematikusokat. Először a lengyeleknek sikerült megfejteni az Enigma titkát. 1938 végén a német titkosszolgálat további keverőtárcsákat épített be a gépbe, amitől a kód ismét ellenállt a feltörési kísérleteknek. Lengyelország lerohanása után a lengyel kódfejtők átadták a szövetségeseknek az addigi eredményeiket.
Az angolok létrehoztak egy rejtjelfejtő központot *Blechley Parkban*, ahol a háború végén már 2000 ember dolgozott. *Alan Turing* angol matematikus tervezte meg a *Turing-bombának* nevezett gépeket, amelyekkel megfejtették az Enigmával kódolt német üzenetek tömegét. Ezt a tényt sikerült a háború végéig titokban tartani a németek előtt. Általános vélemény, hogy a kódolt üzenetek megfejtése a szövetségesek győzelmének döntő tényezője volt.

Navaho nyelv

A rádiós kommunikáció egyrészt felgyorsította, szinte azonnalivá tette egy üzenet elküldését, másrészt sérülékennyé vált az üzenetet továbbító csatorna. A távíró üzenet illetéktelen megszerzéséhez csupán alapvető lehallgatói ismeretekre van szükség, a rádióhullámok pedig a besugározható területen belül mindenütt hallhatók. Például a II. világháború csendes-óceáni hadszínterén a technikailag fejlett ellenség különösebb erőfeszítés nélkül le tudta hallgatni az amerikai tengerészet és légierő rádiós kommunikációját. Az amerikaiak ez ellen technikailag semmit sem tudtak tenni, ezért a legfontosabb információkat egy rendkívül ritka, kevés ember által beszélt *navaho indián nyelven* küldözgették egymásnak.

A modern csatornák bizalmas adatok továbbítására titkosítás nélkül használhatatlanok. Ez fokozottan igaz egy olyan világméretű számítógép-hálózat esetén, mint az Internet, ahol a küldő és a vevő között az üzenet akár többtucatnyi telefontársaság vonalát és közel ugyanennyi adatátviteli szolgáltatást nyújtó

cég eszközeit érinti. Ráadásul elvben szinte mindenütt egyidejűleg jelen lehet a lehallgatáshoz és visszafejtéshez szükséges ember, technika és kapacitás.

Lucifer

A piac igényeire reagálva az IBM pályázatot írt ki számítógépes rejtjelező rendszerre. A versenyt egy blokkos rejtjelező rendszer nyerte meg, amely a LUCIFER nevet kapta. A bináris bitfolyamot blokkokra osztja, és a blokkokon belül hajtja végre a keveréseket és a behelyettesítést. Ezeket a műveleteket többször is megismétli. Ezeket a helyettesítő táblákat angolul *Substitution box*-nak, vagy egyszerűen *S-box*-nak hívják.

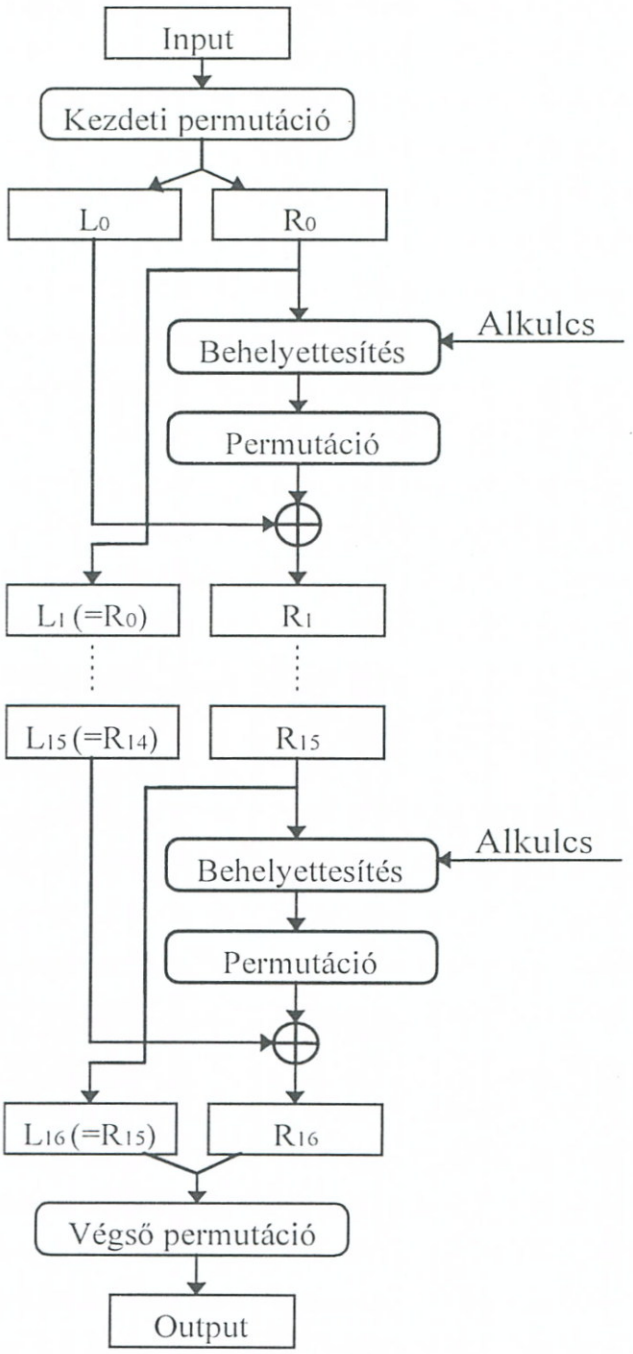
A LUCIFER-nél alkalmazott módszer jelenti az alapját az IBM és a NSA (National Security Agency – Nemzeti Biztonsági Szolgálat) által közösen kifejlesztette a DES-nek (Data Encryption Standard – Adattitkosító Szabvány). A DES az egyik legáltalánosabban használt civil rejtjelező rendszer az USA-ban.

DES

A DES egy 64 bites blokk-rejtjelező rendszer, azaz a nyílt és a rejtjelezet üzenet-blokkok is 64 bitesek. A rejtjelezés csak a kulcstól függ, ezért ha két nyílt blokk megegyezik, akkor a rejtjelezett blokkok is megegyeznek. Mindezek ellenére erős rejtjelezésnek tekinthetjük, mert erőssége a hozzárendelés bonyolultságában rejlik.

A DES 16 egymás után végrehajtott lépésből áll. A 16 egység azonos szerkezetű, de minden lépésben más alkulcsot használunk A fejlesztők úgy alakították ki az egyes lépéseket megvalósító egységeket, hogy azok öninverz lépések legyenek, vagyis a lépések többszöri végrehajtásával a végeredményből visszaállítható a kiindulási állapot. Ennek köszönhetően ugyanaz a DES-egység használható rejtjelezésre és megoldásra is.

A DES sematikus ábrája



6. ábra

Az algoritmus teljesen nyilvános. Számos cikkben jelent meg - különböző programozási nyelveken - korrekt forrásnyelvi leírása is, így egy gyakorlott programozó néhány órai munkával azt realizálni is tudja. A DES jelenleg is használatos, bár általában más módszerekkel kombinálva. A számítási kapacitások rohamos fejlődésének hatására egyre rövidebb idő alatt feltörhető.

Triple-DES és társai

Az eredményes fejtési kísérletek hatására újabb DES változatok készültek. A **Triple-DES** a módszer egyszerű matematikai feljavítása, amely egyszerűen megtöbbszörözi az algoritmus alkalmazását, ezzel a biztonságot kétszeresére növeli. Ez vagy kettő, vagy három 58 bites kulccsal dolgozik.

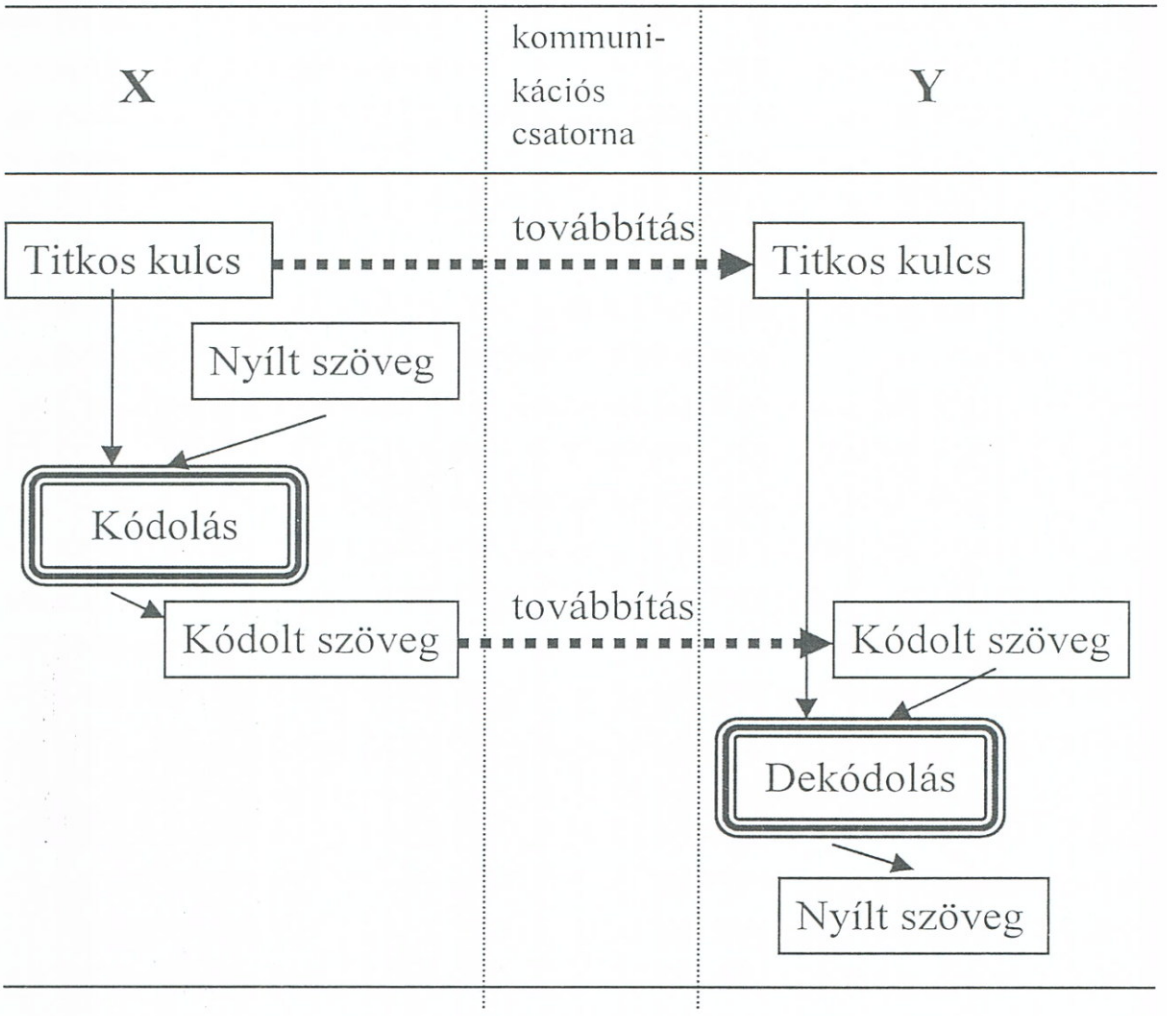
Az üzenetet először az első kulccsal rejtjelzik normál DES módban, majd a második kulccsal a megoldó algoritmust alkalmazzák. Az így nyert közbülső szövegre alkalmazzák ismét az első, három kulcsos rendszerben a harmadik kulcsot. További változatok: DESX, GDES, RDES, DES alternatív S-boxal, stb.

IDEA

Az IDEA (Ideal Data Encryption Algorithm) blokkos rejtjelező algoritmus. Lai és Massey fejlesztette ki 1990-1992 között.
Az IDEA gondosan választott alapvető, de kielégítő bonyolultságú matematikai műveletek speciális kombinációit használja fel. Ezeket a műveleteket 16 bites blokkonként alkalmazza 64 bites nyílt szöveg blokkokra, 128 bites kulcs felhasználása mellett. A blokkon belüli kimenet bitek mindegyike minden bemeneti bittől függ.

Bizonyítottan rendelkezik a Shannon által megkövetelt keverési és szétterjesztési tulajdonságokkal. A matematikai műveletek egyszerűsége gyors és egyszerű technikai megoldásokat tesznek lehetővé mind software, mind pedig hardware szinten. Az egyik legjobb, nyilvánosan hozzáférhető szimmetrikus algoritmus. Az IDEA eljárás számos országban szabadalom védelem alatt áll.

A szimmetrikus, vagy titkos kulcsú rejtjelezés sémája
(X üzenetet küld Y-nak)



7. ábra

Gyenge pont a kulcs

A titkos kulcsú, szimmetrikus kriptográfiai módszernek a gyenge pontja a kulcs. Ha illetéktelen kezekbe jut, vége a titkosságnak. Titkosított üzenet küldésére addig nincs mód, amíg a felek meg nem egyeztek a titkosítás módszerében. Erre az USA kormányzata úgy próbált megoldást találni, hogy az NSA (Nemzetbiztonsági Hivatal) készítette és központilag osztotta ki a kormányszervek kommunikációjához szükséges kulcsokat. Aztán a Ronald W. Pelton NSA-ügynök nevével fémjelzett kémkedési botrány során kiderült, hogy Pelton semmilyen titkos információt nem szolgáltatott ki - csupán kulcsokat.

9.5. Kulcstovábbítási módszerek

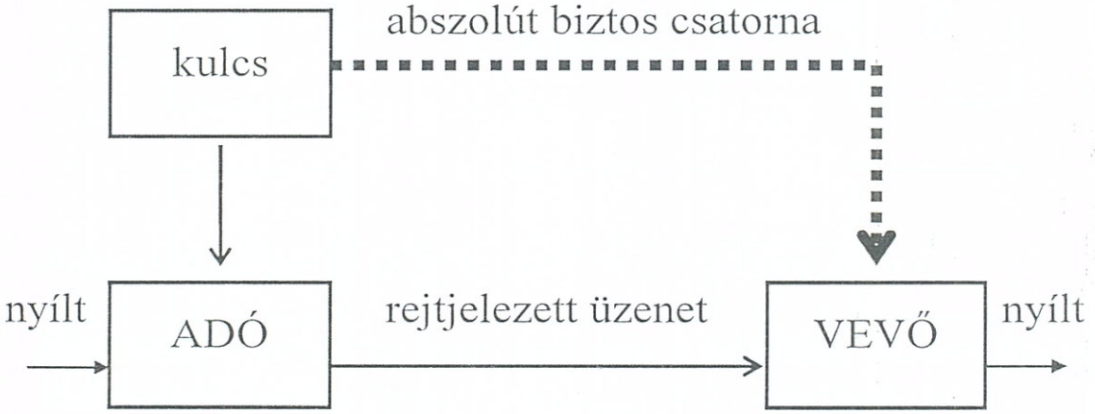
Az előző problémára megoldásokat kerestek. A következő módszerek a kulcsra összpontosítanak.

Abszolút biztos csatorna

Abszolút biztos csatorna

A rejtjelezés - ma már klasszikusnak mondható - Shannon által megfogalmazott alapsémája szerint a rejtjelezés által védett kommunikációs csatornát kiegészíti egy "abszolút biztos csatorna", amelyen a kulcstovábbítás történik.

A megoldó oldalra az üzenet tetszőleges csatornán átküldhető, de a biztonság megmarad, ha a megfejtéshez szükséges kulcsok valamilyen "abszolút biztos" csatornán jutnak el a megoldó oldalra.



8. ábra

Az "abszolút biztos" csatorna - csaknem valamennyi környezetben - a matematikai módszerek mellett is, csak úgy biztosítható, hogy eljárási utasításokat adnak ki a kezelésére. Ezek azonban erősen függnek a technológiai fegyelem betartásától, az emberi tévesztéstől, az esetleges támadásoktól.

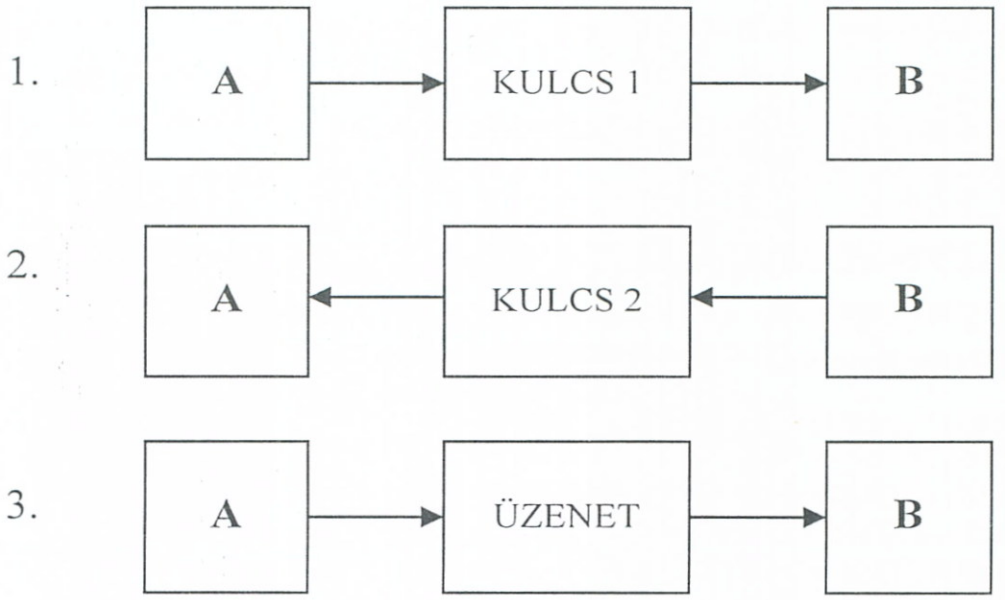
Az emberi tényezők minimálisra szorítása érdekében általában elterjedtek az osztott védelmi rendszerek, amelyekben az "abszolút biztos" csatornát úgy valósítják meg, hogy a kezelő személyek között megosztják a védelmi eszközöket, vagyis nincs egyetlen olyan személy aki minden védelmi eszköz birtokában van. Mindem művelethez minimum két ember kell, és

a rendszerrel kapcsolatos valamennyi tevékenységet dokumentálni kell.

Kétirányú kulcsforgalom, cserekulcs

Cserekulcs

Ez a módszer napjainkban is használt nagy biztonságot jelentő, nehezen támadható megoldás, amely kizárólag a kulcsforgalomra koncentrál. A rendszer feltételezi, hogy a partnerállomások rendelkeznek azonosan installált kulcsrejtjelező kulccsal vagy azzal egyenértékű közös információval, amellyel a küldött, ill. kapott kulcsokat ugyanúgy tudják rejtjelezni és megoldani.



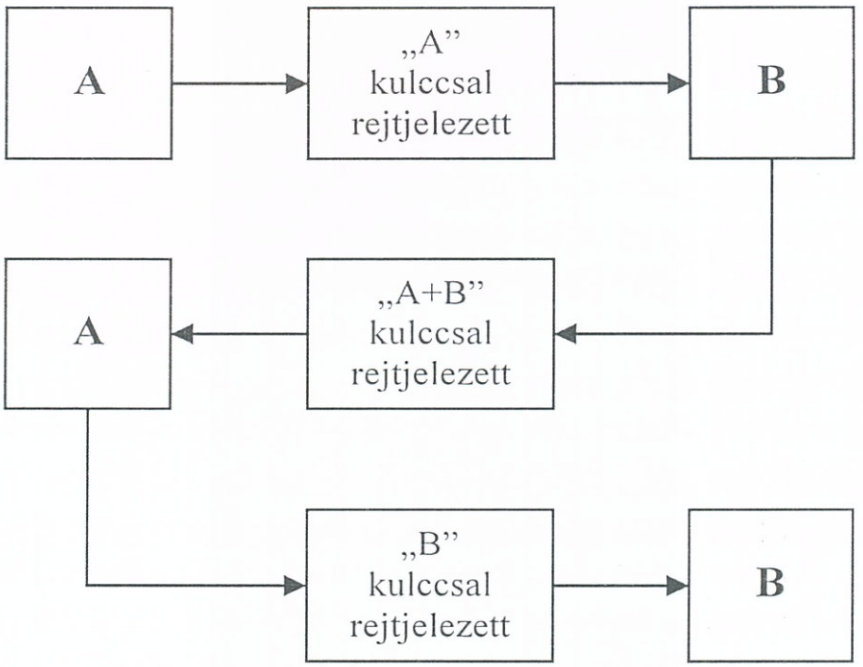
9. ábra.

1. A tényleges (rejtjelezett) üzenet előtt ***A*** rejtjelezett kulcsot (KULCS 1) küld "B"-nek, egyúttal felszólítja ***B***-t válaszkulcs küldésére.
2. ***B*** megfejti a kapott (KULCS 1) kulcsot és az installált konvenciónak megfelelően (KULCS 2) rejtjelezett válaszkulcsot küld vissza ***A*** nak.
3. A kulcscsere lezajlott, mindkét fél rendelkezik olyan közös és csak számukra ismert információval, amelynek alapján a rejtjeles üzenetforgalom elkezdődhet.

Háromutas kulcsforgalom

Háromutas kulcsforgalom

Egyik megoldás a háromutas kulcsforgalom, ahol csak az üzenete küldik, a kulcsot nem:



10. ábra.

1. *A* saját kulcsaival rejtjelezve üzenetet küld *B*-nek.
2. *B* az üzenet megfejtésére nem tesz kísérletet, hanem azt saját kulcsaival ismét rejtjelezi és így küldi vissza *A*-nak.
3. *A* a saját kulcsaival megfejti az üzenetet (*B* rejtjelezése miatt természetesen ez számára érthetetlen) és a már csak *B* - vel rejtjelezett üzenetet küldi vissza *B* - nek, aki ezt saját kulcsaival képes megfejteni.

Hátránya: Ez a módszer csak speciális feltételeknek megfelelő algoritmusoknál használható. Könnyen támadható, ha egy támadó beépül a rendszerbe, megszerezheti az üzenetet. Elegendő B helyett a saját kulcsát rátenni a küldeményre, és a harmadik fázisban már övé is a féltve őrzött üzenet.

9.6. Nyilvános kulcsú kriptográfia

Nyilvános kulcsú, aszimmetrikus kriptográfia

Az érdemi áttörést végül is a *nyilvános kulcsú*, más néven az *aszimmetrikus kriptográfia* hozta meg.

A nyilvános kulcsú kriptográfia története 1974-ben kezdődött. Ralph Merkle a kaliforniai Berkeley egyetem hallgatójaként elhatározta, hogy megoldja egy titkosított kommunikáció két résztvevője között a kulcscsere problémáját. Dolgozatának a *„Biztonságos kommunikáció nem biztonságos csatornán"* címet adta. Professzora egyszerűen nem értette meg Merkle-et, cikkét a *Communications of the ACM* című vezető számítástudományi szaklap is visszadobta első körben. Az egyik bíráló szerint ötlete kriptográfiai nonszensz, hibás tudomány, hiszen mindenki tudja, hogy a kriptográfiai kulcsokat titokban kell tartani.

1975 végén Whitfield Diffie és Martin Hellman kidolgozta a nyilvános kulcsú kriptográfia elvét és publikálták is azt. Működőképes, gyakorlatban alkalmazható modellt még nem produkáltak, csak leírták, hogy milyen módszer lenne alkalmas a feladat megoldására, ha ilyen nyilvános kulcsú módszer már létezne. Matematikai alapja a számelmélet Fermat tétele, és az a tény, hogy a nagy számok osztóinak meghatározása rendkívül bonyolult feladat.

1976 tavaszán három fiatal MIT (Massachusetts Institute of Technology) professzor: Ronald Rivest, Adi Shamir és Len Adleman nekigyürkőzött a feladatnak.

Az algoritmust - felfedezői nevének kezdőbetűiről - **RSA algoritmusnak** nevezték. A meghökkentően egyszerű, napjainkban is legerősebbnek tartott algoritmus publikus, mindenki számára elérhető. Az algoritmus a prímszámok számelméleti tulajdonságára épül: amilyen egyszerű két prímszámot összeszorozni, ugyanolyan nehéz faktorizálni, azaz a szorzat alapján megállapítani, hogy mely számokat is szoroztuk össze.

A feltalálók 1982-ben Jim Bidzosszal összefogva megalapították az RSA Data Security nevű céget. Jelenleg jó néhány titkosítással kapcsolatos szoftvert forgalmaznak, többek között Rivest eddig elkészült algoritmusait: az RC2-t és az RC4-t, RC5-t. Rivest márkavédjegye az RC1-RC9 algoritmus, noha még nincs is mind készen, és RC2 van a Netscape webböngészőben is. Az aktuális algoritmusokat meg lehet találni a WEB-en a www.rsa.com alatt.

A cég tulajdonosai időről-időre pénzjutalmat tűznek ki a legújabb algoritmusok feltörésére. Ilyenkor a világ minden sarkából összefognak a vérbeli „netterek", akik ugyan személyesen soha sem találkoztak, de egy-egy csapatot alkotnak. Ezek a csoportok egymással versengnek, időnként összeolvadnak. Ebben a versenyben rendszeresen vannak magyar résztvevők is. Egy-egy algoritmus megfejtése komoly szakmai presztízst jelent, másrészt nagyszerű – bár roppant időigényes – szórakozás.

PGP

Az RSA felfedezése után néhány évvel, Philip Zimmermann az RSA-algoritmust felhasználóbarát, ügyes szoftverbe csomagolta, melynek a PGP (Pretty Good Privacy - Egészen Tisztességes Titkosítás) nevet adta.
A PGP e-mail-ek és adatfájlok titkosítását teszi lehetővé. Széleskörű szolgáltatásokat biztosít: magában foglalja a kulcsfájlkezelést, az elektronikus aláírást, az adatok tömörítését is. Nagy biztonságot nyújtó titkosító program, mely MSDOS, Unix, VAX/VMS, és sok más operációs rendszer alatt fut.
Megjelenése nagy viharokat váltott ki. AZ USA törvényei szerint erős rejtjelező rendszereket nem lehet onnét exportálni. A

PGP is az exporttilalom alá esett. Csak a legújabb 6.0.2i verzió legális az USA és Kanada területén kívül is.

A PGP megjelenésére ismét fellángoltak a viták: a világon bárhol a PGP révén egy gyakorlatilag feltörhetetlen rendszert használhat bárki. Használhatják bűnözők, maffiózók, anarchisták, kémek - hangzik a bűnüldözők érve. Használhatják befektetők, digitális tranzakciók lefolytatói, bárki, akinek hiteles információra van szüksége, illetve akinek ügylete egyszerűen bizalmas - így a másik, polgárjogi oldal. A programrutin viharos gyorsasággal terjed. A siker oka: Philip Zimmermann a programot az Interneten keresztül mindenkinek a rendelkezésére bocsátotta, ingyen. (Elérhető a www.pgp.com – on.)

Ezzel párhuzamosan az egyre erősebb, nehezebben megfejthető algoritmusok kifejlesztésével számos kutató foglalkozik napjainkban is. Az is érthető, hogy a jónak ítélt algoritmusok megfejtésére is vannak állandó kísérletek. Az elmúlt években az is előfordult, hogy egy szerző saját "feltörhetetlennek" hitt algoritmusának megfejtésével vívott ki magának tudományos elismerést.

Összefoglalva

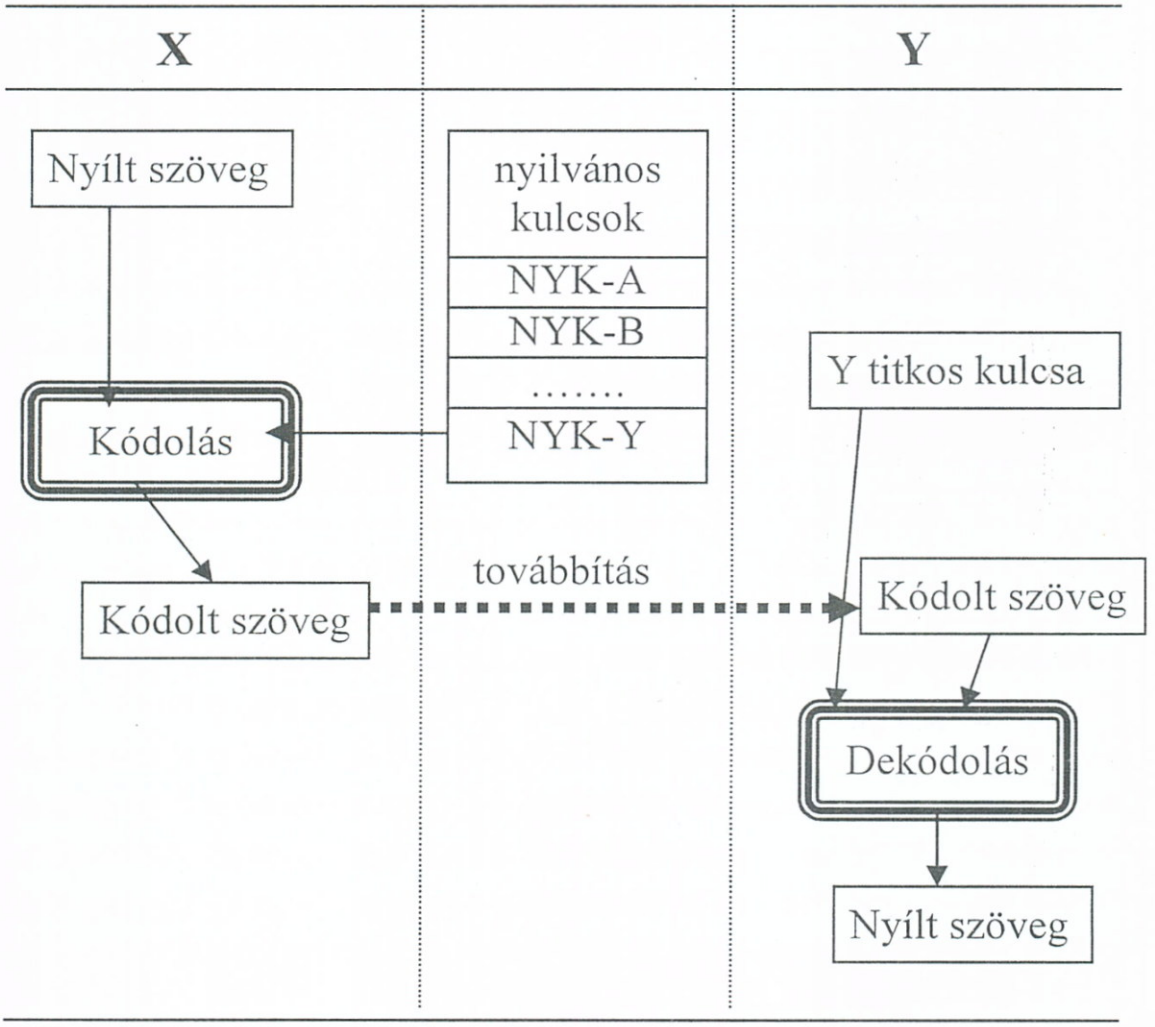
Nyilvános és privát kulcs

A nyilvános kulcsú titkosítás működése egy kétkulcsos lakathoz hasonlítható, amely olyan speciális tulajdonsággal bír, hogy ha az egyik kulccsal bezárták, akkor kizárólag a másikkal nyitható.

A nyilvános kulcsú rendszerek használói két kulccsal rendelkeznek. A mindenki által elérhető kulcsot **nyilvános kulcsnak** nevezik, amelynek ismeretében csak a kódolás végezhető el.
A dekódolásra csupán annak van esélye, aki a nyilvános kulcshoz tartozó **privát vagy titkos kulcsot** ismeri. A nyilvános kulccsal még a kódolást végző sem tudja dekódolni az általa titkosított üzenetet.

Természetesen a nyilvános és a titkos kulcs szoros összetartozása ellenére a nyilvános kulcsból a titkos kulcs előállítására nagyon sok időre lenne szükség, azaz belátható időn belül ez lehetetlen. Megfelelő nagyságú kulcs esetén a megoldás technikai kivitelezhetetlensége szolgáltatja a biztonságot. A „megfelelő nagyság" itt kritikus szerepet játszik: a kezdetben biztonságosnak ítélt 40 bit hosszú kulcsok helyett ma nem nevezhető biztonságosnak 1024-nél rövidebb kulcs. A számítási kapacitások növekedésével ez az érték is nőni fog.

Aszimmetrikus, vagy nyilvános kulcsú rejtjelezés sémája
(X üzenetet küld Y-nak)



11. ábra

9.7. Elektronikus aláírás

Az X.800-as szabvány második biztonsági mechanizmusa a digitális vagy elektronikus aláírás. Ebben a részben ezzel a témával foglalkozunk.

Az elektronikus aláírás fő funkciója, hogy tanúsítsa az aláíró személyazonosságát, vagyis hogy az üzenet tőle és nem mástól származik, illetve, hogy az üzenetet nem változtatták meg illetéktelenül.

A hiteles aláírás rendelkezik az alábbi tulajdonságokkal:

- hamisíthatatlan
- nem használható fel újra
- letagadhatatlan
- megváltoztathatatlan

A digitális aláírás egyik fő eleme az aláírandó szövegből készített kivonat.

Kivonatok

Kivonatok készítése - Hash függvények

A digitális aláírás készítése során a hitelesítendő hosszú dokumentumokhoz egy rövid karaktersorozatot rendelünk. Lényeges, hogy minden dokumentumhoz különböző karaktersorozat tartozzon. A leképezést, amely ezt a feladatot megoldja, **Hash függvénynek** vagy magyarul hasító függvénynek nevezzük. A leképezés eredménye a **kivonat** vagy **digitális újlenyomat** vagy **zúzalék** vagy **Hash érték**. A sok elnevezés közül – az egyszerűség kedvéért - a továbbiakban mi a *kivonatot* használjuk, de a többi is egyenértékű vele.

A kivonatot mindig az aláírandó dokumentumból készítjük. A módszer lényege, hogy a szöveget karakterblokkra osztjuk, és ezeken valamilyen matematikai műveletet hajtunk végre, melynek eredménye egy rövid karaktersor.

A biztonságos Hash függvény rendelkezik az alábbi tulajdonságokkal:

- **egyirányú** - gyakorlatilag lehetetlen belőle előállítani az eredeti szöveget,
- **ütközésmentes** - két szöveg kivonata mindig eltérő,
- **lavina hatású** – a szövegben 1 bit változtatás a kivonatban jelentős változást idéz elő.

Rejtjelezés

A digitális aláírás másik alapeleme a rejtjelezés, ami biztosítja az aláírás egyediségét és hamisíthatatlanságát. A szövegből készült kivonatot valamilyen módszerrel rejtjelezik, és az így kapott karaktersor lesz maga a digitális aláírás.

A kivonat rejtjelezésére bármilyen módszer használható, azonban az előző fejezetben már tárgyalt előnyei miatt az aszimmetrikus vagy nyilvános kulcsú rejtjelezési módokat ajánlja a magyar törvény is.

Az aláírt dokumentum elfogadása csak akkor jöhet létre, ha a kommunikáló felek előre megállapodnak a használandó Hash függvényben és a rejtjelezési módszerben.

Időbélyegző

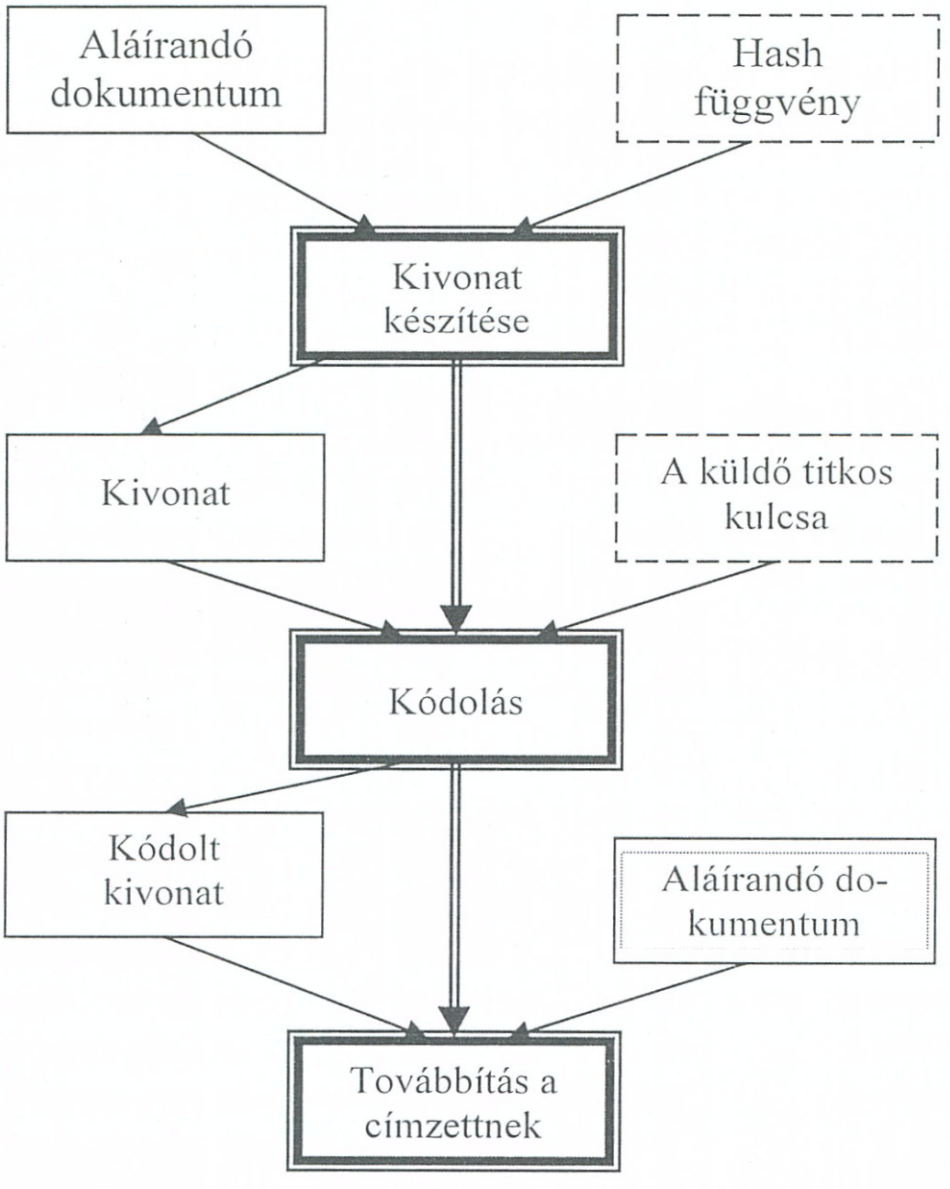
Időbélyegző

Az elektronikus irathoz hozzárendelt igazolást, amely tartalmazza a bélyegzés időpontját, és a dokumentum tartalmához technikailag úgy kapcsolódik hogy minden módosítást érzékelhetővé tesz, időbélyegzőnek vagy időpecsétnek nevezzük.

A digitális aláírás készítése a következő lépésekből áll:

Aláírás készítése

1. Az aláírandó dokumentumból Hash függvény segítségével kivonat készítése.
2. A kivonat kódolása az aláíró titkos kulcsával.
3. Az aláírt dokumentum továbbítása a címzettnek.

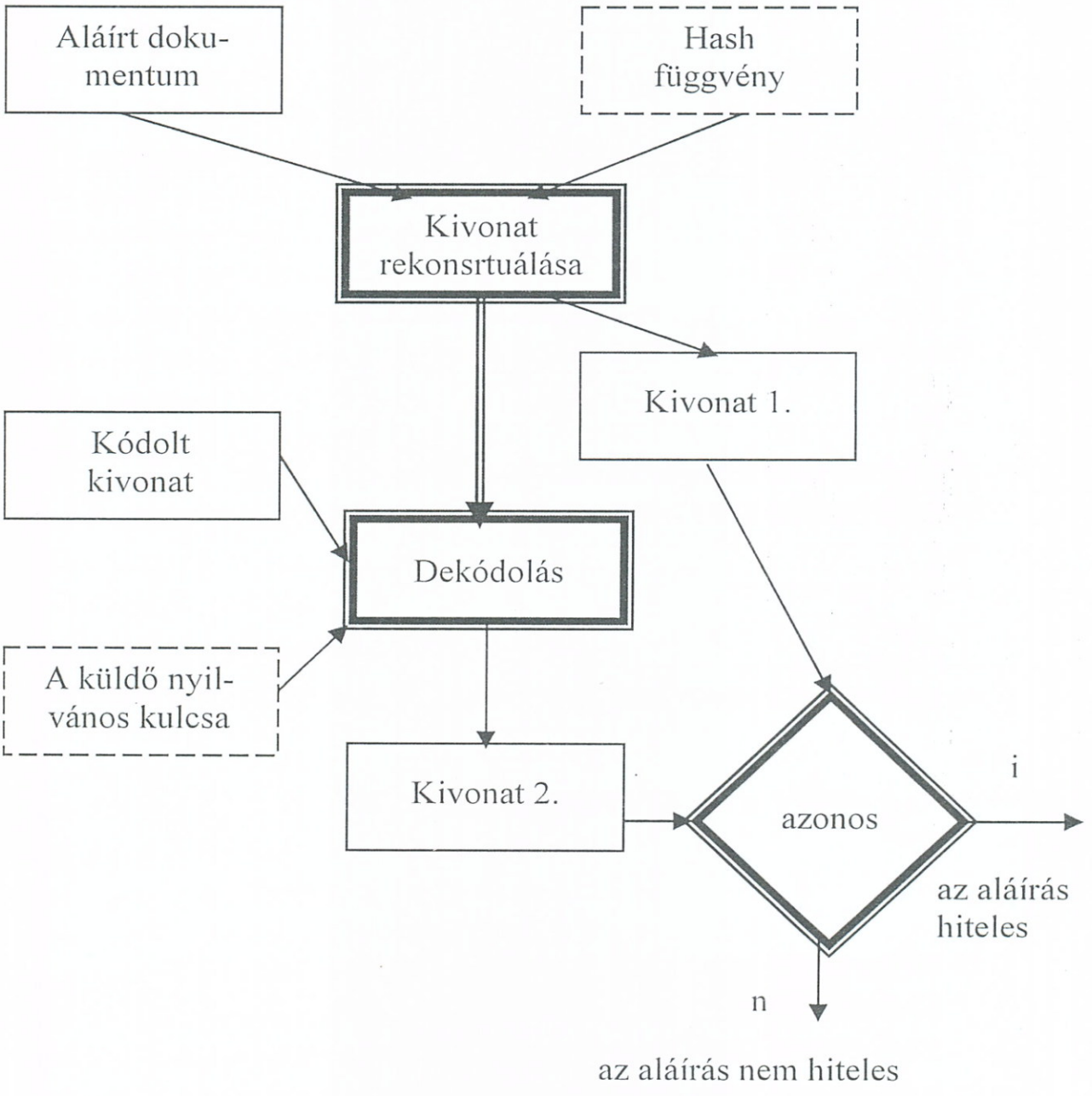


12. sz. ábra

A digitális aláírás ellenőrzése

Aláírás ellenőrzése

1. A megkapott dokumentumból a Hash függvény segítségével a címzett is előállítja a kivonatot.
2. A csatolt kódolt kivonatot a feladó nyilvános kulcsával dekódolja.
3. A két kivonatot összehasonlítja. Az azonosság bizonyítja, hogy a dokumentum szövegét nem változtatták meg és az aláíró személye hiteles, mivel csak az ő kulcsával lehet visszafejteni a kódolt kivonatot.



13. ábra

Törvény az elektronikus aláírásról

2001. évi XXXV. törvény

A Magyar Országgyűlés 2001. május 29-én fogadta el a 2001. évi XXXV. törvényt az elektronikus aláírásról, ami az év szeptemberétől hatályos. Ezzel az állam megteremtette az elektronikus kereskedelem jogi hátterét. A törvény ezt így fogalmazza meg:

„Az Országgyűlés – felismerve és követve az egyetemes fejlődésnek az információs társadalom felé mutató irányát, az új évezred egyik legfontosabb kihívásának eleget téve – törvényt alkot az elektronikus aláírásról annak érdekében, hogy megteremtse a hiteles elektronikus nyilatkozattétel, illetőleg adattovábbítás jogszabályi feltételeit az üzleti életben, a közigazgatásban és az információs társadalom által érintett más életviszonyokban."

Hírközlési Felügyelet

A hiteles elektronikus aláírás jogszabályi feltétele, hogy ezt egy arra jogosult hitelesítés-szolgáltató személy vagy szervezet tanúsítsa. Magyarországon ezeket a szolgáltatókat a Hírközlési Felügyelet (HÍF) veszi nyilvántartásba. A hitelesítő-szolgáltatóknak bejelentést kell tenniük 30 nappal működésük előtt, tevékenységüket pedig csak akkor kezdhetik meg, ha a HÌF felvette őket a nyilvántartásba.

A HÌF rendszeresen ellenőrzi a szolgáltatók működését. Ha szabálytalanságra bukkannak, a figyelmeztetésen túl pénzbüntetést is kiszabhatnak a szolgáltatóra, visszavonathatják az általa kiadott tanúsítványokat, és igazán súlyos esetben akár törölhetik is a nyilvántartásból.

Az elektronikus aláírás alkalmas arra, hogy bármely fajta adatot aláírjanak vele, tehát nemcsak írott szöveget, hanem pl. egy digitális hangfelvételt, képet vagy egy szoftvert. A törvény háromfajta elektronikus dokumentumot különböztet meg.

- *Elektronikus dokumentum:* bármely fajta elektronikus eszköz útján érzékelhető adat, melyet elektronikus aláírással láttak el.
- *Elektronikus irat:* olyan elektronikus dokumentum, melynek funkciója szöveg betűkkel való közlése és a szövegen kívül az olvasó számára érzékelhetően kizárólag olyan egyéb adatokat foglal magában, melyek a szöveggel szoro-

san összefüggenek, annak azonosítását (pl. fejléc), illetve könnyebb megértését (pl. ábra) szolgálják.
- *Elektronikus okirat:* olyan elektronikus irat, mely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy nyilatkozat kötelezőnek elismerését foglalja magában.

A törvény az elektronikus aláírás három típusát különbözteti meg:
- *Egyszerű elektronikus aláírás* - beletartozik mindenfajta technológiai biztonságot nélkülöző eljárás is, ha az aláíró egy elektronikus szöveg végére odaírja a nevét vagy más azonosítóját. Ezt a bíróság sem köteles elfogadni.
- *Fokozott biztonságú elektronikus aláírás* - ez alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető, olyan eszközökkel hozták létre, melyek kizárólag az aláíró befolyása alatt állnak és a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető.
- *Minősített elektronikus aláírás* - a HÍF által nyilvántartásba vett hitelesítés-szolgáltató minősíti, így bizonyíthatóan igazoló erejű.

Adatvédelem

A törvény igazodik az alapvető adatvédelmi normákhoz. A hitelesítés-szolgáltatók csak az aláírótól közvetlenül, vagy annak hozzájárulásával gyűjthetnek személyes adatokat de olyan mértékben, ami a tanúsítvány kiadásához szükséges. Az adatokat az adatalany beleegyezése nélkül nem lehet más célra gyűjteni, felhasználni, valamint harmadik személynek továbbítani.

A hitelesítés-szolgáltató bűncselekmények felderítésére vagy megelőzésére illetőleg nemzetbiztonsági érdekből személyazonosságot igazoló adatokat köteles továbbítani a megfelelő hatóságoknak.

9.8. Információbiztonsággal foglakozó szervezetek

Szinte naponta jelennek meg új szoftverek és hardverek. Ezeknek a beépítése a rendszerbe újabb biztonsági kérdéseket vet fel. A biztonsági kérdésekkel foglakozó szakértők, csoportok és szervezetek állandóan újabb és újabb biztonsági réseket találnak mind az újabb, mind a régebbi termékeken. Az Internet nem csak a betörések útvonala, hanem rengeteg olyan információt találhatunk rajta, amely segít megelőzni a bajt. Vannak hivatalos szervezetek, önszerveződő csoportok, számítástechnikai eszközöket gyártók, speciálisan biztonsági termékeket forgalmazó cégek, amelyek webhelyein hasznos információkat találunk.

CERT

Egyik ilyen a CERT (Computer Emergency Response Team – Számítógépes Vészhelyzet-elhárító Csoport). A fenyegetettség mindig összehozza a szenvedő alanyokat: 1988-ban megalakult az USA-ban a CERT amelyet követtek a többiek Európában és a világ más tájain. A folyamatosan alakuló CERT csoportok nemzetközi koordinációját ellátó FIRST (Forum of Incident Response Teams – Incidens Elhárító Csoportok Bizottsága) megalakítására 1991-ben került sor. 1996-tól létezik a magyar szervezet is HUNGARY CERT néven. Fő feladata a Magyarországon működő Internet kapcsolattal rendelkező számítógéphálózatokkal összefüggő biztonságtechnikai problémák kezelése, illetve azok megelőzése.

Az információk elérhetők a www.cert.org és a www.first.org címeken. A www.cert.hu címen hasznos információk találhatók a különböző védekezési módokról, szoftverekről, gyártókról magyar nyelven.
Az informatikai rendszerek auditálásával a ISACA (Information System Audit and Controll Assitiation) szervezet foglakozik már 1969 óta. A szervezet több szabványt dolgozott ki, pl. a COBIT-ot (lásd a 5.7. pont) Az ISACA szervezi világszerte a biztonsági auditorok vizsgáztatását, amelyen a CISA minősítést lehet megszerezni. (Certifed Information System Auditor).

Bővebb információk a www.isaca.com, illetve a www.isaca.hu címeken.
A Gyártók általában a saját weboldalukon külön fejezetet szentelnek a biztonsági kérdéseknek. Pl. a Microsoft ilyen címe: www.microsoft.com/security/ .

Ellenőrző kérdések

1. Mi a kriptográfia feladata?
2. Mi az alábbi fogalmak meghatározása?
   nyílt információ, rejtjeles információ, rejtjelezés, megfejtés, algoritmus, kulcs.
3. Mit nevezünk szimmetrikus kriptográfiának? Milyen módszereit ismeri?
4. Milyen kulcstovábbító módszereket ismer?
5. Jellemezze a nyilvános kulcsú rendszereket!
6. Hasonlítsa össze a szimmetrikus és az aszimmetrikus kriptográfiai rendszereket!
7. Mit jelent a kulcsmenedzsment?
8. Mi az abszolút biztos csatorna?
9. Mit jelent a háromutas kulcsforgalom?
10. Mik a kriptográfiai rendszer alapelvei, milyen elemei vannak?
11. Mi az elektronikus aláírás?
12. Mik az elektronikus aláírás készítésének és ellenőrzésének lépései?
13. Milyen típusú dokumentumokat és digitális aláírásokat különböztet meg a törvény?
14. Hogyan történik a hitelesítő-szolgáltatók bejegyzése és ellenőrzése?
15. Milyen nemzetközi szervezetek foglakoznak információbiztonsági kérdésekkel?

TÁRGYMUTATÓ

Irodalomjegyzék

Könyvek:

(1) Almási János: Elektronikus aláírás és társai, Sans Serif, 2002.

(2) Bednay Dezső: Szerzői jog, GDF jegyzet, 2001.

(3) Cronin J. Mary: Az Internet üzleti alkalmazásai, Műszaki Könyvkiadó, 1997.

(4) Dénes Tamás: Titok Tan avagy Kódtörő ABC, Bagolyvár Könyvkiadó, 2002.

(5) Dietz Gusztávné dr., Pap Márta: Adatvédelem, adatbiztonság, Novorg, 1995.

(6) Dravecz Tibor, Párkányi Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket, NIIF Információs füzetek, II/8., 1997.

(7) Dreilinger Timea: Vírusvédelem, PANEM, 2004.

(8) Hance, Olivier: Üzlet és jog az Interneten, Panem-McGraw-Hill, 1997.

(9) Ködmön József: Kriptográfia, Computerbooks, 1999.

(10) Kyas Othmar: Számítógépes hálózatok biztonságtechnikája, Kossuth Kiadó, 2000.

(11) Mojzes I., Talyigás J.: Elektronikus kereskedelem, Technika Alapítvány, 2000.

(12) Nemetz T., Vajda I.: Algoritmikus adatvédelem, Akadémiai Kiadó, 1991.

(13) Norton, Peter: A hálózati biztonság alapjai, Kiskapu Kiadó, 2000.

(14) Raffai Mária: A szoftver világa, Novadat, 1995.

(15) Singh, Simon: Kódkönyv, Park Kiadó, 2001.

(16) Szappanos Gábor: Kirándulás a számítástechnika sötét oldalára, VirusBuster, 2003.

(17) Vasvári György: Biztonsági rendszerek szervezése, PRO-SEC Kft. 1997.

(18) Védd magad az Interneten, Kossuth Kiadó, 1997.

(19) Virrasztó Tamás: Titkosítás és adatrejtés, NetAcademia, 2004.

(20) Visnyei Aladár, dr. Vörös Gábor: A számítógépes információbiztonság alapjai, LSI, 1994.

(21) Vossenberg,Thomas: Hacker kézikönyv, Computer Panoráma, 2002.

Cikkek, előadások:

(22) Csajbók Zoltán - Dr. Pozsgai Szilvia: Az egyszázalékos törvény adatvédelmi elemzése, Magyar Közigazgatás, 1997. október

(23) Nemetz Tibor: Kriptográfiai mondanivaló újonnan beinduló adatvédelmi rendszerek szervezői számára, konferenciaelőadás, Mátraháza, 1995.

Internetes anyagok

(24) dr. Jóri András oldalai http://w3.datanet.hu/~jori/
Az adatvédelemről rendszergazdáknak
Online adatvédelem Németországban
Online adatvédelem és kriptográfia magyarországon
Az illetlenség fogalma az amerikai jogban és a CDA

(25) Mogyorósi István: A banktitok,
http://www.cegnet.hu/cv/9909/jogi/37_41.htm

(26) dr. Verebics János oldalai http://www.extra.hu/verebics/
Legyünk az ördög zsákmányai,
Coltok szava délidőben
Az Internet jogi problémáinak áttekintés
Információs bűntetőjog

(27) Vikman László: A kéretlen elektronikus reklámok szabályozása, http://www.jogiforum.hu/publikaciok/

Módszertani anyagok és beszámolók:

(28) Az adatvédelmi biztos web-oldala
http://www.obh.hu/abi/

(29) Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, Informatikai Tárcaközi Bizottság 8, 12, 13 számú ajánlásai, Budapest 1994.-1999. (www.itb.hu)

(30) Oros - Szurday: Adatvédelem az Európai Unióban, Európai Füzetek 35. Külügyminisztérium

(31) Információvédelmi Irányítási Rendszerek
http://www.hopet.hu/1_hu.html

Lingyüjtemények:

(32) http://adatvedelem.lap.hu/

(33) http://informaciobiztonsag.lap.hu/

(34) http://internetbiztonsag.lap.hu/

(35) http://spam.lap.hu/

(36) http://virus.lap.hu/

... stb

1. sz. melléklet

A témához kapcsolódó jogszabályok

1978. évi IV. törvény	A Büntető Törvénykönyvről.
1990. évi LXXXVI.	A tisztességtelen piaci magatartás tilalmáról
1992. évi LXIII. törvény	A személyes adatok védelméről, a közérdekű adatok nyilvánosságáról
1992. évi LXVI. törvény	A polgárok személyes adatainak nyilvántartásáról
1995. évi LXV. törvény	Az államtitokról és a szolgálati titokról
1995. évi LXVI. törvény	A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről
1995. évi CXIX. törvény	A kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről
1996. évi XII. törvény	a hitelintézetekről és a pénzügyi vállalkozásokról
1996. évi XX. törvény	A személyi azonosító jel helyébe lépő azonosítási módokról és azonosító kódok használatáról
1998. évi VI. törvény	Az egyének védelméről a személyes adatok gépi feldolgozása során, Strassbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről
1999. évi LXXVI. törvény	A szerzői jogról
1999. évi LXXXV. törvény	A bűnügyi nyilvántartásról és a hatósági erkölcsi bizonyítványról
2000. évi IV. törvény	Az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről

2001. évi XXXV. törvény	Az elektronikus aláírásról
2001. évi CVIII. törvény	Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
2003. évi XV. törvény.	A pénzmosás megelőzéséről és megakadályozásáról
2003. évi XXXIX. törvény	A hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény módosításáról
2003. évi XLVIII. törvény	A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításáról
2003.évi LIII. törvény	Az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény, valamint azzal összefüggésben más törvények módosításáról
2003. évi XCVII. törvény	Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény módosításáról

A témához kapcsolódó kormányrendeletek:

43/1994. (III.29.) Korm. rendelet	A rejtjeltevékenységről
151/2001. (IX. 1.) Korm. rendelet	A Hírközlési Főfelügyeletnek az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól
232/2001. (XII. 10.) Korm. rendelet	A pénzforgalomról, a pénzforgalmi szolgáltatásokról és az elektronikus fizetési eszközökről