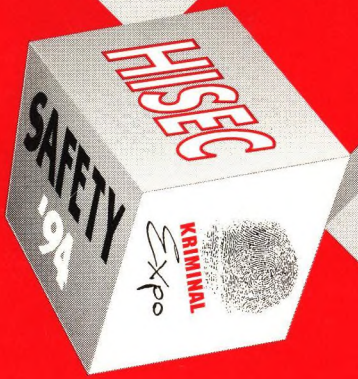


COMPEXPO

ÜGYÉSZEK ORSZÁGOS EGYESÜLETE 1990

nj SZÁT

Budapest, 1994 június 8-11

KOMMUNIKÁCIÓ A BIZTONSÁGOS VILÁGÉRT

Adatvédelem, adatbiztonság

HISEC '94

Budapest, 1994. június 8-11.

Felelős kiadó: *Neumann János Számítógéptudományi Társaság*
Készült: *a CORNER Bt. gondozásában*
Szerkesztette: *Papp György*

ISBN 963 8431 81 4

ELŐSZÓ

A biztonság iránti igény nagy erővel jelenik meg napjainkban mind hazai, mind nemzetközi szinten. Az emberek biztonságos életre vágynak, amelyben szeretnék látni, hogy az emberiség jobb korszakba kerülhet, nem pusztítva el sem önmagát sem környezetét. Az eltérő nagyságrenddel és hangsúllyal megfogalmazódó problémák globálisan jelennek meg a tekintetben, hogy egymás nélkül és egymás ellenében nem oldhatók meg. A problémák kezeléséhez, megoldásához nemcsak nemzeti, hanem nemzetközi összefogásra is szükség van. A nemzeti és nemzetközi együttműködés sikerének minimális követelménye a kommunikáció, a párbeszéd, amelynek segítségével jobban megérthetők az egyedi gondok, jobban felismerhetők az összefüggések.

Magyarországon eddig egymástól elszigetelve, külön rendezvények foglalkoztak biztonság kérdéseivel. Az egyedi célkitűzések egymást erősítő folyamatának érdekében, idén kerül először közös megrendezésre az élet különböző területein jelentkező biztonsági témák megvitatása, keresve az összefüggéseket, a közösen kezelhető megoldások lehetőségeit. A nagyszabású rendezvény felöleli az adatvédelem és adatbiztonság (HISEC) témakörön túl többek között a környezetvédelem, a közlekedésbiztonság, a bűnüldözés, a személyvédelem és a vagyonvédelem kérdésköröket is.

Az adatvédelem és adatbiztonság témakörrel, mint ahogy arra a múlt évi HISEC konferencia is rámutatott, össztársadalmi szinten is foglalkozni kell. Demokratrikus átalakulási folyamatunk különösen fontossá teszi a problémák megértését és kezelhetőségét. Közigazgatásunk reform folyamaton megy át. Az egyéni, a csoport és a társadalmi érdekek nem találkoznak mindig. Ezek, az együttélési normák legfontosabb pilléreinek, a személyiségi jogok védelmének és az információ szabadságnak összeegyeztetésével érvényesíthetők. Társadalmunkban végbemenő változások, európai integrációs törekvésünk ezekből táplálkozhat, függetlenül a kapcsolatrendszertől, legyen az információs rendszer, számítógépes feldolgozórendszer vagy informatikai hálózat.

A második HISEC konferencia szeretne képet adni adatvédelmi hangsúllyal a közigazgatási informatikai átalakulás már megtett és előttünk álló lépéseiről. Ebben a folyamatban különös aktualitása van a képviselői választás adatvédelmi és adatbiztonsági kérdéseinek. Szeretné bemutatni a személyiségi jogok védelme érdekében hozott adatvédelmi jogszabályok (személyi adatok, és annak részterületén az egészségügyi adatok, stb.) terén elért eddigi eredményeinket és rámutatni a még előttünk álló tennivalókra.

A konferencia a jogi ismeret bővítés és probléma felvázoláson túl ismételten teret ad a korszerű számítástechnikai adatbiztonsági megoldások egyedi, valamint rendszerszintű bemutatásának.

Tartalomjegyzék

HISEC '94

Előadások

Az országgyűlési választások információtechnológiai háttere

Kovács Zoltán
Országos Személyiadat- és Lakcímnyilvántartó Hivatal (OSZH)

A számítógép alkalmazások végig kísérik a választási folyamatot, annak majdnem minden mozzanatát a névjegyzékek összeállításától a választás utáni kiadványok nyomdába adásáig.

A választás kitűzése után az első feladat a választói névjegyzékek elkészítése. Ehhez először el kell végezni az úgynevezett körzetesítést, amelynek során minden lakcímhez, illetve az ott lakó választópolgárhoz hozzárendelődik annak a szavazókörnek a száma és címe, ahol a polgár szavazni fog. A választói névjegyzék a személyiadat- és lakcímnyilvántartás alapján készül, amelyből a kiskorúak és külföldiek kihagyásával leválogatásra kerülnek a választójogosultak. Tovább szűkíti ezt a listát azoknak a törlése, akiknek a törvényben meghatározott okokból nincsen választójoga (közügyektől eltíltottak stb.). A választói névjegyzék ezután kinyomtatásra kerül a jegyzők és a választási szervek számára, illetve elkészülnek az választópolgároknak kézbesítendő értesítő szelvények (kopogató cédulák). Az idei parlamenti választásokhoz a

névjegyzékek alapvetően a megyei adatbázisokból készültek (a fővárosban az OSZH adatbázisából), de lehetőség volt arra is, hogy a önkormányzatok maguk állítsák elő azokat. A technikai hátteret illetően a megyei adatbázisok a TÁKISZ-oknál (Területi Államháztartási és Közigazgatási Szolgálat) üzemelnek, ahol egy ETHERNET LAN-ra kapcsolt VAX számítógép működik VMS operációs rendszerrel és DBMS adatbázis kezelővel.

Azok a választópolgárok, akik jelöltként kívánnak indulni, kötelesek 750 ajánlószelvényt összegyűjteni a jelölés bejelentéséhez. Az egyéni választókerületi választási bizottságok a jelölés elfogadásának folyamatában számítógép segítségével ellenőriztethetik az ajánló szelvényeket abból a szempontból, hogy az ajánló választópolgár létezik-e (személyazonosító jele, neve, lakcíme helyesen van-e feltüntetve az ajánlószelvényen), van-e választójoga, illetve lakóhelye abban az egyéni választókerületben van-e, amelyben jelöltet ajánlott. Az ajánlószelvények ellenőrzése a személyiadat- és lakcímnyilvántartás adatbázisa alapján történt, zömében a megyei adatbázisok felhasználásával, de lehetőség volt a helyi adatbázist is lekérdezni. A megyei adatbázis használata a célszerűbb, mert egy egyéni választókerület általában több települést foglal magába.

A választási információrendszerek közül az egyik legfontosabb a jelölt adatbázis. Ez tartalmazza:
- a választáson induló pártok adatait;
- az egyéni jelölteket és az őket indító pártokat;
- az egyéni jelöltek töredékszavazat megosztását;
- a megyei pártlistákat, közös listákat és listakapcsolásokat;
- a megyei listák kisorsolt sorrendjét;
- az országos pártlistákat, közös listákat és listakapcsolásokat;
- az országos listák kisorsort sorrendjét.

A jelölt adatbázis az OSZH VAX gépén üzemelt Rdb adatbázis kezelővel. A jelölt adatbázist távadatfeldolgozó hálózaton keresztül érték el az egyéni és területi választókerületi munkacsoportok, valamint az Országos Választási Munkacsoport. Ez fizikailag azt jelentette, hogy 148 egyéni választókerületi székhely városból, 20 megye székhelyről és Budapesten különböző telephelyekről kellett biztosítani az adatbázis on-line elérését. Az egyéni választókerületekben a technikai hátteret személyi számítógép, 2400 Baud-os modem és kapcsolt telefonvonal jelentette. A megye székhelyektől az OSZH-ig DECnet hálózat működik.

A jelölt adatbázis a teljes jelölési folyamat során gyűjti a választás alapadatait, tájékoztatja a választási szerveket, a pártokat, a jelölteket és a közvéleményt azokról. Ez képezi a szavazatösszesítő rendszerek alapját, de ennek adataiból készíti a nyomda a szavazócédulákat és egyéb választási iratokat is.

Az országgyűlési választási rendszer hierarchiáját jellemzi a 20 megye, a 176 egyéni választókerület, a 3135 település és a mintegy 11.000 szavazókör. Ezekre a pontokra kell eljuttatni megfelelő mennyiségben különböző formájú és adattartalmú választási nyomtatványokat, segédanyagokat. Az idei országgyűlési választásoknál sikerült először elérni, hogy a szavazókörökben kitöltendő adatlapokra és jegyzőkönyvekre előzetesen rá legyenek nyomtatva az ott induló jelöltek és pártok. A nagytömegű papír nyomdai előállítását és elosztási mechanizmusát számítógépes rendszer támogatta.

A választás napján reggel 7-től a napközbeni jelentések információrendszere üzemel, amelynek keretében háromszor összegyűjtjük az addig megjelent választók számát, illetve regisztráljuk a választáson bekövetkezett rendkívüli eseményeket. A rendszer nemcsak a választójogosultak, a szavazókörök és a választáson melgjelentek számáról tájékoztat országosan, megyénként és egyéni választókerületenként, hanem összehasonlításokat is tartalmaz korábbi választások adataival. Technikailag a rendszer a korábbiakban vázolt számítógépes hálózaton üzemel azzal a kiegészítéssel, hogy a országos adatok megjelennek a Duna Palotában is az oda telepített ETHERNET hálózaton, amely egy VAX gépet és 20-30 tájékoztató PC-t tartalmaz. A Duna Palota és az OSZH közötti összeköttetés bérelt vonalakon gyors modemekkel valósult meg.

A választási információrendszerek legnagyobb érdeklődésre számottartó elemei a szavazatösszesítők. Az idei parlamenti választások kiszolgálására két, egymástól független szavazatösszesítő rendszer került kidolgozásra. Az első az előzetes eredményt szolgáló rendszer, amelynek jellemzői, hogy:

- a választást követő éjszakán üzemelt és gyors eredményt adott az erre a célra rendszeresített adatlapok feldolgozásával;
- köztisztviselők működtették;
- eredménye nem hivatalos.

A második összesítő a végleges jogi eredmény megállapítását támogató rendszer, amelyet a szavazóköri jegyzőkönyvek alapján működtetnek a választási szervek, opcionálisan. Ez azt jelenti, hogy a választási szervek alapértelmezésben manuálisan összesítenek, de saját döntésük alapján használhatnak számítógépet is.

Az előzetes szavazatösszesítő rendszer működését a sajtó és a közvélemény az 1990. évivel hasonlította össze, de ez a rendszer sokkal közelebb állt az 1993-as társadalombiztosítási választásoknál használt összesítőhöz. A rendszer négy szinten használ számítógépeket, mivel a szavazókörökben még egyáltalán nincs gépesítés:

- a nem egyéni választókerületi székhely települések az adatlapok rögzítése céljából ún. helyi rögzítő rendszert használhatnak, opcionálisan. Ebben az esetben az egyéni

választókerületi székhelyekre floppyn érkeznek az adatok, ami csökkenti a rögzítési munkát;

- az első kötelező gépesítési szint az egyéni választókerületi székhelyek szavazatösszesítő rendszere. A társadalombiztosítási választásokhoz képest itt történt a legnagyobb változás, az addigi függelten PC-kből álló rögzítő-ellenőrző-összesítő-továbbító konfigurációt egy helyi ETHERNET hálózatra cseréltük, amelynek legnagyobb kapacitású gépe egy IBM RISC/6000 modell 220 vagy 250, attól függően, hogy az önkormányzat kisebb, vagy nagyobb gépet választott. A gépek beszerzése fele-fele arányban önkormányzati, illetve központi forrásból valósult meg. A RISC/6000 kiválasztása versenytárgyalás útján történt, bevonva a döntésbe az önkormányzatok érdekképviseleti szerveit. Ez a beszerzés remélhetőleg elő fogja segíteni az önkormányzatok informatikai fejlődését, mivel az eddigi, szinte kizárólag személyi számítógépekre alapuló fejlesztés és alkalmazás új irányt vehet az átfogó alkalmazások és a nyílt rendszerek felé;
- a megyei rendszer alapját a TÁKISZ-ok VAX gépei képezik, amelyek épületen belül egy ETHERNET hálózaton üzemelnek, egy DECwanrouter-en keresztül pedig az országos DECnet hálózatba vannak kötve. A területi választási bizottságok tájékoztatása sok megyében szintén távadatfeldolgozással történt, vagy úgy, hogy a TÁKISZ-ok ETHERNET-jét terjesztették ki a megyei önkormányzati hivatalig, vagy bérelt távbeszélő vonalon modemmel kommunikáltak;
- a szavazatösszesítés központi rendszere három helyszínre települt. Az OSZH számítóközpontjába futnak be a megyei vonalak és itt üzemel a hálózatvezérlés is. Az OSZH azonban nem látott el tájékoztatási feladatokat, azok végrehajtása a Duna Palotában és a Magyar Televízió 4-es stúdiójában történt. A Duna Palota az OSZH-val DECnet kapcsolatban volt, a Magyar Televízió adatellátása a Duna Palotából történt, a Duna Palota ETHERNET hálózatának kiterjesztésével. Fizikailag a kapcsolat mikrohullámú összeköttetéssel és bérelt vonalon valósult meg, több mint 4 Mbit/sec sebességgel. A Teletext a Magyar Televízió ETHERNET hálózatáról kapta az adatokat.

Az előzetes szavazatösszesítő rendszer biztonságának növelése érdekében a távadatfeldolgozó hálózat mellett tartalék útvonalakat is terveztünk. Magán hálózaton belül is át lehetett állni a bérelt vonalról esetenként kapcsolt vonalra. Ha azonban a távadatfeldolgozás bármilyen okból lehetetlenné vált, akkor a rendszer bármelyik szintje fax-ot is tudott fogadni az előző szint összesített adatainak bevitele céljából. A faxos továbbítás meghiusulása esetén a legrögzített bizonylatokat floppyn, vagy magukat a bizonylatokat kellett volna gépkocsival szállítani.

Külön kell szólni a pártok tájékoztató rendszeréről, amely először valósult meg a magyar választások történetében. A rendszer lényege az, hogy a pártok saját székházukban követhetik a

szavazatösszesítés alakulását, számítógépes hálózaton elérve a szavazatösszesítő adatbázis adatait. Fizikailag az összeköttetés a Telecast rendszerrel valósult meg, amely egy modemen keresztül megkapta az elküldendő adatokat, ezeket lesugározta a Magyar Televízió 1-es csatornáján a Teletext adáshoz hasonlóan kódolva. Ezt az adást azonban csak speciális antennával, dekóderrel és személyi számítógéppel rendelkező állomások foghatták.

Összességében a Duna Palotában tájékozódni kívánók adatokat kaptak a választók részvételi arányáról, a választáson induló jelöltekről, pártokról, az általuk elért szavazatokról és a megszerzett mandátumokról. Akik elemzéseket akartak végezni, azoknak rendelkezésükre állt a korábbi választások adatainak történeti adatbázisa, amely az OSZH IBM AS/400 gépén üzemel. A technikai háttér tehát egy heterogén hálózat volt, amelynek hardverjét személyi számítógépek, különböző IBM és DEC számítógépek alkották, a kommunikációt pedig kapcsolt vonalak, bérelt vonalak, mikrohuullámú összeköttetés, valamint a DECnet és a TCP/IP hálózatvezérlő szoftverek segítették.

A választás végleges jogi eredményének kimunkálását támogató számítógépes rendszer nem tartalmaz hálózati elemeket. Az egyéni országgyűlési választókerületekben személyi számítógépeken rögzítik az egyéni jegyzőkönyveket és összesítés után a választási bizottság állapítja meg az eredményt. A feldolgozás adatai papíron és mágneses adathordozón kerülnek az Országos Választási Bizottsághoz. Hasonló módon dolgozik a területi választási bizottság is a listás jegyzőkönyvekkel és az eredmények szintén az Országos Választási Bizottsághoz érkeznek. Az Országos Választási Bizottság ezután a 196 jegyzőkönyv feldolgozásával állapítja meg a választás végeredményét, melyhez szintén számítógépes támogatást kap.

A választások tisztaságának megőrzése érdekében számítógépes rendszerrel vizsgáljuk azt, hogy egy választópolgár nem szavazott-e kétszer vagy többször. Ez a rendszer a választói névjegyzékek kiadása és a választás között eltelt időben bekövetkezett névjegyzék változási adatokat dolgozza fel. A rendszer a korábbiakban említett számítógépes hálózaton üzemel. Eredménye azoknak a választópolgároknak a listája, akiket egy választási forduló alkalmából kétszer, vagy többször jelöltek meg a szavazatszámláló bizottságok választóként, vagyis két vagy több szavazóhelyiségben tették tiszteletüket.

A választások eredményeiről utólag kiadványok készülnek. Az eredmények rendszerezése és nyomdai formára hozása számítógépek alkalmazásával történik.

Az utolsóként említett, de nem kis fontosságú információrendszer a választási költségvetés tervezését, valamint a választással kapcsolatos szoftverfejlesztési, beruházási, nyomdai, szállítási stb. feladatok finanszírozásának követését szolgálja.

A költségvetésnél tartva megjegyzendő, hogy az eddigiekben felsorolt információrendszerek fejlesztése a választási költségvetés 6 %-át emésztette fel. Ennél színvonalasabb információrendszerek bizonyára vannak más országokban, de olcsóbbak aligha. A színvonalat illetően is csak önkritikára van szükség, mert jelen előadás szövegének leadásáig a tíz fejlesztő által kidolgozott rendszerek mindegyike rendeltetésszerűen működött, az előzetes összesítés pedig a nemzetközi megfigyelők megítélése szerint is sikert aratott.

A VÁLASZTÁSI INFORMATIKAI RENDSZER BIZTONSÁGA

Szekér Kálmán **Forró Tibor**
PROTAN Informatikai Biztonsági Tanácsadó Részvénytársaság

Kivonat:

Az 1994. évi országgyűlési képviselő választást támogató informatikai rendszernek a választás jelentősége, a rendszernek a választás lebonyolításában és a tájékoztatásban betöltött szerepe, és a rendszer működését kísérő nyilvánosság következtében kiemelkedő biztonsági követelményeknek kellett megfelelnie. A megvalósítás keretében külső szakértők bevonása is szolgálta a választási informatikai rendszer biztonságának erősítését. Ennek az együttműködésnek általánosítható tapasztalait kísérli meg összefoglalni az előadás. Ennek során részben a rendszer vizsgálatára, kiértékelésére alkalmas megközelítés, részben a választási informatikai rendszert jellemző biztonsági követelmények és fenyegetések néhány sajátos vonása kerül röviden ismertetésre.

Bevezetés

Az 1994. évi országgyűlési képviselő választást támogató informatikai rendszer sokszereplős, hosszú fejlesztési folyamat eredménye. Ebbe a folyamatba kapcsolódott bele a PROTAN Rt., amikor megbízást kapott a választási informatikai rendszer biztonsági kiértékelésére, a biztonságot erősítő javaslatok megfogalmazására.

Feladatunk sajátos vonásai közé tartozott, hogy egy, a megvalósítás végső szakaszában lévő rendszerről kellett véleményt alkotni. A megvalósítás során a fejlesztők figyelme kiterjedt biztonsággal kapcsolatos problémák kezelésére is. Szerepünk így nem egy újonnan felmerült szempont - a biztonság szempontjának - érvényesítése volt, hanem annak a lehetőségnek a kiaknázása, amelyet minden problémamegoldás esetén egy további ellenőrzési pont, egy független külső vizsgálat jelent.

Tevékenységünk kiterjedt az informatikai rendszert alkotó egyes szoftver modulok, valamint az informatikai rendszer működésének alapját képező adatátviteli rendszer vizsgálatára, a lehetséges problémák és az alkalmazott megoldások kiértékelésére, javaslatok megfogalmazására.

A továbbiakban nem az egyes megoldásokat, illetve javaslatainkat szeretném ismertetni. Ezekről részben más előadásokban szó esik. Úgy gondolom, hogy ennél általánosabb érvényű és tanulságosabb, ha bemutatásra kerül egyfelől az a megközelítés, amelynek alapján egy ilyen, nagy bonyolultságú és kritikus követelményekkel jellemezhető rendszer vizsgálata, kiértékelése elvégezhető, másfelől a választási informatikai rendszert jellemző biztonsági követelmények, fenyegetések néhány sajátos vonása.

1. A kiértékelés módja

A feladattal szembesülve először is meg kellett határozni, hogy a kiértékelésben milyen módszer szerint célszerű eljárni. Nyilvánvaló volt, hogy egyfelől a rendszer mérete, bonyolultsága, másfelől a megvalósítás szintje és a rendelkezésre álló idő nem tesz lehetővé szokványos, a kockázatelemzés és kockázatkezelés formális módszertanára épülő eljárást. Ugyancsak fontos szempont volt, hogy az adatgyűjtés, a vizsgálat a megvalósítás folyamatát, az amúgy is jelentős terheléssel dolgozó fejlesztőket a lehető legkisebb mértékben hátráltassa.

Meg kellett fontolni továbbá, hogy a biztonság növelésének két alapvető feladatkörét, a kockázat elemzését, felmérését és a kockázat kezelését figyelembe véve a választási informatikai rendszer megvalósítását, a biztonság növelését jellemző munkamegosztásban milyen szerep felvállalása valósítható meg és vezethet eredményre.

A főbb problémák a következőkben összegezhetők:

- Az elemzés tárgya nem egy megvalósított, működő rendszer volt. Ennek megfelelően olyan vizsgálati szempontok, mint a megvalósításhoz kapcsolódó szabályozás, a működtetés gyakorlati tapasztalatai, vagy a biztonságot szolgáló előírások betartása a gyakorlatban, nem voltak érvényesíthetők.

- Annak a gazdag tapasztalati ismeretnek a begyűjtésére, amelyet a rendszer tervezői, fejlesztői, üzemeltetői a korábbi projektek során felhalmoztak, csak hosszú idő alatt és ezeknek a szakembereknek jelentős energiaráfordítása árán lehetett volna remény.

- A megoldások kiválasztását tekintve több szempontból kivihetetlen lett volna a megvalósítás menetébe beleavatkozni, azt módosítani.

A kölcsönös erőfeszítések eredményeképpen sikerült kialakítani egy működtethető, ugyanakkor hasznos és eredményre vezető együttműködési formát. Ennek keretében a párhuzamos és független

problémamegoldás alapelvét próbáltuk sajátos módon alkalmazni. Az együttműködés főbb vonásai a következők:

- A választási informatikai rendszer egyes elemeit jellemző értékek, valamint a fenyegető tényezők okainak feltárása az egyes rendszermodulok specifikációja, feladatának, célkitűzéseinek meghatározása alapján történt.

- A rendszer kiértékelésének alapját a modulok logikai rendszerterve, szervezési dokumentációja képezte.

- A megfogalmazott javaslatok részben írásos szakvélemény, részben közvetlen konzultáció formájában jutottak el az egyes modulok fejlesztőihez, akik ezt összevetve a saját megoldásaikkal, dönthettek a megvalósítás módjáról.

Ezen a módon a mind a kockázatok felmérése, mind kezelésük módjának meghatározása egymástól független csatornákon történt meg. Ugyanakkor a megvalósítás teljes egészében a fejlesztők kezében összpontosul, ami ebben a helyzetben összhangban van a megvalósíthatóság kritikus fontosságával.

A fentieknek megfelelően a biztonsági kiértékelés vázlata a következő volt:

- A biztonsági követelményszint

  Ennek keretében történt azoknak az adatállományhoz, szolgáltatáshoz kapcsolódó követelményeknek és értékeknek a meghatározása, amelyek egy adott modulhoz rendelhetők.

- A fenyegető tényezők

  Itt került sor annak az értékelésére, hogy milyen indíték és milyen várható támadási erő kapcsolható az egyes szándékos fenyegető tényezőkhöz, és milyen valószínűség jellemzi az egyes véletlen fenyegető tényezőket.

- Biztonsági kiértékelés

  Ennek során a rendszernek a logikai rendszerterv szintjén meghatározott jellemzőiből kiindulva a lehetséges gyenge pontok és a tervezett védelmi eszközök hatásossága volt a vizsgálat tárgya.

- Javaslatok

  A fentiekben meghatározott, a védelmi igényből és a fenyegetettség mértékéből összetevődő védelmi igény teszi lehetővé a megfelelő, a biztonság erősítését szolgáló javaslatok megfogalmazását.

2. A biztonság kérdéskörének sajátosságai

A fenti módon elvégzett vizsgálat szolgált néhány általánosítható, talán tanulságosnak mondható tapasztalattal.

- A biztonsági követelményszint egy rendszer életciklusa alatt nem mindig állandó.

  Mind a rendszer egésze, mind egyes moduljai esetében megállapítható, hogy az egyes biztonsági alapértékekhez kapcsolódó követelményszint a rendszer életciklusa során változhat. Példa lehet erre egy adattár, amelynek feltöltési fázisában a rendelkezésre állás tekintetében fél napos kiesés is elfogadható lehet, míg az adatszolgáltatási szakaszban esetleg néhány perces leállás sem tolerálható. Másik példa lehet a rendszert kiszolgáló adatátviteli hálózat, amelynek egyes esetekben óránként néhány perces, és a bizalmasságot fenntartó átvitelt kell biztosítania, más időszakokban pedig folyamatos, sértetlenséget biztosító, de nyílt adatátvitelre van szükség. A minden esetben az előfordulható maximumot figyelembe vevő rendszerkialakítás feleslegesen költséges megoldásnak bizonyulhat. Érdemes megvizsgálni optimálisabb lehetőségeket, például a rendelkezésre állás szempontjából kevésbé kritikus szakasz egyszersmind szolgálhatja a kritikus szakaszra való felkészülés üzemi próbáját, stb.

- A biztonság nem merül ki az adatok bizalmasságának fenntartásában, ugyanakkor a bizalmasság szerepet játszik más biztonsági alapértékek, pl. a rendelkezésre állás, sértetlenség fenntartásában.

  A megállapítás első felével most már egyre több helyen találkozhatunk. Ami mégis indokolja azt, hogy itt kitérjünk rá, az az, hogy a választási informatikai rendszerben a bizalmasság követelménye csak nagyon kis súllyal szerepel, míg a biztonság kérdésköre fontos szerepet játszik. Ugyanakkor közvetett módon, más alapértékek védelme céljából mégiscsak szükség van bizalmasságot védő eszközökre is. Például szolgál erre mondjuk egy távadat feldolgozási rendszer, ahol a protokoll bizalmassága a feldolgozás eredményének sértetlenségét, a telefonszámok titkossága a feldolgozás működőképességét, rendelkezésre állását szolgálja.

- A minőségbiztosítás alapvető szerepet játszik a biztonság megvalósításában.

  Egy rendszer megfelelő funkcionalitása nyilvánvaló feltétele a helyes működésnek, ehhez pedig az út a minőségellenőrzésen, minőségbiztosításon keresztül vezet. Hangsúlyozni kell azonban, hogy a mindegyik biztonsági alapérték vonatkozásában alapvető feladat hárul a minőségbiztosításra. Ez lehet közvetlen szerep, például a bizalmasság esetében a védelmi eszközök helyes működésének garantálása, és lehet közvetlen, mint a sértetlenség, hitelesség esetében a feldolgozási folyamatok pontosságának biztosítása. Ennek alapján ki kell emelni, hogy az informatikai biztonság megvalósítása a minőségbiztosítással együttműködve, ahhoz hasonlóan egy rendszer teljes fejlesztési életciklusát átfogva vezet megfelelő eredményre.

- Egy rendszer támadásához néha meglepően egyszerű lehetőségek is adódnak.

  Informatikai rendszerek, adatátviteli hálózatok biztonsági szempontból történő vizsgálata során szükséges a várható támadások, egyéb fenyegető tényezők "erejének", "energiájának" figyelembe vétele. Ugyanakkor könnyű túlbecsülni egy-egy jelentősebb káresemény előidézéséhez szükséges erőfeszítést. Erre csak egy példát szeretnék említeni. Elég arra gondolni, hogy egyre több diák jön rá arra, mi módon lehet egy napra az oktatás rendelkezésre állását felfüggeszteni. Az egész egy telefon árába kerül, és a felderíthetetlensége szinte garantált. Egy számítóközpont esetében is számítani kell ugyanerre az ötletre. Egy biztonsági átvilágítás során ezért nagy gondot kell fordítani látszólag valószínűtlen esetek alapos vizsgálatára is.

Összegzés

Az 1994. évi országgyűlési képviselő választást támogató informatikai rendszer biztonságának fokozását szolgáló erőfeszítések keretében külső szakértők is bekapcsolódtak a rendszer kialakításába. Ez az együttműködés mind a biztonsági átvilágítás feltételeinek, mind az informatikai rendszer biztonsági követelményeinek szempontjából szolgált tanulságokkal. A felvetődő problémákra választ adó megoldásokról részben más előadásokból, azok eredményességéről pedig a két választási forduló sikeres lebonyolítása alapján szerezhettünk tudomást.

Dr. Jávor András

Adatvédelem az egészségügyben

Bevezetés

Az évezredes hagyományokkal rendelkező orvosi szakma képviselői a legbensőségesebb kapcsolatba kerülnek a hozzájuk forduló betegekkel, a lakossággal. Az emberek megengedik, hogy az orvosok a hasukat fölvágják és belenézzenek, így az olyan érzékeny adatok, mint az életkor, nem, stb., amelyekről az adatvédelemről folyó diszkussziók általában szólnak, az egészségügyi munka folytatásához nélkülözhetetlen, folyamatosan használt adatok.

Az orvos tudomására jutott adatok megőrzése, kezelése a szakma évszázados hagyományai alapján az orvosi titoktartás előírásai szerint történik, az orvos felelős az adatok egyetlen cél, a betege és a lakosság egészsége védelmének érdekében való felhasználásért.

Az adatok megkérdezése, egyéb módon való gyűjtése, az adatok értékelése, feldolgozása az orvosi munka része. Éppen úgy szolgálja a gyógyítást, megelőzést, mint a köztudatban elfogadott egyéb orvosi eljárások, a diagnosztikai és terápiás tevékenységek.

A lakosság és az egészségügy, az orvos-beteg kapcsolat nem egyszerűen adatszolgáltató-adatkezelő viszony, annál sokkal több, minőségileg más. Az orvos-beteg kapcsolat, ha nem a teljes bizalmon alapul, a beteg egészségét, életét veszélyezteti. Ezt a kapcsolatot nem lehet egyedileg szabályozni (pl. a beteg írásbeli hozzájárulása minden kapcsolatfelvétel esetén), hanem egészében kell intézményesen biztosítani.

Az előbb több évszázados hagyományokra hivatkoztam. Korunkban azonban annyira felgyorsult a tudományos-műszaki és a társadalmi haladás, hogy már nem lehet kizárólag erre a hagyományra hivatkozni. Megtartva az összes bevált és folytatható gyakorlatot, szükséges felülvizsgálni, újragondolni a nagyon összetett problémát.

Egyrészt az orvostudomány fejlődése következtében egy beteg gyógyításában is több szakma (több orvos és egyéb szakember) szoros együttműködésére van szükség, egyre mélyebb ismeretekre és egyre több adatra.

Másrészt az adattovábbítás, feldolgozás, tárolás technikája is soha nem látott változáson, fejlődésen, ment, megy át, ami óriási lehetőség, de veszély is.

Mindezért az egészségügyi adatok kezelése napjainkban és a jövőben is más probléma, mint a hagyományos, a gyógyításban közvetlenül végzett "adatkezelés" (amit az egészségügyi előírások, törvény szabályoznak), de nem egyezik az állam és a gazdaság működéséhez, a társadalmi tevékenységhez tervezéshez és szervezéséhez szükséges információval, az ennek az érdekében végzett adatkezeléssel sem, amivel az általános adatvédelmi törvény foglalkozik.

Végül: egészségügyünk a rendszerváltozás következtében teljesen átalakul. Az átalakulásban nagyon fontos szerepet kapnak az informatikai módszerek, megoldások.

Hogy szükség van az egészségügyi adatok kezelésének speciális szabályozására, igazolja az is, hogy a számunkra mérvadó nemzetközi szervezetek, pl. az Egészségügyi Világszervezet (World Health Organization), vagy az Európai Közösség (Council of Europe) szakmai bizottságokat hozott létre ajánlások, az egészségügyi adatok kezelési normáinak a kidolgozására.

A jogi helyzet

Egészségügyi rendszerünk működése - a folyamatosan javított, korrigált 1972. évi II. Egészségügyi törvényen, az adatkezelés, adatvédelem általános szabályozása az 1992. évi LXIII. Adatvédelmi törvényen alapul. Az egészségügyi adatok védelmét mindegyik törvény érinti, de a bevezetőben említett okok miatt valójában egyik sem szabályozza tökéletesen. Hogy jelenleg az egészségügy - az adatkezelés szempontjából - jelentősebb zavarok nélkül működik,nagyrészt hagyományokon, szokásjogon alapul. Ebből következik, hogy nem teljesen egységes a gyakorlat, sokszor találkozunk túlhaladott, kifogásolható módszerekkel, megoldásokkal és a változásokra adott ellentmondásos válaszokkal.

Ezen okokból a Népjóléti Minisztérium 1992-ben munkabizottságot hozott létre, amelynek feladata az egészségügyi adatok kezelése, védelme, jogi alapjainak rendezése volt. A bizottság munkájába több minisztérium is delegált szakértőt - elkészítette az Egészségügyi adatok kezeléséről szóló

törvényjavaslatot. A tervezetet a Kormány 1993-ban elfogadta és az Országgyűlés eléterjesztette. Sajnos, az Országgyűlés - óriási túlterheltsége miatt - a törvényjavaslatot nem tudta megvitatni, nem jutott rá ideje. A munka mégsem volt hiábavaló, mert:

- magunk előtt sikerült tisztázni a helyzetet,
- a széleskörű szakmai viták segítettek sok problémás kérdést megoldani
- a törvényjavaslat - elfogadása nélkül is - kezd jogi normává válni, igazodik hozzá a gyakorlat.

A javaslat átvette a nemzetközi ajánlásokat. A szakmai közvélemény elfogadta annak ellenére, hogy jelentős változásokat jelent az elmúlt gyakorlathoz képest.

Törvényjavaslat az egészségügyi adatok kezeléséről:

A törvény célja,hogy meghatározza az egészségügyi állapotra vonatkozó különleges személyes adatok (a továbbiakban: egészségügyi adat) és az ahhoz kapcsolódó személyazonosító adatok kezelésének feltételeit.

A törvény alkalmazásában

a,) egészségügyi adat: az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére és szexuális szokásaira, valamint a megbetegedés körülményeire vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátóhálózat által észlelt, mért, leképzett vagy származtatott adat. Egészségügyi adat továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló bárminemű adat is (pl. magatartás, környezet, foglalkozás), ha annak kezelése az 4.§ szerinti célból történik,

b,) személyazonosító adat: a családi és utónév, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakcím, továbbá a mesterséges személyazonosító jel, együttesen vagy ezek közül bármelyik, amennyiben alkalmas vagy alkalmas lehet az érintett személy azonosítására,

c.) gyógykezelés: a megelőzés, a vizsgálat, a diagnózis megállapítása, a terápia és a rehabilitáció,

d.) orvosi titok: a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelés jellegére vonatkozó, továbbá a gyógykezeléssel kapcsolatban megismert egyéb adat,

e.) orvosi dokumentáció: a gyógyító-megelőző orvosi munka részét képező egészségügyi adatokat tartalmazó feljegyzés, függetlenül annak hordozójától vagy formájától,

f.) kezelőorvos: az érintett gyógykezelését végző vagy abban közreműködő orvos,

g.) betegellátó: a kezelőorvos, az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy, a 4. § (1) bekezdés c.) pontja, illetve az 5. § (4) bekezdése szerinti célból történő adatkezelés esetén a tisztiorvos,

Az adatkezelés célja

(1) Az egészségügyi és személyazonosító adat kezelésének célja

a.) a gyógykezelés eredményes elősegítése,

b.) az érintett egészségi állapotának nyomonkövetése,

c.) a közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele.

(2) Egészségügyi adatot az (1) bekezdésben meghatározottakon túl az alábbi célból lehet kezelni:

a.) egészségügyi szakember-képzés,

b.) a lakosság egészségi állapotának figyelemmel kísérését segítő epidemiológiai és statisztikai vizsgálat,

c.) tudományos kutatás,

d.) az egészségügyi ellátóhálózatot finanszírozó szervezetek feladatainak ellátása,

e.) az egészségügyi adatot kezelő intézmény hatósági vagy törvényességi ellenőrzését, szakmai vagy törvényességi felügyeletét végző szervezetek munkájának elősegítése,

(3) Az (1)-(2) bekezdésekben meghatározott céloktól eltérő célra is lehet - az érintett vagy törvényes képviselője írásbeli hozzájárulásával - egészségügyi és személyazonosító adatot kezelni.

Az egészségügyi ellátóhálózat szerveinek adatkezelése

Egészségügyi és személyazonosító adatot a betegellátó kezelhet.
A közegészség-járványügyi érdekből történő adatkezelés esetén az Állami Népegészségügyi és Tisztiorvosi Szolgálat (ÁNTSZ) városi (fővárosi kerületi), illetve megyei (fővárosi) intézetei keretében dolgozó tisztifőorvos, tisztiorvos jogosult az érintettel egy háztartásban élő személyektől is fölvenni és kezelni egészségügyi és személyazonosító adatot.

A gyógykezelés céljából történő adatkezelés

Az egészségügyi és személyazonosító adatok kezelése során biztosítani kell az adatok védelmét véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.

(1) Az adatkezelő az orvosi titkot köteles megőrizni.
(2) Az adatkezelő mentesül a titoktartási kötelezettség alól, ha
a.) az egészségügyi és személyazonosító adat közlésére az érintett (törvényes képviselője) írásban felhatalmazta,
b.) az egészségügyi és személyazonosító adat továbbítása e törvény előírásai szerint kötelező vagy arra lehetőség van.
(3) Az egészségügyi adatok felvétele a gyógykezelés része, így a kezelőorvos, illetve a tisztiorvos dönti el, hogy mely egészségügyi adat felvétele szükséges.
(4) Az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy a kezelőorvos utasításának megfelelően, illetve a feladatai ellátásához szükséges mértékben vehet föl egészségügyi adatot.
(5) A kezelőorvos felelős az általa vagy a felügyelete alá tartozó személyek által felvett egészségügyi és személyazonosító adatok előírásszerű kezeléséért.

(6) A gyógyítás-megelőzés céljából történő adatkezelés esetén az egészségügyi ellátóhálózaton belül az egészségügyi és személyazonosító adatok továbbíthatók, illetve összekapcsolhatók. Az egészségügyi és személyazonosító adatokat csak addig az időpontig és olyan mértékig lehet összekapcsolni, ameddig az a gyógykezelés, illetve közegészség-járványügyi érdekből feltétlenül szükséges.

(7) A gyógyítás-megelőzés céljából történő adatkezelés esetén az érintett betegségével kapcsolatba hozható minden olyan egészségügyi adat továbbítható, amely a gyógykezelés érdekében fontos, kivéve, ha ezt az érintett írásban kifejezetten megtiltja.

(8) A kezelőorvos az érintettre vonatkozó egészségügyi adatokat továbbítja az érintett választott háziorvosának.

(9) A háziorvos az érintettre vonatkozó, a rendelkezésre álló összes egészségügyi adatról az érintettet - kérelmére - megfelelő módon tájékoztatja.

(10) Az egészségügyi és a személyazonosító adatoknak az érintett részéről történő szolgáltatása önkéntes.

(11) Abban az esetben, ha az érintett önként fordul az egészségügyi ellátóhálózathoz, az egészségügyi és személyazonosító adatainak kezelésére szolgáló hozzájárulását - ellenkező nyilatkozat hiányában - megadottnak kell tekinteni.

(12) Sürgős szükség esetén az önkéntességet vélelmezni kell.

Statisztikai és egyéb célú adatkezelés

(1) Az érintett egészségügyi és személyazonosító adata statisztikai célra személyazonosításra alkalmatlan módon kezelhető.

(2) A társadalombiztosítás szervei részére az érintettnek járó társadalombiztosítási ellátások folyósítása, illetve azok, valamint az egészségügyi ellátóhálózat működésének a társadalombiztosítás szervei által történő ellenőrzése céljából csak a szükséges egészségügyi és személyazonosító adat továbbítható.

(3) A személyazonosításra alkalmatlan egészségügyi adat időbeli és területi korlát nélkül továbbítható.

Az egészségügyi adatok nyilvántartása

Az érintettről felvett, a gyógykezelés érdekében szükséges egészségügyi és személyazonosító adatot, valamint az azok továbbításáról készített feljegyzést nyilván kell tartani.

(1) A nyilvántartásban szereplő hibás egészségügyi adatot a kötelező nyilvántartás ideje alatt törölni nem lehet, azt úgy kell kijavítani, hogy az eredetileg felvett adat megállapítható legyen.

(2) A nyilvántartott adatokról az adatkezelő hiteles másolatot készít, ha ezt az adatbiztonság vagy a tárolt adatok fizikai védelme, illetve az e törvényben előírt adatközlési kötelezettség szükségessé teszi.

(3) Az egészségügyi és személyazonosító adatok feletti rendelkezési jog az érintettet illeti.

(4) Az érintettet, illetve törvényes képviselőjét kérelmére a kezelőorvos köteles megfelelő módon tájékoztatni az általa felvett, az érintettre vonatkozó egészségügyi adatokról és ezzel összefüggésben tett megállapításairól.

(5) A tájékoztatási kötelezettség magában foglalja az orvosi dokumentáció másolatának átadását is, amennyiben ezt a rendelkezési joggal rendelkező személy kéri.

(6) A külföldre történő adattovábbítás esetén is e törvény rendelkezéseit kell alkalmazni azzal, hogy az egészségügyi és személyazonosító adatok csak akkor továbbíthatók, ha az adatvédelem külföldön is biztosítható.

(7) E törvény előírásait alkalmazni kell a meghalt személyre vonatkozó egészségügyi adatok esetén is.

(8) A nyilvánosságra hozatal céljára szánt életrajzban az érintett halálát követő 50 évig csak az érintett leszármazóinak hozzájárulásával szerepelhetnek egészségügyi adatok.

Összefoglalás:

A törvénytervezet alapvető tézisei:

- Az egészségügyi adatok az érintett tulajdonát képezik
- Az adatokhoz való hozzáférés jogosultság alapján történhet, amit vagy az érintett felhatalmazása vagy törvény adhat.
- A titoktartási kötelezettség nincs foglalkozáshoz kötve, mindenkire kiterjed.

- Az adatkezelés során minden olyan technikai eljárás elfogadott, amellyel az adatvédelem biztosítható.

A törvénytervezet szövege jogi mondatokban nem fogalmazza meg, de tartalmazza, hogy azzal a hagyományos felfogással szemben, hogy az adatokhoz (az orvosi titokhoz) való hozzáférés a foglalkozáshoz kötődik, az orvos azért, mert orvos, mindig minden megnézhet, az új megközelítés: az adatokhoz való hozzáférés nem köthető a foglalkozáshoz. Az orvosnak is jogosultságot kell szerezni az adatokhoz való hozzáféréshez (a beteg vagy a törvény felhatalmazása szükséges).

Kitüntetett szerepe van a háziorvosnak (ebből a szempontból is). Az alapvető gondozási feladata miatt az ellátóhálózaton belül betegéről minden információt megkap. Nála gyűlik össze minden fontos egészségügyi adat. Elsősorban azért, hogy a munkáját el tudja látni, de egyéb szempontok is indokolják. A technika fejlődése és terjedése új helyzetet teremtett azzal, hogy már lehetőség van a személyi egészségügyi adathordozó kártyák széleskörű használatára. Ez az adatvédelem területén is új lehetőséget jelent.

AZ EUROKONFORM ADATVÉDELMI JOGALKOTÁS ÉS GYAKORLAT ESÉLYEI

Dr. Hetésy Zsolt

Miniszterelnöki Hivatal

A magyar adatvédelmi jogszabályok elemzése alapján elmondható, hogy a jogalkotás az Európa Tanács dokumentumaival szoros összhangban megfelelő alapokat fektetett le, amelynek bővítésével lehetőség nyílik az Euro-kompatibilis adatvédelmi szabályozás teljes körű megalkotására. Ugyanakkor, mivel a személyes adatok védelme eddig ismeretlen jogtárgyként került be a magyar jogrendszerbe, az ebből fakadó nehézségeket mind a jogi szabályozás, mind a gyakorlati alkalmazás területén érzékelni fogjuk. Hozzájárul ehhez az az ágazati szabályozási technika, amely életszerűsége ellenére nem ismert a magyar jogalkotásban, illetve maga az a tény, hogy folyamatosan változó, ezért állandóan új problémákat rejtő szabályozási tárgyat kell megfelelő jogi rendszerbe foglalni. A tárgykör emberi jogi relevanciája, fontossága elvitathatatlan, ezért minden erőnkkel törekedni kell a még hiányzó jogi szabályozás mielőbbi megalkotására, annak folyamatos megújítására és a jogszabályok gyakorlati alkalmazására.

1. BEVEZETŐ

A tanulmány a magyar adatvédelmi rendszer helyzetét kívánja feldolgozni összevetve azt az Európa Tanács-i Ajánlásokban és egyéb dokumentumokban megfogalmazott alapelvekkel és javaslatokkal. A tanulmány elsődleges célja tehát nem az Európa Tanács és szervei által alkotott adatvédelmi szabályok, tanulmányok, iránymutatások, a jövőbeni irányok részletes bemutatása, hanem a kialakuló magyar jogszabályok és gyakorlat Európa Tanács-i szabályozók tükrében történő értékelése. Így a témakör elemzésére, valamint egyes következtetések levonására a magyar szabályozási rendszert alapul véve, ugyanakkor elsősorban az Európa Tanács által használt megközelítést szem előtt tartva kerül sor.

Elöljáróban le kell szögezni, hogy a Konferencia témakörének megfelelően az adatvédelem fogalmát a tanulmány szűkítetten értelmezve kezeli, vagyis az adatvédelmet elsősorban az Emberi jogok és alapvető szabadságok védelméről szóló egyezmény[1] 8. cikkében megállapított magán- és családi élet, tiszteletben tartásához fűződő joggal való kapcsolódási pontjai tekintetében elemzi. A jelzett téma behatóbb vizsgálatának szükségességét a gyakorlatban bekövetkezett változások indokolják. Az informatika fejlődése, amely lehetővé tette többek között az adatok tárolásának, kezelési lehetőségeinek mennyiségi és minőségi javítását, az adattovábbítás hatékonyabbá tételét, egyben korábban nem tapasztalt veszélyekkel járhat az egyes személy

emberi jogaira és szabadságára, ezen belül a magánélet tiszteletben tartásához és védelméhez fűződő jogaira nézve.

A témakört ugyanakkor nem lehet ezen problémakörre egyszerűsíteni, hiszen mint látni fogjuk, az adatvédelem kérdéskörében egyben megfelelő egyensúlyt kell találni a fent említett alapvető jog és más alapvető értékek, mint például a szabad vélemény nyilvánításhoz vagy a tájékoztatáshoz való jog között is. Ezzel összefüggésben a Konferencia vizsgálni kívánja a közérdekű adatok nyilvánosságára vonatkozó jogi szabályozás és gyakorlat helyzetét is. Ennek figyelembe vételével kerül sor az állam- és szolgálati titok védelmével kapcsolatos szabályozás rövid tárgyalására, amely szoros összefüggésben áll az Európa Tanács által is elismert közérdekű adatokhoz való hozzáférés, mint alapvető jog kérdéskörével. Ilyen értelemben e témakör is beletartozik az Európa Tanács adatvédelmi irányelveibe, következésképpen a magyar adatvédelmi jogalkotás és gyakorlat elemzése során erre is ki kell térni.

2. A KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGÁNAK ALAPELVE

Az állam, illetve szervei által saját érdekéből monopolizálni kívánt adatok fontosságuk miatt úgy külföldön, mint hazánkban is államtitokként, szolgálati titokként, vagy hivatali titokként kerülnek megjelenítésre. E körben elsősorban a preventív védelemre hangsúlyt fektető részletes állami szabályozás mellett a védelmi érdekeket megsértőt fenyegető súlyos szankciók jellemzőek. Ugyannakor az adatok indokolatlanul széles körének jelzett titokkörökbe való sorolása, a társadalom elől történő elzárása sértheti a közérdekű adatok nyilvánosságának alapelvét és a tájékoztatáshoz való jogot. A jelenlegi helyzet tisztázása érdekében célszerűnek tűnik a vonatkozó jogszabályok és az Európa Tanács Parlamenti Közgyűlése által elfogadott 854 /1979/ számú, a Kormányzati dokumentumok nyilvánosságáról, valamint az információszabadságról szóló Ajánlása[2] lehetséges kapcsolódási pontjainak összevetése.

Az Európa Tanács ezen ajánlása megerősítve a tájékoztatáshoz való jog az információszabadság, mint alapérték létezését, és tekintettel arra, hogy egyes információk csak és kizárólag a kormányszervektől szerezhetők be javasolta, hogy a tagállamok /bizonyos indokolt kivételektől eltekintve/ jogszabályban mondják ki a kormányzati dokumentumok nyilvánosságát. Mint ahogy az Európa Tanács jelzett ajánlása is jelzi egyes dokumentum kategóriákat szükségszerűen ki kell zárni a nyilvánosságból. Ezek közé tartoznak az olyan - általánosan és így Magyarországon is elfogadott - területek, mint például a honvédelem, nemzetbiztonság, pénzügyi költségvetési titkok, személyes és azon belül az egészségügyi adatok, ilyenek továbbá általában a közigazgatási munkadokumentumok, javaslatok, tervek stb.

Mindezek mellett az Európa Tanács egyértelmű állásfoglalása az, miszerint a gyakorlatban a legtöbb tagállamban megfigyelhető "titoktartási normákat" fel kell váltani a közigazgatási iratok nyilvánosságának korszerűbb felfogásával. Külön ki kell emelni az érintettek saját személyes adataikhoz való hozzáférési jogát, amelyet a közigazgatás által kezelt adatok területén is biztosítani kell. Mivel azonban a megoldások országról országra változhatnak a tárgy nem alkalmas a mélyebb nemzetközi összehangolásra.

Jelenleg a tagállamok többségében erre vonatkozó kötelezettség nincs, sőt a tisztviselőknek számos esetben hivatali kötelességük, hogy az információ felfedését megakadályozzák. Ellenpéldaként a skandináv

országokat lehet megemíteni, hiszen Svédország már 1776-ban, Finnország, Dánia és Norvégia pedig az 1950-es évek után biztosította az államigazgatási dokumentumok nyilvánosságát. Természetesen a nyilvánosság ezen országokban sem korlát nélküli. A svéd és a finn törvény többszáz tételben taxatíve felsorolja azon dokumentumfajtákat, amelyek titkosak vagy bizalmasak. A dán és norvég törvény csak a dokumentumfajtákat sorolja fel általános jelleggel és a minősítőre bízza az adott dokumentum besorolását.

Az államtitok fogalmának meghatározásában a jelenlegi magyar jogszabály két megoldást alkalmaz. Egyrészt az államtitok és szolgálati titok esetében a védendő érdek meghatározása után a tvr.-ben ugyancsak meghatározott szervek vezetőire bízza a titokkör konkrét megállapítását. Emellett azonban a tvr. ismer olyan adatokat, amelyek ex lege, vagyis a törvényalkotó akaratából minősülnek államtitoknak. A kettős feltétel alapján történő államtitokkör meghatározás lehetősége kellő rugalmasságot biztosít a felhatalmazott vezetők számára. Ugyanakkor a rugalmasság eredményeképpen szinte minden esetben felülbiztosítás, vagyis a kezelt adatok feleslegesen történő besorolása következik be. A felülbiztosítás minőségi és mennyiségi tekintetben egyaránt tettenérhető, vagyis megfigyelhető az egyáltalán nem odatartozó adatok titokkörbe sorolása, és megfigyelhető a nyilvánvalóan kisebb érdeksérelem lehetőségét magába rejtő, és ezért tartalmilag legfeljebb szolgálati titokká minősíthető adatok indokolatlan államtitokkörbe sorolása is.

Magyarországon a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról részletesen az 1992. évi LXIII. törvény III. fejezete rendelkezik. Összefoglalva elmondható, hogy a törvény - a magyar jogalkotásban új elemként - megfelelő jogszabályi kereteket ad a közigazgatási adatokhoz való hozzáférésre, kialakítja annak eljárási szabályait és garanciáit. Ezek közé sorolható az elutasítás indokolási kötelezettsége, az adatvédelmi biztos tájékoztatására vonatkozó kötelezettség, illetve végső megoldásként a bírósági igényérvényesítés lehetősége. A szabályozás elemei ilyen szempontból megfelelnek az Európa Tanács említett ajánlásainak. Külön említést érdemel azonban, hogy a törvény nyilvánosság alóli kivételeket felsoroló szakasza az állam- vagy szolgálati titoknak minősülő adatok kiadásának megtiltása mellett lehetőséget ad arra, hogy más törvények is meghatározzanak olyan adatfajtákat, amelyekhez való hozzáférést meg kell tagadni. Egyértelműnek tűnik tehát, hogy a monopolizálandó adatok magyar jogalkotás által történő megfelelő kiválasztása, védelmi szintjének valósághű meghatározása kiemelkedő fontosságú mind az adatvédelem, mind pedig az információszabadság jogának biztosítása tekintetében, amelyek e kérdéskörben egyben az érem két oldalát is jelentik. Sajnálatos módon éppen ebben a kulcskérdésben érezhető a legnagyobb bizonytalanság, amelyet csak az új, állam- és hivatali titokra vonatkozó, jelenleg előkészületben lévő törvény fog részlegesen megoldani. Mindezek mellett - a szabályozási technikából adódóan - kiemelt figyelmet kell fordítani arra, hogy a későbbiekben megszületendő törvények az említett felhatalmazás alapján a közigazgatásban kezelt adatkokhoz való hozzáférést indokolatlanul ne korlátozhassák.

A témakörrel kapcsolatban röviden fel kell hívni a figyelmet arra a jelenségre, amely közvetve az adatvédelmi szabályozás Európa Tanács általi szabályozásához, annak folyamatos megújításához vezetett. A jelenséget egy szóval informatikai robbanásnak lehet nevezni, jellemzője az adatkezelés hatékonyságának megnövekedése, amely egyben a hagyományos adatvédelmi módszerek és stratégiák elleni kihívást, sokszor azok ellehetetlenülését is jelentette. Az ehhez kapcsolódó alapelv nem emberi jogi, inkább általános, az adatvédelem technikai oldalát érintő alapelv. Nevezetesen hatékony adatvédelemről akkor és csak akkor lehet beszélni, ha annak jogi szabályozása és gyakorlata megfelel az adott kor technikai színvonalának általában, és az adatkezelésre használt eszközök színvonalának speciálisan.

A jelenlegi magyar szabályozás világosan mutatja, hogy a papir alapon zajló adatkezelés idejében keletkezett, és így nem képes a jelenlegi adatáramlási formáknak megfelelő jogi védelemben részesíteni az állam és közigazgatás szempontjából éppen a legfontosabbnak tartott adatcsoportot. A védelmi intézkedésekkel kapcsolatos hatályos jogi szabályozás alapvető jellemzője, hogy nem foglalkozik azzal a ténnyel, miszerint a titkos ügyiratkezelés "hagyománytisztelő" szabályai a számítástechnikai adatkezelésre vonatkozóan igen kevés eligazítást nyújtanak. Pontatlanok a jogszabályok számítástechnikai témakörben kialakított rendelkezései is. Így például a jelenleg hatályos jogszabály rendelkezése a számítástechnikai berendezés fogalmába a magnetofont, a diktafont és a "más adatot feldolgozó, tároló elektronikus eszközök"-et is belefoglalja. A jelenleg hatályos tvr. több jogintézménye napjainkra kiüresedett, túlhaladottá vált, egyes rendelkezései pedig a korszerűsödő jogi szabályozás új intézményeivel kerültek ellentétbe. Ezért e tekintetben a jelzett törvény megalkotása során a rendezés és szabályozás kiinduló pontja a biztonságtechnikai intézkedések újragondolása, és a jelenlegi adatkezelési formákhoz való igazítása kell hogy legyen.

3. A SZEMÉLYES ADATOK VÉDELME

A személyes adatok védelmét az érintetteken kívül az adatokat ugyancsak és elsősorban kezelő állami, kormányzati szerveknek kell felvállalniuk. A más általi megismerés korlátozását ezen adatok tekintetében nem az állami, kormányzati érdekek, hanem az érintett magánszemélyek privát szférájához, magánéletéhez, "magántitkai" védelméhez fűződő jogai indokolják. Ezen adatok védelmét szinte minden országban átfogó szabályozást tartalmazó törvények, egyéb részletes jogszabályok, független felügyeleti rendszerek és a megsértőinek elsősorban polgári jogi, kisebb részben büntetőjogi szankciókkal való fenyegetettsége biztosítják.

Az Európa Tanács már az 1970-es években felismerte az adatvédelemmel kapcsolatos kérdéskör fontosságát, amelynek eredményeképpen a Miniszteri bizottság (73) 22 számú határozata a magánszektor, (74) 29 számú határozata az állami szektor számára alkotott követendő adatvédelmi alapelveket. Ezen első határozatok alapján indult meg a nemzeti adatvédelmi törvények első generációjának megalkotása, amelyek során a tagállamok nagy része egységes alapokon nyugvó szabályokat fogadott el. Rövidesen kiderült azonban, hogy az automatizált adatkezelési rendszerek fejlődése, elterjedése, és az országhatárokon túllépő adatáramlás további olyan, az eredeti határozatokban nem érintett problémákat vet fel, amelyek új szabályozást tesznek szükségessé.

Ez az értékelés, valamint a Gazdasági Együttműködési és Fejlesztési Szervezettel (OECD) való szoros tárgybani együttműködés vezetett el A személyiségnek a személyes adatok automatizált kezelésével kapcsolatos védelméről szóló egyezmény[3] megalkotására, amelyet Magyarország 1993. május 15-én írt alá. Habár az egyezmény az automatizált kezelésű adatokra vonatkozik, lehetőséget ad arra, hogy a szerződő felek az egyezmény szabályait a magán, állami, illetve önkormányzati szektorban történő bármely adatkezelésre vonatkozóan kötelezőnek fogadják el. Az Európa Tanács már a megalkotáskor is az alapszabály szerepét szánta az egyezménynek, amelyet a más más területen eltérő módon jelentkező

adatvédelmi követelményeknek megfelelően szektorális szabályozási technikával további részletszabályokkal kívánt kiegészíteni.

3.1. A MAGYAR "ALAPTÖRVÉNY"

Magyarországon az Alkotmány 59.§-a szerint mindenkit megillet a jóhírnévhez, magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez fűződő jog. Ugyancsak az Alkotmány szerint ezen jogokat érintő szabályokat csak törvényben, a jelenlévő képviselők kétharmadának szavazatával lehet elfogadni.

Magyarországon e témakörben az Európa Tanácsi egyezményhez hasonló "alapszabály-szerepet" szánt a jogalkotó a már említett, A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvénynek. Maga a témakör is új szabályozási tárgyként jelenik meg a magyar jogalkotásban, hiszen az elmúlt időszakra visszatekintve az állampolgárnak nem volt beleszólása abba, hogy személyes adatait mely szerv miért és hogyan kezeli.

Az egyezmény és a törvény összevetésekor alapvető sajátosságként értékelhető, hogy a jogalkotó nem szűkítette le a magyar adatvédelmi törvény hatályát az automatizált adatkezelésre, hanem azt kiterjesztette a manuális adatkezelésre is. Figyelemre méltó, hogy a jogalkotók mind a fogalommeghatározások, mind pedig az anyagi szabályok tekintetében meglehetős pontossággal követték az egyezmény szerkezetét, rendelkezéseit, sokszor szófordulatait is. Igy az egyezményben foglaltak szerint tesz különbséget a törvény a személyes adatok és a különleges adatok között, határozza meg az adatkezelés lehetséges eseteit, célhozkötöttség követelményét és a kezelt adatokkal szemben fennáló követelményeket. Az egyezményben foglaltaknak megfelelően rendelkezik a törvény továbbá a külföldre történő adattovábbítás, az adatbiztonság szabályairól, továbbá felsorolja az érintették jogainak érvényesítésére szolgáló garanciális szabályokat is. Mindezek alapján az érintettnek (bizonyos korlátozások mellett) joga van tájékoztatást kapni a róla kezelt adatokról, kérheti azok törlését illetve helyesbítését is. Az érintett személy jogainak megsértése miatt az adatvédelmi biztoshoz, illetve végső esetben a bírósághoz fordulhat. A bírósági eljárás ugyanakkar nemcsak polgári ügy lehet, hiszen a Büntető törvénykönyvet módosító 1993. évi XVII. törvény jogosulatlan adatkezelés és különleges személyes adatokkal való visszaélés cím alatt két törvényi tényállást is alkotott az adatkezeléssel kapcsolatos jogsértések szankcionálására. Röviden érinti a törvény a személyes adatok kutatóintézetekben való felhasználásának kérdéskörét is, amellyel az Európa Tanács A tudományos kutatások céljából és statisztikai célból felhasznált személyes adatok védelméről szóló (83) 10 számú Ajánlásában[4] foglalkozik. Habár a törvényi szabályozás e tekintetben igen rövid, megfelel az ajánlásban lefektetett alapelveknek és tartalmazza az ajánlás által javasolt garanciák többségét is. Ugyanakkor e tekintetben további szabályozást tartalmaz a Statisztikáról szóló törvény is.

Az adatvédelmi törvény mind szellemében, mind tartalmában alapvetően megfelel az egyezményben foglalt szabályoknak. Mindezek mellett fel kell hívni a figyelmet a törvény és a kapcsolódó gyakorlat több alapvető sajátosságra. Mint ahogy azt az Európa Tanács is leszögezte, a törvény gyakorlati alkalmazása szempontjából kiemelkedő fontosságú, hogy létezik-e és milyen formában létezik olyan szerv vagy személy, amelynek kiemelt feladata az adatvédelemmel kapcsolatos szabályozás elősegítése, az adatkezeléssel kapcsolatos panaszok kivizsgálása, ellenőrzések lefolytatása. A törvény létrehozta az adatvédelmi biztos

intézményét, akinek feladata, jogállása ugyancsak megfelel az Európa Tanács-i szabályokban meghatározott rendelkezéseknek. A törvény ezen része 1993. június 22-én lépett hatályba, ugyanakkor az Országgyűlés ezideig az adatvédelmi biztost nem választotta meg. Ugyancsak ez okból kifolyólag nem állt fel a jogszabályban meghatározott október 22-i határidővel a biztos munkáját támogató Adatvédelmi Iroda, amely tény következésképpen meghiusította a törvény más rendelkezéseinek, mint például az adatkezelők nyilvántartásba vételére vonatkozó rendelkezés megvalósítását is.

A törvénnyel kapcsolatos másik fontos tény, hogy az Egyezmény jellegét követve a magyar jogalkotók is a szektorális szabályozási technikát tartották követendő példának. Mindez azt jelenti, hogy az adatvédelmi törvény alapvetően keretjellegű, amely alapján további törvények kidolgozása elengedhetetlen az adatvédelmi szabályozás teljessé tétele érdekében. Keretjellegű egyrészt a szabályozás, mert például az adatkezelő kötelezettségévé teszi az adatok biztonságáról történő gondoskodást, valamint azon intézkedések és eljárási szabályok kialakítását, amelyek a törvény érvényrejuttatása érdekében szükségesek, ugyanakkor részletszabályokba egyáltalán nem bocsátkozik. Egyben keretjellegű az adatvédelmi törvény azért is, mert más, speciális törvényekre bízza a szinte teljes szabályozás kialakítását olyan kiemelt fontosságú kérdésekben, mint például a külföldre történő adattovábbítás lehetősége, az érintett jogai korlátozása eseteinek felsorolása.

A jogalkotók az adatvédelmi törvény megalkotásakor - figyelemmel az előbb vázolt technikai megoldásra - határidőt tűztek a kapcsolódó törvényi szabályozás előkészítésére és hat hónapos felkészülési időt hagytak a törvény kihirdetése és hatályba lépése között. Szükség volt erre azért is, mert az adatvédelmi törvény hatálybalépése előtt keletkezett törvények a jogtárgy ismeretlensége miatt nem tartalmaztak az adatkezelésre vonatkozó kifejezett szabályokat, márpedig a törvény előírása szerint adatot kezelni, csak az érintett beleegyezése, illetve kifejezett törvényi felhatalmazás alapján lehet.

Az adatvédelmi törvény kihirdetése óta eltelt időszakban többek között ezen előírásnak megfelelően születtek meg olyan törvények, mint A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény, Az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény, A rendőrségről szóló 1994. évi XXXIV. törvény, valamint A honvédelemről szóló 1993. évi CX. törvény. Ugyancsak tartalmaztak az adatkezelésre vonatkozó előírásokat a munkaviszony egyes fajtáit szabályozó törvények, mint például A Munka Törvénykönyvéről szóló 1992. évi XXIII. törvény, A köztisztviselők jogállásáról szóló 1992. évi XXIII. törvény, valamint A közalkalmazottak jogállásáról szóló 1992 évi XXXIII. törvény.

E törvények vonatkozó Európa Tanács-i szabályokkal való rövid összevetése mellett érdemes arra is kitérni, hogy mely területeken van szükség további adatvédelmi szabályozásra.

3.2. A SZEMÉLYES ADATOK NYILVÁNTARTÁSÁRÓL SZÓLÓ TÖRVÉNY

A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény /a továbbiakban: nyilvántartási törvény/ hatálya szerint olyan adatok kezelésére vonatkozó szabályokat tartalmaz, amelyek a polgárok személyazonosságának igazolására, továbbá az igazságszolgáltatási, közigazgatási szervek, a helyi önkormányzatok, valamint más természetes személyek törvényen alapuló adatigénylésének

kielégítésére szolgálnak. A törvény ezáltal olyan Európa Tanácsi okmányokkal mutat szoros összefüggést, mint a Közigazgatási szervek által kezelt személyes adatok harmadik féllel való közléséről szóló /91/ 10 számú Ajánlás[5], valamint az Adatvédelmi Szakértői Bizottság által 1991-ben, A személyi azonosító szám bevezetése és használata: adatvédelmi kérdéskörök címmel elkészített tanulmány.[6]

A nyilvántartási törvény és a végrehajtására kiadott kormányrendelet röviden összefoglalva megfelelően tükrözi az ajánlásban megfogalmazott egyes részterületek irányelveit, vagyis meghatározza a nyilvántartható adatok körét, a nyilvántartás hatásköri, illetékességi szabályait, a nyilvántartás lehetséges adatforrásait, meghatározza, hogy mely szervezetek és milyen feladatok ellátása érdekében jogosultak az egyes adatokhoz való hozzáférésre, részletesen leírja az adatvédelem érdekében teendő intézkedéseket és biztonsági garanciákat. A törvény összhangban áll az ajánlásban szereplő, magánélettel kapcsolatos és adatvédelmi alapelvekkel így az adatátadás feltételeivel, kitér az elektronikus kapcsolattartás, az on-line lekérdezés alapelveire és körülményeire, az adatállományok összekapcsolásának lehetőségére. Lehetőséget ad a törvény /bizonyos korlátozások mellett/ arra, hogy az állampolgár adatainak továbbítását nyilatkozattal megtilthassa. Preciz, a jelenlegi nemzetközi elvárásoknak megfelelő szabályozásával a törvény áttételesen maga is az emberi jogok érvényesítésének eszközévé válhat.

Külön érdemes megemlíteni a személyi azonosító számmal kapcsolatos szabályozást, amely az Alkotmánybíróság vonatkozó döntéseivel összhangban 1995. decemberi határideig engedi meg az univerzális, általános azonosításra alkalmas személyazonosító jel alkalmazását. Mindezek mellett szűk körben határozza meg a törvény azon szerveket, amelyek adatigénylésükkor, feladataik végrehajtása során használhatják a személyazonosító jelet, megállapítja továbbá azon eseteket, amelyek során az állampolgároknak a személyazonosító jelet át kell adniuk.

Az Európa Tanács-i tanulmány szerint az univerzális személyi azonosító szám használata önmagában nem sérti az adatvédelmi érdekeket, illetve a magánélethez való jogot. Előnyei, így hatékonysága, relatív költségkímélő volta mellett azonban fennáll annak potenciális veszélye, hogy segítségével minden nehézség nélkül áttörhető a célhozkötöttség és a funkcionális elkülönítettség elve, vagyis az univerzális azonosító alapján eleve fennáll a lehetőség az adatvédelmi alapelvek megsértésére. Ezért - mint ahogy azt a tanulmány megfogalmazza - ha ilyen azonosító jel létezik, azt csak jogszabály alapján lehet alkalmazni, használatát körültekintően kell szabályozni, az érintettel tudatni kell, hogy személyi azonosítója milyen adatait tartalmazza, valamint közölni kell, hogy milyen esetekben köteles azt átadni. A nyilvántartási törvény mindezen feltételeknek megfelelő korszerű szabályozást nyújt. A törvény mindezek mellett az új - nem egységes - személyi azonosítóra vonatkozó szabályozás kilátásba helyezésével az Európa Tanács szakértőinek egységes azonosítók felváltására tett végső javaslatát is magáévá tette. Hozzá kell azonban tenni, hogy az egyes adatállományok összekötésére az államigazgatási szervek számára nemcsak a személyi azonosító szám, hanem az állampolgárok neve és egyéb adatai alapján is lehetőség nyílik. Éppen ezért az adatállományok összekapcsolására, a funkcionális elkülönítettségre, valamint a célhozkötöttségre vonatkozó alapelveket és garanciákat a nem személyi azonosító számot használó rendszerek esetében is maradéktalanul be kell tartani.

3.3. A MUNKAJOGVISZONNYAL KAPCSOLATOS TÖRVÉNYEK

Habár a magán, önkormányzati és állami szféra munkaviszonnyal kapcsolatos fent említett törvényei már az adatvédelmi törvény előtt megszülettek, a témában folytatott nemzetközi tapasztalatgyűjtés és a vonatkozó külföldi jogszabályok megismerése felhívta a figyelmet az adatkezelés e területen is jelentkező fontosságára. A témával maga az Európa Tanács is behatóan foglalkozott, amelynek eredményeképpen került megalkotásra többek között a Munkáltatási célok érdekében használt személyes adatok védelméről szóló /89/ 2 számú Ajánlás[7] és A fizetési és más kapcsolt tevékenység során a személyes adatok védelméről szóló /90/ 19 számú Ajánlás[8]. Az ajánlások alapelve, hogy a munkáltatónak tiszteletben kell tartania a munkavállaló emberi méltóságát és magánélethez való jogát. Ezt az alapelvet egyrészt alkalmazni kell a munkáltatáshoz szükséges személyes adatok kezelése során, másrészt figyelembe kell venni a dolgozók munkatevékenységének mérésére, mozgásának megfigyelésére szolgáló rendszerek létesítése során. Mindkét tevékenységformához elsősorban jogszabályi szabályozás, illetve a munkavállalók tájékoztatása és beleegyezése szükséges. A munkavállalókról gyűjtött adatoknak a munkáltatási célok figyelembe vételével relevánsoknak kell lenniük, a munkavállalók felvétele és munkáltatása során csak az ahhoz szükséges adatokat lehet tárolni. Amennyiben felméréseket, teszteket végeznek, ezeket csak a munkavállalók beleegyezésével vagy jogszabályi előírás alapján lehet megkövetelni, az eredményről a munkavállalót értesíteni, az őt érintő döntések során felhasznált adatokról tájékoztatni kell. Az ajánlások külön szabályokat dolgoznak ki az adat szerven belüli és szerven kívüli kezelésére, az egyes adatcsoportokra, különösen az érzékeny, köztük az egészségügyi adatokra nézve. Kimondták és részletesen szabályozták a munkavállaló adatmegismeréshez, helyesbítéshez és törléshez való jogát, valamint a munkáltató adatvédelemmel kapcsolatos kötelezettségeit.

Elmondható, hogy habár az említett magyar jogszabályok és különösen A köztisztviselők jogállásáról szóló törvény már tartalmazza a munkahelyi nyilvántartásokkal kapcsolatos szabályok szűkebb körét, meghatározza a kezelhető adatokat, a munkavállalók ezzel kapcsolatos jogait stb., e területen további pontosításra, az Európa Tanácsi speciális adatvédelmi irányelvek mélyebb megismerésére és magyarországi adaptálására van szükség. Várható egyébként, hogy a munkajogviszony sajátos formájaként utolsóként szabályozásra kerülő, a katonák, illetve a rendvédelmi szervek hivatásos állományára vonatkozó szolgálati törvények már kiterjedt - és talán a követelményeknek legjobban megfelelő - adatkezelési szabályozással fognak megszületni.

Nehezíti a helyzetet, hogy az adatvédelem e területen egyrészt nemcsak állami kötelezettség, másrészt a jogszabályi szabályozás mellett a munkáltatók, különösen a magánszféra tekintetében teljesen új szemléletmód elsajátítását követeli meg.

3.4. A RENDŐRSÉGI ÉS A HONVÉDELMI TÖRVÉNY

A korábbiakban említett Rendőrségi törvény az adatkezelés kiemelkedő részelemét szabályozta. A tevékenység fontosságát a rendőri tevékenység sokrétűsége, az állampolgárok életébe való beavatkozásának potenciális lehetősége határozza meg. Ezzel egyidőben a rendőri tevékenység jelentőségét és egyedi jellegét felismerve maga az adatvédelmi egyezmény 9. cikke ad felhatalmazást arra, hogy a

bűncselekmények megelőzése céljából a tagállamok az általános adatkezelési alapelvektől eltérjenek. Mindezek alapján szükségszerű, hogy az Európa Tanács által is elfogadott szektorális szabályozási technikát követve a rendőri ágazatban történő adatkezelés speciális feltételei megfelelően, külön törvényben kerüljenek szabályozásra.

Ezen indokokat figyelembe véve született meg A személyes adatok felhasználásának rendőri ágazatban történő szabályozásáról szóló /87/ 15 számú Ajánlás[9]. Az ajánlás javasolja, hogy minden tagállam a rendőrségtől független ellenőrző szervvel rendelkezzen, amelynek feladata az ajánlásban rögzített elvek betartásának ellenőrzése. Az ajánlás az adatok felvételét jogszabályi felhatalmazás meglétéhez, illetve szigorú célhozkötöttséghez köti, előírja a rendőri adatok feladatonkénti elkülönített kezelését, a tények és vélemények megkülönböztetését, szigorú szabályok közé szorítja a közjogi szervekhez, magánszemélyekhez, illetve a nemzetközi szervekhez való adattovábbítás lehetőségeit, továbbá szigorú feltételeket szab az adatállományok összekapcsolására. Szabályozza továbbá az érintett rendőrség által kezelt adataikhoz való hozzáférésének lehetőségét, a helyesbítési és törlési jogot, amelyben előírja, hogy az érintettnek joga van a kezelt adatokhoz való rendszeres és késedelem nélküli hozzáférésre. Ezt csak a rendőri feladatok végrehajtása, mások jogainak védelme érdekében elengedhetetlenül szükséges esetekben lehet korlátozni. Az érintett számára meg kell adni ezen esetekben a fellebbezés, illetve a jogorvoslat lehetőségét. A rendőrség által tárolt adatok érzékenységére tekintettel külön figyelmet fordítottak az adattárolás időtartamára és a naprakészségre, illetve az adatbiztonsági szabályokra.

A jelenleg hatályos Rendőrségi törvény a fent említett ajánlásban foglalt irányelvek szerint szabályozza a rendőrségi adatkezelést. Elkülöníti a törvény egyrészt a bűnüldözési és az államigazgatási adatkezelést, meghatározza, hogy a rendőrség munkája során mely szervtől milyen adatokat, mi célból vehet át, és adatfajtánként határozza meg az adatok kezelésének lehetséges időtartamát. A szabályozás ugyanakkor tiltja az érintett tájékoztatását a törvényben meghatározott egyes - indokoltnak tartott - esetekben. Részletesen szabályozza a törvény az adat más szervnek, illetve külföldre történő továbbításának, valamint az adatállomány összekapcsolásának lehetőségeit. Részletezi a törvény az érintett adathozzáférési, helyesbítési, törlési lehetőségének biztosítását valamint visszautal az adatvédelmi törvényben szabályozott panasz- és jogorvoslati lehetőségekre is. Mindezek alapján elmondható, hogy a törvény az Európa Tanács ágazati ajánlásának figyelembe vételével került megalkotásra.

Az ugyancsak említett Honvédelmi törvény a "munkáltatói szféra" adatkezelésére vonatkozó szabályozást is tartalmaz, akkor amikor taxatív módon állapítja meg a honvédelmi kötelezettséggel összefüggő adatkezelési normákat, ugyanakkor tartalmaz a honvédelmi tevékenységgel kapcsolatos adatkezelésre vonatkozó rendelkezéseket is. Így jellegét tekintve adatkezelési szempontból a szolgálati jogviszonyt szabályozó törvények és a rendőrségi törvény között helyezkedik el. Kiemelendő, hogy a törvény - az Európa Tanács-i ajánlásokban is elismert - a nemzetbiztonsági érdekeket megfelelő módon előtérbe helyező, így az általános adatvédelmi szabályoktól némiképp eltérő szabályokat alkotott meg akkor, amikor a katonai nemzetbiztonsági szolgálatok adatkezelésének egyes részletkérdéseit rendezte. Ugyanakkor el kell mondani, hogy a nemzetbiztonsággal kapcsolatos adatvédelmi kérdéseket teljes egészében majd csak - a remélhetően mihamarabb megalkotásra kerülő, - a nemzetbiztonsági szolgálatokról szóló kétharmados törvény fogja rendezni.

Tulajdonképpen ezzel érkeztünk el azon területek, ágazatok számbavételéhez, amelyeket az Európa Tanács működése során már megvizsgált, azonban ezen eredmények Magyarországon való felhasználása további jogalkotási tevékenységet kíván meg. Természetesen ezen jogalkotási feladatok nemcsak egyszerű másolási kényszer miatt jelentkeznek, hanem egyenes következményei a szektorális szabályozási technikának.

3.5. TOVÁBBI SZABÁLYOZÁST IGÉNYLŐ TÁRGYKÖRÖK

A különleges személyes adatok nagy részét ölelik fel az egészségügyi adatok amelyeknek fontosságát az Európa Tanács Az automatizált gyógyászati adatbankok szabályairól szóló /81/ 1 számú Ajánlás[10] megalkotásával is elismerte. Az Európa Tanács által érzékenynek minősített - és az orvosi titoktartás által is érintett - adatok tekintetében a többször említett emberi jogok biztosítását a működésbe lépő adatbank és a rá vonatkozó szabályok társadalmi szintű bemutatási kötelezettségével, a különböző /azonosító, igazgatási, orvosi, illetve szociális/ adatok elkülönítésével az adatok bizalmas kezelésével, a hozzáférési és felhasználási szabályok szigorításával, a kezelt adatok érintett számára történő megismertetésével kívánja biztosítani az ajánlás. Magyarországon előkészületben van az egészségügyi adatokról szóló törvény, amelynek rendelkezései minden bizonnyal megfelelő módon tükrözni fogják az ezen ajánlásban foglalt Európa Tanács-i irányelveket.

Ugyancsak foglalkoznia kell a magyar jogalkotásnak a társadalombiztosítási célok érdekében használt személyes adatok védelmével, amelyet az Európa Tanács /86/ 1 számú Ajánlásában[11] tett meg. E témakörön belül külön fel kell hívni a figyelmet arra, hogy a nem állami szférába tartozó tevékenység részletes adatkezelési szabályait kell megállapítani. Tartalmi szempontból figyelmet érdemel az a tény, hogy a társadalombiztosítási szervezeteknek - speciális célhoz kötötten - minden személyről jelentős mennyiségű adat áll rendelkezésükre, ami a szervezeten kívüli felhasználás lehetőség szerinti legnagyobb szűkítését kívánja meg. Különös gondot kell fordítani a személyes azonosító számmal kapcsolatban már elmondottakra a társadalombiztosítási szám képzése és használata során is. Mindezek mellett a munkaügyi és társadalombiztosítási célok érdekében használt adatok tekintetében a külföldi munkavállalási lehetőségek fokozatos növekedése miatt megfelelő szabályokat kell hozni a személyes adatok ilyen célok érdekében történő külföldre juttatásásával kapcsolatban.

Már 1981-ben foglalkozott az Európa Tanács az adatkezelés és adatvédelem egy speciális részkérdésével Az írásos bizonyíték megkövetelésére vonatkozó jogszabályok harmonizációjáról és az iratmásolatok, illetve a számítástechnikai eszközön rögzített adatok elfogadhatóságáról szóló /81/ 20 számú Ajánlásában[12]. Az ajánlás javasolja, hogy a tagállamok kormányai a technikai fejlődést követve dolgozzanak ki olyan szabályokat, amelyek lehetővé teszik többek között a mikrofilmes eljárás útján készített, a más módon reprodukált, illetve a számítógépen rögzített adatok, iratok bizonyítékként való elfogadását az igazságszolgáltatási eljárás során. Mindezek érdekében előírta az ajánlás, hogy az említett módszerekkel készített dokumentumoknak, másolatoknak milyen biztonsági elvárásoknak kell eleget tenniük. A magyar büntető- és polgári eljárási törvények módosításakor különös figyelmet kell fordítani ezen lehetőségek feltárására és esetleges bevezetésére.

További feladatot jelent az olyan területek adatkezelési szempontból való vizsgálata mint a sajtó-, és marketingtevékenység. A jelenlegi tapasztalatok azt mutatják, hogy Magyarországon egyébként e két területen figyelhető meg a legnagyobb bizonytalanság. Az Európa Tanács A direkt marketing célra használt személyes adatok védeméről szóló /85/ 20 számú Ajánlásában[13] felhívja a figyelmet arra, hogy ezen a területen az adatvédelem alapelvei még nem tudatosultak igazán a tagállamokban sem. Mindezek mellett a technikai lehetőségek és a marketing oldaláról jelentkező potenciális érdekek könnyen a magánélethez és az adatvédelemhez való jog megsértéséhez vezethetnek. Mindezt az e célra történő adatfelvétel rendjére, a listák, adatállományok átadására vonatkozó szigorú szabályok megteremtésével, valamint az érintett jogaira, az adatvédelmi szabályokra vonatkozó részletes szabályok kidolgozásával lehet ellensúlyozni. A sajtótevékenység adatvédelmi kérdéseinek tekintetében az Európa Tanács is csak az előzetes állapotfelmérésig az Adatvédelem és a sajtó című tanulmány[14] elkészítéséig jutott, amelyben felhívja a figyelmet a sajtószabadság és az adatvédelmi szabályok között fennálló esetleges ellentétes érdekekre. Erre tekintettel kérte a tagállamok kormányait, az adatvédelemért felelős szerveket arra, hogy e kérdéskört körültekintően vizsgálják meg.

4. ÚJ KIHÍVÁSOK A MAGÁNÉLET VÉDELMÉVEL SZEMBEN

Az Európa Tanács-i dokumentumok és a magyar jogalkotás összevetése során ki kell térni még egy fontos momentumra. Mint ahogy az korábban megemlítésre került, a jogalkotók a jelenlegi szabályok megalkotása során már az adatvédelemre vonatkozó Európa Tanács-i dokumentumok "második generációját, az 1981-ben elfogadott Adatvédelmi Egyezményt és az arra épülő egyéb anyagokat vették alapul. Az Európa Tanács Adatvédelmi Szakértői Bizottsága 1989-ben írt tanulmányában[15] jelezte hivatalosan, hogy az 1981 óta beállott technikai változások mind az adatkezelés minőségi, mind pedig az adatkezelés mennyiségi jellemzői tekintetében megváltoztatták azt a helyzetet, amelyen az 1981-es szabályozás alapult. Az adatkezelés általánossá válása, az időközben megjelenő decentralizált számítógépes rendszerek, a telekommunikáció és az adatkezelés kapcsolódása olyan változásokat hozott, amelyek szükségessé teszik az eddig alkalmazott megközelítés megfelelőségének vizsgálatát. Ilyenek a személyes adatok távolból történő automatikus gyűjtését lehetővé tevő, összefoglalóan "telemetria"-ként elnevezett, például a villamosenergia, víz, gáz fogyasztásának automatikus leolvasására szolgáló rendszerek. Meg kell említeni az olyan - interaktív média néven ismert - adatkezelő rendszereket, amelyek lehetőséget adnak a személyek és a rendszer közötti információcserére a személy kezdeményezése alapján. Továbbá különös figyelmet érdemelnek a már hazánkban is terjedő E-mail, elektronikus üzenetközvetítő rendszerek.

Röviden megvizsgálva ezen kérdéseket látható, hogy például a telemetrikus rendszerek és azok esetleges összekapcsolása lehetővé teszik az adott személy vagy háztartás folyamatos figyelemmel kísérését és ez elvezethet a korábban is előrevetített "átlátszó ember" jelenség kialakulásához. A Norvégiában tervezett, az áramfogyasztás mérésére szolgáló távadatleolvasó rendszer hat percenként szolgáltat majd adatot a központi nyilvántartás számára. Az ilyen rendszerek természetükből adódóan hordoznak magukban magánélet védelméhez kapcsolódó kérdéseket. Ugyancsak vannak veszélyei az interaktív rendszereknek, amelyek például telefonon, számítástechnikai eszközön keresztül igénybevehető banki, kereskedelmi, információs szolgáltatásokat biztosítanak. E rendszerek igénybevétele során az igénybevevő minden esetben azonosítja magát, íly módon a szolgáltatást, vagy a kommunikációs csatornát biztosító szervnél idővel olyan mennyiségű

személyes adat halmozódik fel, amely lehetőséget adhat az adatok másodlagos felhasználására, és - kereskedelmi, valamint egyéb - értékkel bírhat más személyek szervezetek számára. Ez ugyancsak adatvédelmi problémákat vethet fel. Az interaktív rendszerek használatának nyomonkövetése ugyancsak lehetővé teszi a korábban említett felügyeleti jellegű másodagos használatot, amely a probléma újabb dimenzióját jelenti. Az E-mail rendszerekkel kapcsolatos fő problémát az jelenti, hogy habár adatkezelésről és így személyes adat kezeléséről van szó, a rendszer jellemzői a levéltitokhoz fűződő jogok kérdéskörét is magukba kell hogy foglalják. Így a személyes adatok védelmének alapelvét eltérő, de ugyancsak alkalmazandó alapelvekkel is összhangba kell hozni. Adatvédelmi szempontból az E-mail rendszerek adatkezelési megbízhatósága, védelmi színvonala érdemel kiemelt figyelmet.

A Szakértői Bizottság véleménye szerint a jelenleg létező általános nemzeti adatvédelmi szabályok önmagukban nem képesek ezen új kérdéskörök megoldására, ezért azokat alapként felhasználva szükségessé válik új speciális részletszabályok kidolgozása. A szabályok kidolgozásakor ugyanakkor figyelmet kell szentelni az eredeti adatvédelmi alapfogalmak bizonyos mértékű módosulására is. Így például az érintett az összetett rendszerekben nehezen tudja lokalizálni, hogy róla milyen adatokat és hol, mely végpontokon kezelnek. Valószínű, hogy ennek megoldására úgynevezett logikai file-ok rendszerbe állítását kell előírni, amely lehetővé teszi az adott rendszerben az érintettre vonatkozó összes adat összegyűjtését. Nehezen határozható meg az említett okok miatt, hogy ki az "adatállománnyal rendelkező személy vagy szerv". A személy vagy szerv meghatározásának, ugyanakkor adatbiztonsági, jogérvényesítési, felelősségi szempontokból kiemelt jelentősége van. Előfordulhat ezért, hogy az eddig használt alapfogalmakat a "rendszer felett rendelkezési joggal bíró személy"-re kell alkalmazni egyes esetekben. Tovább nem részletezve elmondható, hogy a jogszerű adatgyűjtés, célszerűség, pontosság, adatbiztonság, az érintettek jogai, a jogorvoslati lehetőségek mellett az adatvédelmi egyezmény szinte minden alapfogalmát felül kell vizsgálni az adatkezelés területén beállt új változások fényében. Ez a megfigyelés tovább erősíti az Európa Tanács által korábban is elfogadott szektorális szabályozási elméletet és gyakorlatot. Ezt támasztja alá továbbá az az Európa Tanácsi Ajánlás kidolgozására irányuló javaslat[16], amelyet 1992. szeptemberében nyújtottak be és a személyes adatok védelmét a telemetrikus, telemarketing, interaktív rendszerekre, valamint az időközben beállott fejlődésre tekintettel kívánja újragondolni.

5. ÖSSZEFOGLALÓ

Mindezek alapján a hazai helyzetre visszatérve elmondható, hogy a jogalkotás eddigi jogszabályait az Európa Tanács dokumentumaival szoros összhangban alkotta meg. Az eddig végrehajtott szabályozási tevékenység olyan megfelelő alapokat fektetett le, amelynek bővítésével lehetőség nyílik az Euro-kompatibilis adatvédelmi szabályozás mielőbbi teljes körű megalkotására. Ugyanakkor, mivel a személyes adatok védelme eddig ismeretlen jogtárgyként került be a magyar jogrendszerbe, az ebből fakadó nehézségeket mind a jogi szabályozás, mind a gyakorlati alkalmazás területén érzékelni fogjuk. A nehézségek újabb dimenzióját jelenti az az ágazati szabályozási technika, amely életszerűsége és logikussága ellenére nem ismert a magyar jogalkotásban. Az Európa Tanács által mindezek mellett hivatalosan megállapításra került, hogy az adatvédelem területén folyamatosan változó, ezért állandóan új problémákat rejtő szabályozási tárgyat kell megfelelő jogi rendszerbe foglalni. A tárgykör emberi jogi relevanciája, fontossága elvitathatatlan, ezért

minden erőnkkel törekedni kell a még hiányzó jogi szabályozás mielőbbi megalkotására, annak folyamatos megújítására és a jogszabályok gyakorlati alkalmazására.

Jelen tanulmánynak nem volt témája és nem lehetett feladata az adatvédelem minden aspektusának részletes és teljes bemutatása. Általános jelleggel kívánta bemutatni az adatvédelem kérdéskörének Európa Tanács általi megközelítését, az eddigi magyar jogalkotást, annak helyzetét és rá kívánt mutatni a jövőbeni korszerűbb, átfogó, az informatika területén beállott változásokra is figyelemmel levő szabályozás kialakításának lényegesebb kulcskérdéseire. Ugyanakkor a tanulmányban érintőlegesen felvetett kérdések részletesebb kifejtése, a megfelelő válaszok kidolgozása és a jelzett szabályozások kialakítása csak az érintett szervek, csoportok, szakértők bevonásával, a már megalkotott korszerű hazai jogszabályok, valamint a kapcsolódó nemzetközi egyezmények, normák és ajánlások felhasználásával történhet.

FELHASZNÁLT IRODALOM ÉS JOGSZABÁLYOK

[1] Convention on Human Rights and Fundamental Freedoms;

[2] Recommendation No. R 854 /1979/ on access by public to government records and freedom of information; Parliamentary Assembly of the Council of Europe, Strasbourg;

[3] No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Strasbourg, 1981.;

[4] Recommendation No. R /83/ 10 on the protection of personal data used for scientific research and statistics; Committee of Ministers of the Council of Europe, Strasbourg;

[5] Recommendation No. R /91/ 10 on the communication to third parties of personal data held by public bodies; Committee of Ministers of the Council of Europe, Strasbourg;

[6] Study on the introduction and use of personal identification numbers: the data protection issues; Select Committee of Experts on Data Protection, of the Council of Europe, Strasbourg, 1991.;

[7] Recommendation No. R /89/ 2 on the protection of personal data used for employment purposes; Committee of Ministers of the Council of Europe, Strasbourg;

[8] Recommendation No. R /90/ 19 on the protection of personal data used for payment purposes and other related operations; Committee of Ministers of the Council of Europe, Strasbourg;

[9] Recommendation No. R /87/ 15 Regulating the use of personal data in the police sector; Committee of Ministers of the Council of Europe, Strasbourg;

[10] Recommendation No. R /81/ 1 on the Regulations for automated medical data banks; Committee of Ministers of the Council of Europe, Strasbourg;

[11] Recommendation No. R /86/ 1 on the protection of personal data used for social security purposes; Committee of Ministers of the Council of Europe, Strasbourg;

[12] Recommendation No. R /81/ 20 on the Harmonisation of laws relating to the requirement of written proof and tothe admissibility of reproductions of documents and recordings on computers; Committee of Ministers of the Council of Europe, Strasbourg;

[13] Recommendation No. R /85/ 20 on the protection of personal data used for direct marketing purposes; Committee of Ministers of the Council of Europe, Strasbourg;

[14] Study on data protection and the media; Select Committee of Experts on Data Protection, of the Council of Europe, Strasbourg, 1991.;

[15] Study on New technologies; a challange to privaci protection?; Select Committee of Experts on Data Protection, of the Council of Europe, Strasbourg, 1989.;

[16] Motion for a Recommendation on the protection of personal data in the use of telemarketing, telemetry, interactive media and social progress; presented by Mr. Nunez and others, Strasbourg, 1992.

Adat, információ, informatika - védelem és biztonság

(biztonság az államigazgatásban)

Papp György

Miniszterelnöki Hivatal
Informatikai Koordinációs Iroda

Az emberi célelérés alapvető módja a tevékenységek munkafolyamattá szervezése. Több ember együttes tevékenységének koordinálása általában szervezetek kereteiben történik. Az adott szervezet céljai hierarchikus rendszert alkotnak, amelyek meghatározzák a szervezet funkcióit. A funkciók közül az egyik legfontosabb, ezért általánosan előforduló, a biztonsági funkció. Célja mindazon tényezők kiküszöbölése, amelyek a szervezet működését, esetleg létét veszélyeztetik.

A szervezetekben a folyamatok során különböző eszközöket alkalmaznak a célok elérése érdekében. A modern szervezetek egyik legfontosabb erőforrása az adat és az információ. Mint a vezetés és irányítás eszközét, minden szervezetben felhasználják, éppen ezért a szervezetek jelentős része információk feldolgozására specializálódott. Itt az információ a munkának egyben tárgya is. Az adat és információ feldolgozása egyre bővülő mértékben számítástechnikai eszközök igénybevételével valósul meg. Az adat és információ egyidejűleg a biztonság megteremtésének is fontos eszköze, logikus tehát, hogy a feldolgozás folyamatainak és eszközeinek rendszere, szakmai nevén: az informatika, egyre több szerepet kap a biztonsági feladatok megoldásában.

Az adat- és információ-feldolgozás maga is (rész)folyamat, saját részfolyamatokkal és sajátos fizikai eszköztárral (rendszerelemek) és eljárásokkal. A technikai-gazdasági fejlődés következtében az informatikai szint felértékelődik. Ennek egyik oka a globalizálódó világban megnövő információ-szükséglet (a nagy számosságú és térben távoli folyamat összehangolása érdekében). A másik ok az anyagi folyamatok részbeni kiváltása informatikai eszközökkel pl. a bankélet, a tőzsde területén.

Egy szervezeti tevékenységnek az információ nemcsak eszköze, hanem tárgya is egyben. Ebből adódóan a szervezeti tevékenységben - céljai elérése szempontjából - az adat és az információ a legfontosabb eszköz, a legnagyobb érték. Igaz ez akkor is, ha sok esetben az információ széles körben ismert és könnyen pótolható, esetleg nem jelentkezik formalizálva, mert "fejben van".

Ennek megfelelően az információ minőségének romlása vagy

- közvetlenül veszélyezteti a szervezet céljainak elérését, vagy
- a célelérés támogatását akadályozza.

A biztonság tehát több, mint külső támadástól való védelem, általános értelemben működési állapot fenntartása. Ennek elérése történhet

- a rendszerelemek viszonyrendszerének biztonsági szempontokat figyelembe vevő kialakítása útján, akár különleges, a biztonságot fokozó intézkedések megtételével is, valamint
- speciális rendszerelemek beiktatásával.

Az informatikai biztonság tervezése és megteremtése - analóg módon más biztonsági feladatok megoldásával - a következő kérdések köré épül:

- Mely információk szükségesek a szervezeti célok elérése érdekében?
- Adott információra mely alapfenyegetések érvényesek?
- Hol, milyen rendszerelemhez kötve jelennek meg az információk a rendszerben?
- Adott helyen milyen tényezők válthatják ki az alapfenyegetettség bekövetkeztét?
- Mi a kockázata a fenyegetéseknek?
- Milyen intézkedések tehetők a kockázat csökkentésére?
- Gyakorlatilag lehetséges-e illetve megéri-e az adott védelmi intézkedés?
- Milyen feladatok adódnak az elhatározott intézkedésekből?

A biztonságos informatikai rendszerek megteremtésének számos módszertana létezik, amelyek a vizsgálatba bevont folyamatok körében, illetve az eljárások lépéseinek tagolásában különböznek egymástól. A vázolt kérdések azonban valamilyen formában minden hatásos biztonsági intézkedéseket eredményező módszernek részei.

A fenti megfontolásokra épülő biztonsági rendszer kialakítása különösen fontos a kormányzati informatikai rendszerek esetében, ahol a lakossági elvárások és a személyi jogok érvényesítésének fórumai, a széleskörű és megbízható adatokat igénylő döntési rendszerek, valamint az állam biztonságát közvetlenül is befolyásoló vezetési rendszerek mind nagyfokú biztonsági igénnyel lépnek fel, ugyanakkor egymásnak sokszor ellentmondó követelményeket támasztanak az informatikai biztonsággal szemben.

A Miniszterelnöki Hivatal Informatikai Koordinációs Irodája kidolgozta a kormányzati szervek informatikai rendszerei biztonsága erősítése céljából, nemzetközi ajánlások figyelembevételével az "Informatikai Biztonsági Módszertani Kézikönyv"-et (IBMK). A kézikönyv összhangban van a közigazgatás korszerűsítési és a központi államigazgatási szervek informatikai fejlesztéseinek koordinálási programjával, miszerint a koordinációs testület az informatika területén az Európai Közösség (Unió) előírásaihoz igazodó kormányzati ajánlásokat terjeszt az államigazgatási informatikai fejlesztések gazdaságos és hatékony megteremtésére. Az ajánlásoknak biztosítaniuk kell a "nyílt rendszer" elv érvényesítését, informatikai stratégiai tervek készítését, a tervezéshez minőségjavító módszerek bevezetését, a biztonsági és adatvédelmi követelmények fokozott érvényrejuttatását, a beszerzések megalapozottságának javítását.

A kormány, hasonlóan a fejlett országok gyakorlatához, a kormányzati informatikai fejlesztés alapjául a "nyílt rendszer" elvet jelölte meg, ami szükségessé teszi az informatika és az információs rendszerek biztonságának alapelveit meghatározó, az Európai Közösség által ajánlásként kibocsátott, "Green Book on the Security of Information Systems" és az ITSEC (Information Technology Security Evaluation Criteria) figyelembevételét az informatikai rendszerfejlesztésben. A dokumentumok az informatikai biztonság irányelveit, kereteit, mozgásterét határozzák meg és abból a tényből indulnak ki, hogy a biztonság konkrét megteremtése minden társadalom,

intézmény, szervezet saját feladata. Az IBMK messzemenően figyelembe veszi a nyílt rendszerekre vonatkozó előírásokat mind a technikai normákat, mind az alkalmazott módszertant tekintve.

Az informatikai stratégia a szervezeti célok eléréséhez szükséges informatika-alkalmazások célkitűzéseinek és a célelérés módjának együttes áttekintése. A szervezet informatikai stratégiája a szervezeti stratégia része. A szervezeti stratégiában elfoglalt helyét a szervezet informatikához kötődő folyamatai határozzák meg. Nevezetesen, hogy a legtöbb szervezeti tevékenység informatikai elemeket tartalmaz, a szervezeti célelérés informatika-alkalmazás nélkül a folyamatok többségében nem lehetséges. Különösen nagy jelentőségű az informatikai stratégia azon szervezetek esetében, melyek alaptevékenysége az információfeldolgozás.

Egyéb részek (részstratégiák) mellett ugyancsak integráns eleme a szervezeti stratégiának a biztonsági stratégia. A szervezet célelérését szolgáló tevékenységek végrehajtásának biztonságát szavatoló feladat- (és ebből adódó folyamat-) rendszer a szervezeti stratégia által érintett összes tevékenységet le kell hogy fedje. Enélkül ugyanis a biztonság teljeskörűsége és az egységes biztonsági szint követelménye sérülne. A követelmények szükségessége könnyen belátható. Feltéve, hogy a szervezet a célelérést szolgáló folyamatok nem minden elemének működőképességét tudja biztosítani, az adott elem lehetséges funkciócsökkenéséből (vagy diszfunkcionalitásából) adódó téves célelérési tevékenységek a rendszer-elv alapján, az önmagában talán "biztonságos" többi folyamatot is veszélyezteti.

Fenti megállapításhoz két megjegyzés szükséges:

> A biztonság komplex kategória, tehát - épp az előzőek alapján - különválasztva nem értelmezhető egyes részrendszerek vagy elemek saját biztonsága (ezért az idézőjel).
> Az informatikai biztonság a jelen megközelítés keretei közt nem más, mint a szervezeti tevékenységek informatikai összetevőinek a célok eléréséhez szükséges (megfelelő) állapotban tartása.

Következésképpen az informatikai biztonság integráns része az informatikai rendszernek és egyúttal a szervezeti szintű biztonsági rendszernek is. Köztük szoros kölcsönös kapcsolati mechanizmus érvényesül, ezért nem is mindig lehetséges az egyes elemek elhatárolása, vagy közöttük szigorúan oksági kapcsolat definiálása.

Az informatikai stratégia követelményeket fogalmaz meg. A követelmények közt biztonsági szempontból lényeges elvárások is megjelennek, amelyek a rendszertervezés számára célkitűzésként fogalmazódnak meg. A későbbiekben ezek alapját képezik az informatikai rendszer, az informatikai biztonság tervezésének, majd megvalósításának. Példák bizonyítják, hogy az informatikai rendszer létrehozása után pótlólagosan végrehajtott biztonsági intézkedések, utólagosan beillesztett biztonsági mechanizmusok nemcsak többszörös költséggel valósíthatók meg, de az általuk elért biztonság mértéke sem azonos a rendszer kialakításával egyidőben és szoros kapcsolatban végrehajtott biztonsági fejlesztés eredményével.

A sikeres rendszerműködésnek biztonsági kritériumai is vannak. A gyakorlatban ezek a biztonsági kritériumok rejtetten vannak jelen. A biztonságnak, mint szükséges funkciónak feltárásához és megjelenítéséhez a szervezet tevékenységének teljeskörű átvilágítására és részletes funkcióelemzésére van szükség. Az ennek nyomán feltárt biztonsági funkció az elemzések nyomán kritikus sikertényezővé válhat. Az informatika biztonsági kérdéseinek kritikus sikertényezővé

(KST) való nyilvánítása szükséges ahhoz, hogy az informatikai célok között a biztonságos informatikai rendszer megteremtésének - vagy a biztonság fenntartásának illetve megerősítésének - célja megjelenjen. A funkcióelemzés - KST - célrendszer folyamaton keresztül tisztázott és a stratégiai célrendszerbe beiktatott biztonsági szempontok eredményezik az informatikai stratégiában biztonsági projektek kitűzését. A biztonsági projekt megindításához szükséges biztonsági értékelés jelenti az informatikai biztonság létrehozásának kiinduló pontját.

A tervezési folyamatok párhuzamossága és kölcsönösségi viszonya indukálja a tervezési módszerek nagyfokú párhuzamosságát és rokonságát. Az informatikai biztonság tervezésének módszertana az informatikai rendszertervezés módszertanához sok tekintetben hasonló. Ilyen például a tervező csoport összetétele, az alkalmazott csoportmódszerek és szervezési résztechnikák, valamint a tervezés során végrehajtott lépések.

Az Európai Közösség (Unió) által kidolgozott informatikai és információs rendszerekre vonatkozó biztonsági irányelveket követő különböző szervezési módszertanok (némileg eltérő terminológiával és tartalommal) az informatikai rendszerszervezés szakaszait az alábbiak szerint definiálják.

Szervezési lépések az angol SSADM (Structured Analysis and Design Method) szerint:

- megvalósíthatóság elemzése,
- helyzetfelmérés,
- a rendszerszervezési mód meghatározása,
- a követelmények megfogalmazása,
- technikai alternatívák,
- logikai tervezés,
- fizikai tervezés.

(az SSADM-en kívüli lépések:)

- kivitelezés és tesztelés,
- rendszer működtetés.

Az informatikai biztonság megteremtésének szakaszai a német (IT - Sicherheitsshandbuch KBSt 1991) módszertan szerint:

- a védelmi igény megállapítása,
- fenyegetettség-elemzés,
- kockázatelemzés,
- informatikai biztonsági koncepció készítése,
- az informatikai rendszerek kiválasztása,

(a módszertanban nem szereplő szakaszok:)

- biztonsági szoftverek tervezése, illesztése,
- Informatikai Biztonsági Szabályzat elkészítése,
- informatikai biztonsági követelmények átvezetése más szabályzatokon,
- a rendszer bevezetése, üzemeltetése,
- a biztonsági előírások betartásának és a mechanizmusok működésének ellenőrzése,
- az informatikai biztonsági rendszer felülvizsgálata,
- módosítások a biztonsági rendszerben.

A vázolt analógiák és beágyazódások ellenére az informatikai biztonság megteremtésének folyamata specifikus feladatokat tartalmaz. Specifikumuk a megoldásukhoz szükséges

szemléletmódból és ismeretanyagból fakad. Ezen feladatok módszertani elemeit tartalmazza az informatikai biztonság módszertana.

Az IBMK tartalma nem fedi le az informatikai biztonság megteremtésének teljes folyamatát, de bemutatja az informatikai stratégiából adódó, az informatikai rendszerszervezés során feltételezett célok biztonsági vetületeinek meghatározásától a konkrét rendszer kialakításához szükséges környezeti és számítástechnikai intézkedések megtervezéséig végrehajtandó lépéseket.

Az államigazgatásban, valamint a közigazgatásban az állampolgárok adatainak egyéni és társadalmi érdekeket szolgáló feldolgozásai, az állampolgárok adatainak jogszerű felhasználása, az állam- és közigazgatási feladatok közmegelégedésre számottartó elvégzése növekvő mértékben függ az informatikai és információs rendszerek zavartalan működésétől. Ezért az informatikai és az információs rendszerek biztonságának megteremtése ezeken a területeken különösen fontos. Ez vonatkozik az általános ügykezelésre, az iratkezelés eljárásaira, ezen belül az informatikai rendszerekben megjelenő adatok és információk védelmére, valamint biztonságára egyaránt. Az információk és adatok előállításának illetve felhasználásának jogszerűségét adatvédelmi illetve adatkezeléssel kapcsolatos törvények, rendeletek, utasítások szabályozzák.

A szabályozások keretében biztosítani kell az információk, illetve adatok

- rendelkezésre állását, elérhetőségét az arra jogosultak számára,
- sértetlenségét (sérthetetlenségét, valódiságát),
- az információk illetve adatok jellegétől függő bizalmas kezelést,
- az információk, illetve adatok hitelességét, valamint
- a teljes informatikai, illetve információs rendszer működőképességét.

Ez az öt alapkövetelmény határozza meg az informatikai rendszerben az adatok és információk biztonságos kezelésének alapjait.

Az említett alapkövetelmények teljesítéséhez olyan védelmi intézkedésekre van szükség, amelyek az információk és adatok *rendelkezésre állását*, *sértetlenségét*, *bizalmasságát*, *hitelességét* és *működőképességét* a lehető legkisebb kockázattal és egyenszilárdsággal biztosítják. Ezek az intézkedések kiterjednek:

- az informatikai rendszer tervezésére,
- az informatikai rendszer bevezetésének felügyeletére,
- az informatikai rendszer rendeltetésszerű használatára, a rendszer üzembiztonságára, továbbá
- önmaguknak a biztonsági intézkedéseknek a bevezetésére és betartásuk ellenőrzésére.

Az Informatikai Tárcaközi Bizottság, felismerve az állam- és a közigazgatás szervezeteiben bevezetett informatikai rendszerek biztonságtechnikai hiányosságait, programot dolgozott ki a meglévő rendszerek biztonságának fokozatos javítására, a jövőben létesítendő rendszerekbe megfelelő biztonsági elemek beépítésére, és - az Európai Unióhoz való csatlakozási szándéknak megfelelően - az európai informatikai biztonsági ajánlások átvételére, honosítására, illetve adaptálására.

A program célja:

- folyamatosan felhívni a figyelmet az informatikai rendszer felelősei és felhasználói körében a rendszer tervezése, bevezetése, üzemeltetése és alkalmazása során felmerülő veszélyekre,
- tudatosan kialakítani a veszélyekkel szembeni védekezés formáját és tartalmát,
- az informatikai stratégiai tervezés lépéseivel összhangban fokozatosan elsajátítani és bevezetni az informatikai biztonsági koncepció készítésének módszertanát,
- az átmeneti időszakban is a lehető legnagyobb mértékben biztosítani az informatikával kapcsolatos adatvédelmi törvények és rendeletek betartását.

A program lépései:

- megismertetni az állam- és közigazgatásban dolgozókat az informatikai rendszerek használatával kapcsolatos veszélyforrásokkal veszélyekkel,
- a jelenlegi intézményi keretek között javaslatot tenni a legfontosabb intézkedési lépésekre, ezek révén megteremteni az átmeneti időszak alatti ideiglenes informatikai biztonságot,
- lefektetni az informatika biztonsági koncepció készítésének alapjait, fokozatosan bevezetni a tudatos kockázatelemzés módszereitt, kidolgozni az államigazgatásban a működőképesség és a sértetlenség védelmének, mint a legfontosabb védelmi intézkedésnek a rendszertechnikai alapjait
- kialakítani azt az intézményes hátteret, amely segítséget nyújt és tanácsot ad az állam- és közigazgatás szervezetei számára az informatikai rendszerek biztonságos tervezésével, bevezetésével, üzemeltetésével összefüggő kérdésekben.

A különböző formában megjelenő információknak egyre nagyobb a jelentőségük az egyes polgár számára csakúgy, mint a gazdaságban, a tudományban és az igazgatásban. A gazdaság csaknem kétharmadának teljesítménye és növekedése olyan termelési és szolgáltatási elemekre épül, amelyek erőteljesen függenek az információtechnológiától és ezáltal alapvetően rá vannak utalva az információs rendszerek zavartalan működésére.

Az informatika rendszerek egyre növekvő mértékű alkalmazása és a világméretű hálózatok elérhetősége révén azonban emelkedik a helytelenül, a hibásan, illetve a jogsértő módon bevezetett és működtetett, mindezek következtében fokozottan veszélyeztetett informatikai alkalmazások száma. Vizsgálatok igazolják, hogy az érintett vállakozások mintegy negyven százaléka legfeljebb két évvel, de például a biztosítók és a termelő vállalatok csak néhány nappal élték túl adatállományuk teljes megsemmisülését, elvesztését. A számítógépes bűnözésről, vírusprogramokról, trójai falovakról szóló híradások - mindezek a számítógépek és számítógépes rendszerek fenyegetett világában használt fogalmak - élesen rávilágítanak a növekvő kockázatokra.

A Informatikai Biztonsági Módszertani Kézikönyv (IBMK) feltárja az informatikai rendszereket fenyegető vagy azokban fellépő potenciális veszélyforrásokat. Emellett segítséget nyújt az államigazgatási, a közigazgatási és a gazdálkodó szervezetek számára információs és informatikai rendszerükhöz kapcsolódó rendszer- és felhasználásközpontú kockázatelemzésekhez és az ezeken alapuló biztonsági koncepciók kialakításához.

Az IBMK hasznos adalékokat, rendszerezett módszertani elemeket igyekszik szolgáltatni a számítógépes információs rendszerek fejlesztői, üzemeltetői részére. Nem szabad megfeledkezni

azonban arról, hogy ezeknek a módszertani elemeknek az alkalmazása, a célszerű módszertani "kompozíciók" kialakítása minden esetben csak a helyi sajátosságok megértésén és figyelembevételén alapulhat. Minden konkrét esetben fel kell tárni a biztonsági problémák alaptermészetét, meg kell alkotni az adott rendszerelem, szervezet biztonsági rendszerét. E téren a korszerű rendszerszemlélet kell, hogy vezéreljen, mely szerint a rendszert nem kész elemekből álló halmazként kell tekinteni, hanem mint egész rendszerelemet, amely elvileg különböző tagozódásokat tesz lehetővé de általában véve nem azonos ezeknek a tagozódásoknak az egyszerű összegével.

A rendszer megalkotásához szükség van általános feltételezésekre, úgynevezett alapelvekre, amelyekből következtetéseket lehet levonni a rendszer alapfunkcióit és a funkciók realizálását szolgáló struktúra jellemzőit illetően. A tevékenység, amely az Európai Unió és egy adott nemzet jogrendszerébe illeszkedő adatvédelemmel és adatbiztonsággal kapcsolatos irányelvekre támaszkodhat, két részre oszlik. Először meg kell határozni az alapelveket, másodszor pedig le kell vezetni a belőlük adódó következtetéseket. A módszertani kézikönyv a második feladat elvégzéséhez szolgál megfelelő alapul. Ha tehát egy területen, illetve az összefüggések egy komplexumára sikerül az első feladatot megoldanunk, kellő szorgalom és értelem esetén a siker nem marad el. De az első feladat, vagyis azoknak az alapelveknek a megkeresése, amelyek a deduktív rendszerépítés alapjául szolgálhatnak, egészen más dolog. Itt nincs megtanulható, rendszeres módszer, amely a célhoz vezetne. Azt mondhatjuk, hogy itt csak a tapasztalatba való beleérzésen alapuló intuíció visz sikerre. Az intuíció - ebben az esetben is - csak a rendkívül komoly, megalapozott elméleti felkészültségből táplálkozhat.

Az IBMK célja annak elérése, hogy alkalmazója a kézikönyv segítségével képes legyen:

- a vizsgálatok tárgyát ésszerűen megválasztani és a saját informatika alkalmazásai esetére a biztonsági követelményeket meghatározni (a védelmi igény megállapítása),
- valamennyi lehetséges fenyegető tényező közül kiválasztani azokat az a speciális - meglévő vagy tervezett - informatikai rendszer vonatkozó speciális veszélyeztetettségi elemeket, amelyek meghatározók, relevánsak (fenyegetettség-elemzés),
- a feltárt fenyegető tényezők kihatásait értékelni, ezáltal az adott kockázatokat felfedezni (kockázatelemzés) és
- mindezekkel megteremteni egy biztonsági koncepció összeállításának előfeltételeit.

Az informatika alkalmazójának felelőssége, hogy a mindenkori biztonsági előírásoknak és követelményeknek - adott esetben okmánnyal bizonyítottan is - megfelelő információtechnológiai termékeket is csak saját megelőző védelmi intézkedéseinek megtételét követően vegye használatba. Ezen túlmenően az előírások és törvények alkotóinak a dolga, hogy a jövőben a különösen érzékeny alkalmazói területekre vonatkozó megelőző intézkedéseket kötelezően előírjanak.

Az Informatikai Biztonsági Módszertani Kézkönyv összeállítása és ajánlásként történt közreadása szerves részét képezi annak az ajánlás-sorozatnak, amely az Informatikai Tárcaközi Bizottság felügyelete alatt és jóváhagyásával iránymutatást kíván adni a kormányzati és államigazgatási szervezetek informatikai fejlesztéseihez.

A kézikönyv rendeltetése, hogy segítséget nyújtson elsősorban az említett szervezetek informatikai tevékenysége biztonságos, zavarmentes végzéséhez, az ehhez szükséges feltételek tervszerű kialakításához.

Figyelembe véve, hogy bármilyen irányítási, igazgatási, különösképpen az államigazgatási feladatkör lényegét tekintve folyamatos döntéshozatali tevékenységet igényel, amelynek mindenkor és minden körülmények között információk képezik az alapját, nem vitatható az informatika kiemelkedő jelentősége, fontossága ezeken a területeken. A társadalmi, gazdasági fejlődés következtében "megsűrűsödött" döntési kényszer egyúttal annak kényszerét is jelenti, hogy az információk alig belátható tömegének célirányos feldolgozása minden eddiginél gyorsabban és megbízhatóbban történjék. Ez a követelmény, illetve ennek kielégítése az intézmények, szervezetek létfeltétele, indokolt tehát, hogy a tudomány és a technikai adott színvonalán elérhető valamennyi olyan eszközt igénybe kell venni, amelyek jó döntések meghozatalát segítik elő az azokhoz szükséges információk rendelkzésre állásának biztosításával.

Az informatikai tevékenység eredményeinek megbízható létrejötte és minősége számos biztonsági tényezőjétől függ, amelyek megismerése, alkalmazása csakis a szervezet összbiztonságát befolyásoló tényezők együttesében értelmezhető. Ahhoz azonban, hogy ebben az együttesben az informatikai biztonság kérdéseire jelentőségüknek megfelelően lehessen koncentrálni, szükséges ezek elhatárolt tárgyalása akkor is, ha közben tudjuk, hogy - bármilyen súllyal szerepel is - csak az összbiztonság egy speciális területéről van szó.

A módszertani kézikönyv, utalva az említett összefüggésre, ebben a szellemben foglalkozik az informatikai biztonság elemeivel, ilymódon törekszik elősegíteni azt, hogy az érintett szervezetek kielégítő minőségű biztonsági rendszert alakítsanak ki saját tevékenységük és feltételeik szem előtt tartásával.

Az elmondottakból kiinduló megfontolásokra támaszkodva a vonatkozó, meglehetősen terjedelmes ismeretanyag a következő tagolásban került megszerkesztésre:

"Vezetői tájékoztató" (1. fejezet), amely a vezetői feladatokat jelöli meg az informatikai biztonsági projekt koncepciójának kialakításában. Ehhez kisegítő ismereteket nyújt az informatikai biztonság jelentőségéről a kormányzati munkában, az informatikai stratégiában elfoglalt helyéről, valamint ez utóbbi tervezési ciklusaival fennálló kapcsolatáról.

"Projekt vezetési segédlet az informatikai biztonsági koncepció kialakításához" (2. fejezet), amely a koncepció-kialakítás alapjairól, résztvevőiről és eljárásáról, illetve annak tagolásáról ad részletes ismeretést az erre irányuló projekt irányítóinak teendőit szem előtt tartva.

"Végrehajtási segédlet az informatikai biztonsági koncepció kialakításához" (3. fejezet), amely a koncepcióban praktikusan figyelembe veendő informatikai elemcsoportokhoz kapcsolódóan mutatja be azok gyenge pontjait, fenyegető tényezőit és a konkretizált biztonsági hiányok révén keletkezhető károk értékelési rendszerét. Mindezt kiegészíti az elemcsoportok veszély-szempontú összefüggéseinek felvázolásával, a lehetséges és szükséges biztonsági inzézkedések felsorolásával, majd javaslatot tartalmaz az informatikai biztonsági koncepció felépítésére.

"Útmutató az informatikai biztonsági szabályzat elkészítéséhez" (4. fejezet), amely bemutatja ennek a szabályzatnak a helyét és szerepét a szervezet szabályzati rendszerében, valamint tartalmi sémát ad a szabályzat gyakorlati kialakítására, szerkezetére.

A tulajdonképpeni módszertani fejezeteket kielégítő kezelhetősége érdekében a kézikönyv még kiegészül egy 5. fejezettel, "Jogszabályok és szakirodalmi kitekintés" cím alatt, valamint egy "Értelmező tárgymutató"-val (6. fejezet).

Adott szervezet informatikai biztonságának követelményeit, az informatikai biztonság megteremtése érdekében szükséges intézkedéseket, ezek kölcsönhatásait és következményeit az informatikai biztonsági koncepció (IBK) tartalmazza. Az informatikai biztonsági koncepció megléte előfeltétele a szervezet egységes biztonsági szemlélete kialakításának, és alapját képezi a további tevékenységnek. Ezért az informatikai biztonsági koncepció kialakítása kulcseleme az informatikai biztonság megvalósításának. A koncepció összetett folyamat terméke, tartalmazza az informatikai biztonság megteremtésének lépései eredményeként létrejövő dokumentumokat.

Az informatikai biztonsági koncepció főbb tartalmi összetevői:

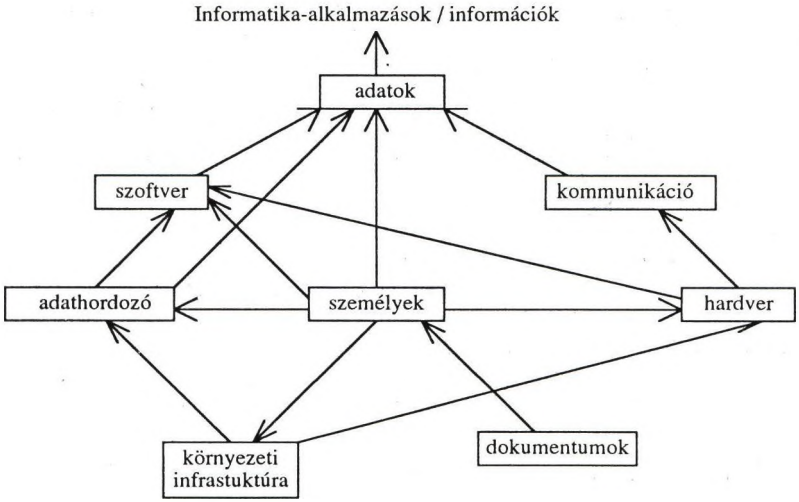
- a védelmi igény leírása (meglévő állapot, fenyegetettségek, fennálló kockázatok),
- az intézkedések fő irányai (kockázat-menedzselés),
- a feladatok és felelősségek megosztása (az intézkedések megvalósítása során),
- időterv (megvalósítási ütemekre és az IBK felülvizsgálatára).

A fenyegető tényezők az informatikai rendszerelemekhez kapcsolódnak és azokon keresztül okozhatnak károkat, miután az informatika-alkalmazás függ a rendszerelemektől. Éppen ezért kell megvédeni a rendszerelemeket a fenyegető tényezők ellen. Ehhez a következő meglévő rendszerelem-csoportokat kell áttekinteni :

Tárgyiasult elemcsoportok	környezeti infrastruktúra
	hardver
	adathordozók
	dokumentumok, iratok
Logikai elemcsoportok	szoftver
	adatok
	kommunikáció
Személyi elemcsoport	személyzet, felhasználók, ellenőrök

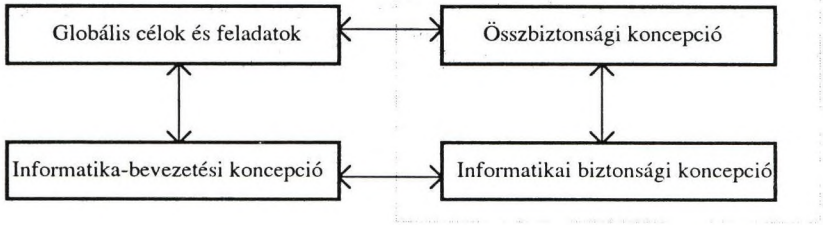
1. ábra: A rendszerelemek nyolc csoportja

Az egyes elemcsoportok között alapvetően komplex függőségek állnak fenn abban az értelemben, hogy egy rendszerelem rendelkezésre állása, sértetlensége bizalmassága, hitelessége és működőképessége más rendszerelemek rendelkezésre állását, sértetlenségét bizalmasságát, hitelességét és működőképességét feltételezi. Durva megközelítésben a következő ábra szemlélteti azokat a függőségeket, amelyek a nyolc rendszerelem-csoport között fennállnak.



2. ábra: Az elemcsoportok függőségi viszonyai

Az informatika biztonsági koncepciót az adott cég, szervezet, vagy hatóság összbiztonsági koncepciójába kell integrálni. Ez utóbbiban kell meghatározni a biztonsági stratégiát, azaz a biztonságot érintő általános célkitűzéseket. Az általános biztonsági stratégiából vezethetők le a még elviselhető maradványkockázatok mértékei és a tervezett intézkedések elfogadhatósága. Ha még nem létezik biztonsági stratégia, akkor annak a kiindulópontjául lehet tekinteni az informatika biztonsági koncepcióban szereplő megállapításokat, ezek segítségével megfogalmazni a generális biztonsági célokat és irányelveket. Ugyanakkor az IBK-t egyeztetni kell az informatikai bevezetési koncepcióval is, mint ahogyan - ideális esetben - a biztonsági stratégiának össze kell csengenie az adott szervezet feladataival és céljaival:

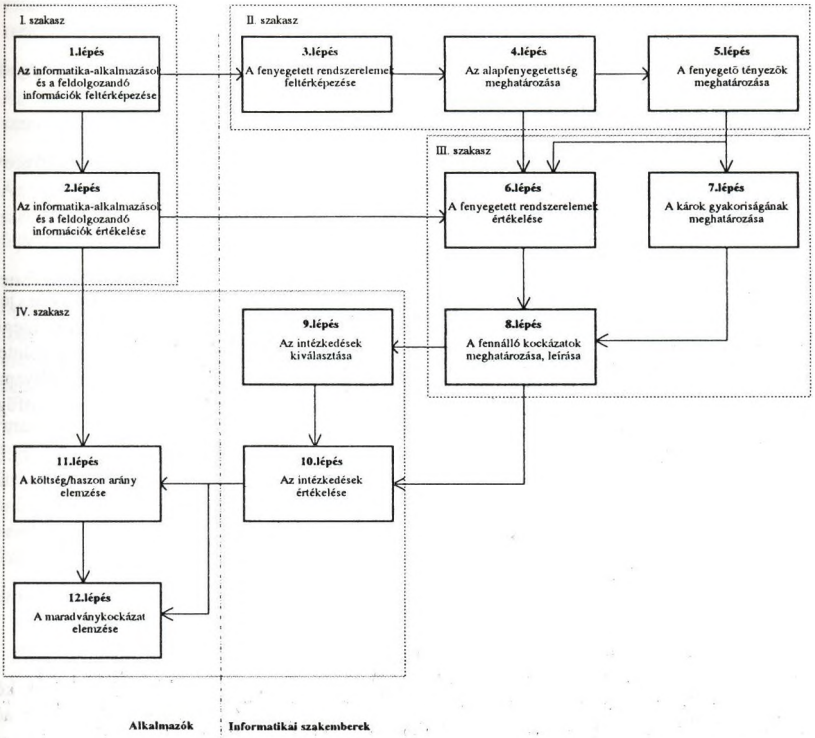


3. ábra: Az IBK beágyazódása

Az IBK kialakítási folyamata - tartalmának megfelelően - eljárási szakaszokra, azon belül pedig lépésekre bontható.

Az első szakaszban a szervezet szempontjából kiválasztják és behatárolják a további vizsgálódások tárgyát. Ehhez meg kell állapítani, hogy mely informatika-alkalmazások érdemesek a védelemre értékük alapján. A második szakaszban feltárják mindazon fenyegető tényezőket, amelyek az első szakaszban kiválasztott informatika-alkalmazásokra veszélyesek lehetnek. Ennek során vizsgálni kell az informatikai rendszer úgynevezett gyenge pontjait. A harmadik szakaszban azt értékelik, milyen káros hatása lehet a fenyegető tényezőknek az informatikai rendszerre, azaz mely kockázatok állnak fenn. A negyedik szakaszban fenyegető tényezők elleni intézkedéseket választanak ki és hatásaikat értékelik. Ennek során el kell dönteni, mely intézkedések vehetők figyelembe és milyen maradványkockázatok viselhetők el.

A négy szakaszt 12 lépés tagolja. A 4. ábra az lépések kapcsolatait és az általuk reprezentált tevékenységek alkalmazók, illetve informatikai szakemberek közötti megoszlását mutatja be.



4. ábra Az eljárás lépéseinek összefüggései

Az IBMK-ban az adat, az információ, az adatvédelem, az adatbiztonság általános informatikai rendszer szintű összefüggései a következő fogalmi elemek köré csoportosulnak:

Adat

Adat, mint fogalom alatt a tények, az elképzelések nem értelmezett, de értelmezhető formában való közlését értjük.

legfontosabb adatcsoportok az állam- és közigazgatásban:

- államtitok — *1987. évi 5. törvényerejű rendelet és a végrehajtására kiadott 17/1987 (VI.9.) MT rendelet*
- szolgálati titok (hivatali titok)
- személyes adat — *1992. évi LXIII. törvény*
- statisztikai adat — *1993. évi XLXI. törvény, 170/1993 (XII.3.) Korm.rendelet*
- egészségügyi adat
- közérdekű adat

stb.

adat előfordulási helyek:

- irat (papíralapú hordozó),
- mágneses adathordozó,
- film, microfilm, CD lemez, stb.,
- számítógép memória (ROM, RAM, stb.),
- képernyő, elektromágneses sugárzás,
- kommunikációs csatornák,

stb.

Információ

*Információ*nak nevezzük azon szimbólumok összességét, amelyek valamilyen jelentést hordozó adatokat tartalmaz és olyan új ismeretet szolgáltat az információt megismerő személy számára, hogy képes a személy valamilyen bizonytatlanságát megszüntetni és célirányos cselekvését kiváltani. Az *információ* általános értelemben a valóság folyamatairól és dologi viszonyairól szóló felvilágosítás. Ebből következően értelmezése kapcsolatfüggő.

Az emberek számára érthető információk többek között

a) térben láthatóan:

- számok,
- betűk,
- szövegek és
- képek formájában

b) vagy időben hallhatóan:

- beszéd,
- zene és
- zajok formájában jelenhetnek meg.

Informatikai értelemben, azaz az informatikai rendszereken belül az információk kódolva, adatok formájában fordulnak elő. Ahhoz, hogy az informatikai rendszerben tárolt adatokat ember számára érthetővé tegyük, át kell alakítani, vagy interpretálni, magyarázni kell azokat. Az informatikai rendszerben ma az információk kettes számrendszerre ("0" és "1" számjegyek) transzformált alakban jelennek meg.

Adatfeldolgozás, információ-feldolgozás

Az *adat-* és *információ-feldolgozás* alatt értjük általános értelemben az adatok, illetve információk

- begyűjtését,
- feltérképezését/feltárását,
- használatát,
- tárolását,
- továbbítását,
- programvezérelt feldolgozását (szoros értelemben) és
- ábrázolását.

Adatvédelem

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.

Adatbiztonság

Az adatok jogosulatlan megszerzése, módosulása és tönkremenetele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

Informatika

Az *informatika* a számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

Információ rendszer

*Információ rendszer*nek nevezzük az adat és információ gyűjtésére, tárolására, feldolgozására (bevitelére, módosítására, rendszerezésére, aggregálására stb.) továbbítására, fogadására, megjelenítésére, megsemmísitésére stb. alkalmas rendszert. Ha ez a rendszer számítógéppel támogatott, akkor számítógépes információ rendszerről (informatikai rendszerről) beszélünk.

Informatikai rendszer

Egy informatikai rendszer a számítástechnikai és telekommunikációs rendszerekből felépített információ rendszer, azaz a hardverek és szoftverek olyan kombinációjából áll, amit az információ-feldolgozás különböző feladatainak teljesítésére alkalmazunk. Az informatikai rendszerek különleges tulajdonsága a szabad programozhatóság. Az informatikai rendszerek közé soroljuk tipikusan a "cél számítógépeket" és a "általános célú számítógépeket".

Védelmi intézkedések, védelmi eljárások

A védelem megvalósítása alapjában véve a védelem érdekében tett védelmi intézkedések és védelmi eljárások együttese értendő. A legtöbb irodalom ezen együttest három nagy csoportra osztja:

- fizikai védelemre,
- ügyviteli védelemre és
- algoritmikus védelemre,

A *fizikai védelmi intézkedések* az informatikai rendszer környezetére vonatkoznak, magukba foglalják az épületeket, az emeleteket, a szobákat, az ablakokat, az ajtókat és a védett kabinokat. Az ügyviteli védelmi intézkedések két csoportra bonthatók, szervezeti- és személyi intézkedésekre. A *szervezeti védelmi intézkedések* minden olyan belső rendeletet, utasítást takarnak, amelyek az informatikai rendszer biztonsági eljárás rendjére, az informatikai rendszer felhasználóinak feladat- és hatásköreire vonatkoznak. A szervezet ezen kívül *személyi védelmi intézkedés* révén határozza meg az informatikai rendszer felhasználásának formáját, a személy tevékenységi normáit. Személyi intézkedések közé sorolható például az információ átadási szabálya, a továbbképzés, az ellenőrzés lefolytatása stb. A *algoritmikus védelmi eljárásokat* a szoftver és hardver rendszerelemekben valósítják meg azzal a céllal, hogy erősítsék a biztonságot.

Az adatvédelem szabályozási szintjei

Az adatvédelem jelenlegi szabályozása négy szinten valósul meg:

1. szint: adatvédelmi törvények
2. szint: műszaki normatívák, szabványok, irányelvek, rendeletek
3. szint: ágazati, tárcaszintű végrehajtási utasítások
4. szint: helyi szabályzatok

Az első szinten lévő adatvédelmi törvények az adatvédelmi rendszer kereteit határozzák meg, ugyanis egy általános védelmi rendszer teljes köre egy adott pillanatban nem határozható meg, az dinamikusan változik, és az információrendszer jellegétől függően más és más szabályhalmazt jelent. Természetes, hogy nem azonos az igénye egy ügyviteli adatfeldolgozó rendszernek és egy technológiai folyamatot értékelő programnak. Így az informatikai rendszer bármilyen szintű kialakítása során, egyedileg kell megvizsgálni és megszervezni a védelmi környezetet, a terület sajátosságaihoz alkalmazkodva.

A második szinthez tartozó műszaki normatívák, szabványok, irányelvek, rendeletek védelmi körbe soroljuk:

- az építésügyi szabványok, rendeletek, normatívák gyűjteményét;
- a tűzvédelemre vonatkozó jogszabályokat, műszaki irányelveket;
- a beruházásokra vonatkozó jogszabályokat;
- nemzeti és nemzetközi szabványokat, ajánlásokat;
- általános és speciális iratkezelésre vonatkozó irányelvek (levéltár)
- specifikus titokvédelmi szabályzások, rendeletek;
- stb.

Az ágazati, tárcaszintű végrehajtási utasításokban kerül meghatározásra:

- az államtitok köre;
- a szolgálati (hivatali) titok köre;
- az információfeldolgozási feladatok kiosztása;
- stb.

A negyedik szinten jelennek meg az adatvédelmi rendszer konkrét intézkedési elemei, mint az Informatikai Biztonsági Szabályzat. A szervezet belső rendjét előíró szabályozásoknak az alábbi területeken kell teljesen összhangban lenni a kialakítandó Informatikai Biztonsági Szabályzattal.

Az irányítás területéről:

- a szervezeti rend (Szervezeti és Működési Szabályzat);
- a szervezeti ügymenet rendje (Ügyrend);
- a munkavállalás rendje;
- a titkos ügykezelés rendje (TÜK);
- a külföldi kapcsolati rendszer szabályai
- a tömegkommunikációs kapcsolatokra vonatkozó előírások, stb.

A technikai területről:

- az ügyiratkezelés rendszere (Iratkezelési Szabályzat);
- a hírközlési eszközök használata;
- selejtezési, megsemmisítési eljárások;
- a sokszorosítás, kiadványozás előírásai;
- biztonságtechnikai házirend, rendészeti előírások;
- tárolási, szállítási előírások, stb.

Speciális területekről:

- tűzvédelmi szabályzat;
- munkavédelmi szabályzat;
- rendkívüli események intézkedési programjai, stb.

Informatikai Biztonsági Szabályzat

Az Informatikai Biztonsági Szabályzat egy olyan belső szervezeti intézkedés, amely a szervezeten belül működtetett informatikai rendszerekre vonatkozóan szabályozza az informatikai rendszerrel kapcsolatos biztonsági intézkedéseket, szervesen illeszkedve a szervezet egyéb működési és ügyrendi előírásaihoz. A korábbi szervezeti rendben ez a Számítástechnika Védelmi Szabályzat című előírásként szerepelt, amely a mai jogi viszonyok között sem megnevezésében, sem tartalmában már nem megfelelő. A számítástechnika megjelölés azért nem megfelelő, mert nem választja el az informatikai rendszereket a számítástechnikai eszközökkel támogatott automata rendszerektől, és egyéb vezérlő, irányító rendszerektől.

Az adatvédelem oldaláról megközelítve viszont jelen esetben csak az adatokkal, mint informatikai elemekkel foglalkozó rendszerek biztonságát kell megteremteni, ami a természeténél fogva számítástechnikai eszközök felhasználását is jelenti. A számítástechnika védelménél többről van szó, mert a számítástechnikai eszközök az informatikai rendszer részei, és azokhoz hozzátartozik az előző fejezetben megismert rendszerelem-csoport valamennyi eleme: az informatikai környezeti infrastruktúra, a számítástechnikai eszközök (hardver), az adathordozók, az informatikai rendszerhez tartozó iratok, a szoftverek, az alkalmazói adatok, a kommunikáció és az informatikai rendszert használó személyzet.
Az Informatikai Biztonsági Szabályzatban olyan intézkedéseket kell tenni, amelyek ezen rendszerelemekre korlátozódnak és az előírások lehetővé teszik az informatikai rendszerre irányuló veszélyek, veszélyforrások hatásainak elviselhető mértékűre való csökkentését.

Hálózati operációs rendszerek biztonsági minősítési problémái: A C2 követelményrendszer megvalósítása a NetWare 4.0 hálózatban

Várkonyi Béla, CNI és CNE,
E-mail: varkonyi@leila.mti.bme.hu
Rab Ildikó
E-mail: rab@leila.mti.bme.hu

BME Mérnöktovábbképző Intézet, Novell Oktatóközpont
1111 Bp. Egry J. u. 20-22.
1502 Bp. Pf. 91.

KIVONAT:

A NetWare utóbbi években kiadott verziói viszonylag megbízható védelmi funkciókkal rendelkeztek. Azonban eddig még nem kerültek hivatalos biztonsági minősítésre. Ugyanakkor az egyébként C2 minősítésű operációs rendszerek hálózati alkalmazása igen komoly biztonsági problémákat vet fel, s minősítésük az ilyen környezetekre nem érvényes. Az újonnan megjelent NetWare 4 azonban - a jelenleg elérhető hasonló termékek között - méltán pályázhat a legmegbízhatóbb hálózati operációs rendszer címére, s megkezdődött a hivatalos minősítéséhez szükséges bevizsgálása is.

A cikk megadja a kereskedelmi hálózati biztonság és a hálózati C2-es biztonsági követelményrendszer definícióját. Bemutatja a kritériumrendszer fontosabb kategóriáit, mint biztonsági politika, auditálási képesség, szavatosság, dokumentáltság.

A cikk ismerteti a Novell Globális Biztonsági Architektúráját, valamint a korábbi verziókhoz képest történt változásokat, bővítéseket. Kifejti, hogy a NetWare 4.0 miképpen felel meg a C2-es osztály legfontosabb követelményeinek.

A szerzők tippeket adnak a védelmi rendszer tökéletesítésére, mint pl. a szerver fizikai védelmének módozataira, vagy a munkaállomások biztonságának növelésére. Beszámolnak a NetWare 4.0 használatának eddigi gyakorlati tapasztalairól is. Végül ismertetik a továbbfejlesztés irányait, lehetőségeit.

1. Bevezetés

A Novell NetWare operációs rendszer a legelterjedtebb hálózati szoftver. Különösen nagy a piaci részaránya Kelet-Európában ill. Magyarországon. A helyi specialitásokból adódóan sokszor olyan informatikai rendszerek is erre a platformra kerülnek, amelyek máshol jellemzően a nagygépes világ speciális szolgáltatásaira építenek. Az egyik legkritikusabb problémája a vállalati, intézményi átfogó jellegű informatikai rendszereknek a biztonság.

A kezdeti Novell NetWare termékek igen kevés funkcióval támogatták a biztonságos hálózatok kialakítását. A 3.x verziók azonban már sok tekintetben megfeleltek a kereskedelmi igényeknek. A NetWare

4.0 verzió megjelenésével vált lehetővé az ennél is magasabb szintű biztonság elérése, amely már a nagyvállalati környezetben is vetélytársa lehet ezen a téren is a nagygépes rendszereknek.

2. A hálózati biztonság szintjei és a C2 követelményrendszer

A kereskedelmi hálózati biztonságnak két általános szintjét különböztetjük meg: a hétköznapit és a megbízhatót. A hétköznapi (vagy egyszerű) biztonság alig igényel többet, mint egy jelszót és egy azonosítót felhasználónként. Ez a szint azonban feltételezi, hogy a felhasználók mindig tisztességesen viselkednek, és egy profi betörő támadásának valószínűsége nagyon alacsony. A legtöbb hálózat biztosítja legalább ezt a minimális szintű információ védelmet.

A második szint a megbízható rendszereké, mellyek sokkal komolyabb védelmet nyújtanak a hétköznapi szintnél. A napjainkban hozzáférhető hálózati operációs rendszerek azonban valahol a két szint között helyezkednek el. A NetWare 4 az első olyan rendszer, mely képes megbízható rendszerré válni, és az első hálózati operációs rendszer, melyet C2-es minősítésre terjesztettek az NSCS (National Computer Security Center) és a közel azonos E2-esre az európai ITSEC elé. Itt meg kell jegyeznünk, hogy a C2-es osztályba sorolásnak két típusa van: a C2 Certification és a kevésbé szigorú C2 Evaluation (ld. pl. [5]-t). A NetWare 4-et az utóbbi vizsgálatnak vetették alá. (Az értékelés jelenleg - a cikk írása alatt - is folyik.)

A cikkben részletesen csak a C2-es osztály követelményrendszerével foglalkozunk.

2.1. A követelményrendszer osztályai

Az Egyesült államok védelmi minisztériuma 1985. decemberére dolgozta ki a TCSEC (Trusted Computer System Evaluation Criteria) követelményrendszert, azaz a Megbízható Számítógép Rendszerek Kiértékelési Kritériumát. Ez a szabvány csak egyedi számítógépekre volt alkalmazható. Azonban a hálózati változat kidolgozása sem váratott sokáig magára, már 1987. júliusában megjelent, mint a TCSEC interpretálása megbízható hálózatokra (Trusted Network Interpretation of the TCSEC).

A szabvány hét osztályba sorolja a hálózati operációs rendszereket. Ezek növekvő biztonság szerint a következők:

D	Minimális védelem
C1	Diszkrét biztonsági védelem
C2	Szabályozott hozzáférési védelem
B1	Cimkézett biztonsági védelem
B2	Struktúrált védelem
B3	Biztonsági területek
A1	Bizonyított tervezés

Ezek az osztályok mérőszámokat állítanak a következő hat követelményhez, mint védelmi politika, azonosítás, megjelölés (minden objektum fel van ruházva egy cimkével, mely a védelmi szintjét jelzi), könyvelés, szavatosság (hogy a rendszer mindig megfelel a specifikációnak) és a folyamatos védelem (a biztonsági célokat szolgáló hardver és szoftver mechanizmusok védelme az illegális változtatásoktól). (Részletesebb leírás a [2]-ben található.)

2.2. A C2-es osztály definíciója

A C2-es minősítés banki rendszereknél a minimálszint. Az általa állított kritérium alkalmas annak

megítélésére, hogy rendszerünk megfelel-e a megbízható szint követelményeinek. A kiértékelés által érintett négy kategória: védelmi politika, könyvelés, szavatosság és dokumentáltság. Ezek a kategóriák alapelvei és vezérfonalai egy megbízható rendszer konstuálásának. Hogy megértsük, a Novell miképpen építette fel nyitott biztonsági architektúráját, előbb vizsgáljuk meg közelebbről e négy alapelvet!

2.2.1. A védelmi politika

A védelmi politika két funkcionális területre oszlik: a diszkrét hozzáférési kontrollra és az ismételten használt objektumok problémájára.

A diszkrét hozzáférési kontroll annyit jelent, hogy különböző típusú felhasználókat különböző szintű hozzáférési jogokkal ruházunk fel, attól függően, hogy mi az a minimális metszete a rendszernek, melyre a felhasználónak szüksége van. A hálózat szigorúan betartja e rendelkezéseket. A felhasználók a gyakorlatban lehetnek egyének, csoportok, erőforrások vagy processzek.

A védelmi politika másik aspektusa az objektumok ismételt használata. Ez annyit jelent, hogy minden, az objektumhoz tartozó engedélyt vissza kell vonnunk, mielőtt az objektumot újra kiosztanánk. Tipikus példa erre a hálózat és hoszt közötti kapcsolat megosztása. Ha egy felhasználó kijelentkezik a hálózatról, akkor a privilégiumait teljesen törölnünk kell, mielőtt egy másik személy használná a kapcsolatot. Ha ez nem történik meg, akkor a második felhasználó örökölheti az első jogait, annak ellenére, hogy az már kijelentkezett a hálózatról.

2.2.2. Könyvelés

A könyvelésnek szintén két aspektusa van: az azonosítás és hitelesítés, valamint a naplózás.

A felhasználónak azonosítania kell magát, mielőtt a rendszer hozzáférést engedélyez a számára. A hozzáférés elnyerése előtt azonban az azonosítást a rendszernek hitelesítenie kell. Mindig komoly problémát jelentett, hogy milyen messzire menjünk el a hitelesítés megbízhatóságában. Minimálisan egy jelszó azonosít egy felhasználót. Azonban a jelszavak soha nem biztosíthatnak teljes hitelt, hiszen a felhasználók megoszthatják egymással őket, vagy a túl egyszerű jelszavak felderíthetőek találgatási stratégiák segítségével. Megoldás lehet tokenek, mágneskártyák használata, vagy az egyedi fizikai karakterisztikák vizsgálata, mint pl. ujjlenyomat, hang, vagy retina.

Fontos szempont, hogy miután a felhasználó hitelt nyert, a rendszer szigorúan betartassa a hozzáférési jogokat, és védje a biztonság szempontjából érzékeny objektumokat.

A másik idetartozó funkció az auditálás. A C2-es minősítésű rendszer képes a naplók kreálására, karbantartására, valamint a módosítás és illetéktelen hozzáférés elleni védelemre. A rendszerben kell lennie tehát egy naplózott eseményeket tartalmazó állománynak, melyhez csak privilegizált felhasználó férhet, és nem törölhető vagy rongálható bárki által a hálózaton.

2.2.3. Szavatosság

A szavatosság három részterületre oszlik, mint rendszer arhitektúra, rendszer integritás és biztonsági tesztelés.

A rendszer architektúra annyit jelent, hogy a rendszernek meg kell védenie sajátmagát, azaz az operációs rendszer állományait és erőforrásait a külső támadások ellen.

A rendszer integritás azokra a funkciókra vonatkozik, melyek alkalmasak a rendszer korrekt működésének tesztelésére és érvényesítésére biztonsági szemszögből.

A biztonsági tesztelés ellenőrzési lehetőséget biztosít annak érdekében, hogy a rendszer folyamatosan

megfeleljen a publikált specifikációnak.

2.2.4. Dokumentáltság

A dokumentáltság négy fő területe: a biztonsági funkciók felhasználói leírása, a megbízható eszközök kézikönyve, a teszt dokumentáció valamint a tervezési dokumentáció.

2.2.5. A kiértékelés egyéb kritériumai

A hálózatok elosztott rendszerek. Ez az elosztottság mind hardverben, mind szoftverben megnyilvánul. A megbízható rendszerek szempontjából talán az utóbbi a fontosabb.

Egy egyedülálló számítógép védelme a hálózatokéval szemben sokkal egyszerűbb feladat, hiszen a számítások egyetlen processzoron hajtódnak végre. De a számítási műveletek szétosztása több tucatnyi - vagy akár több száz - gépre, jelentősen megnehezíti az erőforrások védelmét. Csupán a szerver és a munkaállomások védelme nem elegendő: magát a hálózati rendszert kell védenünk. Az erőforrások mellett tehát az összeköttetéseknek is figyelmet kell szentelnünk. Az operációs rendszernek biztosítania kell egy olyan eljárást, mely lehetővé teszi a hálózati elemek összefűzését egy megbízható rendszerré (DOS esetén ez különös kihívást jelent). (Részletesebb leírás [1]-ben található.)

3. A NetWare operációs rendszer biztonsága és védelme

A Novell felismerte, hogy megnőtt a kereskedelmi igény egy olyan hálózati operációs rendszerre, melyet könnyű implementálni, nagyra méretezhető, kiváló teljesítményre képes, valamint erőteljes kontroll eszközökkel rendelkezik egy elosztott környezetben. E szempontokat igyekezett szigorúan szem előtt tartani a NetWare 4 fejlesztésénél. (A NetWare 3 biztonsági elemzését lásd pl. a [4]-ben.)

A NetWare 4 kiterjesztett biztonságával és auditáló funkcióival erős védelmi vonalat biztosít a betörési kísérletekkel szemben ugyanúgy, mint az apró napi hibákkal kapcsolatban. A rendszer nagyvállalati szinten menedzselhető. Azonban a megbízható hálózat kiépítéséhez szükség van mind a tervezők, mind az adminisztrátorok, mind a felhasználók aktív közreműködésére a lokális és globális szinten egyaránt.

A Netware 4 rugalmas, többszintű biztonságot kínál, mely kontrollálja a hozzáférést a hálózathoz és annak erőforrásaihoz. Az idetartozó funkciók, melyek a C és B osztályok számos elvárásának megfelelnek, az NDS (NetWare Directory Service) ill. a file rendszer erőforrás menedzsment részei. Ezek az eszközök a hálózat, a hozzáférések, a bejelentkezések, a jogok, az attribútumok, a file szerver, valamint az információk védelmét kontrollálják. Segítségükkel a rendszer adminisztrátor az NDS, a hálózat, a szerver vagy a file rendszer szintjén meghatározhatja, hogy:

- kinek biztosít hozzáférést a hálózathoz,
- milyen erőforrásokat vehetnek igénybe a felhasználók,
- miképpen használhatják az erőforrásokat a felhasználók,
- ki hajthat végre feladatokat a szerver konzolnál.

E feladatok végrehajtásához a NetWare a következő funkciókat biztosítja:

- felhasználó azonosítás az egyéni, csoport, valamint a menedzsment szinten,
- felhasználó hitelesítés (szolgálat kérés orientált),
- jelszó menedzsment (beleértve a jelszó kódolást),
- hálózati erőforrásokhoz való hozzáférés a jogok és attribútumok alapján,

• konzol biztonság (csak a megfelelő biztonsági ekvivalensek férhessenek a szerver konzolhoz.

3.1. NetWare specifikus biztonsági problémák

A továbbiakban felsoroljuk azokat a problémákat, melyekkel a hálózati menedzsmentnek a leggyakrabban kell szembenéznie a NetWare operációs rendszer használata esetén.

3.1.1. A szerver pozíciója

A hálózati adminisztrátoroknak biztosítaniuk kell, hogy a NetWare szerverekhez ne férhessen hozzá illetéktelen felhasználó. Ezért célszerű őket egy zárható helységben tartani, és nyílvántartani, hogy ki férhet hozzá a kulcshoz. A szerver konzolról ugyanis a védelmi rendszer kikapcsolható ill. kikerülhető. A konzol valamennyi operációs rendszernél lehetővé tesz hasonló funkciókat, ami bizonyos esetekben elengedhetetlenül szükséges is. A NetWare-nél azonban alapesetben különösen egyszerű ezen funkciók aktivizálása, bár léteznek eszközök a lehetőségek korlátozására.

3.1.2. NLM támadások

Számos NLM (Network Loadable Modul) ismert, melyek segítségével az ADMIN jelszó lecserélhető a régi ismerete nélkül. Ezek az NLM hívások a SetBinderyObjectPassword funkciót használják, mely teljesen dokumentált a NetWare szerver alkalmazói program interfészben. Mivel az NLM-ek az operációs rendszer kiterjesztései, használhatják a rendszerhívásokat. A hálózati adminisztrátornak tisztában kell lennie a hálózaton futó NLM-ek természetével és funkciójával.

3.1.3. A Login procedúra

A hálózatok egyik legkényesebb pontja a bejelentkezési folyamat. Felsoroljuk a leggyakoribb támadásokat és problémákat.

3.1.3.1. Trójai faló

Trójai falónak nevezzük azt a programot, amely külsőre egy hasznos program alakját ölti magára, valójában azonban a biztonsági rendszert kompromittálja. Példa erre egy olyan program, mely látszólag úgy működik, mint a login program, de emellett a felhasználó által begépelt jelszót egy titkos naplóba irányítja.

3.1.3.2. Hálózati analizátor

A hálózati forgalom figyelésével egy hálózati analizátor begyűjtheti a bejelentkezési kérelmet továbbító csomagokat, melyekből a jelszavak kinyerhetők (részletesebben ld. pl. a [3]-ban). Ez a passzív támadás azonban egyszerűen kivédhető kódolt jelszavak használatával.

3.1.3.3. Támadás szótár segítségével

A támadó program egy szótár szavait, mint lehetséges jelszavakat próbálgatva kísérel meg bejelentkezni a hálózatra. Egy ilyen szótár tetszőlegesen bő lehet. Tartalmazhatja a teljes anyanyelvet, idegen nyelveket, szlengeket, közkedvelt dolgokat, ezeket kombinálhatja a felhasználók neveivel stb... Az ilyen típusú támadás könnyedén kivédhető olyan "nehéz" jelszavak választásával, melyek nem szerepelnek egyetlen szótárban sem (pl. betűk, szimbólumok és számok keverése). Védekezhetünk a betörés detektáló funkcióval is (intruder

lockout), mely bizonyos számú sikertelen belépési kísérlet után meghatározott időre letiltja a témaszámot.

3.1.3.5. Kimerítő kereséses támadás

Kimerítő keresésnek nevezzük azt a támadást, amikor a támadó minden lehetséges jelszóval próbálkozik, tehát minden elképzelhető billentyű kombinációt végigzongorázik. Ez az eljárás csak rövid jelszavak esetében vezethet eredményre, hiszen a hossz növelésével a lehetséges kombinációk száma exponenciálisan növekszik. Ajánlott védekezési módszer a megfelelő jelszó menedzsment (egy minimális jelszóhossz megkövetelése, maximum 30-40 napos jelszó változtatási periódus, egyedi jelszó stb...) és a betörés detektáló funkció bekapcsolása.

3.1.3.6. Algoritmus támadás

Támadási felületet jelentenek a jelszó kódoló eljárások gyenge pontjai is. A NetWare 2.2-t és 3.11-et megelőző verziókban a kódoló algoritmus rendelkezett egy ilyen hibával. Ha a szerver által küldött (véletlenszerűen választott) kulcs egy palindróm volt, akkor a kódoló eljárás kimenete csupa nullát eredményezett. Az algoritmusnak ezt a gyengeségét használta ki a KNOCK.EXE nevezetű program, méghozzá úgy, hogy folyamatosan próbált belépni a szerverre jelszó megadása nélkül. Ez átlagosan 10.000 alkalmanként egyszer sikerült is (ez volt kb. egy palindróm előfordulási valószínűsége).

3.1.3.7. Hamisított csomagok

A hamisított csomagok nem csak a NetWare, hanem minden hálózat számára komoly problémát jelentenek. A holland eredetű HACK.EXE program egy NCP (NetWare Core Protocol) kérést tartalmazó csomagot juttatott be egy nyitott, privilegizált kapcsolatba, azzal a céllal, hogy jogokat szerezzen a betörő számára. A Novell első lépésként az NCP csomagokat digitális szignatúrával látta el, megakadályozva ezáltal a hamis csomagok közbeiktatását. A második lépés a teljes NCP csomag kódolása lehet.

3.1.3.8. Print szerver támadás

Igen fontos, de sokszor figyelmen kívül hagyott támadási felületet jelentenek a print szerverek. Egy ilyen szerver ugyanis azon a biztonsági szinten hajtja végre a processzeit, mint amilyennel a kiszolgálandó feladat (job) tulajdonosa rendelkezik. Ha valaki egy print szervert megfelelően preparál a hálózaton, akkor nem kell másra várnia, csak egy olyan job-ra, mely az ADMIN felhasználótól érkezik. Ezután tetszőleges funkciót végrehajthathat a supervisor-i szinten.

Az effektív védelem érdekében nem árt gondoskodni arról, hogy minden print szerver használjon jelszót. Hasznos még a komkurens kapcsolatok limitálása, vagy az állomás cím és az idő korlátozások megadása. Érdemes a print szervereket a file szerverekkel együtt zárt szobában tartani.

3.1.3.9. Login script támadás

Potenciális veszélyt jelent az is, ha egy privilegizált felhasználónak nincsen login scriptje (az egyéni bejelentkezési parancsfájl). A login script a felhasználó mail könyvtárában tárolódik, azaz a levelezéshez használt alkönyvtárban, ahová alapértelmezés szerint bárkinek, aki a hálózatra belépett van fájl kreálási joga. Ez annyit jelent, hogy létrehozhat egy új fájlt, és írhatja is addig, amíg le nem zárta. Bár többszöri megnyitásra nem jogosít fel a "create" jog, ez éppen elegendő ahhoz, hogy a támadó az általa készített programocskát becsempéssze egy újonnan létrehozott login nevezetű fájlba. Miután a felhasználó bejelentkezik, a program az ő privilégium szintjén fog lefutni.

Védekezési lehetőségek:

• Gondoskodjunk arról, hogy minden felhasználónak legyen login script-je!
• Biztosítsuk, hogy minden felhasználó kilép a rendszer login scriptből! (Ez az EXIT paranccsal történik, ekkor az egyedi login scriptek nem hajtódnak végre.)
• Távolítsuk el a MAIL könyvtárhoz rendelt publikus jogokat!

3.2. A NetWare 4 védelmi rendszere

A NetWare 4 biztonsági rendszere a korábbi verziókhoz képest két szintre bomlott: a fájl rendszer védelem és a NetWare Directory Services (a későbbiekben mint NDS fogunk hivatkozni rá).

3.2.1. A NetWare Könyvtár Szolgáltatás (NDS)

A biztonsági rendszerrel kapcsolatos információk az NDS nevezetű nevezetű hierarchikus, azaz fastruktúrájú elosztott adatbázisban tárolódnak. Az adatbázis a teljes nagyvállalatot felöleli, ellentétben a korábbi verziókban szereplő Bindery-vel, mely csak egyetlen szerverre vonatkozó információkat tárolt. Az NDS szolgál az objektumok (felhasználó, szerver stb.) és az objektumokhoz rendelt tulajdonságok menedzselésére. Az NDS biztonsági funkciói hasonlóak azokhoz a supervisori funkciókhoz, melyek a korábbi verziókban nem a fájl rendszerrel voltak kapcsolatosak. Példa erre a felhasználók létrehozása, a login script-ek editálása, nyomtatók és print szerverek kreálása. Ide tartozik még az NDS objektumokra és azok tulajdonságaira vonatkozó jogok adása is.

3.2.2. A fájl rendszer védelem

A számos köteten elhelyezkedő fájlok és könyvtárak biztonságával a fájl rendszer erőforrás menedzsment foglalkozik. Kontrollálja az alkalmazói programokat és adatállományaikat. A NetWare 4 fájl rendszer biztonsági rendszere lényegében ugyanaz, mint a 3.1x verzióban. Néhány kiegészítő attribútum került bevezetésre az új adatösszehasonlítási technikák és az (új szerverre) költöztető eljárás miatt, egy pár terminológia megváltozott, de a funkció ugyanaz maradt: szabályozott hozzáférést biztosítani a felhasználóknak a könyvtárakhoz és az állományokhoz.

A NetWare 4-ben már nincs szükség abszolút felhasználóra, aki korlátlan jogokkal rendelkezik az egész hálózaton. A korábbi verziókkal ellentétben lehetőség van a hagyományos SUPERVISOR témaszámot szétosztani a hálózat különböző felhasználói között. A NetWare 4-ben az alapértelmezés szerint az ADMIN témaszám az, amely inicializáláskor minden jogot megkap. Ezt a feladatkört azonban érdemes tagolni az NDS menedzsment és a fájl rendszer jogok körére, hiszen a két terület teljesen elkülönül. Sőt, nagy hálózat esetén érdemes a részfákat még több adminisztrátor között szétosztani, hiszen egy-egy ilyen részfa más-más városokban lévő szervezeteket ölelhet fel.

4. A NetWare 4 és a C2-es osztály követelményei

A NetWare 4 információ védelmének kulcsa a Globális Biztonsági Architektúra. Ez egy olyan nyitott biztonsági rendszer, mely jelentős szerver alapú védelmet biztosít, és lehetővé teszi a biztonsági eszközöket fejlesztő kívülállók számára, hogy terméküket szorosan a rendszerbe integrálják.

A következő részben bemutatjuk, hogy a Globális Biztonsági Architektúra miképpen kezeli a C2-es modell öt legfontosabb aspektusát.

4.1. Azonosítás és hitelesítés

Az azonosítás és a hitelesítés a bejelentkezési procedúrával kezdődik. Mivel a jelszóval történő azonosítás a hálózati rendszerek gyenge pontja, a jövő API-jei (Application Programing Interface) lehetővé fogják tenni tokenek (pl. mágneskártyák) használatát.

Amikor a felhasználó elsőként fordul egy erőforráshoz, akkor a hitelesítő eljárás feladata igazolni, hogy a felhasználó valóban az, mint akinek mondja magát. A hitelesítést a Novell az RSA nyilvános kulcsú kriptográfia felhasználásával implementálta. A procedúra két lépésben valósul meg, ezek a kezdeti és a háttérbeli hitelesítés.

4.1.1. Kezdeti hitelesítés

Amikor a felhasználó elindítja a bejelentkezési procedúrát, a kliens szoftver hitelesítést kér a hálózattól. A NetWare visszaküld egy kódolt privát jelszót, mely a felhasználó sajátja (a felhasználó felvételénél hozta létre a hálózat). A jelszó dekódolja a privát kulcsot. Miután ez megtörtént, a jelszó törlődik a memóriából. Ez fokozza a hálózati biztonságot, hiszen a jelszó sosem hagyja el a munkaállomást. A felhasználó azonosítójából, az állomás címéből és a kapcsolat számából létrejön egy egyedi azonosító, melyet a továbbiakban hitelesítőnek hívunk. A kliens szoftver kreál egy digitális szignatúrát a hitelesítő és a privát kulcs felhasználásával. Ezután a privát kulcs is törlődik a memóriából, hogy ezentúl a hitelesítő és az aláírás igazolja a felhasználót. A szerver ellenőrzi a bizonyítékot, majd küld egy üzenetet az elfogadás tényéről.

4.1.2. Háttérben zajló hitelesítés

A hitelesítés a háttérben folyamatosan zajlik tovább, amint a felhasználó hálózati szolgáltatást igényel. A kérés, mely továbbítódik a hitelesítő szolgálathoz, tartalmazza az üzenetet, a hitelesítőt és egy bizonyítékot. A bizonyíték az üzenet és az aláírás kódolásából tevődik össze. A digitális aláírás nem hagyja el a munkaállomást.

A hitelesítő eljárás olyan hálózati szolgáltatás, mely teljesen áttetsző a felhasználó számára. A kapcsolat-orientált procedúra lehet folytonos és kölcsönös.

Az NDS-nek köszönhetően nincs többé szükség arra, hogy a felhasználó minden szerverre egyenként bejelentkezzen, melyet használni kíván. A kódolt hitelesítő lehetővé teszi minden olyan erőforrás elérését, melyhez a felhasználónak joga van. Tehát a NetWare nagyvállalati rendszerén belül a felhasználók már egyszeri azonosítás után elfogadást nyerhetnek a teljes hálózaton.

Ha a felhasználó egy 3-as főverziójú, vagy korábbi NetWare szerverre kíván bejelentkezni, akkor szükség van a login procedúra újraindítására, hiszen ezek a szerverek lokális adatbázissal rendelkeznek (Bindery), nem pedig elosztottal, mint a hierarchikus fába szervezett NDS.

4.2. Diszkrét hozzáférési kontroll

A diszkrét hozzáférési kontroll a Novell Globális Biztonsági Architektúrájában az operációs rendszeren keresztül valósul meg. Ha a felhasználó használni kíván egy objektumot, akkor a hálózat ellenőrzi a hozzáférési jogokat, melyek a felhasználó kezelői (trustee) jogain alapulnak. A NetWare 4 a fájlokon és könyvtárakon kívül a hálózat számos egyéb elemét tekinti objektumoknak, mint pl. print szerver, printer, csoport, kötet, felhasználó, konténer stb.

A diszkrét hozzáférési kontroll azon alapszik, hogy egy felhasználót csak azokkal a jogokkal szabad felruházni, melyekre feltétlenül szüksége van. A NetWare 4 a hozzáférési jogoknak széles skáláját kínálja. Az

általános, több felhasználó által igényelt jogok megadására is lehetőség van, ha a jogok szűrésével és a hozzáférések kontrollálásával csoport szinten kombinálunk. Ha a jogokat egy csoport objektumhoz rendeljük, akkor a csoport minden tagja rendelkezni fog azokkal.

A különböző hozzáférési jogok négy csoportba oszthatók: a fájlokhoz és könyvtárakhoz rendelt jogok (fájl rendszer biztonság), valamint az objektumokhoz és az objektumok tulajdonságaihoz rendelt jogok (NDS). Minden objektumnak van egy kötelező tulajdonsága (property), az elérési kontroll lista. Ez a lista tartalmazza, hogy ki és miképpen férhet hozzá az objektumhoz. (A jövőbeli használhatóság érdekében a listát úgy tervezték, hogy ne csak NetWare objektumokat tartalmazhasson.) A NetWare 4 nagyvállalat szerte érvényes listákat használ, szemben a korábbi verziókkal, melyek a Bindery-t használták erre a célra. A Bindery nem alkalmas a nagyvállalaton belüli menedzselésre, hiszen az NDS-sel szemben nem elosztott adatbázis, és a különböző szerverek Bindery-jei között nincs semmi kapcsolat. A NetWare 4 hozzáférési kontroll listái viszont a teljes hálózaton belül elérhetők az NDS-nek köszönhetően. Ez az elosztottság kényelmes átlátszóságot biztosít, azaz a felhasználó a hálózat bármely objektumához hozzáférhet anélkül, hogy tudnia kéne, hol helyezkedik el az pontosan.

4.3. Naplózás

Az auditálási funkció mindig gyenge pontja volt a PC alapú LAN-oknak (ld. pl [4]-t a NetWare 3 lehetőségeinek elemzésére). A NetWare 4 AUDITCON utility-je viszont egy robusztus naplózási metódust biztosít.

4.3.1. Auditorok

Az első lépés a megfelelő személyek kiválasztása az auditori szerepkörre. Az auditorok száma természetesen a nagyvállalat és a szervezetek méretétől függ, hiszen a hálózat akár több várost is összeköthet. Érdemes minden kötethez kijelölni egy auditort, leszámítva azt az esetet, amikor erősen centralizált biztonsági adminisztrációra van szükség. A Novell igyekezett az auditálás módját a pénzügyi gyakorlatban bevett eljáráshoz közelíteni.

A biztonsági adminisztrátorok és auditorok legyenek olyan személyek, akiknek nincsen privilegizált státuszuk, vagy különös érdekeltségük a rendszer működésében. Nem szabad, hogy felelősek legyenek a hálózatnak azért a területéért, melyeknek ők látják el a "könyvvizsgálói" funkcióit.

4.3.2. Az auditálás szintjei

Az auditálás két szinten történik: az NDS-re épülő konténer (ez egy részfát jelent a hierarchikus struktúrában), ill. a fájl rendszerbeli kötet szintjén. Mindkét típusnál használható jelszó, melyet csak az auditor ismer.

4.3.2.1. Auditálás az NDS konténer szinten

Naplózhatunk események vagy felhasználók szerint. Egy rekord keletkezik a naplófájlban, ha a kiválasztott esemény bekövetkezik az adott konténeren belül, vagy ha a kiválasztott felhasználó egy naplózandó akciót hajt végre.

4.3.2.2. Auditálás kötet szinten

Naplózhatunk események, fájlok és könyvtárak, valamint felhasználók és ezek tetszőleges kombinációja

szerint.

Az események szerinti naplózásnál választhatunk a fájl/könyvtár, a nyomtatási sorok, a szerver és a felhasználói események közül. Auditálható pl. az az esemény, amikor egy bizonyos érzékeny rendszerfájlon egy kijelölt vagy bármely felhasználó egy bizonyos vagy bármilyen műveletet hajt végre (pl. törlés, olvasás, írás).

A másik két naplózási típusnál ugyanezeket a kombinációkat állíthatjuk elő, csak ott a többi szempontot részesíthetjük előnyben, ezzel megkönnyítve a navigálást a kombinációk összeállításában.

4.3.4. Auditálási riport

A naplófájlok általában nagyon nagyok, és ezért áttekinthetetlenek. Sok fölösleges információt szolgáltatnak egy adott, jól meghatározott célú vizsgálat szempontjából. Ezért lehetőség van szűrési feltételek megadására az auditálási riport készítésekor.

Szűrési feltételként megadhatunk egy időintervallumot vagy bizonyos típusú eseményeket. Kiemelhetünk felhasználói, fájl vagy könyvtár neveket azzal a céllal, hogy csak a megadott neveket, vagy éppen ellenkezőleg az összes többit tartalmazza az auditálási riport.

A szűrési feltételeket tetszőlegesen kombinálhatjuk, és el is menthetjük. Így bármikor alkalmazhatjuk a korábban definiált feltétellistát, anélkül, hogy újra kéne szerkesztenünk azt.

4.3.5. Naplófájlok karbantartása

Mivel a naplófájlok idővel kolosszális méretet ölthetnek, az auditornak gondoskodnia kell arról, hogy nehogy beteljen valamelyik kötet a napló állandó növekedése miatt. Megadható a napló méretének felső korlátja. Ha a fájl eléri ezt a méretet, akkor két dolog történhet a NetWare 4.01-ben: leáll a rendszer, vagy leáll az auditáló processz. Célszerű az utóbbit választani. Lehetőség van arra, hogy a hálózat riassza az auditort, ha a napló mérete megközelítené a megadott határt. Ekkor az auditornak módja van időben archiválni a naplófájlt.

Az auditáló processz flag-eket, ill. attribútumokat illeszt minden naplózandó fájlhoz, könyvtárhoz vagy NDS objektumhoz. Ezek az attribútumok láthatatlanok az AUDITCON kivételével minden felhasználó, ill. applikáció számára. Csak speciális, kódolt NCP hívásokon keresztül változtathatók.

4.4. Objektum újrahasználat

Az objektumok újrahasználata kulcskérdése minden szerver alapú rendszernek. A Globális Biztonsági Architektúra két területen foglalkozik a problémával: a memóriát és a háttértárolót illetően.

Ha egy felhasználó kijelentkezik a hálózatról, akkor az általa használt memóriát törölni kell, mielőtt egy másik felhasználó allokálná. Ugyanezt a módszert kell alkalmazni a háttértároló esetén is. Utóbbival azonban óvatosan kell bánni, mert egy file hagyományos törlése nem elegendő, az adatok könnyűszerrel visszaállíthatóak.

A NetWare 4 nem foglal memóriát a szerveren a felhasználók számára. Mivel a kliens alkalmazások nem a szerveren futnak, a szerver cache memóriáját a hatékonyság növelése érdekében a szerver és a kliens közötti adat és program mozgatására használják.

A NetWare 4 a cache blokkokat kétféleképpen kezeli. Az első esetben az egyes blokkok kérésre dinamikusan allokálódnak. Ha egy blokk felszabadul, visszakerül a kiosztható blokkok listájára. Tartalma a következő allokálásnál felülíródik. A második kezelési mód esetén az operációs rendszer felülírja nullákkal a cache blokkot abban az esetben, ha az újraallokálásnál a felülírás nem lenne teljes. Így a megelőző használat minden nyoma törlődik.

Bár kliens alkalmazások nem, NLM-ek azonban futnak a szerveren. A NetWare operációs rendszer azonosítás, hozzáférési jogok és objektum újrahasználat szempontjából ugyanúgy kezeli az NLM-eket, mint bármely más, a rendszer által menedzselt objektumot.

4.5. Szavatosság és önvédelem

A szavatosság és önvédelem kulcs aspektusai a Globális Biztonsági Architektúrának. A NetWare 4 számos segédeszközt nyújt a rendszer kulcsfontosságú részeinek védelméhez. A betörések megakadályozásának szempontjából a legfontosabb egy kódolt kapcsolat azonosító, mely megakadályozza a felhasználói kapcsolatok hamisítását. Ehhez hasonló funkciót töltenek be az egyedi csomag azonosítók is.

Supervisori jogot csak felhasználók és munkaállomások birtokolhatnak. Processzek soha nem rendelkezhetnek vele. Ez kizárja azt a lehetőséget, hogy egy betörő olyan programot készít, mely supervisori jogokkal elérheti a hozzáférési kontroll listákat (ACL) vagy más, a biztonság szempontjából kritikus objektumokat.

Az audit programok feladata információk gyűjtése és karbantartása, melyek analizálásával detektálhatók a potenciális vagy aktuális sérülések a rendszer biztonsági politikájában. Az audit procedúrák a következő stratégiai területekre oszthatók:

- platform definíció (használt hardver és szoftver, NDS szerkezet, kommunikáció)
- technológia szabályozás (szerver pozíciója, munkaállomás operációs rendszere)
- NetWare operációs rendszer (hálózati környezet, opciók és alapértelmezések)
- rendszer hozzáférés (pl. jelszó és témaszám menedzsment)
- rendszer operációk, karbantartás, vészhelyzetkezelés
- erőforrás kihasználtság
- backup, visszaállítás

Mindezen funkciók helyes használata megteremti a lehetőségét egy C2-es biztonsági szintű hálózat kialakításának.

5. Tanácsok a biztonság növeléséhez

5.1. Adminisztrátori témaszámok menedzselése

Az adminisztratív, privilegizált témaszámok ismeretét korlátozzuk maximum két vagy három megbízható hálózati adminisztrátorra. Egy személy nem elegendő az esetleges rendkívüli helyzetek előfordulása miatt. Az adminisztrátori funkciókat célszerű egy Admin-ekvivalens témaszámon végrehajtani, melynek a neve nem árulkodó. (A SUPERVISOR vagy a ROOT elnevezés szinte mindenki számára nyilvánvaló.)

5.2. Felhasználói témaszámok menedzselése

A témaszámok megfelelő menedzsmentje fontos részét képezi a hálózat biztonságának. A frissen felvett felhasználóknak soha ne adjunk több jogot, mint amennyire feltétlenül szükségük van!

Ha egy felhasználó hosszabb időre, vagy véglegesen távozik a társaságról, azonnal töröljük, vagy tiltsuk le a témaszámát!

A felhasználókkal meg kell értetni a jelszavak fontosságát és azok megfelelő használatának módját.

A jelszó feleljen meg a következő kritériumoknak:

- Hossza legyen minimum 8 karakter!
- Legyen egyedi, és mások által könnyedén nem kitalálható!
- Tartalmazzon legalább egy, betűtől különböző karaktert!
- Ne tárolják, vagy jegyezzék fel sehová! (Pl. noteszbe, munkaállomásra, a billentyűzet aljára stb.)

5.3. Jelszó kódolás

A NetWare-nek van egy funkciója, mely a jelszó kódolás használatát szabályozza. Egy paranccsal engedélyezhető kódolatlan jelszavak használata is. Erre akkor lehet szükség, ha a hálózaton található a NetWare 3.0-ás verziójánál régebbi szerver. A korábbi verziókban ugyanis a jelszavak kódolatlanul továbbítódtak a hálózaton. Ezért tanácsos a NetWare 3.1x utility-ket átmásolni ezekhez a szerverekhez. Ha ezt nem tesszük meg, akkor ne engedélyezzük a kódolatlan jelszavak használatát! (SET ALLOW UNENCRYPTED PASSWORDS = OFF) Ebben az esetben néhány felhasználónak problémája lesz a bejelentkezéssel, de ez még mindig jobb, mint a hálózati csomagokból kiolvasható jelszavak.

5.4. SECURE CONSOLE utility

E utility segítségével elérhetjük, hogy a rendszerben futó NLM-ek kizárólag a SYS:SYSTEM könyvtárból legyenek a szerver memóriájába tölthetők, valamint, hogy a rendszer órája csak a konzol operátor által legyen változtatható. (Több védelmi funkció helyes működése múlik az utóbbin.)

5.5. XCONSOLE.NLM

Ha nem feltétlenül szükséges, akkor kerüljük az XCONSOLE.NLM használatát! A probléma, hogy terminál emulátoros protokollon alapul, emiatt a használt jelszó kódolatlanul, karakterenként továbbítódik a hálózaton (ld. részletesen [3]-t).

5.6. Kijelentkezés a hálózatról

Szoktassuk hozzá felhasználóinkat ahhoz, hogy mindig lépjenek ki a hálózatról, mielőtt otthagynák a munkaállomást, ahol dolgoztak. Ha ezt az állapotot szeretnénk automatikusan biztosítani, akkor érdemes készíteni egy olyan biztonsági utility-t, mely egy bizonyos inaktív periódus letelte után zárolja a kapcsolatot a munkaállomással.

5.8. Kliens biztonság

A NetWare 4 szerver-alapú védelmet biztosít a hálózat számára, azonban addig nem beszélhetünk teljes biztonságról, amíg a munkaállomások megfelelő védelme megoldatlan probléma. Hiába védjük a rendszert minden eszközzel, ha a kliens számítógépekhez akárki hozzáférhet. Elegendő egy rosszindulatú, rezidens programot elhelyezni valamelyik gépen, amely például begyűjtheti a lokálisan begépelt jelszavakat. Az egyik megoldás, hogy a munkaállomásokat is védett helyen tartsuk, a másik pedig megfelelő kliens szoftverek fejlesztése.

6. Összefoglalás

A Novell megteremtette az alapját egy biztonságos, jól menedzselhető nagyvállalati hálózatnak. A Globális Biztonsági Architektúrának, valamint a kívülállók által tervezett védlemi termékek integrálási lehetőségének kombinációja lehetővé teszi a C2-es biztonsági szint elérését. Ennek érdekében azonban szakértelemre, megfelelő implementálásra és menedzsmentre van szükség, mely biztosítani képes a felhasználók számára egy megfelelően védett információs infrastruktúrát.

A NetWare 4 fejlesztés alatt álló új verziói jelenlegi információink szerint nem a biztonsági szolgáltatások továbbfejlesztésére helyezik a hangsúlyt. A NetWare 4 megismerése a profi fejlesztőknek is komoly munkát jelent. 1995-ben azonban várhatóan megjelennek harmadik cégek olyan termékei, amelyek tovább növelik a biztonság rendszer lehetőségeit. Ez a folyamat a NetWare 3 esetén is éveket vett igénybe. Információink szerint többen foglalkoznak a B1 ill. a B2 kritériumoknak megfelelő kiegészítések tervezésével. A Novell hosszabb távon a NetWare és a UnixWare teljes integrálását tervezi, ami a biztonsági problémák (jelenleg még igazán fel sem mérhető) széles körét fogja felvetni.

A BME Mérnöktovábbképző Intézetében 1994 januárjától használjuk üzemszerűen a NetWare 4 operációs rendszert. Az eddigi tapasztalatok szerint a nyitott és veszélyes egyetemi környezetben is megbízható védelmet nyújt, de csak akkor, ha átgondolt ügyviteli és fizikai védelem is alkalmazásra kerül. Ezen a téren vannak még a legnagyobb hiányosságok. Komolyabb betörési kísérletről eddig még nincsen tudomásunk.

A BME MTI új tanfolyamok bevezetésével is szolgálni kívánja az ismeretek jobb elterjedését, a megfelelő gyakorlat kialakulását.

Köszönetnyilvánítás

A BME Mérnöktovábbképző Intézetének Novell Oktatóközpontja nagy mértékben segített a megfelelő eszközök és információk rendelkezésre bocsátásával. Külön köszönet ezért Bakonyi Tamásnak az Oktatóközpont vezetőjének.

Irodalomjegyzék

[1] Peter Stephenson: "C-2 security and NetWare's Global Security Arcitecture", CNEPA Network News, Feb. 1994.

[2] Building and Auditing a Trusted Network Environment with NetWare 4, Novell Application Notes, Apr. 1994.

[3] Várkonyi Béla, Nagy Gábor: "Terminálemulátor protokollok biztonsági problémái és kezelésük", Networkshop '94, Keszthely, NJSZT-IIF, Budapest, 1994.

[4] Várkonyi Béla, Rab Ildikó: "Operációs rendszer naplózások elemzése biztonsági szempontok szerint", Networkshop '94, Keszthely, NJSZT-IIF, Budapest, 1994.

[5] Carl Allen: "NetWare Security in a Trusted Computing Environment", BrainShare '94, European Edition, Novell Inc., Provo, Utah, USA, 1994.

SECURE

Dr. h. c. K.-P. Timmann

1) *New developments and guidelines for data and message security in civil computer systems are presented.*

2) *Proposals for integration of these developments into new military cipher systems for data, messages, fax, and voice are made with availability references.*

1. Introduction

SECURE hardware & software products are becoming increasingly important within civil government areas. This is evidenced by the fact that more and more countries are giving directives for the protection of classified and/or sensitive information.
Financial institutions, airlines, multinational manufacturing and trading corporations as well as nuclear power organizations are recognizing the need to take measures to protect valuable information.
These requirements have led to the availability of a great variety of SECURE products on the civil market. Mainframe computer manufacturers have SECURE products to offer. Usually, the products of US companies are not readily available on the international market. After the official cancellation of the US DES (Data Encryption Standard), there seems to be uncertainty on the market.
SECURE systems requirements may be categorized into:

1.1 TEMPEST

This is the codeword for the engineering practice established to ensure radiation protection of "clear" information.
Electronic systems generate electromagnetic radiation. This may be detected with commercially available equipment at considerable distances and data may be recreated. To protect the information, equipments and connecting cables have to be shielded. Software, driving terminals and scanning keyboards have to be designed to reduce traceability of "clear" information.

Fiber optic connections having no electromagnetic radiation at all are now available.
The specifications set forth are:
NATO: Here, the NACSIM 5100A standard is NATO-SECRET, and is not internationally available.
National specifications of similar severity exist in France, Germany, UK, and some other countries, which are published and internationally available.
Less stringent radiation protection may be required for less sensitive data or when the system's location is far away from a possible intercept point.

1.2 On-Site Protection

1.2.1 General

These are security measures whose development for civil systems has recently been strongly pushed. They consist in:

a) Establishing a security policy that specifies who is allowed to do what
b) Creating a physical and organisational environment that specifies where and how the security policy will be implemented.
c) Implementing mechanisms and controls to enforce the security policy

A site (or operation center) will have a system / security manager assigned to implement the security policy in the way consistent with the requirements of his organization. This involves a realistic consideration of these needs and their implementation with appropriate and effective procedures.
Close cooperation with the users is of great importance in establishing and later controlling the mechanisms.
Many security breaches result from the user's failure to take elementary precautions rather than from a sophisticated effort to defeat system security:
A user who leaves his terminal unattended while logged-in has left the door open to "his" system, rendering it vulnerable to intruders.
Fostering a positive attitude toward security is one of the most important functions of the system security manager.
Note that human errors and omissions are responsible for approx. 70% of the annual data related losses, inside deliberate transgressions by authorized users approx. 20%, and outside intrusions only about 10%. These, however, are extremely difficult to trace and present an ever increasing problem.

1.2.2 User

The User Identification Code (UIC) is assigned by the system/security manager either individually or to groups (marketing/purchasing/payroll department 1, payroll department 2, payroll department 3). This allows access to certain data only, and user name dependent Access Control Lists (ACLs) can be established by the manager. This ACL gives a USER access to different multiple data (e.g. the comptroller has access to payroll 1, 2 and 3. This technique is now widely used.

1.2.3 Password Management

This is one of the most effective means of an ON-SITE Protection policy.
The first requirement for a password is to be unguessable. This eliminates many obvious choices, such as wife's and pet's name etc. It is imperative that the password has a minimal length of 8 ASCII characters. Also, it has to be stored in enciphered form, the ciphering algorithm has to be of high complexity and non-reversible. Specific hardware-assisted ciphering is highly superior to software only, as it strongly defeats the intruder.
Even a system or security manager cannot retrieve a user's password from the storage media. If the user changes or forgets his password, the system/security manager can set a temporary new one to allow work, then the user has to choose another password.
Additional passwords can be introduced to restrict access to certain terminals.

- A system password is a system-wide password applied to selected out-terminals.
  It conceals from an intruder the name of the system he is attempting to probe.
- Primary and secondary passwords are used when two users have access to the system, and one only has no permission. One user inputs the primary and consecutively the second user the secondary password.
  Passwords are not prompted on the display. This minimizes the risk of unauthorized access and has proven to be a very effective security policy.

The password should be very random to defeat guessing, common word probing, and even "dictionary search".

Use of a random Password Generator can be imposed on the user or programmed into the system software. This can be purely stochastic and alphanumeric or, if it has to be remembered by persons, can be password choices that resemble words, but are pseudowords not found in a dictionary.
Entering a valid UIC and PASSWORD provides the user a LOGIN (access to the authorized system).

1.2.4 Login - Timing

The amount of information displayed at LOGIN has to be carefully considered. At highest security level only the file-numbers (message numbers) should be displayed.
Intruders, in case they have defeated the UIC and PASSWORD barriers, should not be given software version numbers, file lengths and locations, nodes etc. The last LOGIN parameters may likewise be suppressed.
With each LOGIN, the system's Real Time Clock (RTC) will note the operator's IN/OUT TIME, which is stored in enciphered form (see 2.3). This enables the system/security manager to closely follow the system activity.
Additional check procedures to verify the RTC have lately been developed on cipher basis to enable verification of IN/OUT TIME for the system/security manager.

1.2.5 Check on Retries

for UIC & PASSWORD, limiting the number of retry attempts to 3 within 20 sec, is a common practice. In case this limit is surpassed, the terminal can either be disabled for a certain time or blocked until intervention of the system/security manager.

1.2.6 Securing Stored Data

Data can be stored in ciphered form on disk or tape to defeat duplication out of the site. Here the same aspects count as mentioned in paragraph 2.3.
Any other procedure than ciphering will be unsatisfying, although frequently implemented.

1.3 Secure Networks

1.3.1 General

Local Area Networks (LAN), Products by IBM, DEC, XEROX etc., Integrated Systems Digital Networks (ISDN) with the B&D channels as well as Leased Line Networks (infrared, microwave, coaxial cable), and Dial-up Data communications are increasingly brought into use. Protocols like X-modem, BLAST, BISYNC 2780, BISYNC 3270, ASDLC/HDLC, X.24 are standardized.
It is here that more and more computer fraud is taking place. The system/security manager has a variety of possibilities to counter this threat.

1.3.2 Fiber Optic Networks

The use of SECURE optical interfaces between processors and/or terminals has begun recently, but these can be implemented in LANs only. The optic fiber can not be tapped without notable loss in signal strength, which is detected and an alarm is generated. This does not give any security against misuse of the terminals or processors. Fiber optic networks are frequently specified for TEMPEST reasons.

1.3.3 Secure Modem Access

This technique is designed to protect data in DIAL-UP networks.
The intelligent modem is password-protected and stores a set of Call-Back-Numbers. Once it receives a call, it requests a code number for the Call-Back-Number (e.g. 1...99). It then hangs up and calls this number back. The procedure thus defeats data communication sessions with unauthorized phone numbers.
Audit-trails are stored under password protection, unauthorized attempts to gain access to the system is also monitored.

1.3.4 CPU Data Ciphering

To provide network security, data can be enciphered inside the CPU, before being applied to the external interface. This can be done with software only or hardware-assisted. The security thus achieved is questionable, because either the user or an intruder could circumvent the ciphering software and/or hardware, and gain access in clear mode. Software packages and plug-in boards are now available for this concept.

1.3.5 I/O Port Data Ciphering

This seems to be the ultimate solution to SECURE DATA networks in all possible configurations. Data are enciphered after leaving the CPU/Terminal and have to be deciphered before entering. An intruder would have to know the key setting to gain access to the CPU/Terminal.
The security depends solely on the keys and the algorithm of the cipher set (module). The set-up of variables and keys is password-protected, and attempts to gain access to the system are monitored.
Products are available as plug-in boards (also combined with the modem), or as stand-alone sets connecting between the serial I/O of the CPU/Terminal and the modem.
Stand-alone modems including this SECURE concept are also available now.
Equipments are offered using the provable (but limited) SECURE Public Key system, the US DES-CIPHER which is now officially cancelled, and proprietary algorithms ranging up to key periods of 10 E 80 and 4-fold key hierarchy (incl. primary and secondary keys (see paragraph 2.3) and 10 E 98 key variables. Key management has to be established by the system/security manager (similar to the ON-SITE passwords). Downloading operational keys from a central CPU is a new feature.
For US government use special sets are built (KG-series (KGs: 28, 29, 43, 44, 46, 57, KGRs: 61, 62, 96), KY-series, and the STU-III), which are not internationally available.
Equipments must be selected for the degree of security required, for network compatibility (protocols like Ethernet, X.25, DECNET, IBM SNA, ISO OPEN) and data rate (Bps).
Bit-error rate increase by cipher feedback) has to be observed.
References and further publications for paragraph 1:

Security for Computer Networks
D.W. Davies and W.L. Price
ISBN 0-471-90063-X
Computer and Network Security
M.D. Abrams and H.J. Podell
ISBN 0-8186-0756-4, IEEE, Computer Society

2. Introduction

SECURE Military Systems today differ in many aspects from civil systems:
- In general, it is assumed that the USER is trustworthy, as he is screened personnel
- It is assured by controlled physical access to CPUs/Terminals and cipher equipments that no intruder can come on site.
- OFF-line communication and courier service are available
- the amount of data is usually less than in civil networks.

However, due to the availability of the "SECURE" technological know-how from the civil sector, the question arises whether this should not be implemented to further increase military security, make the systems more flexible, and improve the human interface. The military USER may come from a school where he has already been working with computers, so the basic knowledge of UIC and passwords for LOGIN is already there.

2.1 & 2.2 Military TEMPEST and On-Site Protection

should be considered according to what has been stated and explained in paragraph 1.1 and 1.2.
Multilevel password hierarchy is proposed because there surely will be one on-site system/security Officer and the Chief Cipher Officer from the country's Cipher Bureau, commanding the site.
This concept protects the site's data also in war-time, in case the location has to be left behind.
Passwords instead of the usual mechanical locks will be implemented in future equipment designs, also in field-type SECURE message and data terminals.
In military environment the equipment will not only be blocked if the password is probed 3 times within 20 sec, but an Emergency Erase of the information will take place.
Ciphering data files in storage is necessary and must be done by hardware-assisted procedures for highest security.
LOGIN times for data/message preparation from the system's RTC have to be coded or enciphered.
In OFF-line operations, - to control time delay between generation and receiving -, the time with a time checksum must be added to the data or message to enable the recipient to check the correctness of the indicated time.

2.3 Secure Military Networks

Please refer to 1.3.

Here, it is obvious that only I/O port ciphering will provide the degree of security required by military operations. Stand-alone cipher sets are used to clearly separate the "Red" side (CLEAR DATA) from the "Black" side (SECURE DATA).

Key Management Units (KMUs) are available instead of the simple key-fill devices (KYK-13, KYX-15, KO1-18).

Since military cipher standards only exist for US and NATO border-crossing traffic, it is the country's cipher bureau's responsibility to select equipment of highest security from experienced, long established firms, and have the security tested under the aspects of TEMPEST, statistical output, correlations, keystream period, key variables and their bit by bit influence on the key generator output.

Other aspects like temperature range, MTBF, ease of maintenance and operation, are quite different from the civil applications, especially when field-type equipments are considered like tactical message terminals. Here also, PASSWORD access control is used by some manufacturers.

Apart from the existent KW-7 Nato cipher set for border-crossing traffic there are newest KG and KY equipments put into service, also "Sunburst" sets compatible with various KGs will be used by US and Nato shortly.

Siemens, Telefunken, TST (FRG), Philips USFA (Netherlands), Plessey, Racal, Marconi, (UK) provide SECURE military equipment for non-border crossing traffic within Nato in Europe.

Some of their equipments are internationally available.

Since in military operations weather charts, maps etc. are of great importance, fax equipments are gaining importance.

TEMPEST-proved FAX-sets are now available. High security FAX cipher equipments with TEMPEST approval or National Radiation specs - are coming on the international market.

They operate with multiple passwords and key hierarchy, similar to the data cipher devices, and should be stand-alone equipments to enable the user quick disconnect of the high reliability cipher set from the less reliable fax machine for maintenance purposes.

Since analogue transmission voice "scramblers" are out because of their lack of security, digital vocoder-based systems with integrated cipher processing and modem are available, also with multiple key hierarchy. Only very few sets yet can be used in the field, because of size, weight, and power consumption. Password access control will be available to prevent misuse.

Although a vast amount of military communication and data/information is handled via commercial or military satellites, there is an increasing use of HF as a back-up medium. Here, the 2.4 kbps error correcting DATA-modems with integrated or external ciphering are getting available, permitting transfer of CPU-data, message information, FAX, or digital voice via HF (Cossor, Marconi (UK), Fredericks,

Harris, GTE, E-Systems (US), Telefunken, TST (FRG), offer latest state-of-the-art signal processor-controlled equipments, some being available for the international market.

Military satellite communications are enciphered, and standards have been set in the US. The "Ricebird" KG (A) for spacecraft is available as a chipset with compatibility to KG 28, 29, 46, 57, KGR 61, 62, 96. The "Ricebird" KG (B) is compatible with KG 43/44 equipments. KG (A) data rate goes to 10 Mbps, KG (B) up to 30 Mbps, key downloading, REKEY (up-loading) is possible.

Other space nations have also developed satellite cipher modules.

For details on 2.:

JANES MILITARY COMMUNICATIONS 1989
10th edition
ISBN 0-7106-0877-2

The Key to Cyphers
Klaus-P. Timmann
MILTRONICS, Vol. 9, No. 2, 1988

Kriptográfiai applikációk

dr. Dudás József

ITEA Kft.
A KFKI Számítástechnikai Csoport tagja

KIVONAT:

Számítógépes információs rendszerekben adatvédelmi szempontok szerint különböző típusú feladatok léteznek, melyek több esetben egymással ellentétes körülmények kielégítését igénylik. Szemléletes példa a tárolt adatok, vagy kommunikációs adatok rejtjelzéséhez felhasznált kulcsok elérési módja, vagy az aktualitás időtartama. Tárolt adatok esetén a kulcs mindig elérhető és a tárolás teljes időtartamára (esetleg több év) érvényes. A kommunikációs környezetben csak a kapcsolattartás idejére vonatkozik a kulcs elérhetősége és aktualitása. Az előadás egy univerzálisan kialakított kroptográfiai eszköz igényrendszerét foglalja össze és tárgyalja azokat a körülményeket, melyek egy univerzális eszköz használatával feladatorientált, "testreszabott" lehetőségeket biztosítanak az optimális és magas szintű kriptográfiai adatvédelem céljaihoz.

1. KRIPTOGRÁFIAI ALAPESZKÖZ

Egy komplex információs rendszer éppen a komplexitás miatt változatos számítógépes erőforrásokat használ.
A tárolt adatok:

- adatbázisok,
- levelezések,
- dokumentumok

védelme éppoly jelentőséggel bír, mint a védett kommunikációs csatorna biztonsága, amely

- hagyományos modemes átvitelt,
- csomagkapcsolt hálózatokat,

- rádiótelekommunikációt,
- satelites összeköttetéseket

egyaránt felölel. A rendszerek jellegzetessége az is, hogy a számítógépek többnyire lokális hálózatban, vagy egymással összekapcsolt lokális hálózatokban működnek.

Az univerzális környezetben kialakított adatvédelem univerzális kriptográfiai eszköz kialakítását sugallja, mely a különböző szituációkban is az elérhető legmagasabb védelmi szinten optimálisan működik. Az alapeszköznek rendszertechnikai elemei a következők:

- szabványos, illetve lecserélhető algoritmus
- komplett kulcs kialakítási rendszer, mely képes az adott célnak legjobban megfelelő és legmagasabb védelmi szintet biztosító kulcs kialakítására
- osztott védelmi rendszer. A teljes berendezés csak a hardware, software és logikai eszközök együttes birtoklásával válik működőképessé.
- önálló központi kulcsellátó rendszer (KMC)
- password és jogosultság ellenőrző, naplózó endszer

A kriptográfiai alapeszközt rendszertechnikailag a védendő adat keletkezési, illetve felhasználási helyén, tehát az adatbevitelt, vagy adatlekérdezést végző munkaállomásokban (terminálokban) célszerű elhelyezni. A munkaállomásként használt PC valamennyi erőforrása felügyelhető és "szándék szerint", vagy "kényszerpályán" kötelezően végezhető valamennyi kriptográfiai művelet. A megoldás azon az elven alapul, hogy az operációs rendszerek a belső memóriába mozgatják az adatokat és onnan irányitják a berendezés egyéb erőforrásaihoz (disk-ek, kiegészítő kártyák - telekommunikáció, fax, hálózati kártya, stb.) A memóriában lévő adatok bármelyike "átbuktatható" a kriptográfiai eszközön ahol azok vagy rejtjelzetté, vagy nyilttá válnak.

2. TÁROLT ADATOK VÉDELME

Tárolt adatok védelme esetén rejtjelzéssel elérhető, hogy a nyilt információ csak ideiglenesen (az adat bevitelekor, ill. lekérdezésekor) áll elő a központi memóriában.

A klasszikus kriptográfiai elv - ott kell az adatokat rejtjelezni ahol azok keletkeznek és csak a közvetlen felhasználás idejére és helyén szabad azokat nyílttá tenni - csak látszólag költségesebb megoldás, hiszen egy ilyen kriptográfiai megoldás mellett a kevésbé védett hálózati összeköttetésen sem mozog információ és szabványos hálózati, ill. kommunikációs software is alkalmazható.

3. TELEKOMMUNIKÁCIÓS VÉDELMEK.

(Az adattovábbitás nyilvános csatornán (telefonhálózat - modem, számítógép hálózat - X25, radió, vagy satelit összekőttetésen keresztül történik.)

Az adatátviteli szabványokban a legmagasabb "OSI szinten" - a user felületen javasolt a különböző rejtjelzési védelem.

Számos berendezés - főleg céleszközök - eltér ettől az ajánlástól és a rejtjelzést látszólag átteszi a fizikai szintre.
Telekommunikációs közegben ez azt jelenti, hogy valamilyen szabványos interface felületet RS232, V24, X25, G703, stb. megbontanak és annak DTE - DCE oldalai közé illesztik a rejtjelző eszközt.

A fizikai szinten történő rejtjelzés csak látszólagos, hiszen a vezérlő karakterek, vagy a különböző header-ek rejtjelzése nem megengedett. Ezeket az alkalmazott telekommunikációs protokollnak megfelelően le kell válogatni (általában az OSI legfelső szintjéig). Végül az így elért adatokat rejtjelzés vagy megoldás után új telekommunikációs csomaggá kell összeállítani, és a rendszernek átadni.

Az így kialakított rendszereknek számos hátránya mellett egyetlen előnye a transzparencia. Hátrányai közül meg kell említeni az erős hardware függést valamint azt, hogy a kripto protokollok alacsony védelmi szintjét tudják csak elérni. Számos közegben (csomagkapcsolt hálózatok) ugyanis sem az üzenet hosszabbodás, sem új önálló blokk beiktatása nem megengedett. (pl: X25, X4000)

Hasonló megállapítások érvényesek a kriptográfiai célberendezésekre kripto fax, kripto modem, stb. ahol sem a korszerű kripto protokollok, sem a napjainkban egyre nagyobb jelentőséggel bíró egyéb kriptográfiai szolgáltatások (pl. hitelesítés, digitális aláírás) megvalósítására semmilyen lehetőség nincs.

A telekommunikációs adatok védelmére olyan kriptográfiai alapeszközt célszerű használni, mely minimálisan az alábbi szolgáltatásokat biztosítja.

- **Viszonylatfüggő rejtjelzés.**

A kulcskialakítással megvalósított viszonylatfüggő rejtjelzés az adateredet hitelességét kriptográfiai eszközökkel biztosítja. Az adatátviteli protokollok által biztosított szolgáltatást - állandó és időszakos kapcsolatok létrehozása - a titkosító keretprogram csak a címzésekhez használja, az adatvédelem szempontjából gyakorlatilag redundáns elem marad.

A küldő oldal a célállomás hitelességéről kap egyértelmű megnyugtatást. A viszonylatfüggő

rejtjelzéssel minden végpont bizonyos lehet abban hogy a küldött üzenetét (még lehallgatással támadott esetben is) csak az az állomás érti meg, mely ennek fogadására illetékes.

A viszonylatfüggő rejtjelzésben a automatikus szolgáltatás a "message everybody", vagy "brodcast" (körlevél) üzenet.

- **Üzeneti kulcs**

A kapcsolatteremtés idejére fizikai véletlen számon alapuló üzeneti kulcs küldése/fogadása. A "pillanatnyi" üzeneti kulccsal megvalósított rejtjelzés kulcsa megismételhetetlenül csak a kapcsolattartás idejére "él".

Az üzeneti kulcs alkalmazása főleg nagy számú üzenetforgalom esetén növeli egyértelműen a kriptográfiai erősséget. Megakadályozza a más rejtjelzéshez használt (fix) kulcsok kompromittálódását, melyek "abszolút biztos csatornán" installálláskor vagy évenkéti, félévenkéti generális kulcs csere alkalmával jutnak el a rendszer elemeihez.

- **Hitelesítés**

A kriptográfiai alapeszköz rejtjelzés és megoldás esetén is generál egy kulcstól függő ellenörző összeget, melyet az üzenet adattartalmához lehet fűzni. Az hitelesítés ellenőrzése az alapeszköz feladata - a sikertelen ellenőrzés a kapott üzenet abortációját eredményezi.

A kriptográfiai hitelesítés az üzenetmanipulációs (megszemélyesítés tipusú) támadások ellen is véd.

- **Digitális aláírás és időpecsét**

Bármely nyílt vagy rejtjelzett üzenethez előállítható a nyilvános kulcsú rejtjelzés felhasználásával olyan "ellenőrző kód" amely bármely felhasználó számára értelmezhető, de egyértelműen (meghamisíthatatlanul) képes az üzenet feladójának kilétét, a keletkezés helyét, időpontját bizonyítani. Az RSA típusú PKS felhasználása lehetővé teszi, hogy adott, publikus kulcs-információk felhasználásával bárki, bármikor ellenőrízheti az aláírás hitelességét. A feladó biztonságát pedig az egyedül nála meglévő titkos kulcsinformáció garantálja.

4. LOKÁLIS HALÓZAT (LAN) VÉDELMEK.

(Az adattovábbitás ellenőrzött csatornán és általában egy épületen belül - koaxiális kábelen, üvegszálon keresztül történik.)

A file server alapú lokális hálózatok védelmi rendszerét a stand alone védelmi rendszerhez hasonlóan a munkaállomásokon kell megvalósítani. A server nem tartalmaz kritográfiai eszközt (ez rendszertechnikailag is helytelen). A serveren minden adat rejtjelzetten tárolódik, csak a munkaállomásokon válik nyilttá a felhasználás idejére. Ennek a megoldásnak sajnálatos hátránya, hogy a server nem képes a tárolt adatokon semmilyen felhasználást végezni. Ha a serveren futó program képes kezelni, itt is elhelyezhető kriptográfiai alapeszköz. Ezzel a megoldással a védelem kismértékű csorbításával futhat a központi feldolgozás.

Hálózatok összekapcsolására (protokoll konverterek, bridge-ek rooter-ek) léteznek ugyan hardware applikációk (nagy sebességű kripto berendezések), de ezek kriptográfiai erősségére is a telekommunikáció célberendezéseknél tett kritikai megjegyzések érvényesek. Részben a nagy sebesség, részben a felhasznált protokollok kötöttségei miatt a telekommunikációban leírt "minimális kriptográfiai elvárás" is nehezen valósítható meg.

5. VEGYES (NYILT-REJTJELZETT) KRIPTOGRÁFIAI RENDSZEREK VÉDELME.

Különleges problémát jelentenek az olyan rendszerek, melyekben nyílt és rejtjelzett (védett) adatok forgalmazása együttesen is előfordul. Ha a folyamatokat csak rezsimutasítások szabályozzák, az emberi tévesztésnek kellemetlen következményei lehetnek.

A rezsimutasításokat olyan hardware és software erőforrásokkal szükséges megerősíteni, amelyek a megbízható működtetést lehetővé teszik.

- **felhasználó tiltás:** hogy privilegizált műveleteket, vagy vegyes (rejtjelzett és nyílt) a forgalmazást felhasználóknak csak a jogusultsággal rendelkező köre tehet.

- **hierarchikus tiltás:** az elérhető adatok hierarchikus rendben csak bizonyos felhasználók számára visszafejthetők.

- **programtiltás:** meghatározott programok futtatása jogosultsághoz kötött

- **erőforrás tiltás:** bizonyos erőforrások használata (kommunikációs port, nyíltan olvasható floppy, nyiltan írható floppy) felhasználói jogosultsághoz kötött.

6. TÁROLT ADATOK KRIPTOGRÁFIAI VÉDELME.

Bizonyos programok (programrendszerek) kriptográfiai szempontból a számítógépes architektrúrákkal analóg problémákat vethetnek fel.

- archiváló rendszerekben ahol file beviteli, editálási és file kiviteli munkafolyamatok jelentkeznek, a hozzáférési és hitelesítési problémák kerülnek előtérbe. Egyébként a

lényegesebb kriptográfiai szempontok a stand alone védelemmel csaknem azonosak. A hozzáféréssel kapcsolatban jelentős szerephez jutnak a rezsimutasítások.

- elektronikus levelező rendszerekben (e-mail) kriptográfiai szempontból a hierarchikus kulcsokon kívül a "levelező kulcs" kialakítása válik szükségessé, mely a viszonylati kulcsot a hálózat végpontjain belül különböző felhasználók között is megvalósítja. A különböző végpontokon a felhasználók közötti hierarchia kiosztás (témánként, felhasználónként, felhasználói csoportonként, stb.) a rendszer konkrét tervezésekor jelentős feladat. A kézhez vett (bontott) "leveleket" nemcsak a tárolókapacitás kímélése miatt, hanem a kriptográfiai védelmi rendszer erősítése érdekében is célszerű törölni.

- adatbázis rendszerek esetén a hierarchikus kulcsok felhasználásával akár mező szintű (mezőnként különböző) rejtjelzés kialakítása is megengedett. A mező szintű rejtjelzésre a konkrét adatbázis program (pl clipper, dBase) megírásakor kell kriptográfiailag felkészülni.

Megjegyzés: a mező szintű rejtjelzés nyílt indexű rejtjelzett tartalmú adatbázisoknál lehetséges.

A rekord szintű rejtjelzés a programoktól függetlenül az operációs rendszerben is végezhető, ekkor az indexállomány rejtjelzése is megoldható.

A file szintű rejtjelzés nem javasolt forma, - főleg nagy méretű állományok esetén - a rekordszintű elérések jelentős lassulása miatt.

7. ADATHORDOZÓK KRIPTOGRÁFIAI VÉDELME.

A szállítható adathordozó védelme a "nyílt írás", "nyílt olvasás" problémáján kívül kulcskialakítási kérdéseket is felvet. A rendszerbe nyílt adatok bevitelét vagy az őrzött adatok nyílt kivitelét jogosultsági előírások, ill. rezsim utasítások szabályozzák. A kulcskialakítással a konkrét feladatnak megfelelően biztosítani lehet, hogy

- a rejtjelzett adathordozó a hálózat valamennyi állomásán "leolvasható" legyen (postázás mágneses adathordozón)

- a rejtjelzett adathordozó csak azon az állomáson olvasható le, ahol készült (archiválási, mentési feladat)

- a rejtjelzett adathordozó a hálózat valamennyi állomásán, de csak meghatározott felhasználói körben olvasható le (szelektív, password-ös rejtjelzés)

- a rejtjelzett adathordozót a időszakos kulcs-csere alkalmával frissíteni (átrejtjelezni) kell

- az adathordozó rejtjelzése egységes, vagy "track-sector függő"

A különböző számítógépes rendszerekben az adatvédelemre vonatkozó igények jelentősen különböznek egymástól. Minden szituációban működő egységes kriptográfia nem tud optimális védelmet nyújtani. A jó megoldást olyan univerzális kriptográfiai alapeszköz alkalmazása jelenti, mely "hangolható" és a feladat igényeinek megfelelően magas szintű védelmet biztosít. Különösen fontos a kriptográfiai paraméterek változtathatósága a többfelhasználós (nem dedikált) rendszerekben. Az előadás gazdaságossági kérdésekkel nem foglalkozik, de jó becslésnek tekinthető, hogy egy univerzális eszköz használata olcsóbb, mint az egyfunkciójú kriptográfiai céleszközök telepítése.

BIZTONSÁGI KÉRDÉSEK UNIX OPERÁCIÓS RENDSZERŰ GÉPEKEN

Cser András <acser@eik.bme.hu>,
Fekete László <fekete@eik.bme.hu>
Budapesti Műszaki Egyetem, Egyetemi Információs Központ
1111 Bp. Műegyetem rkp. 9.
1502 Bp. Pf. 91.

Várkonyi Béla, CNI és CNE <varkonyi@leila.mti.bme.hu>
BME Mérnöktovábbképző Intézet, Novell Oktatóközpont
1111 Bp. Egry J. u. 20-22.
1502 Bp. Pf. 91.

KIVONAT:

A cikk kitér a UNIX rendszerek biztonsági lyukainak (security hole) vizsgálatára, elemzi azok megszüntetésének lehetőségeit. A szerzők kiemelt súllyal foglalkoznak az egyetemi környezetben megszokott Internet hálózathoz való csatlakozás problémáival és biztonsági kérdéseivel. Feltárják a leggyakoribb hacker-módszereket, kitérnek az azok ellen felhasználható stratégiákra és megelőző stratégiákra, elvekre. Megismertetik a hallgatót a hálózati adattitkosítás és rendszerbetörésre szolgáló illetéktelen lehallgatás elleni védekezéssel. Vázolják a biztonságosnak tekinthető UNIX rendszerek legfontosabb paramétereit és beállításait. A hálózati ablakozó rendszerek (X Window System) veszélyforrásai. A hálózati eszközök fizikai és szoftver védelme: routerek, firewall-ok, host-ok, bridge-ek. A hálózati biztonsággal foglalkozó szervezetek.

Néhány a tárgyalt témák közül:

- *password (jelszó) védelmi kérdések*
- *jelszavakat használó alkalmazások*
- *anonymous szolgáltatások: ftp, tftp*
- *logging: milyen mértékben?*
- *egy régi kedvenc: sendmail & fingerd*
- *mailhub-megoldás*
- *NNTP News*
- *Az "R" szolgáltatások pro és kontra: rlogin, rcp. .rhosts, hosts.equiv*
- *Anonymous NFS*
- *tcpdump, etherfind: OK UNIX-okon. És a PC-kkel mi a helyzet?*

1. Bevezetés

A mai számítástechnikában egyre nagyobb szerepet játszik a biztonságtechnika, adataink védelme az illetéktelen módosítástól és betekintéstől, egyszóval hozzáféréstől. A UNIX operációs rendszer elterjedésével nem járt együtt az egyéb operációs rendszereken (pl. VMS) megszokott védelmi módszerek elterjedése. Ehelyett - lévén a UNIX egy nyílt rendszer - minden gyártó kifejlesztette a saját, az alap operációs rendszer biztonsági "berendezéseinél" sokkal fejlettebb változatait. Függően a befektetett munkától, a biztonsági rendszerek egyes implementációi nagyon eltérőek minőségüket és szolgáltatásaikat tekintve. Hogy miért ilyen cudar a helyzet? A válasz erre a kérdésre egyszerű: a UNIX operációs rendszer megalkotói egy nyílt rendszernek szánták, amelyben több programozó dolgozik együtt, akiknek együttműködését nem akarták feleslegesen megnehezíteni. A 80-as években több egyetem vette át a UNIX-ot és adaptálta a saját, az eredetihez hasonló igényei (nyílt környezet könnyű együttműködés, stb.) kielégítésére. Itt sem volt szükség túlzottan szigorú biztonsági előírások betar(ta)tására. A helyzetet csak tovább bonyolította, hogy egyre több kiegészítés és alkalmazás született a UNIX-hoz, a legtöbb gép ma már hálózatba van kapcsolva. Ezzel megszűnt a gépek fizikai védelmének lehetősége. Ebben az előadásban elsősorban az egyetemi környezetben és hálózatban üzemeltetett UNIX-os gépek problémáival foglalkozunk.

A biztonság fontos és UNIX rendszereink és adataink védelme sohasem lesz tökéletes ("Az a gép biztonságos, amelyet betettek egy földalatti betonbunkerbe és be sem kapcsoltak..."), mégis igyekszünk néhány olyan pontra felhívni figyelmüket, amelyek valóban a UNIX rendszer Achilles-sarkai, más szóval legismertebb biztonsági lyukai (security hole). Ezek betömése sokat segít a rendszer biztonságossá tételében.

2. A jelszavak kezelése

Minden rendszer biztonságának alapköve a rendszerbe belépésre jogosító password-ök védelme. A UNIX rendszer eredeti implementációja a password-öket a /etc/passwd file-ban tárolja kódolt formában. A kódolás egy módosított DES (Data Encryption Standard) algoritmuson alapszik, amelynek jellemzője, hogy a generált kód nem visszafejthető. A rendszer a felhasználó login password-jét a fentemlített algoritmussal kódolja és összehasonlítja a /etc/passwd file-ban tárolt kóddal. (Újabb UNIX-okon a /etc/passwd file password mezejében egy x van, maga a kódolt password egy /etc/shadow nevű file-ban van tárolva, amelyre senkinek semmilyen joga nincs. A magyarázatot ld. később.) Ha a kettő egyezik, a felhasználót belépteti a rendszerbe. Ezért fontos, hogy password-ünket **senkinek** se áruljuk el, hiszen nem biztosítható ily módon annak terjedésének ellenőrzése. (Erre felhasználóinkat kötelezni lehet egy Felhasználói Szabályzat formanyomtatvány kitöltetésével és aláírattatásával.) Hasznos lehet a jelszavak változtatásának félévenkénti megkövetelése is, természetesen úgy, hogy ne legyen lehetséges két jelszó közötti váltogatásra. A password megválasztásakor figyelembe kell venni, hogy egy potenciális betörőnek, amennyiben valaki jelszavát kívánja megfejteni, nincs más lehetősége, mint a nyers erőn alapuló próbálgatás. Vannak azonban olyan lehetőségek, amelyek kézenfekvők, ezért ezekre itt külön és részletesen szeretnénk kitérni.

- Ne használjunk login nevünket (pl. zkiraly) semmilyen formában: eredeti formában, fordított betűsorrendben (ylarikz), nagybetűvel (ZkIralY), megkettőzve (zkiralyzkiraly), stb.
- Ne használjuk vezeték és keresztnevünket semmilyen formában és kombinációban.
- Ne használjuk házastársunk vagy gyermekünk nevét.

- Ne használjunk semmilyen könnyen megtudható információt: telefonszám, autómárka, utcanév, ahol lakunk, stb.

- Ne használjunk csak számokból álló, vagy többszörözött betűkből álló password-öket. (12345678, zzzzzzz)

- Ne használjunk a /usr/dict/words file-ban lévő angol szólistán, vagy bármilyen (magyar!!!) szólistán szereplő szót direkt formában. Sajnos közkézen forog több magyar szólista is, amely a kitalálást (crack-elést) nagymértékben megkönnyíti.

- Ne használjunk 6 karakternél rövidebb jelszavakat.

- Ne használjunk ilyen jelszavakat: gabor1, 4peter, geza32.

- Használjunk kis és nagybetűkből álló jelszavakat.

- Használjunk központozást és egyéb nem alfanumerikus karaktereket tartalmazó password-öket.

- Használjunk könnyen megjegyezhető jelszavakat, hogy azokat ne kelljen leírni.

- Használjunk olyan jelszavakat, amelyeket könnyen és gyorsan be tudunk gépelni, csökkentve annak esélyét, hogy valaki a hátunk mögött a billentyűzetről leolvassa, mit írtunk.

Sajnos a modern jelszótörő algoritmusok már könnyedén megbirkóznak olyan jelszavakkal, mint pl. dog+cat, alma.pohar, stb, ezért a központozásból érdemes többet és nem egyformát használni. A jelszavak helyes megválasztásának fontosságát nem lehet eléggé hangsúlyozni. Semmi értelme nincs bedeszkázni a pinceablakokat, ha főbejárat ajtaját szélesre tárjuk.

A UNIX rendszeren a jelszó megváltoztatását a passwd programmal kezdeményezhetjük. A legtöbb gyártó által a rendszerhez adott passwd program ma már figyel a fenti követelmények nagyrészének betartatására, kivéve talán a szólistákban való keresést. Természetesen anonym ftp-vel elérhető nagyon sok passwd program, amely az ellenőrzést parametrizálhatóvá teszi. (Meg lehet például a minimális és maximális jelszóméretet adni. A maximális jelszóméret a legtöbb rendszeren 8 karakter, a 8 karakter feletti karaktereket a rendszer elfogadja, de figyelmen kívül hagyja.) Természetesen az ellenőrzés szigorától függően vannak engedékenyebb és kifejezetten erőszakos passwd programok is.

Sok rendszeren vannak guest account-ok is, amelyeket biztonságtechnikailag tilos lenne egyszerű password-ökkel (vagy esetleg anélkül) hagyni. Gyakorlatilag ezek közé tartoznak az egyszerű parancsokat végrehajtó account-ok is. pl. lpq, date, who, operator, shutdown, stb. Ezek közül néhány leggyakrabban ugyanis supervisor-i (root) jogkörrel (suid) felruházott programokat futtat (mentés szalagra, merevlemezek mount-olása, értékes adatok nyomtatása, stb), amelyek illetéktelen kezekbe jutva ("...csak a Ferinek mondtam meg a mount password-jét...") nemcsak munkánkat pusztító rombolást okozhatnak, hanem nyomkövetésük is bizonytalan. Ki tudja megmondani, hogy a backup login-t tudó operátorok közül ki, kinek és mikor mondta meg a password-öt? A log-ból pedig csak annyit fogunk megtudni a "vérbefagyott" konzolról (jó esetben!), hogy:

```
syslog: ... : user "backup" umounted ufs /dev/dsk/c0t0d0s0
```

Az ehhez hasonló problémák könnyen elkerülhetők a felhasználók átgondolt csoport-rendszerbe való beosztásával. További segítséget nyújthat a sudo segédprogram használata, amely lehetővé teszi, hogy a supervisor egy file-ban rögzítse, melyik felhasználó milyen suid root programokat hajthat végre.

Hálózatba kapcsolt gépek esetében felmerül, érdemes-e engedélyezni, hogy a supervisor (root) egy távoli hálózatos terminálról bejelntkezzen? A válasz: nem. Bár ennek rengeteg előnye lenne (elsősorban kényelmi szempontok), nem követhető politika, mivel a root bejelentkezése nem loggolt megfelelőképpen.

3. Az anonymous szolgáltatások

3.1 ftp

A file transfer protokoll-t megvalósító UNIX szerver neve: ftpd, vagy in.ftpd. Ezzel lehetősége nyílik a rendszer felhasználóinak, hogy file-jaikat más gépekre átvigyék, hálózaton keresztül. Az ftp-vel kapcsolatban meg kell jegyeznünk, hogy amennyiben gépünkön olyan adatok vannak, amelyek kijutását mindenképp meg kell akadályoznunk, abban az esetben szóba jöhet, hogy letiltjuk teljes egészében az ftp démont. Ez nem túl elegáns megoldás, viszont lehetővé tesz egy elég hatékony adatvédelmet. Természetesen gondoskodni kell ilyen esetben arról is, hogy a UNIX-os gép felhasználói se tudjanak kifelé kapcsolatot kezdeményezni. Amennyiben gépünket olyan felhasználóknak is hozzáférhetővé kívánjunk tenni, akiknek nincs account-juk, ebben az esetben megoldást az anonymous vagy ftp, password nélküli, virtuális user bevezetése jelenti. Ebben az esetben célszerű ftp démonunkat lecserélni a Western University of St. Louis által fejlesztett wu-ftpd-re lecserélni, amelynek loggolási képességei messze felülmúlják gyártónk által szállított ftp démonunk szolgáltatásait. Ebben az esetben anonym bejelentkezőnk e-mail címével mint password-del bejelentkezhet és korlátozott (chroot) eléréssel file-okat tölthet le rendszerünkről. (Egy ügyesen megépített és átgondolt file szerverrel megoldható egy intézményben a szoftverek disztribúciója is.) Természetesen, amennyiben elkonfiguráljuk szerverünket, úgy támadási felületet adunk a betörőknek.

3.2 tftp

A tftp abban különbözik az ftp-től, hogy nincs benne jelszavas védelem, így bárki file-okat tölthet le a rendszerről. Ezt a szervert elsősorban diskless kliens gépek boot-olására találták ki, egyébként túl sok értelme nincs. Az első kérdés, amelyet fel kell tennünk magunknak: van-e egyáltalában szükségem tftp-re? Ha nincs, akkor célszerű leállítani ezt a szolgáltatást. Egy betörő például letöltheti vele a /etc/passwd file-unkat, hogy aztán kényelmesen probálgathassa jelszófeltörőjével...

4. A betörők régi kedvencei: sendmail és fingerd

4.1 sendmail

A levelezés az a szolgáltatás, amelyért a világ UNIX-os számítógépeinek több, mint felét *kizárólag* üzemeltetik. A legtöbb UNIX-os rendszer ma már az SMTP-t (Simple Mail Transfer Protocol) használja,

amelyben több, nagyon komoly biztonsági lyuk van. Mivel a protokollt arra tervezték, hogy hatékony legyen, ezért szinte semmilyen ellenőrzést3 nem csinál feladata ellátása közben, pl. feladó létezésének ellenőrzése, digitális aláírás, stb. Ez egy tervezési hiba, amely ellen jelenleg nem sokat lehet tenni. Rövidtávú megoldásként lehet javasolni, hogy felhasználóinkat tájékoztassuk arról, hogy kapott leveleik feladói nem feltétlenül léteznek, pl. Bill Clinton-nak nincs nyilvános email címe... Figyelmeztessük felhasználóinkat, hogy gondolkodjanak email-jük olvasása közben. Léteznek olyan sendmail implementációk, amelyek képesek kiterjedt loggolásra, viszonylag kis teljesítménytöbblet árán. Megjelentek olyan kísérleti implementációk is, amelyekkel lehetőség van nyilvános kulcsú digitális aláírást tartalmazó levelek kezelésére.

Lehetőség van arra is, hogy egy beérkező levelet a sendmail egy aliasnak és/vagy egy programnak adja át. Ekkor az elindított program root jogokkal fut(hat), amely egy biztonsági lyuk, ugyanis innen már semmibe nem kerül pl. egy olyan file-t küldeni egy alkalmas alias-ra, amely továbbadja a file-t egy C fordítónak, lefordítja azt, majd az így lefordított program mail-ben visszaküldi a /etc/passwd file-t a feladónak. Több - főleg régebbi sendmail implementációba beépítették a debug és wiz parancsokat. Ezeket a /etc/sendmail.cf file-ban hatástalaníthatjuk. Amennyiben gépünk operációs rendszerével ilyet szállítanak, akkor sendmail programunkat sürgősen cseréljük le!

Természetesen lehetőség van - elsősorban egy szoros szervezetű intézményben - egy ún. mailhub vagyis mail relay host vagyis mailserver felállítására. Ebben az esetben intézményünk gépei ezen a gépen keresztül leveleznek. Ekkor a kimenő leveleket minden gép az intézményben ennek a mailhub-nak adja, foglalkozzon ő a továbbküldéssel. A kimenő levelekben a feladó címét a mailhub kicseréli valamilyen egységes címre, és az így egységesített címre érkező bejövő leveleket szortírozza a címzett neve szerint. Ez természetesen többletfeladatot jelent mind a mailhubnak, mint annak adminisztrátorának, de így valamelyest ellenőrizhető, hogy ki küldött esetleg egy hamis feladójú levelet kifelé. A belső, intézményen belüli levelezést is lehet hasonló módon egységesíteni.

4.2 fingerd

A fingerd feladata, hogy információkat adjon a gép felhasználóiról. Amennyiben a kérdéses felhasználó nincs bejelentkezve, úgy lehetőség van a home-directory-jában elhelyezett .plan file megtekintésére. A legtöbb rendszer a fingerd démont root userként futtatja, így kézenfekvő a következő megoldás a password file elolvasására:

```
rm ~/.plan
ln -s /etc/passwd ~/.plan
```

Ezzel létrehoztunk egy szimbolikus linket a password file-ra. A root-ként futó fingerd démon pedig kiválóan olvassa a password file-t, ha nem vagyunk bejelentkezve!!! A biztonsági lyuk betömésének lehetőségei:

- leállítjuk a fingerd-t (/etc/inetd.conf)
- nobody-ként futtatjuk a fingerd-t
- Installáljuk a wu-fingerd (Western University of St. Louis) démont, amely "nem szereti" a linkeket, nem olvassa azokat

A finger lehetőséget ad arra, hogy információkat szerezzünk rendszerünk felhasználóiról. Természetesen felmerül a kérdés, hasznos ez az információ egy betörő kezében?

5. Usenet News (NNTP News)

Az NNTP (Network News Transfer Protocol) News-zal foglalkozó, azt tároló gépek tagjai a USENET News virtuális hálózatának. Természetesen ebbe a hálózatba bárki beléphet, aki egy másik már a hálózatban lévő tagtól tölteni tudja a cikkeket, és azokat tárolni esetleg továbbadni is tudja. Az NNTP-t sem úgy tervezték, hogy kiemelt jelentőséget tulajdonítottak volna a biztonságnak, a protokoll nem tartalmaz semmiféle verifikációt azt illetően, hogy egy adott cikk honnan is származik valójában. Ezzel tisztában kell lenniük felhasználóinknak. Megoldási lehetőségek: 1) vannak úgynevezett moderált csoportok, amelyekbe csak a moderátor postolhat. Amikor ebbe a csoportba kívánunk írni, küldenünk kell egy levelet a csoport moderátorának, ő bírálja el, hogy az adott cikk megjelenhet-e. 2) Újabb implementációkban (C News, Inn) lehetőség van annak megadására, hogy mely gépekről mely csoportokba lehessen cikket küldeni. 3) Ezekben az implementációkban lehetőség van arra is, hogy a postolni kívánó felhasználót jelszóval azonosítsuk.

6. Az "R" szolgáltatások

Az "R" szolgáltatások (rlogin, rcp, rmt, rsh) parancsok távoli futtatását, távoli számítógépre történő password nélküli bejelentkezést, file-másolást, távoli szalagegység kezelését, stb. teszik lehetővé. Használatuk nagymértékben kényelmessé teszi és leegyszerűsíti a mindennapi feladatok elvégzését számítógépeink között. Kérdés természetesen, hogy ha illetéktelen betörő egy rendszerbe be tud lépni, onnan útja akadálytalan a többi gépre. Azokat a gépeket, amelyekről engedélyezzük a jelszó nélküli belépést, trusted hostoknak nevezzük. Ezeket rendszerszinten a /etc/hosts.equiv file-ban, user szinten pedig a ~/.rhosts file-ban tároljuk. Természetesen nagyon fontos, hogy kinek, van írási és olvasási joga ezekre a file-okra. Amennyiben olyan gépekről is engedélyezzük a belépést, amelyek nem a mi adminisztrációnk alá tartoznak, már nem mi tartjuk kézben rendszerünk biztonságát. Sok hátránya mellett azonban van egy előnye is az "R" szolgáltatásoknak: nem mennek át kódolatlan password-ök a hálózaton. Mindezek ellenére nem javaslom az "R" szolgáltatások használatát. Ha olyan rendszerre van szükségünk, amelybe bármely számítógép bármely felhasználója bárhol beléphet, használjuk inkább a Yellow Pages szolgáltatásokat, amelyek ezeket korrekt és viszonylag biztonságos formában implementálják.

7. NFS (Network File System)

Az NFS célja és lényege, hogy egy számítógép filerendszerét vagy annak egy részét egy másik számítógép filerendszerének részeként lássuk. Amennyiben olyan diszkterületeket is exportálnunk kell, amelyek fontos/titkos adatok vannak, akkor read-only jogokkal exportáljuk azokat. A SUN által bevezetett secure NFS hatékony védelmet kínál. Lehetőség van arra, hogy root jogokkal exportáljunk egy filerendszert egy kliensnek. Ilyenkor a kliensnek általunk adminisztrált, de legalábbis trusted gépnek kell lennie.

8. Hálózatvizsgáló programok

Vannak olyan public domain programok, amelyekkel a helyi hálózat közvetlenül monitorozható, csomagjai filterezhetők. Ilyen programok pl. tcpdump, etherfind, stb. Ezekkel megfigyelhető a hálózaton átvitt csomagok 90-99%-a. (Csomagveszteséggel számolva.) Ezeknek a programoknak futtatásához

leggyakrabban root jogkörökre van szükség, tehát UNIX-os gépen csak akkor jelentenek veszélyt, ha illetéktelen is tudja futtatni, tehát mindenki számára installálva van a program. Ezek hasznos eszközök egy hálózati manager kezében, de használatuk végzetes lehet, ha illetéktelen kezekbe kerülnek. Sajnos a TCP/IP protokoll nem biztosítja, hogy az adatok kódolt formában menjenek át a hálózaton. A PC-kel kapcsolatban még reménytelenebb a helyzet. Hálózatmonitorozó programokat nem nehéz írni. Egy költséges megoldás lehet ebben az esetben hardware kódolást használó FDDI/Ethernet kártyák használata. Egy másik megoldás lehet, hogy a fontos és bizalmas adatokat átvivő hálózatot egy firewall gateway-el kapcsoljuk hozzá hálózatunk más részeihez. Ez a firewall (tűzfal) csak meghatározott gépekről meghatározott gépekre enged át csomagokat. Erre a célra egy PC is megfelel kisebb hálózat és routolási feltételrendszer esetén, nagyobb feladatokra routereket kell használnunk. A firewall rendszert egyébként elsősorban arra találták ki, hogy szelektív adatforgalmat bonyolítson le saját belső hálózatunk és az Internet között. Az ilyen firewall-ok figyelik és szűrik a rajtuk áthaladó forgalmat. Vannak olyan programok pl. gatekeeper.dec.com:/pub/DEC/screend/*, tcpwrapper, melyek figyelik egy adott gép TCP/IP protokollú csomagforgalmát. Természetesen a célberendezések mindezeket a szűréseket hardware-ből valósítják meg.

9. Ablakozó rendszerek (X-Window System)

Az X-Window rendszer lehetőséget teremt arra, hogy gépünk erőforrásait más gépek használhassák. Ilyen erőforrások pl. egy képernyő tartalma vagy a bebillentyűzött szavak. Sok felhasználó teljesen kikapcsolja az X-Window biztonsági szolgáltatásait, hogy kényelmesebben tudjon dolgozni. Ekkor egy betörőnek semmi más feladata nincs, csak hogy írjon egy olyan programot, amely egy X terminált monitoroz és kiolvassa egy adott xterm ablakból a felhasználó password-jét. Megoldás: usereink tájékoztatása a biztonságos X-Window használatról.

10. Szervezetek

- CERT: Computer Emergency Response Team. Ezt a szervezetet 1988-ban hozták létre. Az USA Védelmi Minisztériuma finanszírozza. Legjobb információforrása a biztonsági incidenseknek, információknak, tapasztalatoknak, stb. Email: cert@cert.org
  Telefon: 00-1-412-2687090

- FIRST: Forum of Incident Response and Security Teams. Fő támogatói: USA Védelmi Minisztériuma, NASA, vezető számítógépgyártók.

- IETF: Internet Engineering Task Force: Főleg a megbízhatóbb levelezéssel (privacy enhanced mail PEM) foglalkozó emberek számára fontos. Email: pem-dev-request@tis.com

- Információ források:
  - USENET comp.virus és comp.security.announce, comp.unix.security csoportok.
  - VIRUS-L: Levelezési lista. Email: listserv@ibm1.cc.lehigh.edu (vagy Bitnet-en listserv@lehiibm1.bitnet) egy

SUB VIRUS-L nevunk
tartalmú levéllel.
Nyilvános beszélgetés számítógépes vírusokról (PC, Mac, stb.)

- VALERT-L: Levelezési lista. Email: listserv@ibm1.cc.lehigh.edu (vagy Bitnet-en listserv@lehiibm1.bitnet) egy
  SUB VALERT-L nevunk
  tartalmú levéllel.
  Ebben a listában lehet felhívni a többiek figyelmét egy általunk talált új vírusra.
- Archívum: cert.sei.cmu.edu:/pub/virus-l
- További listák: cert-tools-request@cert.sei.cmu.edu
  cert-advisory-request@cert.sei.cmu.edu

Irodalomjegyzék

[1] David A. Curry: "Improving the security of your UNIX system", SRI International, 1990.
[2] John McMahon: "Survival on the Internet", 1992 Spring DECUS Symposium (presentation)
[3] Solaris 2.2 Manual Pages, Sun Microsystems, Inc.

A SZÁMÍTÓGÉPES BŰNÜLDÖZÉS ELKÖVETÉSÉNEK MÓDJAI

Szüle László

BM Tolna Megyei TÁKISZ Szekszárd

A számítógépes bűnözés viszonylag új kategória, bár megjelenése megfigyelhető a számítástechnikai eszközök alkalmazásának korai szakaszában is. Az alkalmazók számára egyre fokozódó veszélyt jelent e bűnözés, elkövetésének módjai szinte kimeríthetetlenek. A fejlett informatikával rendelkező országok jogrendjükben nálunk korábban szankcionálták a számítógépes bűnözést. Magyarországon fontos feladat, hogy e téren megszüntessük a jogrendszerünkben meglévő hézagokat, hiányosságokat.

1. A SZÁMÍTÓGÉPES BŰNÖZÉS KIALAKULÁSA ÉS JELENLEGI HELYZETE

A számítógépes bűnözés (computer crime) viszonylag új kategória. Sokat és sokan vitatkoznak arról, hogy vajon szinonim fogalom-e a számítógéppel kapcsolatos bűnözéssel (computer related crime). Az angol szakirodalom mindenesetre homonim (azonos alakú, de eltérő jelentésű) fogalomként kezeli ezeket a fogalmakat.

A számítógépes bűnözés fogalmán minden olyan tényállás értendő, amelyben az elektronikus adatfeldolgozás a tett eszköze és/vagy a tett tárgya, és amelyek megalapozzák egy bűntett gyanúját.

Donn B.Parker neves amerikai szakíró az 1970-es években nagy feltűnést keltett könyvével, melyben az addig ismertté vált 669 számítógépes bűnesetet tárta fel. Ezek közül az egyik legismertebb módszer az úgynevezett "szalámi módszer", amikor a programmanipuláció kamatszámítás, bérszámfejtés esetén a kerekítéseket gyűjti a programozó saját számláján. E módszernek sajátossága, hogy tulajdonképpen nincsenek kárvallottak, akik keresnék pénzüket, hiszen csak minimális veszteség érte őket, de több ezer számlatulajdonosnál e módszer alkalmazása jelentékeny összeget tehet ki, például egy ismert esetben 80 ezer dollárt "gyűjtött össze" így egy programozó a saját számláján.

Kezdetben "fehér galléros" bűnözőkről beszéltünk. A bűnözés bonyolultabbá válásával ma "intellektuális bűnözésről" beszélünk, utalva arra, hogy az elkövetéshez nagyfokú tudás, intellektus szükséges.

Az idei évben eléggé ismert az az eset, amikor az INTERNET hálózatban néhány óra alatt 4000 számítógépet fertőztek meg illetéktelen behatolók.
"A rendszergazdák a világon mindenütt pánikszerűen lecserélték az addig érvényes jelszavakat a számítógép-hálózatokban.
Tették mindezt a CERT, az amerikai kormány által üzemeltetett INTERNET-figyelő szolgálat ama közleménye nyomán, amely több tízezernyi számítógépes hozzáférési jogosultság sérülését tartotta lehetségesnek. Tényleges betörést azonban csak néhány amerikai egyetem jelzett - egyiküknél például egy hetes leállást és számos állomány megsérülését okozta a támadás - de a többség tagadta, hogy bármiféle zavar keletkezett volna a hálózatában". (1)

A téma fontosságát mutatja, hogy ma már ENSZ dokumentum foglalkozik a számítógépes bűnözéssel.

Az FBI becslése szerint a manuális módszerekkel elkövetett csalások átlagos értéke 23 ezer dollár, míg a számítógépes környezetben elkövetett csalásoké 600 ezer dollár.
Más publikáció szerint egy számítógépes bűncselekményre 3.322.000 dollár, míg egy fegyveres bankrablásra 115.000 dollár jut.

A veszélyek tehát anyagi és egyéb szempontból beláthatatlanok.

2. A SZÁMÍTÓGÉPES BŰNÖZÉS ELKÖVETÉSÉNEK KÖRÜLMÉNYEI

A bűn elkövetésének alapvető feltétele a bűnös szándék. Ellenkező esetben legfeljebb gondatlanságról beszélhetünk. Azt is tisztázni kell, hogy mi az ami a jog szerint etikátlan, ám mégis belefér a jogi szabályozásba és mi a valóban illegális cselekmény, a büncselekmény. A jogi válasznak, megtorlásnak ezzel arányosnak kell lennie. Bűncselekmény fogalmának kimerítéséhez vagyoni kár okozása és a társadalomra való veszélyesség bizonyítása is szükséges.

A számítógépes bűnözés szereplői:

Potenciális áldozat (bárki lehet)	-	Potenciális elkövetők: intelligens, nagyszerű átlátó- és szintetizáló képességekkel rendelkezők, akik az erkölcsi értékekkel állnak hadilábon.

RICHARD H.BAKER Computer Security Handbook című munkájában olvasható az a meghökkentő adat, hogy az ismertté vált

számítógépes bűncselekmények a valóban elkövetetteknek mindössze 1-10 százalékát teszik ki.

Az alkalmazottaknak kb. 40 %-a feltétlenül becsületes, 30 %-a bizonyos körülmények között képes kriminológiai tett elkövetésére, a maradék 30 % pedig aktuálisan is keresi annak a lehetőségét, hogy illegális előnyhöz jusson. Ezt az ökölszabályt az USA ipari környezeteiben végzett több felmérés és számos tanulmány is alátámasztja, így pl. az US COMMERCE DEPARTEMENT 1983-as tanulmánya, mely szerint az alkalmazottak kb. 1/3-a lop a vállalatától. Gondolkodjunk el ezen!

Hűtlenség elkövetésére soha nem volt egy átlagos alkalmazott számára akkora lehetőség és persze kísértés, mint manapság, amikor szinte mindenkinek a keze ügyében van egy hálózati számítógép. Az American Bar Association által közelmúltban készített tanulmány azt mutatta ki, hogy a számítógépes bűnesetek 78 %-ában a megkárosított intézmény állományába tartozott az elkövető.

A számítógépes bűnözés elleni védekezésnél több probléma is felmerül:

- az ehhez a területhez kapcsolódó bűncselekmények nehezen mutathatók ki (nincs bizonyíték),

- egy felismert bűntett esetén sem mindig bizonyítható az elkövető személye,

- a számítógépeknek nincs intelligenciájuk és áttekintő képességük, így nem ismerik fel, hogy kijátszák őket,

- átlagos felhasználó nem ért annyit a számítógépekhez, hogy egy bűntettet idejében felismerjen.

Miért sebezhető a számítógép? Mert:

- a működésük során keltett elektromágneses tér útján kisugározzák a bennük zajló folyamatokat, amelyek megfelelő vevővel és értelmező programmal adatokká alakíthatók. Sőt kívülről keltett elektromágneses kisugárzással még bizonyos gépek működése is befolyásolható,

- az emberi tényező veszélyei is igen fontosak (privilegizált jogok),

- a bemenő információk és az adatfeldolgozó eszközök, a számítástechnikai adatok és adattárak, a számítógépes berendezések, az output és maga a kommunikáció is támadási felületet kínál a bűnözőknek.

3. A SZÁMÍTÓGÉPES BŰNÖZÉSI FORMÁK ISMERTETÉSE

Németországban 1987. óta van érvényben a Gazdasági bűnözés elleni kűzdelemmel foglalkozó második törvény. A számítógépes bűnözést a következő kategóriákba sorolja:

- Pénzkiadó, illetve pénztár automatákkal kapcsolatos csalás: Az emberiséget már régóta izgatja az a probléma, hogyan lehet munka nélkül pénzt szerezni. Alighanem ez a legegyszerűbb módja. Ugye hallottak már Önök a magyar telefonkártyával kapcsolatos csalásokról? Ide tartozik többek között a hitelkártya hamisítás, vagy ha az eredeti hitelkártyát többször lemásolják.

- Számítógépes csalás (a német jog fogalmai szerint):
"Aki szándékosan vagy részben jogtalanul szerez számottevő előnyt oly módon, hogy az adatfeldolgozás eredményét hamis programmal, megváltoztatott vagy hiányos adatokkal, vagy illetéktelen adatok felhasználásával befolyásolja, az öt évig terjedő szabadságvesztéssel vagy pénzbírsággal büntetendő". (2)

- Bizonyíték jellegű adatok meghamisítása és jogi eljárásokkal kapcsolatos megtévesztés,

- Adatok megváltoztatása, számítógépes szabotázs:
Az adatok inputjának manipulációja a leggazdaságosabb és a legnehezebben felfedezhető cselekmény.

- Adatok kikémlelése,

- Számítógépszoftver-kalózkodás:
  - programok módosítása, törlése,
  - számítógépes programok és adatbázisok vírusokkal, vagy trójai programokkal, esetleg másolásvédelmi büntetőrutinokkal történő rongálása (legritkábban bizonyítható a jog által megkívánt igényességgel),

- Hacking (számítógépek működésének káros befolyásolása)
Külső támadási lehetőségek:

  - lehallgatás,
  - megszemélyesítés (más nevében fellépés),
  - üzenet hamisítás,
  - üzenet elvétel,
  - üzenet betoldás.

- Üzemi és üzleti titkok elárulása,

- Illegális technológia átadás: mely veszélyezteti a számítógép konstrukcióját, vagy magát a feldolgozási folyamatot (így könnyebben sebezhető a rendszer),

- Visszaélés számítógépekkel:
  - gépidő eltulajdonítás,
  - számítógépes hamisítás.

- Egyéb számítógépes csalás (minden, ami az előzőekbe be nem sorolható)

Más csoportosítás szerint legalább hét olyan terület van, amely az információval kapcsolatos visszaélések forrása lehet. Ezek a hét E-nek is nevezett veszélyterületek a következők:

- hiba (error),
- elektronikus lehallgatás (eavesdropping),
- ellenségeskedés (enmity),
- kémkedés (espionage),
- sikkasztás (embezzlement),
- személyiség (ego),
- zsarolás (extortion).

A számítógépes bűnözés módjai a technikai fejlődés függvényében jóformán kimeríthetetlenek. A visszaélések számának emelkedő tendenciája mellett, a visszaélések által okozott károk nagysága is nő.

4. A SZÁMÍTÓGÉPES BŰNÖZÉS JOGI SZANKCIONÁLÁSA A MAGYAR JOGRENDSZERBEN

A számítástechnikai kultúra terjedésével természetesen nálunk is törekedtek a számítógépes bűnözés jogi úton történő megfékezésére. Elegendő itt arra hivatkoznom, hogy az adatok védelmét közel 30 jogszabály biztosítja. Ezek közül a néhány legfontosabb:

- 1978. évi IV. törvény a Büntető Törvénykönyvről, mely az alábbi minősített eseteket írja elő:

  - jogosulatlan adatkezelés,
  - különleges személyes adatokkal visszaélés,
  - az államtitok és a szolgálati titok megsértése,
  - számítógépes csalás: aki jogtalan haszonszerzés végett, vagy kárt okozva valamely számítógépes adatfeldolgozás eredményét a program megváltoztatásával, törléssel, téves vagy hiányos adatok betáplálásával, illetve egyéb, meg nem engedett műveletek végzésével befolyásolja, büntettet követ el és három évig terjedő szabadságvesztéssel büntetendő.

    A büntetés
    - öt évig terjedő szabadságvesztés, ha a számítógépes csalás jelentős kárt okoz,
    - két évtől nyolc évig terjedő szabadságvesztés, ha a számítógépes csalás különösen nagy kárt okoz.

- 1959. évi IV. törvény a Magyar Köztársaság Polgári Törvénykönyvéről, mely a következő jogsértést szankcionálja:

  - a személyhez fűződő jogok megsértése,
  - polgári jogi felelősség, mely nem vagyoni kárra is kártérítést ír elő.

- 1968. évi I. törvény a Szabálysértésekről, mely az itt felsorolt szabálysértéseket büntetni:

  - Adatvédelmi szabálysértés, aki
    - a technikai adatvédelem követelményeinek nem tesz eleget,
    - az érintettet a személyes adatok védelméhez vagy a közérdekű adatok nyilvánosságához való jogának gyakorlásában akadályozza.
  - Titokvédelmi szabálysértés.

- Számos törvény előírja a titoktartási kötelezettséget (pl. egészségügyben, pénzintézetekben, postánál, távközlésben, statisztikában stb.).

5. A SZÁMÍTÓGÉPES BŰNÖZÉS ELLENI JOGALKOTÁS IDŐSZERŰ FELADATAI MAGYARORSZÁGON

Hazánkban fontos feladat a jogállamiság megteremtése. Ez magával kell, hogy hozza a számítógépes bűnözés teljeskörű jogi szankcionálását is. Fontos feladat a már meglévő jogi szabályzások megismertetése, illetve a még hiányzó jogszabályok kidolgozására egy jogszabályalkotó munka megindítása, a jogszabályi hézagok megszüntetése.

Sűrgetően szükség lenne a számítógépvírusok fejlesztése és tudatos terjesztése, az adatlopás, a számítógépes szabotázs, távadatközlő rendszerek elleni büncselekmények jogi szankcionálására. E felsorolás korántsem teljes. A jelenleg meglévő jogszabályok szükségesek, de nem elégségesek.

E jogszabályalkotó munkában együttműködő partnerek lehetnek:

- Igazságügyminisztérium,
- Belügyminisztérium,
- Ügyészek Országos Egyesülete,
- Szerzői Jogvédő Hivatal,
- Magyar adatvédelmi biztos,
- NJSZT, vagy annak Etikai Bizottsága, vagy Számítástechnikai Kamara.

E közös és felelősségteljes munkához jó együttműködést, szívós kitartást és sok sikert kívánok!

IRODALOMJEGYZÉK, HIVATKOZÁSOK

Dr. BORDA JÓZSEF: Számítógépes rendszerek ellenőrzése és biztonsága
KSH SZÁMOK Budapest 1978.

(1) SZÁMÍTÁSTECHNIKA: Támadás az INTERNET ellen
1994. 02. 22. 94/8. szám

SZÁMÍTÁSTECHNIKA: SCHUKKERT ANDRÁS (ORFK) nyilatkozata
1993. november 23.

HISEC '93 Konferencia előadásai

(2) MICHAEL HORSCH: Számítógépvírusok
Műszaki Könyvkiadó 1992. 116. oldal

1978. évi IV. törvény a Büntető Törvénykönyvről

1959. évi IV. törvény a Magyar Köztársaság Polgári Törvénykönyvéről

1968. évi I. törvény a Szabálysértésekről

NJSZT Etikai Kódexe 1993.

Számítógép és ellenőrzés

a számítógépes ellenőrzési és adatvédelmi ismeretek "terjedésének" lehetséges formái

Csajbók Zoltán

Adó- és Pénzügyi Ellenőrzési Hivatal

Szabolcs-Szatmár-Bereg megyei Igazgatósága

KIVONAT

Az adatvédelem és adatbiztonság témakörében az Európai Közösségben széleskörű *elméleti* kutatások folynak egy jól megalapozott módszertan kidolgozására. A következőkben egy alapvetően más alapfilozófián nyugvó konstrukció kerül bemutatásra. Elsőként a számítógépes ellenőrzési és adatvédelmi ismereteknek a *mindennapokban* betöltött fontos szerepére mutatunk rá. Ezt követően ezen ismeretek két hagyományosnak tekinthető "terjedési" formáját, az *oktatást*, és az ellenőrzési ismeretek egyik legnagyobb felhasználójának, az *adóhivatal számítógépes ellenőrzési gyakorlatát* tekintjük át vázlatosan. Ezek mintegy ellenpontul szolgálnak alaptémánk kifejtéséhez, egy 25 éves nemzetközi számítógépes ellenőrzési szervezet, az Információrendszerek Ellenőrzési és Kontroll Egyesülete gyakorlatának bemutatásához. Ez a szervezet tagjai *öntevékenységére* épít, és a tagság napi munkája során szerzett *tapasztalatokból* igyekszik egy jól szerkesztett elvi-gyakorlati módszertant kidolgozni.

1. SZÁMÍTÓGÉP, ELLENŐRZÉS ÉS ADATVÉDELEM A MINDENNAPOKBAN

A számítógépes információrendszerekben tárolt adatok védelme és biztonsága, az információfeldolgozás minősége egyre égetőbb kérdéssé válik. Gyakran nem is gondolunk arra, hogy milyen óriási kockázatokkal (is) jár egy számítógépes rendszer alkalmazása, használata. Különösen igaz ez akkor, ha nem ötvöződik korszerű ellenőrzési ismeretekkel, illetve az adott környezethez legjobban illeszkedő védő-megelőző adatvédelmi intézkedésekkel. A számítógép megjenésével egy hallatlan *térbeli adatkoncentráció* megy végbe: egy rendkívül szűk térrészbe (ez ma gyakran csak néhány dm^3) zsúfolódik össze valamely szervezet valamennyi igen fontos és értékes adata. A számítógépes információs rendszerek biztonsága tehát rendkívül élesen vetődik fel: *vagy meg tudjuk őrizni a teljes adattömeg épségét és biztonságát, vagy igen nagy valószínűséggel a teljes adattartalom vész el, illetve válik hozzáférhetővé arra illetéktelen személyek számára.*

A számítástechnika széleskörű elterjedésével párhuzamosan rohamos tempóban nő a kevésbé képzett szoftvervásárlók aránya is. Ők "egyszerű" szolgáltatásként veszik meg a számítógépes programokat. Nyilvánvalóan kiszolgáltatott helyzetben vannak, hiszen esetleg még azt sem tudják megitélni, hogy mire képes egy program. Nem beszélve annak megitéléséről, hogy amit igér azt ténylegesen és megfelelő minőségben tudja-e?

Szakmai körökben egyre terjed az a nézet, hogy ki kellene találni valamiféle szoftverminősítési szisztémát. Mindez azonban számos elvi-jogi-etikai kérdést vet fel: Legyen egy számítástechnikai "Kiváló áruk fóruma"?! Szakmai vagy érdekképviseleti szervezetek vállaljanak-e fel ilyen feladatokat? Vagy magáncégek foglalkozzanak mindezzel? Nemkevésbé súlyos kérdés, hogy ki és milyen jogon végezhet ilyen minősítéseket? Hogy lehetne például kizárni az összefonódásokat, a részrehajlásokat? Aki kedvező minősítést kap az nyilvánvalóan nem különösebben tiltakozna ezen döntés/vélemény ellen, a rendszer működésének elvi problémái sem izgatná - de akire nézve kedvezőtlen végeredmény születik...? Vagy mindezt bízzuk kizárólag a piacra?

Az ellenőrzés tartalmi követelményei az adatfeldolgozás számítógépesítésével nem változnak meg. Magától értetődő azonban, hogy például egy számítógépes számviteli rendszert nem lehet pusztán a hagyományos módszerekkel ellenőrizni, végrehajtásához alapvető számítástechnikai ismeretekre mindenképp szükség van. Az összetettebb esetek - mint például egy számítógépes visszaélés felfedése - az alapismereteken túlmenően még mélyebb és még speciálisabb tudást tételez fel, amely esetleg már csak számítástechnikai szakember bevonásával oldható meg. *Számítógépes környezetben tehát, a célok változatlansága mellett, az ellenőrzés új módszereire van szükség.*

Az ellenőrzés szó hallatán általában egy állami hatóság központilag szervezett külső ellenőri tevékenységére asszociálunk. Ezzel szemben - pontosabban: e mellett - egy ellenőr fontos feladata lehet, hogy elemezze és értékelje, *akár üzleti alapon is*, megbízója információs rendszerét és tudjon jobb megoldást javasolni ha valamit nem talál rendben. Ez túlmutat a nálunk hagyományosnak tekinthető ellenőrzés-felfogáson: ez esetben az ellenőr egy számítógépes információrendszert, *mint terméket értékel és minősít* (amolyan számítógépes MEO funkciót tölt be). Az ellenőrzés eredményéről jelentés (beszámoló) készül, amely az átvizsgált rendszert kritikusan véleményezi, és - a biztonságos működtetés érdekében - javaslatokat ad a hibák kijavítására.

Nyugaton általában csak az említett vizsgálatokon átesett és jó minősítést kapott rendszerek a piacképesek. Magyarországon jelenleg még csak néhány cég nyújt ilyen jellegű szolgáltatást. Biztos

azonban, hogy előbb-utóbb mind a szoftverfejlesztők, mind az alkalmazók tudatára ébrednek annak, hogy az ő (anyagi!) érdekük is az általuk fejlesztett, illetve használt számítógépes rendszerek szakmai minősítése.

Az információrendszer ellenőrzés illetve az adatvédelem és adatbiztonság között a nyilvánvaló különbözőségek mellett számtalan kapcsolódási pont is van. A két szakterület műveléséhez szükséges számítástechnikai ismeretanyag jórészt azonosnak tekinthető, inkább a hagsúlyokban van eltérés. A legtöbb kidolgozott eljárást, módszert egyaránt hasznosítani tudja mind az ellenőrzési szakember, mind az adatvédelemi felelős. A továbbiakban ezen ellenőrzési-adatvédelmi ismeretek lehetséges *"terjedési" formáit* vesszük számba. Néhány példán keresztül azt vizsgáljuk meg, hogy ez a kiterjedt és kétségkívül fontos tudásanyag milyen úton-módon juthat el az érintettekhez, miképpen épülhet be a számítógépes - és nem számítógépes! - társadalom mindennapi tevékenységébe, életébe.

2. SZÁMÍTÓGÉPES ELLENŐRZÉSI ISMERETEK OKTATÁSA

A '70-es évek végétől egészen a '80-as évek közepéig minden bizonnyal túlzás nélkül állítható, hogy világszínvonalú volt Magyarországon e szakterület művelése. Ez egyszerre két dolgot is jelentett: egyrészt a számítógépes ellenőrzési ismeretek többé-kevésbé szinkronban álltak az e téren fejlett országok elméleti tudásával. Másrészt - legalábbis elvi szinten - lépést tartott a számítástechnika fejlődésével. Azóta azonban úgy tűnik, hogy kb. a kötegelt (batch) feldolgozás után, valahol az adatbázisok és az online feldolgozások kezdeteinél megállt a fejlődés.

Egy számítógépes rendszer biztonsága igen összetett kérdés. Így nem meglepő, hogy e probléma-együtteshez kapcsolódva a nálunk fejlettebb számítástechnikai kultúrával rendelkező országokban kialakult egy új foglalkozási ág, az úgynevezett *információrendszer ellenőrzés (számítástechnikai szakrevízió);* aki pedig e szakterületet műveli az az *információrendszer ellenőr (számítástechnikai szakrevizor).* A számítástechnikai szakrevízió eredendően interdiszciplináris szakma, szükségképpen több szakterület ismeretanyagából is merít:

- mindenekelőtt számítástechnikai, illetve a vizsgált szakterületre vonatkozó jogi, szakmai ismeretek;
- rendszerelmélet, rendszerszervezés;
- üzem- és munkaszervezés;
- adatvédelem, adatbiztonság stb.

Néhány évvel ezelőtt még hazánkban is külön "szakma" volt a számítástechnika és az ellenőrzés kapcsolatával foglalkozni, a szakrevizori ismeretanyagot külön képzés keretében is el lehetett sajátítani. Jelenleg ilyen lehetőség nincs, nyilvánvaló célszerű lenne ismét beindítani, az igény mindenképp létezik.

A szakrevizori képzés újraindítását az is indokolja, hogy a tanult ismeretek felhasználási, alkalmazási területe, *széles elméleti háttere* és *szoros gyakorlati kötődése* miatt, rendkívül sokirányú. A "gyakorló" ellenőrök illetve adatvédelmi felelősök munkájához természetesen nélkülözhetetlen. Van azonban néhány olyan terület, ahol a felhasználás lehetősége nem ennyire kézenfekvő, de annál hasznosabb lehet:

- Hatékonyan felhasználható gazdálkodó szervezetek *felső- és középszintű vezetőinek* irányító tevékenységében. Segítséget nyújthat pl. egy számítógépes információrendszer megtervezésének, kivitelezésének és működtetésének irányításhoz és ellenőrzéséhez; vagy számítógépes eszközök, alkalmazói programok beszerzéséhez.

- Helyet kaphat *belső ellenőrök* tevékenységében is. Tevékenységi - ellenőrzési - körük kibővül(het) például számítóközpont működésének, számítógépes alkalmazási rendszerek fejlesztésének, valamint mindezek folyamatos üzemeltetésének *felügyeletével*. A nemzetközi tapasztalatok azt mutatják, hogy számítógépes rendszerek esetén a belső ellenőrzés súlypontja az eredmények kiértékeléséről és jóváhagyásáról a *feldolgozás folyamatába épített* ellenőrzési módoknak a megtervezésére, értékelésére és jóváhagyására terjed ki.

- A *folyamat- és rendszerszervezők, valamint programozók* munkájuk során közvetlenül használhatják fel a rendszerfejlesztés és az implementációs munka során a szakrevizori ismereteket.

Az nem valószínű, és minden bizonnyal nem is szükséges, hogy valamely felsőfokú tanitézet önálló szakként beindítana egy információrendszer ellenőri képzést. Mindenképp célszerű lenne azonban, ha az ellenőrzési illetve adatvédelmi ismeretek valamilyen formában *megjelennének* a számítástechnikát hallgatók tantervében. Másik lehetőség szakmai szervezetek, magáncégek bekapcsolódása a szakrevizori oktatás megszervezésbe.

3. SZÁMÍTÁSTECHNIKAI SZAKREVÍZIÓ AZ APEH-BEN

Abból kiindulva, hogy számítógépes környezetben a módszerek, eszközök változása mellett az ellenőrzési céloknak változatlanoknak kell maradniuk, az adóhivatalban a számítástechnikai szakrevízió az ellenőrzés *egyik* módszere, és *nem térhet el az adóellenőrzés céljaitól.* A szakrevizori ellenőrzések célja általánosságban annak megállapítása, hogy a számítógépes feldolgozás, illetve annak eredménye mennyiben felel meg az érvényes rendeleteknek, törvényi előírásoknak. Az adóhivatal a számítógépes információrendszerek ellenőrzésének nemzetközileg is elfogadott szempontjai közül a valódiság és szabályszerűség, a teljesség, az operativitás, az ellenőrizhetőség és a biztonság vizsgálati szempontjait érvényesíti.

A számítástechnikai szakrevíziók tervezésének és irányításának elveiről az APEH Elnökének 13/1989. számú utasítása szól (Adó és Ellenőrzési Értesítő, I. évfolyam 4. szám). Az utasítás a szakrevízió elveiről megállapítja, hogy az az adóellenőrzés szerves része, így azzal együtt kell kezelni mind a megbízólevél, mind az indító értekezlet, valamint a vizsgálati program ügyében is. A szakrevizor részére külön megbízólevél nem készül, nevét az adóellenőrzést végző revizor megbízólevélre kell rávezetni. A helyszíni tájékozódást követően a szakrevizor az adóellenőrzés programja alapján "Szakrevizori vizsgálati program" javaslatot készít, amelyet a vizsgálatvezető revizorral egyeztet, szignáltat. A szakrevizori vizsgálati program főbb szerkezeti részei:

- a gazdálkodószerv jelenlegi (és tervezett) számítástechnikai helyzetének áttekintése;
- a kijelölt számítógépes rendszer(ek) működési megoldásának célorientált ellenőrzése;
- az adóellenőrzés programjában foglaltak számítástechnikai adaptációja.

A számítástechnikai szakrevizor észrevételeiről, megállapításairól, a program végrehajtásáról szakrevizori jelentést készít. Az ebben foglaltakat egyezteti a vizsgálatvezető revizorral és a gazdálkodószerv illetékes vezetőivel. E jelentésből a jegyzőkönyvezendő megállapításokat a szakrevizor - a vizsgálatvezető revizorral együttműködve - a jegyzőkönyvvezetés előírásainak megfelelően is megfogalmazza. A megállapításokat a vizsgálatvezető revizor beépíti az adóellenőrzés jegyzőkönyvének megfelelő fejezetébe, illetve a szabályszerűséget értékelő jelentésbe. (A szakrevizori ellenőrzések szakmai tapsztalatait az APEH szaklapjában, az APEH HÍR-ADÓ 1993. 12. számában Filó Mihályné foglalta össze részletesen.)

4. INFORMÁCIÓRENDSZEREK ELLENŐRZÉSI ÉS KONTROLL EGYESÜLETE

4.1 Egy öntevékeny szakrevizori szervezet

A fejlett számítástechnikai kultúrával rendelkező országokban a nagyobb cégek, különösen a pénzintézetek főállású információrendszer ellenőrt (szakrevizort) alkalmaznak. Sőt, nemzetközi szervezetük is van, amelyet 1969-ben (!) a kliforniai Los Angelesben dolgozó szakrevizorok alapítottak. Ma is ez az egyetlen olyan, az egész világra kiterjedő nemzetközi szervezet, amely kifejezetten számítógépes rendszerek ellenőrzésével, biztonsági problémáinak megoldásával foglalkozó szakembereket tömörít.

Ez a szervezet az Electronic Data Processing Auditors Association, Inc., vagy rövidebben EDP Auditors Association, illetve angol nyelvű rövidítéssel: EDPAA. Magyarul, nem egészen szó szerinti fordításban: Elektronikus Adatfeldolgozó Rendszer Ellenőrök Nemzetközi Szövetsége. A szervezet 25 éves fennállása alatt a számítástechnika rohamos fejlődésen ment át: egykor elképzelhetetlen (vagy éppen, hogy csak a képzeletben élő) képességű számítógépek használata vált *mindennaposság*. E lényegi változásra tekintettel a szervezet 1994 júniusától új nevet választott: *The Information Systems Audit and Control Association (ISACA) - Információrendszerek Ellenőrzési és Kontroll Egyesülete*. Az ISACA szervezeti felépítése többszintű:

- Alapzatát, legszélesebb rétegét az ún. chapterek képezik. Magyarul tagozatnak vagy tagszervezetnek lehet fordítani. A tagszervezeteket közvetlenül a tagok alkotják.
- A tagszervezetek földrajzi szerveződés alapján ún. régiókat (regions) alkotnak. Összesen 10 régió van:
    1. régió: Western United States (nyugat USA)
    2. régió: Midwestern United States (közép-nyugat USA)
    3. régió: Northeastern United States (észak-kelet USA)
    4. régió: Southwestern United States (dél-nyugat USA)
    5. régió: Central and South America (Közép- és Dél-Amerika)
    6. régió: Canada (Kanada)
    7. régió: Southeastern United States (dél-kelet USA)
    8. régió: Australia and New Zealand (Ausztrália és Új-Zéland)
    9. régió: Africa, Europe and Middle East (Afrika, Európa és Közel-Kelet - Magyarország!)
    10. régió: Asia (Ázsia)

- És végül van maga az ISACA, amely széleskörű szolgáltatásaival áll tagsága rendelkezésére, és koordinálja a teljes szövetség munkáját.

A tagszervezetek 1979-ban létrehoztak egy alapítványt, amely az ISACA mellett működik: EDP Auditors Foundation (EDPAF). Célja a szervezet üzleti tevékenységének, a továbbképzések, a kutatás-fejlesztés, valamint a kiadványszervezés irányítása, szervezése.

A nemzetközi szövetségnek a világ minden tájáról vannak tagjai: számuk jelenleg 13.000 fő körül van, és a világ közel 60 országában 130 helyi tagszervezet működik. A tagság a legkülönbözőbb szakterületekről, a legkülönbözőbb beosztásokból kerül ki: külső és belső ellenőrök, a közigazgatási szférában (pl. adóhivatal) dolgozó revizorok, pénzügyi-banki revizorok, programozók, rendszerszervezők, adatbázis adaminisztrátorok, adatvédelmi szakemberek, egyetemi és főiskolai tanárok stb. stb.

Az első nemzetközi (tehát nem amerikai) szervezet 1975-ben alakult Mexikóvárosban és az ausztráliai Sydney-ben. Európában Olaszországé az elsőség dicsősége: Milánóban alakították meg az első európai szervezetet.

A "jubileumi" 125. tagszervezet - egyszersmind Kelet-Európában az első és mindmáig az egyetlen - Magyarországon alakult meg dr. BORDA József irányítása mellett. Hivatalos neve: Információrendszer Ellenőrök Egyesülete. Ezzel lehetővé vált, hogy az ISACA nemzetközi szervezetnek hazánk szakemberei is tagjaivá válhassanak. A belső ellenőrzés és az információrendszer ellenőrzés szoros kapcsolatára utal az is, hogy a magyar tagszervezet egyben tagja a belső ellenőrök nemzetközi szervezetének is, a The Institute of Internal Auditors, azaz a Belső Ellenőrök Intézetének.

Az egyesületnek bármely *természetes személy* (egyelőre csak természetes személy) lehet tagja. A tagsági feltételek nem túl kötöttek: "csak" azt várják el a tagoktól, hogy - a tagsági díj megfizetése mellett - betartsák az egyesület etikai kódexét és az egyesület szakmai szabályainak megfelelően végezzék munkájukat.

A tagsági díj évi 15.000 Ft, amely nagyságrendileg megfelel az egyesület által nyújtott ingyenes szolgáltatásoknak és kedvezményeknek. A tagdíjat *munkatársára nevesítve* természetesen bármely munkáltató is befizetheti.

A tagdíj ellenében az ISACA tagjainak átfogó szolgáltatásokat nyújt: széleskörű szakmai fórumok; az ellenőrzés etikai kódexének illetve szabványainak kidolgozása: kutatások támogatása; nemzetközileg elismert szakrevizori képesítést nyújtó vizsgarendszer működtetése; folyamatos továbbképzés; publikálási lehetőségek, ellenőrzési szakkönyvek kiadása, terjesztése.

SZÉLESKÖRŰ SZAKMAI FÓRUM. Minden tagozat havonta egyszer szakmai találkozót szervez egy-egy témáról (ez természetesen a tagság önnön aktivitásának is függvénye). Ez a nagyon fontos közvetlen személyes találkozásokra ad lehetőséget a legkülönfélébb szakterületeken dolgozó, de az ellenőrzési kérdésekben közösen érintett szakemberek számára. A régiók illetve maga az ISACA is szervez szakmai fórumokat, konferenciákat. Ezeket a tagok kedvezményes áron vehetik igénybe.

SZABVÁNYOSÍTÁS. A számítástechnika fejlődésével párhuzamosan robbanásszerűen fejlődik azok alkalmazása is. Mindezzel az ellenőrzésnek is lépést kell(ene) tartania. Az ISACA egyik konferenciáján, az Egyesült Államokbeli Salt Lake-ben, 1985-ben határozták el, hogy ellenőrzési standardokat, azaz ajánlásokat, irányelveket dolgoznak ki.

E célból megalakították a Standards Board-ot (Szabványosítási Igazgatóság) valamint a Standards Comittee-t (Szabványosítási Bizottság). Ezen testületek célja olyan etikai kódex és szakmai szabványok kidolgozása valamint folyamatos felügyeletük, "karbantartása", amelyek a számítógépes ellenőrzések vezérfonalául szolgálhatnak, *amikhez képes ellenőrizni lehet.* 1985 óta folyamatos erőfeszítések történnek ezen szabványok finomítása és aktualizálása, illetve széleskörű megismertetésük, elterjesztésük érdekében. A tagoktól elvárják, hogy ezeknek megfelelően végezzék munkájukat.

KUTATÁSOK. Az ISACA alapítványi része, az EDPAF szervezi és irányítja, támogatja a kutatási projekteket. Ezek alapvető célja az előbb említett ellenőrzési szakemberek számára szóló etikai kódex és szabványok elméleti - egyszersmind gyakorlati - hátterének megalapozása.

KÉPESÍTÉS. Az ellenőrzési szabványok elterjesztésének és betartásának elősegítése és nem utolsósorban az információrendszer ellenőrök szakmai felkészültségének lemérése céljából az ISACA egy ún. Certified Information Systems Auditor (CISA - Okleveles Információs Rendszer Ellenőr) szakvizsga programot működtet. Az eredményes vizsgához a jelöltnek egyrészt bizonyos szakmai gyakorlattal kell rendelkeznie, másrészt egy meglehetősen nehéz és átfogó vizsgát kell letennie.

A CISA vizsga lebonyolítását, adminisztrációit a világ minden részén megtalálható több mint 130 ún. teszt központból álló nemzetközi hálózat végzi. Jelenleg 8 nyelven lehet vizsgát tenni: holland, angol, francia, német, héber, olasz, japán és spanyol nyelveken. Vizsgázni egy évben csak egyszer lehet. A "vizsgaidőszak" minden év júniusában van. A CISA képesítés azonban nem örökéletű cím: aki egyszer megkapta annak vagy folyamatos továbbképzésen kell részt vennie vagy újra le kell tennie a vizsgát ahhoz, hogy oklevelét megtarthassa. Jelenleg kb. 11.500 személy rendelkezik ezzel a képesítéssel.

FOLYAMATOS TOVÁBBKÉPZÉS. Az ISACA a legkülönfélébb értékes oktatási programokat támogat szerte a világon. A tagok révén egyre növekvő számban, egyre több főiskolán és egyetemen indulnak be az információrendszerek ellenőrzésével kapcsolatos kurzusok. A helyi szervezetek is szerveznek regionális és globális konferenciákat.

PUBLIKÁLÁS. A jövő fejlődési irányába eső publikációk széles választékát nyújtja az ISACA. Ennek keretében a tagok számos szolgáltatást vehetnek igénybe:

Control Objectives - Ellenőrzési célok: Átfogó kézikönyv, amely szabályzat formájában a hatékony információrendszer ellenőrzések alapvető követelmény- és célrendszerét, módszertani alapelveit rögzíti. Ismeretanyagát a számítástechnika fejlődésével párhuzamosan állandóan aktualizálják. Használata feltétlenül ajánlott gyakorló információrendszer ellenőröknek. Tagoknak díjmentes.

The EDP Auditor Journal: Az ISACA elektronikus adatfeldolgozás ellenőrzési kérdéseivel foglalkozó szakfolyóirata. Cikkei segítségével naprakészen követhetők a legújabb információrendszer ellenőrzési ismeretek, módszerek, az új szoftver eszközök (ellenőrzési programcsomagok) stb. Tanulságképpen beszámol rázósabb számítógépes visszaélésekről is. Tagoknak szintén díjmentes.

General Standards for Information Systems Auditing and Statements on Information Systems Auditing Standards: A Szabványosítási Igazgatóság (Standards Board) és a Szabványosítási Bizottság (Standards Comittee) hivatalos kiadványa a szabványokról.

Szakkönyvterjesztés; az EDPAF alapítvány publikációi: Szakkönyvek széles választéka; továbbá tudományos művek, monográfiák, oktatási kézikönyvek és szakfolyóiratok.

Felkészítő anyagok a CISA vizsgára: Kidolgozott minta tesztek megoldásokkal; számítógépes oktató programok; CISA vizsgára jelentkezők kézikönyve: A Candidate's Guide to the CISA Examination.

4.2 Az elméleti kutatás szervezete

Az elméleti kutatások a tagság széleskörű részvételén nyugszanak: a szervezet *bármely* tagja javasolhat témát, továbbá a kutatás beindításának legelső lépése az *érdeklődő szakemberek (tagok) összegyűjtése.* Egy kutatási projekt témájának meghatározása kétféle módon történhet: egyrészt az EDPAF Kutatási Igazgatósága (Research Board) "hivatalosan" kijelöli a problémát, másrészt a tagok javaslata alapján. A program hivatalos kijelölésére a szakmát, a tagságot széles körben érintő átfogóbb témakörök esetén kerül sor. (Jelenleg ilyen a UNIX biztonsági kérdéseivel foglalkozó projekt.) Maguk a tagszervezetek és a régiók is kezdeményezhetnek saját kutatási tevékenységet. Mindez azt jelenti, hogy a tagoknak jó esélyük van arra, hogy kisebb-nagyobb mértékben mindenki részt vehet valamilyen formában egy kutatási programban.

A tagok által javasolt témák az ISACA Nemzetközi Irodája (International Office) elé kerül. Itt a Kutatási és Szabványügyi Igazgató (Director of Research and Standards) áttekinti a javaslatokat és észrevételeivel együtt átadja az EDPAF Kutatási Igazgatóságának véleményezésre. Ha a Kutatási Igazgatóság elfogadta a javasolt témakört, akkor a Kutatási és Szabványügyi Igazgató felveszi a kapcsolatot a javaslattevővel és együtt részletesen kidolgozzák a kutatási projekt további feltételeit.

A kutatási eredmények 3 kisebb-nagyobb kiadványban látnak napvilágot; szándék szerint mindhárom szinten ötvöződnek a elméleti és gyakorlati ismeretek, de különböznek a téma kifejtésének mélységében, illetve a megcélzott felhasználói kör nagyságában. Az *Ellenőrzési Jelentés* (Control Bulletins) inkább figyelemfelhívó kis füzet. Egy rövid áttekintés, amely a szakmát aktuálisan foglalkoztató alapvető ellenőrzési kérdésekről szól, illetve esetleg felhívja a figyelmet egy-egy új szoftver ellenőrzési szempontból lehetséges veszélyforrásaira. Gyakorlatilag mindenki haszonnal forgathatja, aki számítógép közelébe kerül. A *Távlatok* (Perspectives) című kiadvány egy adott témakör oktatási célú összefoglalója: kiterjed a feldolgozott témakörnek mind a számítástechnikai mind az ellenőrzési, biztonsági vonatkozásaira. A szakma szélesebb közvéleményének szól, terjedelme 20-60 oldal között mozog. A *Monográfiák* (Monographs) elsősorban szakemberek, specialisták számára készülnek. Egy-egy témakör részletes kifejtését adják, inkább a tapasztalt szakemberek forgathatják haszonnal. Terjedelme 30 oldalnál kezdődik.

A számítógépes vírusok matematikai modellje

Leitold Ferenc
Hunix Kft.

KIVONAT:

A legtöbb számítógépes vírus a DOS operációs rendszer alatt futó IBM PC-s környezetben terjed. Azonban más hardver platformok is egyre nagyobb támadási felületet jelentenek a vírusok számára. Az alábbiakban az automataelmélet eddigi főbb eredményeit tekintem át, különös tekintettel a matematikai számítógépmodellekre. Ezt követően a számítógépes vírusok matematikai modelljét, valamint működési környezetét biztosító matematikai számítógépmodellt és operációs rendszert ismertetem. Ebben a rendszerben matematikai eszközökkel vizsgálom a vírusok felismerhetőségének elvi korlátait. A modellen vizsgálom továbbá a jól ismert szekvencikereső algoritmus használhatóságának feltételeit. majd egy, a vírusok szélesebb körére alkalmazható vírusfelismerő algoritmust ismertetek, amely nemcsak ismert vírusok, hanem általános vírustevékenységek detektálására is alkalmas.

1. MATEMATIKAI SZÁMÍTÓGÉPMODELLEK

A következő szakaszokban számítóeszközök néhány alapvető modelljét tárgyalom, a legfontosabbak közülük: a közvetlen elérésű gép, a közvetlen elérésű tárolt programú gép és a Turing-gép. A három gép számítási képessége ekvivalens, de sebességük eltérő.

1.1. KÖZVETLEN ELÉRÉSŰ GÉPEK

A közvetlen elérésű gép (KEG) hasonlatos egy olyan egyakkumulátoros számítógépmodellhez, amelyben önmagukat módosító utasítások nincsenek megengedve. A KEG a következő egységekből áll: egy csak olvasásra használható bemenő szalag, egy csak kiírásra használható kimenő szalag, a program és a tár (memória). A bemenő szalag rekeszek sorozata, minden négyzetben egy (esetleg negatív) egész szám áll. Amennyiben egy jel a bemenő szalagról beolvasásra kerül, az olvasófej eggyel jobbra lép. A kimenő szalagra csak írni lehet, kezdetben ez üres rekeszekből áll. Kiírási utasítás végrehajtásakor az éppen az írófej alatt álló rekeszbe a gép egy egész számot nyomtat, majd az írófejet eggyel jobbra mozgatja. A kimenő jel kiírás után már nem módosítható. A tár a rekeszeknek egy $r_0, r_1, \ldots, r_i, \ldots$

sorozatából áll, melyek egy tetszőleges nagyságú egész számot tartalmazhatnak. Az r_0 rekeszt akkumulátornak nevezzük. A használható rekeszek számára nincs felső korlát. Ez az általánosítás akkor jogos, ha

- a probléma olyan kis méretű, hogy elfér egy számítógép központi tárában, és
- a számítás során használt egészek olyan kicsik, hogy elférnek egy gépi szóban.

A KEG programját a tár nem tárolja. Ebből persze adódik a feltevés, hogy a program nem más, mint egy (esetleg címkézett) utasításokból álló sorozat. Mindegyik utasítás két részből áll: műveleti kódból és címből. A programban használható utasításokat a következő táblázat tartalmazza.

Művelet	Cím	Jelentés
LOAD	operandus	Az operandus által meghatározott érték töltése az akkumulátorba.
STORE	operandus	Az akkumulátor másolása az operandus által meghatározott helyre.
ADD	operandus	Az operandus által meghatározott érték hozzáadása az akkumulátorhoz.
SUB	operandus	Az operandus által meghatározott érték kivonása az akkumulátorból.
MULT	operandus	Az akkumulátor szorzása az operandus által meghatározott értékkel.
DIV	operandus	Az akkumulátor osztása az operandus által meghatározott értékkel.
READ	operandus	Olvasás a bemeneti szalagról az operandus által meghatározott helyre.
WRITE	operandus	Az operandus által meghatározott érték írása a kimeneti szalagra.
JUMP	címke	Az utasításszámláló módosítása a címke által meghatározott helyre.
JGTZ	címke	Az utasításszámláló módosítása a címke által meghatározott helyre, ha az akkumulátor pozitív.
JZERO	címke	Az utasításszámláló módosítása a címke által meghatározott helyre, ha az akkumulátor zérus.
HALT	-	Leállítja a gép működését

Az a utasításhalmaz elvileg bővíthető bármely más, a számítógépeknél valóságosan előforduló utasítással (pl. logikai utasításokkal), anélkül, hogy ezzel a problémák nagyságrendjén változtatnánk.
Az operandusok az alábbiak lehetnek:

- i magát az i egészet jelöli;
- [i] nemnegatív i egész esetén az i rekesz tartalmát jelöli;

- [[i]] indirekt címzést jelez, vagyis az operandus a j rekesz tartalma, ahol j az i rekeszben talált egész szám, $j < 0$ esetén a gép leáll.

A gép indulásakor valamennyi memóriarekesz értéke zérus. Az utasításszámláló a program első utasítására van beállítva, a kimenő szalag pedig végig üres. A program k-adik utasításának végrehajtása után az utasításszámláló automatikusan a k+1-edik (tehát a következő) utasításra áll, kivéve, ha a k-adik utasítás JUMP, HALT, JGTZ vagy JZERO.

A KEG akkor áll le, ha HALT utasításhoz ér, 0-val kellene osztania, vagy negatív című memóriarekesszel kellene műveletet végeznie vagy nem definiált utasításhoz ér. Nem definiált utasítás például a STORE i, vagy a READ i utasítások.

Általában egy KEG program egy leképezést definiál a bemenő szalagokról a kimenő szalagokra. Mivel a program esetleg nem minden bemenő szalaggal áll meg, a leképezés nem feltétlenül teljes (bizonyos bemenetekre definiálatlan maradhat). Ezt a leképezést értelmezhetjük függvényként és nyelvként is.

1.2. KÖZVETLEN ELÉRÉSŰ TÁROLT PROGRAMÚ GÉPEK

Mivel a KEG programot nem tárolja a KEG tára, a program nem tudja önmagát módosítani. Most egy másik számítógépmodellt adunk meg, a közvetlen elérésű tárolt programú gépet (KETPG), amely mindenben hasonló a KEG-hez, kivéve, hogy a program a tárban van, s így módosíthatja önmagát.

A KETPG utasításainak halmaza azonos a KEG utasításainak halmazával, csak az indirekt címzés nem megengedett, hiszen nincs rá szükség, mivel a KETPG szimulálni tudja azzal, hogy a program végrehajtása során módosítja saját utasításait.

A KETPG szerkezete megegyezik a KEG szerkezetével, csak annyit teszünk fel, hogy a KETPG programja a tár rekeszeiben helyezkedik el. Minden egyes KETPG utasítás két egymás utáni tárrekeszt foglal el. Az első rekesz a műveleti kódot, a második rekesz a címet tartalmazza. Minden egyes utasításhoz tehát egy műveleti kódot rendelünk, melyek egész számok.

A KETPG indulásakor az utasításszámláló valamely meghatározott rekeszre van beállítva. A memóriában a gép indulásakor helyezzük el a programot. Ahhoz azonban ragaszkodunk, hogy véges sok rekesz kivételével minden rekeszben, valamint az akkumulátorban is nulla van. Minden egyes utasítás végrehajtása után az utasításszámláló kettővel megnövekszik, kivéve a következő utasításoknál: JUMP, JGTZ (ha az akkumulátor pozitív) és JZERO (ha az akkumulátorban nulla van), ezekben az esetekben az utasításszámláló i-re változik. Az egyes utasítások hatása azonos a megfelelő KEG utasítások hatásával.

1.3. A TURING-GÉP

Turing 1936-ban alkotta meg azt matematikai objektumot, a róla elnevezett automatát vagy gépet, mint olyan szerkezetet, mellyel matematikai problémák megoldhatók.

Matematikailag a Turing-gépet egy olyan $T = < Q, \Sigma, I, \{l,r\}, \delta, q_0, F >$ hetes írja le, melyben

- Q az állapotok véges halmaza,

- Σ a bemeneti jelek halmaza,
- Γ a szalag szimbólumainak a halmaza,
- $\{l,r\}$ az író/olvasófej mozgási lehetőségeinek megfelelő halmaz,
- δ a mozgási szabályok halmaza,
- q_0 a kezdő állapot,
- F az elfogadó állapotok halmaza.

A Turing-gép induláskor a szalagon a bemeneti jelsorozat található, amely természetesen a bemeneti jelek szimbólumaiból áll, így a bemeneti jelek Σ halmaza a Γ halmaznak részhalmaza: $\Sigma \subset \Gamma$. A részhalmaz valódi részhalmaz, hiszen az üres szimbólum eleme a Γ, de nem eleme a Σ halmaznak. A továbbiakban az üres szimbólumot jelölje #.

Az {l, r} halmaz a mozgás irányát adja meg. Elvben a szalag az automata működése során helyben is maradhat, de ez nem növeli az automata erejét.

A mozgási szabályok egy leképezést reprezentálnak. A mozgás csakis az automata állapottól és az olvasott szimbólumtól függ. A mozgás során megváltozik az automata állapota, az olvasott szimbólum felülíródik, végül az író-olvasófej vagy jobbra vagy balra elmozdul. A leképezés tehát a következőképpen szemléltethető:

$$Q \times \Gamma \rightarrow Q \times \{ \Gamma - \# \} \times \{ l, r \}$$

Míg a mozgás meghatározásakor bármely szimbólum, így a # is szerepelhet, addig felülírásra ez a szimbólum nem használható. A leképezés nem zár ki olyan mozgási szabályokat, ahol az olvasott szimbólum a #. Ebből következik, hogy az író/olvasófej elkalandozhat a szalag bemeneti jelsorozattal nem érintett részére is. Mivel a szalag mindkét irányban potenciálisan végtelen hosszú, az író/olvasófej tetszőlegesen messze távozhat kiindulási helyzetétől. Ugyanakkor mindig pontosan lehet tudni, melyek a szalag még érintetlen részei, ugyanis itt, és csakis itt hordoz a szalag # szimbólumot. Természetesen használhatunk felülírásra egy, a # szimbólum szemantikájával azonos szemantikájú szimbólumot. Ilyen értelemben mondhatjuk, hogy egy karaktert a # szimbólummal írtunk felül.

A Turing-gép egy jelsorozatot akkor fogad el, ha a jelsorozattal mint bemenettel elindítva létezik olyan mozgássorozata, hogy a Turing-gép elfogadó állapotban megáll. A Turing-gép akkor áll meg, ha egy olyan szituációba kerül, amelyre nézve nincs mozgási szabály.

Mint minden automata a Turing-gép is egy számítási potenciált képvisel. Felmerül a kérdés, hogy milyen mértékű a Turing-gép számítási képessége. Erre vonatkozóan **Church** deklarált egy feltételezést, amely **Church-tézis** néven ismert.

A Church-tézis azt állítja, hogy minden probléma, melynek kiszámítására eljárás szerkeszthető, Turing-géppel megoldható. Ez nagyon súlyos kijelentés, hiszen ez annyit jelent, hogy a Turing-gép képviseli a matematikai értelemben vett megismerhetőség határát. Az ember tehát azokra, és csakis azokra a kérdésekre képes választ adni, amelyekre a Turing-gép is képes.

Bizonyítható, hogy a KEG-en, a KETPG-n, valamint a Turing-gépen végzett számítások végrehajtási ideje polinomiálisan összehasonlíthatók.

1.1. tétel: Nem készíthető olyan Turing-gép, amely egy Turing-gép specifikációjáról és a bemeneti jelsorozatról eldönti, hogy a megadott Turing-gép az adott jelsorozatra valaha is megáll.

Bizonyítás: Nyílvánvaló, hogy a Turing-gépek száma magszámlál-hatóan végtelen, hiszen minden Turing-gép leírható egy véges jelsorozattal. Tételezzük fel a tétel ellenkezőjét, vagyis azt, hogy létezik egy, az $\mathcal{L}_{02}$ nyelvet elfogadó Turing-gép. Ez a gép ez esetben egyike a megszámlálható Turing-gépeknek, így ennek is van specifikációja, és ennek a gépnek is odaadható saját leírása. Kérdés, hogyan reagál ez a gép a saját leírására? Ha elfogadja, az hiba, mert ekkor a leírás nem mondata az $\mathcal{L}_{02}$ nyelvnek, így a gép nem fogadhatná el. Viszont az is baj, ha nem fogadja el, ugyanis akkor ez egy olyan leírás, amit saját gépe nem fogadott el, tehát mondata az $\mathcal{L}_{02}$ nyelvnek, és így el kellene fogadnia. Mindkét esetben ellentmondásra jutottunk, ezek szerint eredeti feltevésünk volt helytelen. Nincsen tehát az $\mathcal{L}_{02}$ nyelvet elfogadó Turing-gép. □

2. A VÍRUSOK MATEMATIKAI MODELLJE

A számítógépes vírusok megismeréséhez, tulajdonságaik vizsgálatához olyan matematikai modellre van szükség, mely alkalmas arra, hogy rajta a vírusokat definiáljuk. Az 1. fejezetben tárgyalt automaták, gépek közvetlenül nem alkalmasak a vírusok vizsgálatára, mivel ezen eszközök csupán egyetlen programot képesek tárolni és végrehajtani. Nincs lehetőség ezen gépek esetén a programok, programterületek közti kapcsolatra (az egyik program módosíthatja a másikat), így nem terjedhet vírus. Ahhoz, hogy a vírusok működését modellezhessük, egy olyan gépmodellre van szükség, amelyen definiálható az operációs rendszer, amely már nem csupán egy, hanem több program kezelésére is alkalmas. Ezután az ismert vagy feltételezett vírusok matematikai modellje megalkotható.

2.1. HÁTTÉRTÁRRAL KIEGÉSZÍTETT KETPG

Ahhoz, hogy a programok közti kapcsolatot megteremtsük szükség van egy olyan területre, szalagra, melyen a programok, programállományok tárolhatók. Ezt a szalagot - nevezzük *háttértár*nak - valamennyi futó program elérheti, olvashatja, illetve módosíthatja.

2.1. Definíció: Háttértárral rendelkező, közvetlen elérésű, tárolt programú gépnek (HRKETPG) egy olyan $G = < V,U,T,f,q,M >$ hatost nevezünk, melyben

- V a bemeneti jelek, a kimeneti jelek és a háttértár szalagon lévő jelek, valamint a memória rekeszeiben elhelyezhető jelek közös nem üres halmaza, a *szalag abc.*
- U a műveleti kódok nem üres halmaza, $U \subseteq V$;
- T a processzor által elvégezhető tevékenységek nem üres halmaza;
- f kölcsönösen egyértelmű függvény, melyre: f: U → T;
- q az utasítás számláló kezdeti értéke,
- M a tárolóegység kezdeti tartalma.

Feltételezzük, hogy a V szalag abc és az egész számok egy véges halmaza között kölcsönösen egyértelmű leképezés létesíthető. (Így a HRKETPG bemenő és kimenő szalagja, valamint a memóriája kölcsönösen egymásnak megfeleltethető szimbólumokat tartalmaz.)
A HRKETPG rendelkezik egy bemenő, egy kimenő és egy háttértár szalaggal melyek mindegyike végtelen hosszúságú. A bemenő szalag csak olvasásra, a kimenő szalag csak írásra, míg a háttértár szalag mindkét műveletre használható. A szalagok az olvasó, illetve író fejeken keresztül érhetők el. Ezen olvasó/író fejek egy szimbólum olvasásával, illetve írásával eggyel jobbra mozdulnak. A háttértár szalag esetén lehetőség van az olvasó/író fej közvetlen mozgatására is. A továbbiakban legyen a szalag abc az egész számok halmaza.
A gép tartalmaz továbbá egy ugyancsak végtelen nagyságú memóriát (tárat) is, mely a szalagoktól eltérően közvetlenül címezhető (olvasható, írható). A memória első rekesze kitüntetett tulajdonságú, ezt a KEG-hez hasonlóan *akkumulátor*nak nevezzük.
A HRKETPG-ben a szalagok és a memória kezelését a processzor végzi. Tekintsük az $U \subset V$ *véges* halmazt. Az f függvény ezen U halmaz minden elemének egy-egy T-beli tevékenységet feleltet meg. Az $x \in U$ műveleti kódhoz tartozó $f(x)$ tevékenységet *utasítás*nak nevezzük. A HRKETPG-ben a processzor az utasításszámláló által meghatározott rekeszben lévő műveleti kódot (utasítást) hajtja végre, majd beállítja az utasításszámláló új értékét. A műveleti kódot a memória egyetlen rekesze tartalmazza. A memóriában ezt követi a műveleti kód paramétere. A HRKETPG utasításait tehát két rekesz tartalmazza: a műveleti kódot és a hozzá tartozó paramétert tartalmazó rekesz. A lehetséges utasítások megegyeznek a KEG utasításaival, kivéve, hogy a HRKETPG nem tartalmazza a HALT utasítást, tartalmaz viszont néhány, a háttértár szalagra vonatkozó műveletet:

Művelet	Cím	Jelentés
GET	operandus	Olvasás a háttértár szalagról az operandus által meghatározott helyre.
PUT	operandus	Az operandus által meghatározott érték írása a kimeneti szalagra.
SEEK	operandus	A háttértár szalag író/olvasó fejének a mozgatása az operandus által megjelölt helyre.

Mivel a tárolt programú modellben a program módosíthatja önmagát, így a [[i]] típusú operandusú utasítások helyettesíthetők a többi utasítással, valamint néhány művelet is helyettesíthető más műveletek sorozatával.
Természetesen nem mindegyik művelethez tartozik valamennyi lehetséges operandus, hiszen például a READ műveletnek csak a [i], illetve [[i]] típusú operandusa lehet.
Abban az esetben, ha az utasításszámláló olyan rekesz(ek) tartalmát címzi meg, amelyben olyan $x \in V$ található, amelyre $x \notin U$ (tehát nem műveleti kód, nem tartozik hozzá utasítás), úgy a gép leáll.

A gép bekapcsolásakor az utasításszámláló a kezdeti q értéket veszi fel, a processzor először a q értékkel címzett utasítást hajtja végre. Azt, hogy a gép milyen programot, milyen algoritmust hajt végre a memóriában lévő utasítások, tehát a memória kezdeti tartalma (M) határozza meg. A gép akkor áll le, ha kikapcsolják, vagy pedig ha olyan utasításhoz ér, amely nem műveleti kód, illetve, ha 0-val osztana. A KEG-től eltérően tehát nincs olyan utasítás, amely leállítaná a gépet.
A memória tartalma minden bekapcsoláskor a kezdeti M értéket tartalmazza, minden kikapcsoláskor pedig törlődik. A háttértár viszont a kikapcsoláskor is megtartja tartalmát. Előfordulhat, hogy a háttértárat a gépből kivesszük és egy másik géphez illesztve használjuk. Ennek nyilván akkor van értelme, ha egy HRKETPG egyszerre több háttértárhoz is kapcsolódhat. A *több háttértár szalaggal rendelkező HRKETPG*-t egy újabb utasítás bevezetésével definiálhatjuk: a processzor elvégezhet egy olyan utasítást, amely kijelöli az aktuális háttértár szalagot:

Művelet	Cím	Jelentés
SETDRIVE	operandus	Az aktuális háttértárszalag az operandusban meghatározott sorszámú háttértár szalag lesz.

Az utasítás végrehajtását követően minden háttértár szalagra vonatkozó művelet az aktuális háttértár szalagon történik. Abban az esetben, ha olyan háttértár szalagra vonatkozó utasítást hajt végre a gép, melyet nem előz meg SETDRIVE utasítás, úgy a gép leáll. Az ilyen, több háttértárral rendelkező HRKETPG azonban szimulálható az egy háttértárral rendelkező HRKETPG-vel.

2.1. Tétel: Bármely HRKETPG szimulálható KETPG-vel, a szimuláló program költségfüggvényei megegyeznek a szimulált program költségfüggvényeinek konstansszorosával.

Bizonyítás: Fésüljük össze a memória és a háttértár tartalmát egy új memóriába. Ekkor egy háttértárral nem rendelkező, azaz KETPG-t kaptunk. Az összefésülést úgy kell elvégezni, hogy a memória elején fenntartsunk egy rekeszt, mely az író/olvasó fej aktuális helyzetét tartalmazza. □

A tétel következménye a következő:

2.2. Tétel: A Turing-gép és a HRKETPG számítási képessége megegyezik, költségeik polinomiálisan összehasonlíthatók.

Bizonyítás: Mivel a HRKETPG szimulálható KETPG-vel (2.1. tétel) és viszont (triviális), a KETPG pedig szimulálható Turing-géppel és viszont, ezért a HRKETPG is szimulálható Turing-géppel és viszont. □

2.2. OPERÁCIÓS RENDSZEREK

2.2. Definíció: *Operációs rendszernek* nevezzük az olyan programrendszert, amely alkalmas arra, hogy különálló programokat, adatállományokat kezeljen.

Az operációs rendszert tartalmazhatja egyrészt a memória M kezdeti értéke, másrészt pedig elhelyezkedhet a háttértáron is. Ez utóbbi esetben a memória kezdeti M értéke egy olyan programot tartalmaz, amely a háttértárról betölti és futtatja az operációs rendszert. Ebben az esetben az operációs rendszert betöltő programot nem tekintjük az operációs rendszer részének.
Amennyiben a memória kezdeti M értéke tartalmazza az operációs rendszert, úgy a HRKETPG megadásával definiáltuk az operációs rendszert is. Így ebben az esetben a HRKETP gépen csak a gép saját operációs rendszere használható. (Természetesen készíthető olyan program amely egy másik operációs rendszert szimulál.) Az ilyen típusú operációs rendszert *gépspecifikus operációs rendszer*nek nevezzük.
Abban az esetben viszont, ha a háttértár szalagja tartalmazza az operációs rendszert, úgy egy HRKETP géphez több operációs rendszert is megadhatunk. Ehhez csupán a háttértár szalagot kell cserélni. Így ezeket az operációs rendszereket *gépfüggetlen operációs rendszer*nek nevezzük.

2.3. VÍRUSOK A HRKETPG-N

Az előző pontban definiáltuk az operációs rendszer fogalmát, mely egy olyan programrendszer, amely programállományok kezelésére, azok futtatására alkalmas. Így a vírusok definícióját a HRKETPG-n is megadhatjuk:

2.3. Definíció: *Számítógépes vírusnak* nevezzük az olyan, valamely programterülethez kapcsolódó programrészletet, amely alkalmas arra, hogy önmagát másolva más programterületekhez kapcsolódjon. Amennyiben egy programterülethez vírus kapcsolódik, úgy ezen programterület végrehajtásakor a vírusprogram végrehajtódik.

2.3.1. A VÍRUSOK LEHETSÉGES TERJEDÉSI MÓDJAI

Egy vírus többféle programterülethez is kapcsolódhat. A különböző programterületekhez való kapcsolódást *terjedési mód*oknak nevezzük. Egy vírus rendelkezhet akár több különböző típusú terjedési móddal is.

2.4. Definíció: *Gépspecifikus*nak nevezzük egy vírus *terjedési mód*ját, ha a vírus ezen terjedési módja során felhasználja a gép valamely tulajdonságát, szolgáltatását. Abban az esetben, ha egy terjedési mód során a vírus nem használja fel a gép szolgáltatását, vagy valamely tulajdonságát, úgy *gépfüggetlen terjedési mód*ról beszélünk.

2.5. Definíció: *Operációs rendszertől függőnek* nevezzük egy vírus *terjedési mód*ját, ha a vírus ezen terjedési módja során felhasználja az operációs rendszer valamely tulajdonságát, szolgáltatását. Abban az esetben, ha egy terjedési mód során a vírus nem használja fel az operációs rendszer szolgáltatását, vagy valamely tulajdonságát, úgy *operációs rendszertől független terjedési mód*ról beszélünk.

2.6. Definíció: *Gépspecifikus vírusnak* nevezzük a csak gépspecifikus terjedési móddal rendelkező vírust, *gépfüggetlen vírus*nak pedig a csak gépfüggetlen terjedési móddal rendelkező vírust.

Hasonlóan definiálhatjuk a vírusok operációs rendszertől való függőségét:

2.7. Definíció: A csak operációs rendszertől függő terjedési móddal rendelkező vírus *operációs rendszertől függő vírus*, míg a csak operációs rendszertől független terjedési móddal rendelkező vírus *operációs rendszertől független vírus.*

2.8. Definíció: *Közvetlen terjedési mód*ról beszélünk abban az esetben, ha a vírus a terjedési mód során végrehajtható állományhoz kapcsolódik, szemben a *közvetett terjedési mód*dal, melynek során a vírus nem végrehajtható állományhoz kapcsolódik.

A közvetett terjedési móddal rendelkező vírusok esetén a fordítótól és a szerkesztőtől függően a vírusok megjelenési formája a végrehajtható állományokban más és más lehet. A vírus ilyenkor teljesen beépül a hordozó programba.

2.3.2. POLIMORF VÍRUSOK

Az eddig tárgyalt számítógépes vírusok megjelenési formája minden egyes fertőzésnél megegyezik. Elképzelhető azonban olyan vírus is, amely fertőzésenként valamilyen úton-módon megváltoztatja formáját:

2.9. Definíció: *Polimorf terjedési mód*nak nevezzük egy vírus terjedési módját, ha létezik két olyan, a terjedési mód során fertőzött állomány, melyben a vírusprogram kódsorozata különböző.

2.10. Definíció: *Polimorf, vagy mutációra képes vírus*nak nevezünk egy vírust, ha az rendelkezik polimorf terjedési móddal.

A polimorf vírusok egy lehetséges megvalósítási módja, hogy a vírusprogramot egy véletlen kulccsal lekódoljuk, majd az így titkosított vírust egy visszatitkosító résszel látjuk el.
A polimorf vírusok bonyolultabb változatai a visszatitkosító részt is változtatgatják. Ezt megtehetik egyrészt úgy, hogy néhány előre elkészített visszatitkosító rutinból választanak véletlenszerűen. Másrészt elérhető ez oly módon is, hogy a terjedési mód során a vírus véletlenszerűen generálja a rutin utasításait. Ezt például az alábbi módszerekkel érheti el:

- változtathatja a visszatitkosító rutin utasításainak a sorrendjét,
- kihasználhatja, hogy a processzor egy műveletet több utasítással, több utasítássorozattal is elvégezheti,
- a visszatitkosító rutint véletlenszerűen töltelékutasításokkal láthatja el.

2.4. A VÍRUS-FELISMERÉSI PROBLÉMA

A számítógépes vírusok megjelenésével együtt felmerül a vírusok felismerésének a problémája:

2.11. Definíció: *Vírusfelismerési problémának* nevezzük azt az algoritmuselméleti kérdést, mely szerint létezik-e olyan algoritmus, amely egy állományról eldönti, hogy tartalmaz-e terjedőképes vírust vagy sem.

Feltételezzük, hogy az állomány formátumáról minden információ rendelkezésre áll. Ez alatt azt értjük, hogy végrehajtható állomány esetén ismerjük a processzor utasításkészletét, az egyes utasítások működését; forrásfile-ok esetén pedig ismerjük a programnyelv szintaktikáját, a fordító működését.

2.4.1. AZ ÁLTALÁNOS VÍRUS-FELISMERÉSI PROBLÉMA

A Church-tézist szem előtt tartva, ha létezik olyan algoritmus, amely választ adna a vírus-felismerési problémára, úgy ezen algoritmus elvégzésére készíthető Turing-gép. Sajnos ilyen Turing-gép még egyszerűsített esetben sem készíthető:

2.4. Tétel: Nem készíthető olyan Turing-gép, amely egy HRKETPG végrehajtható állományról eldönti, hogy tartalmaz-e vírust, vagy sem.

Bizonyítás: A 2.3. tétel értelmében minden Turing-géphez készíthető egy, a Turing-gépet szimuláló KETPG, illetve HRKETPG. (Az, hogy a szimuláció hatására az eljárás költségfüggvénye hogyan módosul a tétel bizonyítása szempontjából lényegtelen.) Egy Turing-gépből ily módon készíthetünk egy HRKETPG-beli P programot, amely a kimeneti szalagra egy 1-est ír, ha a szimulált Turing-gép elfogadó állapotban megállt. Tekintsünk egy olyan egyszerű vírust, amely csak a végrehajtható állományokat fertőzi meg. Egy fertőzött állomány futtatásakor megvizsgálja, hogy a következő állomány fertőzött-e, vagy sem. Ha még nem fertőzött, úgy megfertőzi. Módosítsuk ezt a vírust úgy, hogy a vírus tartalmazza az említett P programot oly módon, hogy először a P program hajtódjon végre egy B véletlenszerű, de rögzített bemenetre, majd ezt követően fusson a vírus. Ez megtehető oly módon, hogy P-hez hozzáfűzzük a vírust, P minden 1-est kiíró utasítása után egy JUMP utasítást szúrunk be, mely a vírusprogram első utasítására ugrik. A vírusprogramot is módosítjuk oly módon, hogy fertőzéskor ne csupán a vírusprogramot, hanem a P programot, valamint a rögzített B bemenetet is másolja.
A fenti módszerrel minden Turing-géphez készíthető egy HRKETPG-beli V program, mely akkor vírus, ha valóban terjedőképes. Nyilvánvaló, hogy a V program akkor lesz terjedőképes, ha a P program és így a Turing-gép is megáll a rögzített bemenet esetén.
Indirekt tegyük fel, hogy létezik egy olyan T Turing-gép, amely minden HRKETPG-beli programot a bemenetről elolvasva 1-est ír ki, ha az tartalmaz vírust, 0-át, ha nem. Abban az esetben, ha a T Turing-gép a V programra, mint bemenetre 1-essel válaszol, akkor a P program, illetve a neki megfelelő Turing-gép a B bemenetre biztosan megáll, ha viszont 0-át válaszol, akkor biztosan nem áll meg. Így a T Turing-gép képes eldönteni, hogy egy tetszőleges Turing-gép egy tetszőleges bemenetre megáll-e, vagy sem. Ez viszont az 1.1. tétel értelmében nem lehetséges. □

A vírusok felismerése tehát a Church-tézist figyelembe véve nem algoritmizálható. Célszerű tehát a vírus-felismerési problémát úgy egyszerűsíteni, hogy az algoritmizálható és így a gyakorlatban is használható legyen.

2.4.2. VÍRUS-FELISMERÉSI MÓDSZEREK

Az általános vírus-felismerési probléma egy lehetséges egyszerűsítése, ha csupán "néhány" ismert vírussal foglalkozunk. Ekkor a vírusfelismerés algoritmizálásához felhasználhatjuk az ismert vírusokat is. Minden ismert vírusból vegyünk egy kódsorozatot, amely minden egyes fertőzéskor a fertőzött állományban előfordul. Nevezzük ezt a kódsorozatot *szekvenciának*. Az vírusfelismerő algoritmusnak már csak ezeket a szekvenciákat kell keresnie a programterületeken. Az ezen az elven működő algoritmussal kapcsolatban azonban további problémák merülnek fel:

- polimorf vírusok esetén nem biztos, hogy lehet találni egy nem változó szekvenciát;
- milyen valószínűséggel kapunk vakriasztást, azaz találunk meg véletlenül egy szekvenciát egy állományban;
- milyen költségkritériumok mellett valósítható meg a szekvenciakereső algoritmus.

Nyilvánvaló, hogy a polimorf vírusok felismerésére a módszer nem használható, ezen vírusokra más eljárást kell keresni.

A vakriasztás mértéke attól függ, hogy milyen hosszúak a szekvenciák, és a programállományokban lévő rekeszek melyik értéket milyen valószínűséggel tartalmazzák. Abban az esetben, ha egy szekvencia hossza N, egy rekeszben n érték szerepelhet egyenlő valószínűséggel és összesen M darab szekvenciánk van és a vizsgált állományok összhossza $L >> N$, akkor annak a valószínűsége, hogy valamelyik szekvencia előfordul valamely állományban:

$$p \approx L \cdot M \cdot \frac{1}{n^N}.$$

Ez azt jelenti, hogy például 2000 darab 30 byte-os szekvencia esetén annak a valószínűsége, hogy valamelyik szekvencia előfordul egy 100 Mbyte-os véletlenszerűen generált egységben: $p \approx 1{,}19 \cdot 10^{-61}$. Sajnos a vakriasztás teljes mértékben nem zárható ki, de a megfelelő hosszúságú szekvenciák véletlenszerű előfordulásának csekély valószínűsége miatt a szekvenciakeresési módszert biztonságosnak nevezhetjük.

Vizsgáljuk meg, hogy milyen költségkritériummal valósítható meg a szekvenciakeresési algoritmus. Mivel a gyakorlatban használt számítógépek a HRKETPG-től eltérően fix rekeszmérettel és memóriával rendelkeznek, így minden utasítás költsége egy konstans érték alatt marad. Ezért célszerű a költségkritérium megállapításánál uniform költséggel számolni. A szekvenciakeresési algoritmus minden vizsgálandó rekesz tartalmát összehasonlítja a szekvenciák első rekeszével. Ehhez $L \cdot M$ darab összehasonlításra van szükség abban az esetben, ha külön-külön végezzük a vizsgálatot. A

szekvenciákat azonban az első rekeszük tartalma alapján sorba rendezhetjük. A vizsgálatot a sorban a középső helyen állóval kezdjük, majd haladunk a megfelelő irányba. Ezt a módszert használva átlagosan csak $L \cdot \lceil \log M \rceil$* darab összehasonlítást kell végezni, feltéve, ha a szekvenciák első rekeszeinek tartalmai különbözők. Abban az esetben, ha a szekvenciák első rekeszeinek a vizsgálatával azonosságot találtunk, meg kell vizsgálni a 2. rekeszek tartalmát. A szükséges további vizsgálatok számának várható értéke $L \cdot M \cdot \frac{1}{n}$, így ennyi újabb vizsgálatra van szükség. A k-adik vizsgálat egyezősége esetén tehát újabb $L \cdot M \cdot \frac{1}{n^k}$ vizsgálatra van szükség. Mindezek alapján a szükséges vizsgálatok számának várható értéke:

$$s = L \cdot M \cdot \left(1 + \frac{1}{n} + \frac{1}{n^2} + \ldots + \frac{1}{n^{N-1}}\right) = L \cdot M \cdot \frac{\frac{1}{n^N} - 1}{\frac{1}{n} - 1}$$

A legrosszabb esetet vizsgálva, az összehasonlítások számára $s = L \cdot M \cdot N$ adódik. Mivel az algoritmus időigénye becsülhető az összehasonlítások számával, így a szekvenciakereső algoritmus polinomidőben megvalósítható.

A **polimorf vírusok** azonosítására egy szimulációs módszert használhatunk. A módszer lényege, hogy processzor emulálása (szimulálása) alatt elkezdjük végrehajtani a vizsgált programállományt. A végrehajtott utasításokról statisztikát készítünk, melyet folyamatosan hasonlítjuk az ismert polimorf vírusok már meglévő statisztikájával. Amennyiben egyezőséget tapasztalunk, akkor vírust találtunk. A módszerrel így a visszatitkosítás után vizsgáljuk a gyanús program műveleti kódjait. A szekvenciakereséshez hasonlítva itt nem a kódsorozat egy részletének a hasonlítása történik, hanem a kódsorozat valamely részletének műveleti kódjaiból készített statisztikát vizsgáljuk. Így egyrészt az utasítások felcserélése esetén is azonosíthatóak a vírusok, viszont a szekvenciakereséshez mérhető biztonságú keresés eléréséhez jóval több műveleti kódból képzett statisztikára van szükség.

Az emulátor alapú keresési eljárás viszont nem valósítható meg polinomiális időkeretek között, mivel létezhet olyan vírus, melynek a visszatitkosító rutinja egy véletlenszámtól függően exponenciális idő alatt fut le.

---

* $\lceil x \rceil$ jelenti az x-nél nem kisebb, legkisebb egész számot.

Az **ismeretlen vírusok** keresésének egy lehetséges módszere a polimorf vírusok azonosításakor említett processzoremulátor alapú eljárás. Ekkor azonban nem statisztikát készítünk, hanem jellemző vírustevékenységeket figyelünk. Ilyen jellemző vírustevékenység például, ha egy program

- módosít egy másik programállományt,
- megpróbál más programállományt módosítani,
- megpróbálja az operációs rendszert módosítani.

ÖSSZEFOGLALÁS

A cikkben egy olyan matematikai modellt állítottam fel, amelyen a számítógépes vírusok felismerhetőségének vizsgálata matematikai módszerekkel elvégezhető. A modellt a számításelméletben ismert automata- és gépmodellekből vezettem le. A modell más operációs rendszert igénylő problémák vizsgálatánál is felhasználható.
Bizonyítottam, hogy teljesen általánosan a vírusok felismerése eldönthetetlen probléma, ezért a vírusok felismerésére általános megoldást nyújtani nem lehet. Platform és operációs rendszertől függő megoldások kidolgozására van szükség. IBM PC-n DOS operációs rendszer alá algoritmusokat dolgoztam ki a vírusok felismerésére és eltávolítására.

IRODALOMJEGYZÉK

[1] Aho, A. V.; Hopcroft, J. E.; Ullman, J. D.:
Számítógép-algoritmusok tervezése és analízise. Műszaki Könyvkiadó, Budapest, 1982.
[2] Demetrovics, J.; Denev, J.; Pavlov, R.:
A számítástudomány matematikai alapjai. Tankönyvkiadó, Budapest, 1985.
[3] Bach, I: Számítástechnikai nyelvészet. BME, Budapest, 1991.
[4] Gács, L; Lovász, L.: Algoritmusok. Tankönyvkiadó, Budapest, 1987.
[5] Virus Bulletin: Survivor's guide to computer viruses. Virus Bulletin, Abingdon, 1993.
[6] Brunnstein, K.:Practical security in PCs and PC-LANs.
Tutorial of HISEC'93 conference, Budapest, 1993.

Windows NT — biztonság és megbízhatóság

Jamrik Ferenc, Janek Gábor, Lóki Róbert

Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutató Intézet

Levélcím: 1518 Budapest, Pf. 63. Telefon: 166-5644

KIVONAT:

Egy modern számítógépes operációs rendszerben elengedhetetlen a megfelelő szintű biztonság (security, védelem) és megbízhatóság (reliability) szolgáltatása. Azonban ahhoz, hogy ezeket a szolgáltatásokat hatékonyan, a céloknak megfelelően és a lehetőségeket teljes mértékben kihasználva lehessen alkalmazni, fontos a rendszerek védelmi lehetőségeinek kimerítő ismerete. Ezt szem előtt tartva szeretnénk ismertetni —az egyik legújabb operációs rendszer— a Windows NT által ezen a téren nyújtott lehetőségeket, s így egyben áttekinthetjük a ma alkalmazott biztonság és megbízhatóság növelő módszereket, eszközöket.

1. BEVEZETÉS

1.1. Általános biztonsági kérdések

Az operációs rendszerek által nyújtott biztonsági és megbízhatósági szolgáltatások alkalmazásakor figyelembe kell venni, hogy mely adatok mennyire titkosak, fontosak, értékesek, milyen könnyen pótolhatóak.

A biztonság eléréséhez a rendszerek bevezették a felhasználók azonosítását (logon), valamint az objektumok elérésének szabályozását. Ez azt jelenti, hogy egy felhasználó egy adott rendszerben nem érhet el minden információt, nem végezhet el bármilyen tevékenységet.

Megbízhatóság alatt a számítógépen tárolt információk hibátlan tárolását, más szavakkal az egyes hardver és szoftver zavarok által okozott adatvesztések elkerülését, minimalizálását (fault tolerance) értjük.

A biztonság és a megbízhatóság növelésére egyaránt léteznek hardver és szoftver megoldások. Általában egy rendszer biztonságának és megbízhatóságának elérése plusz adminisztrációval jár. Ennek egyszerűsítése érdekében egyre gyakoribbak a vállalati szintű egységes megvalósítások, melyek kényelmes és biztonságos munka környezetet teremtenek a felhasználók számára.

1.2. Microsoft Windows NT

A Windows NT a Microsoft által kifejlesztett többfelhasználós, hálózati operációs rendszer. Az NT —az angol New Technology (új technológia) szavak rövidítéséből összeállt— betűszó olyan újszerű technológiára utal, amelynek legfontosabb jellemzője az operációs rendszer platform-függetlensége. Maga az operációs rendszer két rétegre bontható, amelyből csak az alsó a hardverfüggő, a felső (felhasználó közeli) réteg minden platformon ugyanaz marad. Így a Windows NT nem kizárólag PC-ken fut —bár a PC-ken való futtathatósága szigorú szempont volt— hanem például RISC processzorokon is. A Windows NT megjelenésében a Windows 3.1-re hasonlít, a grafikus felhasználói felületen viszonylag kevés eltérés van a két rendszer között. Mivel többfelhasználós operációs rendszer, így minden felhasználó számára saját környezetet biztosít.

A Windows NT hálózati értelemben vett 'könnyűsúlyú' párja a Windows for Workgroups, amely a Windows NT-hez nagyon hasonló szolgáltatásokat nyújt. Ezek a szolgáltatások röviden a következőképpen összegezhetők. Egy Windows NT-s hálózat minden gépe képes bizonyos erőforrásait — nyomtatót, könyvtárat, faxmodemet— a hálózat egyéb gépeinek szolgáltatni. Fordítva, minden Windows NT gép képes felhasználni az ily módon kiajánlott erőforrásokat, amelyek ezután a felhasználónak úgy jelennek meg, mintha a saját rendszerének részét képeznék. Ezt összegezve azt mondhatjuk, hogy a hálózat minden gépe potenciális szerver és kliens is egyben. Természetesen a megosztott erőforrás hálózaton keresztül történő eléréséhez és felhasználásához rendelkezni kell a szerver gépen a megfelelő jogokkal. A Windows NT esetében —biztonsági szempontokból— erőforrás elérése csak a rendszerbe regisztrált felhasználó számára lehetséges.

A processzorfüggetlenségen túlmenően a fő különbség a Windows NT és a Windows változatai között a Windows NT által nyújtott biztonsági és megbízhatósági garanciák. Ezek a rendszer szerves, integrált részét alkotják, nem különálló programok, mint az sok más rendszernél tapasztalható. Ezeket a szolgáltatásokat fogjuk a továbbiakban részletesebben áttekinteni.

A Windows NT további szerver funkciókkal ellátott változata a Windows NT Advanced Server (NTAS), amely egyrészről a biztonságos tárolás nagy hatékonyságú támogatását, másrészről szervezeti egységek Windows NT felhasználóinak közös nyilvántartását (domainek), valamint ezen domainek közötti kapcsolatokat —annak minden biztonsággal kapcsolatos elvárásainak betartásával együtt— biztosítja.

A Windows NT jelentősége az, hogy az igen elterjedt Windows felhasználói felületet kiegészíti a ma már elengedhetetlen biztonsági és megbízhatósági elvárásokkal.

A következőkben szó lesz a felhasználói szintű biztonságról és megbízhatóságról, valamint a programok biztonságáról és megbízhatóságáról.

2. BIZTONSÁG

2.1. C2 biztonsági osztály és a Windows NT

Az Amerikai Védelmi Minisztérium által definiált számítógépes rendszerek megbízhatósági kritériumai közül legtöbbet a C2-t szokás emlegetni. Ezt számos UNIX rendszer mellett a Windows NT is teljesíti, mégpedig nemcsak lokálisan, hanem a Windows NT gépek között, a hálózati kommunikáció során is. A C2, mely egy felhasználói szintű biztonsági modell, a következőket követeli meg:

- a felhasználók egyedi azonosítását, amely általában valamilyen bejelentkezési procedúrával történik, (unique user identifier, felhasználói azonosító, jelszó),
- a rendszer a felhasználók azonosításához szükséges jelszót minden esetben kódolt formában tárolja, így továbbítja a hálózaton is azt,
- a felhasználók hozzáférését az egyes objektumokhoz az objektumok tulajdonosai szabályozhatják, (discretionary access control), hozzáférési jogokat adhatnak felhasználóknak illetve visszavonhatnak felhasználóktól, pl. fájl elérés,
- a rendszerből kitörölt objektumok véletlen vagy szándékos újrafelhasználását nem teszi lehetővé. Ezzel magyarázható, hogy törölt fájlokat és formatált lemezeket nem lehet visszaállítani, programok által használt és elengedett memóriát nem kaphat meg egy másik program, illetve hogy egy a rendszerből kitörölt felhasználót nem lehet eredeti jogaival együtt újra felvenni.
- a biztonsági rendszerrel kapcsolatos események (pl. bejelentkezés) naplózása (auditing).

Ezen kritériumokon túl a Windows NT további szolgáltatásokat is nyújt. Így például:

- a felhasználók különböző csoportokba sorolhatók, melyek szintén hozzáférési jogokkal rendelkezhetnek; valamint számítógépek tartozhatnak egy domainbe, melynek eredményeként egy globális bejelentkezés után a domain összes erőforrása elérhetővé válik,
- továbbá a legtöbb joggal rendelkező felhasználó, így az adminisztrátor sem tud más nevében cselekedni. Például, ha van egy fájl, amit az adminisztrátor nem nézhet meg, akkor azt csak úgy tudja megnézni, ha átveszi a tulajdonosi jogát annak a fájlnak, de természetesen ez már nem marad rejtve a fájl eredeti tulajdonosa előtt.
- a biztonsági rendszerekkel kapcsolatos naplózható események az általánostól —mint pl. egy adott szolgáltatás indulása— az egészen speciálisig —mint egy adott fájl egy adott user által történő módosítása— terjednek.

Mind biztonsági, mind megbízhatósági szempontból lényeges, hogy az egész rendszert érintő, globális tevékenységet —mint pl. új felhasználó felvétele, felhasználói jogok módosítása, szervizek/hardver meghajtók installálása és beállítása, könyvtár és nyomtató megosztása a hálózaton stb.— csak az adminisztrátor végezhet.

A Windows NT az ígéretek szerint a következő verziókban a B2-es biztonsági szintet fogja megvalósítani. A következőkben a Windows NT biztonsági rendszerének alapjait tekintjük át.

2.2. Biztonsági modell a Windows NT-ben

A Windows NT — felhasználói oldalról tekintve — kétirányú biztonsági stratégiát követ. Egyrészt az egyes felhasználók számára az egész rendszerre vonatkozó általános jogok (rights) adhatók meg, amelyek globálisan szabályozzák, hogy milyen tevékenységeket hajthatnak végre a rendszerben, másrészt engedélyek (permissions) definiálhatók, amelyek a rendszer egyes objektumaihoz kötődnek. A jogok az egész rendszerre vonatkoznak és előfordulhat, hogy az objektumokhoz rendelt engedélyeket felülírják. Például a Backup Operátor akkor is el tudja menteni a fájl rendszert, ha egyébként nem rendelkezik egy adott fájlra olvasási joggal.

Négy alapvető fogalom tisztázásával a Windows NT teljes biztonsági modellje érthetővé válik, ezek a fogalmak a felhasználó, az objektum, a naplózás és a domain.

Felhasználó

Mindenkinek, aki hozzá kíván férni a rendszerhez, rendelkeznie kell egy azonosítóval, amelyet az adminisztrátor biztosít számára. Az egy felhasználóra vonatkozó adatokat, amelyek őt azonosítják és a rendszerhez való hozzáférését globálisan meghatározzák accountnak nevezzük. Ennek része a felhasználói azonosító (login name) és a jelszó (password). A jelszó beírásakor egyirányú technikával kódolódik, nem fejthető vissza. Tehát, amikor a felhasználó bejelentkezik, akkor a beírás során kódolt jelszó kerül összehasonlításra a gépen szintén kódolt formában tárolt változattal. Egy account létrehozója (pl.: adminisztrátor) előírhatja, hogy a jelszó meddig érvényes, milyen gyakran kell a felhasználónak azt megváltoztatnia, mekkora legyen a minimális hossza, illetve, hogy hány régi jelszót tároljon a gép. Ez utóbbi arra szolgál, hogy ha elő van írva a felhasználó számára, hogy bizonyos időnként pl.: félévente változtassa meg a jelszavát, akkor ennek a listának a segítségével a rendszer megakadályozhatja azt, hogy a felhasználó csak két-három 'kedvenc' jelszavát cserélgesse.

A felhasználók belső azonosítására egy egyedi azonosítót generál a rendszer (Security Identification Number, SID), — nem a felhasználói név szolgál azonosításra, az akár meg is változtatható — azonban, ha egy felhasználó accountját a rendszerből véglegesen kitörli az adminisztrátor, akkor ezt követően ugyanazzal a felhasználói névvel létrehozva egy accountot, új SID generálódik. Így az új felhasználó nem lesz azonos a korábban ugyanazzal a felhasználói névvel rendelkező felhasználóval, így annak esetleg meglévő objektumait (fájlok, nyomtató stb.), jogait sem birtokolhatja.

Minden egyes felhasználóra megadható, hogy általánosan milyen jogokkal rendelkezzen, a rendszer mely erőforrásait használhatja és milyen módon. Az egyes felhasználók csoportokba (groupokba) szervezhetők. A csoportok és az egyéni felhasználók számos szempontból azonosan kezelődnek, így ugyanúgy jogok rendelhetők hozzájuk, illetve újabb csoportokba lehet őket szervezni. Ez nagymértékben megkönnyíti a jogosultságok kezelését, adminisztrálását. Egy felhasználó természetesen több csoportba is tartozhat és az egyes csoportok által a számára biztosított jogok összeadódnak.

Objektum

Nem csak az egyes felhasználókra határozható meg, hogy milyen jogokkal rendelkezzenek, hanem az egyes objektumok — fájlok, nyomtatók — védelme is biztosított. Minden egyes objektumra megadható, hogy melyik felhasználó, illetve csoport férhet hozzá, milyen tevékenységeket hajthat végre rajta. Minden objektumtípushoz létezik az elemi engedélyeknek egy csoportja, amellyel az adott objektumtípussal végezhető összes művelet leírható. Például fájlok esetén Read, Write, Delete, Execute, Change Permission, Take Ownership (tulajdonjog átvétele). Ezekből az elemi engedélyekből állnak össze, az úgynevezett standard engedélyek, amelyek egy-egy komplexebb műveletet írnak le, pl.: List, Add & Read, Full Control. Általában a standard engedélyek elegendőek a rendszer és az objektumok védelméhez, de az elemi engedélyek kombinációjával speciális engedélyek is megadhatók.

Egy felhasználó számára minden olyan engedély biztosított, amely az őt tartalmazó csoportok számára is megengedett. Tehát a csoportok által biztosított jogok kumulatívak. Például, ha egy *user1* tagja a *group1* és *group2* csoportnak és a *group1* olyan engedéllyel rendelkezik amely egy könyvtár listázását biztosítja számára, a *group2* pedig írás és olvasási jogokat biztosít, akkor *user1* listázási, írási és olvasási jogokkal egyaránt fog rendelkezni. Egyetlen esetben van csak eltérés a fent leírt szabálytól, ha a példánál maradva *group1* 'No Access' jogot biztosit a felhasználónak (amely azt jelenti, hogy a könyvtár semmilyen elérését nem engedélyezi), ekkor a jogok nem adódnak össze, hanem a 'No Access' jog lesz kizárólag érvényes, a többi figyelmen kívül marad.

Minden objektumnak van tulajdonosa és általában minden felhasználó tulajdonosa az általa létrehozott objektumnak. A tulajdonos az objektum elérésének kizárólagos szabályzója, így a többi felhasználó csak olyan engedélyekkel rendelkezhet, amelyet az objektum tulajdonosa számára biztosít. Engedélyek tehát csak kaphatók és nem szerezhetők. Egy objektum létrehozásakor automatikusan beállítódnak a hozzá tartozó engedélyek. Előfordulhat, hogy az objektum valamilyen módon örökli ezeket, például a fájlok az őket tartalmazó könyvtár engedélyeit örökölhetik. Az adminisztrátornak különleges privilégiumai vannak, azonban korlátlanul és főként úgy, hogy ne maradna nyoma, nem tevékenykedhet. Az adminisztrátor számára mindig biztosítva van az a jog, hogy ő váljon egy objektum tulajdonosává (Take Ownership), de egy másik személy számára csak úgy tudja "átadni" ezt az objektumot, ha ezen személynek erre az objektumra biztosítja a Take Ownership engedélyt és ő ezek után "átveheti" azt. Így, ha az adminisztrátor nem olvashat egy fájlt, de azt a tulajdonos beleegyezése nélkül is meg akarja nézni, akkor ezt csak úgy teheti meg, ha ő válik annak tulajdonosává. A tulajdonosváltást természetesen látni fogja az eredeti tulajdonos is.

Az objektumok (fájlok, nyomtatók stb.) a hálózaton keresztül megoszthatók és az elérésük a Windows NT felhasználói jogain keresztül szabályozható. Természetesen a hálózaton keresztül a felhasználó nem kaphat nagyobb jogosultságot egy objektumra, mint amilyennel lokálisan rendelkezik.

Naplózás

Biztonsági és megbízhatósági szempontból is fontos, hogy a rendszerben bekövetkező, a működés szempontjából kritikus események feljegyzésre kerüljenek. A Windows NT-ben ennek megvalósítását szolgálja a naplózás.

Az események három szempont szerint kerülnek följegyzésre:

- A rendszer működésével, a Windows NT rendszer komponenseivel kapcsolatos események, mint például a rendszer indítása, leállítása, eszköz meghajtók sikeres vagy sikertelen betöltése, szolgáltatások indítása, leállítása, stb.
- A biztonsági rendszert érintő események, sikeres, illetve sikertelen bejelentkezési kísérletek, objektumokat érintő tevékenységek.
- Az alkalmazásokkal kapcsolatos események. Az alkalmazói programok is naplózhatják tevékenységeiket, egy adatbázis kezelő program például naplózhatja a törléseket, fájl hibákat, stb.

A felhasználók és a biztonsági rendszer viszonyának nyomon követését kétféleképp lehet szabályozni, egyrészt megadható általános naplózási stratégia, amely azt határozza meg hogy milyen típusú események kerüljenek feljegyzésre, másrészt az egyes objektumokra (fájl, nyomtató, stb.) definiálható, hogy mely felhasználó, illetve mely csoportok milyen tevékenységei naplózódjanak.

A rendszer eseményeinek függvényében különböző tevékenységek hajthatók végre, például üzenet küldése egy adott felhasználónak vagy egy tetszőleges program elindítása.

Domain

Lehetőség van a számítógépek egy csoportját logikailag összetartozónak kezelni, egy ilyen összetartozó csoportot nevezünk domainnek. Egy domainen belül kell lenni egy elsődleges szervernek (Primary Domain Controller, PDC), amely centralizáltan nyilvántartja a felhasználók adatait. A felhasználók adatainak egyszeres nyilvántartása teszi kényelmessé a domainek használatát az adminisztrátorok számára. Domain szerveri kapacitásokkal csak a Windows NT Advanced Server rendelkezik. A domainhez tartozhat több szerver (Backup Domain Controller, BDC) is, amelyek szintén tartalmazzák a felhasználói adatbázis másolatát. Ez ugyan redundanciát jelent, de a PDC kiesése esetén bármelyik BDC átveheti a szerepét. Egy felhasználónak egy domainen belül csak egyetlen felhasználói azonosítóval kell rendelkeznie, amelyet a domain bármelyik gépe elfogad. Egy felhasználó adatainak módosítása a PDC-n történik és ezek után a domainen belül bármelyik számítógépen bejelentkezhet az új felhasználó, és minden erőforrást használhat, anélkül hogy mindegyikhez külön meg kellene adnia a felhasználói azonosítót és a jelszót. Ez teszi kényelmessé a felhasználók számára a domainek használatát.

Domaineknek lehetőségük van arra, hogy megbízzanak egymásban (trusted domain). Ez azt jelenti, hogy ha egy felhasználó rendelkezik accounttal *domain1*-en, akkor megvalósítható, hogy *domain2* megbízzon *domain1*-ben és így *domain2* elfogadja a felhasználó *domain1*-en érvényes felhasználói azonosítóját és jelszavát és ezzel lehetővé teszi számára, hogy a felhasználó a *domain2* erőforrásait használhassa. Természetesen a megvalósítás eleget tesz minden racionális biztonsági elvárásnak, így a felhasználónak érvényes azonosítóval kell rendelkeznie a *domain1*-ben; a jelszó kódolt formában kerül a hálózatra; és a felhasználó azonosítását és jogainak ellenőrzését a *domain1* kontrollere végzi.

A domainek használatának lényege hogy több számítógép együttes, központi konfigurálását az adminisztrátornak illetve ezek használatát a felhasználónak kényelmessé teszi

A felhasználók adminisztrálása a grafikus UserManager-rel történik, az objektum engedélyek beállítása az adott objektumtípust felsoroló eszközön belül lehetséges, így a fájlok esetében a File Manager-ben, a nyomtatók esetében a Print Manager-ben stb. Összefoglalásképpen érdemes megemlíteni, hogy a felhasználók adatait, jogait csak az adminisztrátor módosíthatja, míg az objektumok hozzáférési engedélyeit mindig az adott objektum tulajdonosa kezelheti.

2.3. Illeszkedés más biztonsági rendszerekhez

A Windows NT, mivel elosztott (distributed) számítógépes környezet megvalósítására szánták, számos hálózati protokollt tartalmazó operációs rendszerrel képes kapcsolatot fenntartani. Ehhez természetesen megoldották a biztonságos kommunikáció egyik alapfeltételét, a biztonságos felhasználó azonosítást, ami a gépek között a kulcsszó (password) kódolt hálózati átvitelét jelenti. Tud kommunikálni a LAN Manager és az azzal kompatibilis protokollokat futtató gépekkel: MS-NET, IBM LAN Server, LAN Manager for UNIX, LAN Manager for OS/2, Windows for Workgroups, Windows 3.1/MS-DOS + LAN Manager, DEC Pathworks stb. Ezen kompatibilis rendszerek számára lehetővé válik a domainek használata is. A Windows NT ezen rendszereknek azok saját, natív biztonsági modelljükként prezentálja a Windows NT biztonsági modelljét. Ugyanez igaz a Windows NT Advanced Serverben található Macintosh szolgáltatásokra is, amely a Windows NT-n elhelyezkedő fájlok és könyvtárak engedélyeit automatikusan a Macintosh megfelelőkre transzformálja.

A hálózati rendszereken kívül a POSIX alrendszer biztonsági előírásait is integrálták a Windows NT-be, ilyen például a felhasználói csoport azonosító (a group security ID). A Windows NT tartalmaz egy TCP/IP implementációt is. Mivel számos applikáció (telnet, ftp stb.), amelyik ezt a protokollt használja a jelszót kódolatlan formában küldi tovább a hálózaton, ajánlatos, hogy azokon a számítógépeken, melyeket ezekkel a programokkal érünk el, más jelszót használjunk, mint a Windows NT-n.

A telefon vonalon, távoli elérést lehetővé tevő Remote Access Service (RAS) azon felül, hogy támogatja a biztonságos domain elérést, lehetőséget ad egyéb biztonsági hardverek (security host) használatára is. A domainbe való bejelentkezés előtt egy, a Remote Access szerver elérését biztosító bejelentkezést is végre kell hajtani. A felhasználókhoz külön engedély tartozik, amely szabályozza, hogy telefonon elérhetik-e az adott Windows NT-t, domaint. Lehetőség van annak a beállítására is, hogy a Windows NT visszahívja (callback) a távoli klienst, ezzel biztosítva, hogy ténylegesen a felhasználói adatbázisban megadott telefonszámról történt a hívás. A telefonvonalon történt bejelentkezés esetén is lehet a tevékenységeket naplózni, illetve az egyes megosztott erőforrások elérését tovább lehet korlátozni.

3. MEGBÍZHATÓSÁG

A következőkben a Windows NT által biztosított megbízhatósági rendszer elemeit tárgyaljuk részletesebben. Ezek az elemek az NT új fájlrendszere, az adatmentő program, a szünetmentes áramforrás kezelés valamint a konfiguráció visszaállításának lehetősége.

3.1. A Windows NT fájlrendszere és a RAID

A Windows NT két módszert biztosít a lemezeken tárolt adatok megbízhatóságának növelésére, az egyik a tranzakció alapú fájl kezelés, a másik a RAID-ek használata.

A Windows NT háromféle fájlrendszert ismer. A DOS által használt FAT-et, az OS/2 által használt HPFS-t, és a saját fájlrendszerét az NTFS-t. A lokális fájlokkal kapcsolatos minden szintű biztonsági szolgáltatás kizárólag az NTFS fájlrendszeren alkalmazható, ugyanakkor a hálózaton keresztül kiajánlott partíciók esetén a DOS és a HPFS partíciókhoz is lehet hozzáférési engedélyeket rendelni. Az NTFS használata általában célszerűbb a másik két támogatott fájlrendszerénél. A hosszú és rövid — DOS típusú— fájlnevek együttes tárolása, a kis és nagybetűk megkülönböztethetősége, a rendszer hatékonysága és kapacitása valamint a megbízhatósági szolgáltatásai is ezt sugallják. Az NTFS rugalmasan terjeszthető ki más fájlrendszerek —mint pl. AppleShare és NFS— irányába.

Megbízhatósági szempontból az NTFS —az adatbáziskezelésből jól ismert technikát alkalmazva— tranzakció alapú fájlrendszer, így a fájlokat mindig konzisztens állapotban tartja, amelyet a fájl műveletek naplózásával ér el. Az NTFS a lemezhibákból fellépő rögzítési sikertelenségeket automatikusan javítja ki. Emellett támogatja a RAID 0 kvázi szabványt, a Windows NT Advanced Server szervereken pedig a RAID 1 és RAID 5 szinteket is.

A RAID (Redundant Array of Inexpensive/Intelligent/Independent Disks) rendszerek fő célja az adatvesztés valószínűségének minimális szinten tartása az adatok redundáns tárolásának segítségével. Alapelve az adat több lemezen való tárolása, amely megoldás mellékes hatásaként az adattárolás -és visszaolvasás sebességét is növelheti. RAID rendszerek egyrészről hardverben valósíthatók meg, amely esetben sem a felhasználónak sem a számítógépnek nem kell tudnia arról, hogy adatai esetleg több fizikai diszken tárolódnak. Másrészről —és a mi esetünkben ez a lényeges— az operációs rendszer is előállhat ilyen szolgáltatással. Ebben az esetben az adminisztrátor a számítógépéhez tartozó lemezegységek közül jelölhet ki néhányat redundáns tárolás céljára így az operációs rendszer gondoskodik a tárolásról és hiba felmerülése esetén a hibajavításról is. Ez természetesen a felhasználó előtt rejtve marad.

A RAID 0 szint az angolul data striping-nak nevezett technológiát jelenti, amelynek lényege az adat több fizikai egységen való szétszórása redundancia nélkül. Ezen technika főként a hatékonyság növelésére alkalmas.

A RAID 1 a legegyszerűbb redundáns tárolást a lemez tükrözését (mirroring) jelenti, amelynek lényege az adat párhuzamos rögzítése két hardver diszken. Amennyiben az egyik meghibásodik, az adat nagy valószínűséggel visszanyerhető a másikról. Természetesen a két lemez együttes meghibásodásának esélye igen csekély.

A RAID 5 az 1-es szintnél hatékonyabb redundáns tárolást alkalmaz. Az adat —és az adathoz készülő, a hibajavítást szolgáló— paritás szegmensek különböző fizikai lemezeken tárolódnak. Ha az adat hibásodik meg a paritás szegmens alkalmas lehet a rekonstrukcióra, ha a paritás szegmens károsul, az önmagában nem eredményez adatvesztést.

Ezekkel a technikákkal az elsődleges adattároló, a lemez megbízhatóságát lényegesen megnöveli a Windows NT. A fentiek kezelése, beállítása a grafikus Disk Manager program segítségével történik.

3.2. Adatmentés, backup

Az egyik legfontosabb adatvédelmi módszer a rendszeres adatmentés. Ehhez nyújt segítséget a Windows NT-ben található Backup program, mely a rendszer jól átgondolt, szerves része. A felhasználó által kijelölt fájlokat tudja szalagra (tape) menteni, illetve azokat onnan visszatölteni. Az egész rendszert átfogó adatmentést/visszatöltést csak az arra jogosult, ún. backup operátor végezheti, a többi felhasználó csak azokra a fájlokra végezheti el ugyanezt, melyek eléréséhez megfelelő jogosultságokkal rendelkezik. Egy szalagra több mentést is végezhetünk, illetve egy nagyobb mentés több szalagra is kerülhet. Minden egyes mentéshez tartozik egy katalógus is, mely az elmentett fájlokról tartalmaz információt —például a fájlok hozzáférési engedélyeit is—, melyeket szintén vissza lehet tölteni. Kérhetjük az adatmentés és a visszaállítás naplózását, valamint az adatok írásának ellenőrzését.

A Backup program segítségével nemcsak a lokális fájlokat menthetjük szalagra, hanem a hálózaton keresztül elérhetőket, így MS-DOS, Windows for Workgroups, LAN Manager, másik Windows NT stb. gépeken elhelyezkedőket is. Lényeges, hogy az operációs rendszer és az egyéb programok összes beállítását tartalmazó ún. Regisztrációs Adatbázist (Registry Database-t) is elmenthetjük illetve visszatölthetjük, ezt később a konfiguráció helyreállításával foglalkozó részben szintén megemlítjük.

A rendszeres adatmentés esetében incremental típusú backup-ot szokás használni, mely során csak az utolsó mentés óta megváltozott fájlok kerülnek a szalagra. További segítség, hogy az adatmentést a háttérben futó program segítségével, a többi program futását nem zavarva is elvégezhetjük, és ezt a tevékenységet bármilyen időpontra automatikus végrehajtásra ütemezhetjük.

Az elmentett fájlokat nemcsak az eredeti helyükre tölthetjük vissza, hanem új elhelyezést is specifikálhatunk nekik, sőt átvihetjük azokat másik gépre is. Ez utóbbi esetben a fájlok letöltését csak az adminisztrátor végezheti. Ilyenkor a fájl hozzáférési engedélyek visszatöltésének nincs értelme, mivel a felhasználók nem egyeznek meg a két gépen.

Biztonsági szempontból lényeges, hogy a szalagok elérése korlátozható, mely esetben csak az adatmentést elvégző felhasználó és az adminisztrátor érheti el a szalagon az adatokat, ők is csak azon a gépen, melyen a mentés történt.

3.3. Szünetmentes áramforrás

A szünetmentes áramforrások (UPS — Uninterruptible Power Supply) manapság nemcsak az áramkimaradás ellen nyújtanak védelmet, hanem egyéb az elektromos hálózatban létrejövő zavarokkal

szemben is. Így például egy hirtelen nagy feszültségű impulzus lecsökkentése értékes hardver eszközöket menthet meg. Általában az is lényeges döntés eredménye, hogy egy számítógépes rendszer mely elemeit lássuk el szünetmentes áramforrással (szerverek, kliensek, nyomtatók, a hálózat aktív elemei), mely adatok a legfontosabbak. A szünetmentes áramforrások kezelése az operációs rendszer alapjaiba van beépítve, a Windows NT integrált részét képezi. Számos más rendszerhez kapcsolható szünetmentes áramforrás —így például a hálózati operációs rendszerekhez, LAN Manager, Novell— , lényeges különbség azonban, hogy ezeknél egy külön, az operációs rendszer szolgáltatásaira épülő program kezeli ezt, és nem az operációs rendszer integrált részei. A Windows NT a külső eszköz segítségével észleli az áramkimaradást, figyelmezteti a felhasználókat erről, és amikor a szünetmentes áramforrás másodlagos energiaforrása kifogyóban van egy biztonságos rendszer lezárást hajt végre, lezárja az alkalmazásokat, a szolgáltatásokat és a fájlrendszert. Ezzel a Windows NT értékes adatok elvesztését akadályozza meg, mivel a memóriában tárolt adatokat időben lemezre tudja menteni. Azon túl, hogy a Windows NT lezárja a rendszert áramkimaradás esetén, megadható egy parancs fájl is, melyet a rendszer a lezárás előtt végrehajt, ahol elvégezhetők az olyan tevékenységek, mint például a távoli kapcsolatok lezárása stb. A rendszer az áramkimaradásokat feljegyzi. Rövidebb áramkimaradás esetén egy szünetmentes áramforrás elegendő energiát szolgáltathat ahhoz, hogy a felhasználók mit sem sejtve nyugodtan dolgozhassanak tovább, csak a rendszer naplózza az eseményt.

A szünetmentes áramforrás és a Windows NT a számítógép soros portján keresztül kommunikálnak egymással. A Windows NT annál zökkenőmentesebben szolgálja ki a felhasználókat, minél több szolgáltatást nyújt egy szünetmentes áramforrás. E célból eltárolja a szünetmentes áramforrás számos paraméterét, mint például a szünetmentes áramforrásban levő tartalék áramforrás kapacitását, az akkumulátorok újra feltöltéséhez szükséges időt, stb.

3.4. Konfiguráció helyreállítás

Új hardver és szoftver elemek installálásakor és konfigurálásakor előfordul, hogy azok beállításánál helytelen értékeket adunk meg. Ez számos esetben nem csak az adott program helytelen működését eredményezheti, hanem akár más programokra is kihatással lehet. Ezen esetekben szükségünk lehet a hiba elhárításához egy korábbi állapot visszaállítására. Ehhez a Windows NT a következő segítséget nyújtja:

- az operációs rendszer és egyéb programok összes beállítását tartalmazó Regisztrációs Adatbázist egy adott állapotában szalagra menthetjük, majd egy későbbi időpontban, amikor helytelen viselkedést észlelünk, visszatölthetjük. Ennek a módszernek a hátránya, hogy a mentés és visszatöltés között történt változtatások elvesznek, ezért ezzel óvatosan kell bánni. Természetesen ez feltételezi, hogy az operációs rendszert és a Backup programot még tudjuk futtatni. Ha nem, rendelkezésünkre áll a következő lehetőség:
- rendszer indítás során az operációs rendszer betöltése előtt kérhetjük az utolsó jónak ismert konfiguráció visszaállítását (Use Last Known Good Configuration). Erre azért van lehetőségünk, mert a Windows NT minden egyes indítás után, ha sikeresen elindult minden szolgáltatás, akkor az adott konfigurációt elmenti. Ekkor persze az utolsó sikeres indítás óta a rendszer konfigurá-

ción történt változtatások elvesznek. Ha ez a lehetőség sem áll rendelkezésünkre, pl. ha rendszerfájlok hibásodtak meg, akkor

- lehetőség van a Windows NT installációja során készített Emergency Repair lemez segítségével a kezdeti, az installáció során beállított konfiguráció visszaállítására. Ilyenkor az összes, az installáció óta a rendszer konfiguráción történt változtatást tartalmazó és a Repair program által hibásnak vélt fájl tartalma elveszik. Egy másik —történetesen szintén Repair nevű— segédprogram segítségével az Emergency Repair lemezen tárolt információkat rendszeresen frissíthetjük, így nem csak az installációkor készített beállítást lehet visszaállítani.

4. PROGRAMOK BIZTONSÁGA ÉS MEGBÍZHATÓSÁGA

Most tekintsük át röviden, hogy programozási szempontból milyen megbízhatósági és biztonsági eszközöket nyújt a Windows NT.

Memória

A Windows NT az egyes alkalmazások számára folytonos memóriacímzést biztosít. Ez eltér a DOS és Windows rendszerekben alkalmazott szegmentált memória modelltől. Az alkalmazás folytonosan címzett memória területet használhat és az operációs rendszer gondoskodik arról, hogy ez a 'folytonos' terület, a valóságban hogyan tárolódjon a fizikai memóriában.

Minden egyes —a felhasználó által elindított— program hatására az operációs rendszer egy processzt hoz létre. Egy processz nem láthatja a rendszer más processzeinek memóriaterületét. Ez azt jelenti, hogy nemcsak átírni —megbízhatóság—, de megtekinteni, olvasni —biztonság— sincs lehetősége. Ezzel persze sem a 'rosszindulatú' programok nem képesek a rendszerből információt kicsalni, vagy azt módosítani, sem a rossz programok nem tehetik tönkre a rendszer részeit. Az egyes programok által használt és elengedett memória területet a Windows NT csak a memória terület törlése után adja ki újra. Így, bár a memóriában tárolva van a kódolt jelszó is, azt illetéktelen programok mégsem érheti el.

DOS és Windows programok

Mivel a Windows NT képes más operációs rendszerek programjainak futtatására is, így biztosítania kell nemcsak a Windows NT programok, de a DOS és a Windows programok megfelelését a biztonsági és megbízhatósági elvárásoknak. Erre szolgál a Windows NT-ben használatos ún. virtuális gép (virtual machine, VM). Ez végső soron egy hardver emuláció, amely alkalmas arra, hogy például egy DOS programmal elhitesse azt, hogy egy PC-n 'egyedül' fut. A virtuális gépnek nevezett, szeparált memória területre szorított DOS program így természetesen nem férhet hozzá a Windows NT rendszer egyéb memóriaterületeihez sem szándékosan, sem véletlenül. A közvetlen hardver elérés nyomán esetleg fellépő problémákra maguk a virtuális gépek nem adnának megoldást, ezért az említett egyéb operációs rendszerbeli alkalmazások számára a fizikai hardver virtuális eszköz meghajtókon (virtual device driver, VDD) keresztül érhető el. Ezeket a VDD-ket —lévén szoftver komponen-

sek— az operációs rendszer a kezében tartja, megtartva a lehetőséget arra, hogy bizonyos műveleteket bizonyos hardvereken letiltson vagy módosítson.

A hibás és rosszindulatú programok elleni védelem a vírusok terjedését is megnehezíti a Windows NT operációs rendszerben. Egyrészt egy program nem írhatja át mások programjainak a kódját a lemezen az NT fájlrendszer védelme miatt; másrészt a memóriában sem garázdálkodhatnak felelőtlenül.

5. IRODALOMJEGYZÉK

Microsoft Windows NT System Guide, Microsoft Corporation

Microsoft Windows NT Resorce Kit, Volume 1 of the 3 volume set, Windows NT Resource Guide, Microsoft Press

Microsoft Windows NT Inside Track, Technical Training Kit, Microsoft Corporation

Helen Cluster: Inside Windows NT, Microsoft Press, 1993

Jim Groves: Windows NT Answer Book, Microsoft Press, 1993

Bill Taylor: RAID to the Rescue, PC Magazine, September 14, 1993, pp273-295

Howard Gershen: RAID and Reliability, RS/Magazine, September 1992, pp54-57

Winn L. Rosch: Keeping Up with UPSs, Power Protection, PC Magazine, September 14, 1993, pp309-326

A Számítógépközpontok zavarvédelme

Előadó: Stampok László

Kivonat:

A számítógépközpontok kialakításának gyakorlati tapasztalatai, a sugárzott és vezetett zavarok elleni védekezés megvalósítása. Az elméleti megfontolások gyakorlati megvalósíthatóságának problémái, korlátai. EMC probléma és az információvédelem kapcsolata. A számítógépközpontok zavarvédettségének főbb területei: sugárzott zavarok, vezetett zavarok. A zavarvédettség szükséges mértéke. Az alkalmazott anyagok és technológiák. A kivitelezés során követendő szempontok, eljárások.

A számítógépes helyiség (polgári célú is) rádiófrekvenciás védelme, ennek megfelelő hálózati zavarszűrés és túlfeszültség védelem biztosítása a rádiófrekvenciás és hálózati zavarok ellen, fontos követelmény. A kialakítás során alkalmazott egyéb elemek beépítésénél (pl. álmenyezet, álpadló, üvegfal stb.) a fentiekből adódó védelmi szempontokat konzekvensen érvényesíteni szükséges.A számítógépközpontba álpadló, álmenyezet kerül beépítésre, a meglévő ablakot általában megszüntetjük. Üvegfal választja le az operátori helyiséget. A levegő szükséges hőmérsékletét és a friss levegő utánpótlását klímaberendezés biztosítja. A számítógépes helyiség tűzjelző és vagyonvédelmi elektronikával felszerelt, igény esetén tűzoltó berendezéssel ellátott, amely automatikus indítású is lehet. A bejárat biztonsági ajtó, amely átadó ablakkal és átbeszélő elektronikával lehet kialakítva.

Egy, már meglévő helyiség számítógép központtá történő kialakításakor az alábbi munkálatokat szükséges elvégezni úgy, hogy az elektromos zavarvédelmi követelményeknek is eleget tegyünk:

Ablak befalazás száraz technológiával, oldalfalak RF árnyékolása, árnyékoló álmenyezet, árnyékoló, antisztatikus álpadló, megfelelő világítótestek beépítése, hálózati zavarszűrés, túlfeszültségvédelem, földelési rendszer kiépítése helyszíni vizsgálat alapján, térelválasztó üvegfal, néhány esetben üvegfal RF fóliázás, klímaberendezés kiépitése, biztonsági bejárati ajtó, szükség esetén mikrofonos átbeszélővel, berregővel, vagy intelligens beléptető rendszer, tűzjelző,- és vagyonvédelmi elektronika, (lehet rádiós, vagy vezetéken továbbított jelzés-átvitel), adattároló széf, vagy szoba kialakitása. A tervezési fázisban, valamint a központ beüzemelése előtt műszeres méréseket kell végezni szükség szerint, a csillapitási értékek egzakt meghatározására.

A számítógépterem sugárzott és vezetett külső elektromos zavarokkal szembeni védelme illetve az adatfeldolgozás során a számítógépek környezetében lehetséges "lehallgatás", elleni védelem megvalósításánál a következő szempontok kerülnek figyelembe vételre:

Elektromos készülék üzemeltetése során létrejövő elektromágneses tér idő és térbeli eloszlása a gerjesztés spektrumától, a forrás geometriai tulajdonságaitól és a hullámhossztól függően igen változatos lehet. Ennek megfelelően alakul az árnyékolás és a tér kölcsönhatása, vagyis az árnyékolás hatásossága is. A gyakorlatban előforduló eseteket alapvetően két csoportra vezethetjük vissza. Ezek antennás szóhasználattal élve a távoltéri ill. közeltéri elektromágneses terek. Az elektromágneses térben az elektromos és mágneses térerősség amplitudójának távolságfüggését 1/r, $1/r^2$ és $1/r^3$ szorzójú tagok írják le. Valódi sugárzó energiát csak az 1/r-es tagok hordoznak, ezeket a komponenseket nevezzük távoltéri komponenseknek. A forrástól elegendő távolságban ezek sikhullámnak tekinthetők. Sikhullám esetén az elektromos (E) és mágneses (H) térerősség egymásra merőleges, hányadosuk megegyezik a szabadtér hullámimpedanciájával (E/H = 377 Ω). Azt a térrészt, ahol ezek a komponensek dominálnak távoltérnek nevezzük. A távoltér határa a forrástól függően meghatározható. Az $1/r^2$, $1/r^3$ szorzójú tagok a forrás közelében valódi sugárzó energiát nem hordozó reaktáns teret létesítenek. A tér felépítése a gerjesztéstől függően kétféle lehet. A villamos dipólus un. nagy impedanciáju (E/H > 377Ω) teret, a hullámhosszhoz képest kis méretű áramhurok kis impedanciáju (E/H < 377Ω) teret létesít. Az előzőeknek megfelelően a szoba méreteiből adódóan 50 MHz alatt közeltéri és távoltéri méréseket, 50 MHz felett távoltéri méréseket végzünk. A mérőhelyek megválasztása a belső tér kijutásának vizsgálatára úgy történik, hogy azokat a legközelebbi helyeket keressük meg, ahol illetéktelenek is megfordulhatnak.

A belső tér kijutásának vizsgálatát a titokvédelem teszi szükségessé. Ennek megfelelően olyan gerjesztési feltételeket hozhatunk létre, amelyek a várható üzemi körülményeknek megfelelő teret hoznak létre, vagyis mintegy lemodellezzük a telepített számítógép esetén várható sugárzást.

A külső tér bejutásának viszgálatát a beállítandó érzékeny berendezések zavarása miatt kell megvizsgálni. Zavarforrásként elsősorban nagy térerejű helyi rádióadók jönnek számításba. Ezek a vételi helyen sikhullámot állítanak elő, vagyis a mérési eredmények a szoba árnyékoló hatását mutatják távoltéri komponensekre. Mint ismeretes a sugárforrás alakjától függően az itt szokásos esetekben a távoltér kezdete lamda/6-lamda/2 távolságra van, és itt a hullám már sikhullámnak tekinthető. Sok esetben a szoba méreteiből adódóan az URH sávban a középen elhelyezett forrástól a fal már jó közelítéssel a sugárzás távolterében van. Ebből következik, hogy a belülről kijutó ill. a kívülről bejutó hullám csillapítása azonos, és az adó és a vevő helye felcserélhető.

A gyakorlati tapasztalatok azt mutatják, hogy a huzalhálóból készült árnyékolások beiktatási csillapítása egyetlen frekvencián sem éri el a szükséges csillapítási értéket és 50MHz felett a csillapítás szinte kiszámíthatatlanul ingadozik. Az információtechnikai ezközök titokvédelme szempontjából mérvadó előírás tehát hálószerű konstrukcióval nem teljesíthető. Polgári célú számítástechnikai alkalmazásoknál 1000MHz felső frekvenciáig 40-60dB csillapítás gyakorlatilag elegendő. Az üvegfalak irányában az épület csillapítása elhanyagolható, ezért a csillapítási követelmény megvalósítása ezen a felületen a legkritikusabb. Arra kell törekedni, hogy nyílászáró ezen a felületen ne legyen, az áttöréseket pedig pontosan méretezett védelemmel kell tervezni. A zavarokkal jelentős mértékben terhelt falszakaszokon (pl. nyomda, elektromos átalakító) megfontolandó a kettős falú árnyékolás kialakítása.

Az alkalmazott fólia anyaga lehet alumínium, vastagsága 10mm. A mechanikai sérülés megakadályozására a fólia vékony műanyag bevonattal van ellátva és két réteg papírtapétával van burkolva. A fémfólia jó vezetőképességet biztosít, de alkalmazása igen munkaigényes és precíz kialakítást igényel különösen a komplex profilú tárgyak esetén.

Az ajtók megfelelő árnyékoló hatásának biztosítása (az ajtó nagy mérete miatt igen széles frekvenciatartományban az egész szoba árnyékolási csillapítását meghatározza). Az ajtónak eleget kell tennie a menekülő útvonal követelményeknek is.

Szűretlen hálózat hatásának vizsgálata során megvizsgáljuk, hogy az árnyékolt szobába bevezetett külső tápfeszültség hogyan változtatja meg a távolteri csillapítás értékét. A gyakorlati mérések azt mutatják, hogy a szűretlen hálózat bevezetése kb. 25 db-lel csökkenti a szoba csillapítását. Tapasztalataink szerint hasonló megállapítás vonatkozik a telefon és egyéb jelvezetékre is. E romlás a be- és kimenő vezetékek megfelelő szürésével elhárítható. A fenti okokon kívül, az URH sávban mintegy 400 MHz felett a légkondicionáló befújó nyilása is áteresztheti. Ennek kialakításánál szabály, hogy a nyilás legnagyobb mérete nem érheti el a legrövidebb hullámhossz felét. Felhívjuk a figyelmet arra, hogy meg kell oldani a fémes kötések korrózió elleni védelmét, hogy a jó elektromos kontaktus folyamatosan meglegyen. Érintésvédelmi célokra külön földelést szükséges kiépiteni.

Az MSZ 1600/10 jelű magyar szabvány szerint a világításra és gépi berendezések működtetésére független hálózatot kell létesíteni, ezért a hálózati szűrők szükséges darabszámát ennek figyelembevételével kell megállapítani. A világítótestek kiválasztása során zavarmentességre kell törekedni (armatúrák, gyújtás tranziens védelme). A hálózati szűrők és a helyiség árnyékolása között megbízható villamos átvezetést kell biztosítani, a reaktáns áramok kiküszöbölésére.

A tervezés a következő munkafázisokból áll:

1. Helyszíni bejárás során fel kell térképezni a

1.1. kialakítandó központ közvetlen környezetét,
1.2. közelben lévő elektromos energiaátalakító (pl. BKV) állomásokat, trafóházakat.
1.3. közelben lévő és az épület hálózati táplálására hatással lévő nagy energiaigényű üzemeket (pl. nyomda), fogyasztókat.
1.4. minden olyan külső tényezőt, amely a hálózatra hatással lehet.

1.5. számba kell venni a lehetséges külső rádiófrekvenciás zavarforrásokat (pl. pályaudvar közelsége).
1.6. fel kell térképezni az épületen meglévő villámhárító rendszert, annak műszaki állapotát.
1.7. lehetőség szerint tanulmányozni kell az épület elektromos és villámhárító rendszerének dokumentációit, a földelési rendszer kialakítását,
1.8. meglévő (vagy tervezett) szünetmentes áramforrás műszaki állapotát.

2. A tervezési időszakban az alábbi műszeres méréseket célszerű elvégezni:

2.1. Számítógépközpontba becsatlakozó elektromos vezetékek zavarvizsgálata. Hosszú idejű (kb. 14 nap) hálózati zavarvizsgálat telepített műszerekkel, a helyiségbe becsatlakozó elektromos hálózaton megjelenő zavarok folyamatos rögzítése.
2.2. Hálózati zavartérkép felvétele.
2.3. Az elektromos hálózati csatlakozások megbontása, a becsatlakozó elektromos hálózat teljes átvizsgálása.
2.4. Szünetmentes áramforrás által keltett zavarok vizsgálata.
2.5. A zöld-sárga ekvipotenciálra hozó vezeték állapotának ellenőrzése.
2.6. A földhurok induktivitás ellenőrzése.
2.7. A különböző forrásokból származó túlfeszültség okozta veszélyforrások vizsgálata (pl. nyomda, BKV energia átalakító, stb.).
2.8. Az árnyékolások, földelések, összekötések rendszerének vizsgálata.
2.9. A meglévő villámvédelmi rendszer szabványossági vizsgálata.
— Felülvizsgálat az MSZ 274/1-4 szabványsorozat alapján.
— Az épület villámvédelmi besorolása az MSZ 274/2-81 alapján.
— A szükséges villámvédelmi fokozat meghatározása az MSZ 274/3-81 (M 1985) alapján.
— Az épületen található, meglévő villámhárító berendezés vizsgálata a fenti fokozat alapul vételével, az MSZ 274/4-77 alapján.
2.10 A számítógépközpontban rádiófrekvenciás zavartatás és térerő mérések elvégzése.
2.11. Az épület rádiófrekvenciás csillapítás mérése.
2.12. A vizsgálati tapasztalatok és elemzések birtokában szakértői konzultáció a kivitelező szakembereivel.
2.13. A számítógépterembe telepítendő berendezések és egységek számbavétele, a berendezések zavarvédettségének vizsgálata a vonatkozó dokumentumok alapján.

3. Tervezés

3.1. A fenti vizsgálati eredmények és információk alapján a helyiségbe becsatlakozó elektromos hálózat zavarvédelmének, szűrőrendszerének (1 kör, 2 kör, 3 kör) megtervezése a nemzetközi normákhoz igazodva, a szükséges szűrők meghatározása.

3.2. A sugárzott zavarmérés eredményeinek függvényében a rádiófrekvenciás árnyékolás megtervezése.

3.3. Az eredmények birtokában a számítógépközpont zavarvédettségének teljes müszaki technológiai megtervezése.

3.4. A villámvédelem megtervezése.

Az esős idő és a zavar keletkezésének tapasztalatai, hogy a földelő szondák földelési értékei megváltoznak, javulnak figyelembe véve az EPH hiányát, ez teljesen megváltoztatja az ellenállás osztót olymódón, hogy a levezetőre nagyobb másodlagos indukált feszültség kerül. Az esetleg meglévő földelési hurok megszüntetésével a feszültséggenerátoros hatás kiküszöbölhető.

Egy számítógépközpont kialakítása -különös tekintettel a jelenlegi nagyvárosi környezetre- fokozott műszaki feltételrendszert igényel. A gépterem környezete a számítástechnikai hardveren kívül eső szempontokra is kiterjed, amelyek befolyásolhatják a berendezés működését illetve megbízhatóságát. A környezet fizikai jellemzői közé tartozik az elhelyezés, elrendezés, hűtés, páratartalom, szennyezettség, ütés és rázkódás. Az elektromos környezet kiterjed a tápáramellátás minőségére és megbízhatóságára, a berendezések, a berendezések földelésére és az elektromágneses interferenciára (EMI).

A megbízhatóságot befolyásoló üzemeltetési szempontok a következő elemeket tartalmazzák: megfelelő karbantartás, a berendezés helyes üzemeltetése, háttértámogatás a telepítés helyén, a rendszer adathordozóinak kezelése és tárolása, tűz- és árvíz védelem, fizikai biztonság, tisztítás.

A konkrét alkalmazás és használat által megkívánt megbízhatóság alapján kell meghatározni a számítástechnikai berendezések környezetszabályozásának mértékét. Kisebb rendszerek tulajdonosaitól csak azt várjuk el, hogy a környezetszabályozás bizonyos elemeit alkalmazzák. A szükséges környezetszabályozási szint meghatározásához fel kell mérni a számítógép tervezett telepítésének helyét, valamint fizikai, elektromos és működési környezetét. Minél rosszabb és kevésbé kézbentartott a környezet, annál bonyolultabb a szabályozott működési környezet kialakításához szükséges tervezés és a védelem. A géptermek környezetkialakításának meghatározásakor fontos szempont annak a felmérése, hogy milyen költségekkel járnak a környezeti viszonyokra visszavezethető rendszerhibák vagy a nem tervszerű leállások. Ha a teljes rendszert egy helyszínen telepítették, akkor csak abban az esetben lesz megbízható, ha a környezet a leggyengébb "láncszem" követelményeinek felel meg. El kell dönteni, hogy a számítástechnikai berendezést gépterembe, irodai környezetbe vagy laboratóriumba, illetve termelőüzemi körülmények közé telepítik.

Kevés perifériával rendelkező kis rendszereknél nincs szükség álpadlóra. A legtöbb rendszerhez mégis célszerű az álpadló alkalmazása a következő előnyök miatt: vezetékek mechanikai védelme, rugalmasabb telepithetőség, Rf árnyékolás, légcsere, stb. Az építőanyagok kiválasztásánál kívánatos tulajdonságok például a tűzállósági fok, a zajszigetelés, az elektrosztatikus kisülések elnyelőképessége, könnyű karbantarthatóság és tartósság. A felsoroltak mellett egyes elemek jobb védelmet nyújtanak, ha további jellemzőkkel egészülnek ki. A burkolóanyag föld-szigetelési ellenállása legalább 1.0 MOhm, és legfeljebb 20.000 MOhm legyen, 40-60 százalékos üzemi relatív páratartalom és 180 C-240 C hőmérséklet mellett. Hogy ezt elérjük az álpadlóval, a padlót alátámasztó oszloptalpakat az épület földelésére kell kötni. Ez kihatással lehet a felületburkoló anyagokat a felület alapjához kötő ragasztóanyag kiválasztására is, mivel csak villamosan vezető ragasztót lehet használni.

Emellett a berendezések elrendezésének megtervezésekor figyelembe veendő tekintélyes szempontlista mellett nem szabad elfelejteni, hogy a legfontosabb cél a számítógép megbízhatóságának, (Bekapcsolt állapotú) rendelkezésre állásának és teljesítményének növelése. Így a megbízhatósági szempontoknak, mint pl. légáramlás és karbantartás, elsőbbséget kell élvezniük az esztétikai szempontokkal szemben. Egy számítástechnikai létesítmény egy dinamikus környezet, ahol sokféle tevékenység fordul elő rendszeresen. A számítástechnikai, a légkondicionáló rendszert, a nyílvános telefonrendszert és a létesítmény építészeti elemeit bővítik és karbantartják, az új és kiegészítő áramforrások, adatbiztonsági- és tűzvédelmi áramkörök telepítése rendszeresen előfordul. Megfelelő tervezéssel ezeket a tevékenységeket úgy kell kivitelezni, hogy a lehető legkissebb mértékben zavarják a számítástechnikai rendszert.

Az adatvédelem szabályozása a BME-n

Fekete László, *szmts., BME Egyetemi Információs Központ*
E-mail: fekete@eik.eik.bme.hu
Várkonyi Béla, *ts., BME Folyamatszabályozási Tanszék*
E-mail: varkonyi@fsz.bme.hu

1111 Budapest, Műegyetem rkp. 9. R.ép.
1502 Budapest, Pf.91.

Kivonat:

A szerzők a Budapesti Műszaki Egyetem adatvédelmi szabályainak kidolgozását mutatják be. A javasolt szabályzatok többéves elemző és egyeztető munka eredményeit tartalmazzák. A biztonsági szabályzat része a teljes számítógépes infrastruktúra használatot és üzemeltetést szabályozó sorozatnak.

Az adatvédelmi előírások a biztonsági feladatok megfogalmazására alapulnak. A szabályozást egy belső minősítési rendszer fogja össze. A szerzők részletesen elemzik azt, hogy milyen fizikai védelmi módszereket célszerű alkalmazni. Megmutatják azt, hogy a személyzeti védelmi előírások miként befolyásolják az adatvédelem sikerességét. A nagyobb méretű, erősen tagolt szervezetekben szükség van az egyes egységeknél saját helyi szabályok kialakítására. A szerzők javaslatot tesznek ennek rendszerére is. A hardver és szoftver védelmi eszközök alkalmazásánál rámutatnak az ajánlható eljárások lehetséges módozataira. Külön kiemelten foglalkoznak a lokális és távoli hálózatoknál szükséges speciális rendszabályokkal. A megfogalmazott feladatok ellátáshoz a szerzők megadják a szükséges munkakörök, hatáskörök leírását is. Végül a szoftver csomagok installálásával kapcsolatban további eljárási szabályozást javasolnak.

A bemutatott adatvédelmi szabályozás most kerül bevezetésre a BME-n. Egyes részeit azonban már sikeresen alkalmazták néhány szervezeti egységnél.

1. Bevezetés

A számítógépes hálózatok széleskörű elterjedése új feladatok elé állítja az üzemeltetőket. A nagyméretű hálózatokban már igen nehéz átlátni, kézben tartani a különböző erőforrásokhoz a hozzáférési jogosultságokat. Az ad hoc módszereket fel kell váltani szisztematikus ügyviteli szabályozással. E nélkül a számítógépes rendszer biztonságát támogató hardver és szoftver eszközök megfelelő alkalmazása elképzelhetetlen.

A BME Folyamatszabályozási Tanszékén már a nyolcvanas évek második felében elkezdődött a biztonsági szabályzatok kidolgozásával kapcsolatos munka. A kilencvenes évek elején az Egyetemi Információs Központtal közösen folyt a gondolkodás. Ennek eredményeként 1992-ben készült el az első átfogó javaslat a számítógépes infrastruktúra szabályzatainak elkészítésére (ld.[1]-t). Ez a tanulmány a későbbiekben a BME rendszermenedzsereinek közössége elé került megvitatásra. Sajnos néhányan még a létjogosultságát is

megkérdőjelezték. Ezen túl komoly hatásköri, belső politikai kérdések is felmerültek. 1994-ben vált csak lehetővé egy ideiglenes szabályzat kibocsátása (ld. [2]-t). Időközben más intézmények is fontolóra vették hasonló szabályzatok kidolgozását, de csak részleges eredményekről van tudomásunk.

A továbbiakban a BME ideiglenes szabályzatainak kifejezetten biztonsági kérdésekkel foglalkozó részét ismertetjük.

2. Biztonsági szabályzatok

A biztonsági szabályzatok az üzemeltetők részére fogalmazzák meg az adatvédelemmel kapcsolatos előírásokat. Természetesen a felhasználói szabályzatoknak is vannak az adatvédelmre vonatkozó részei. Az egyetemi biztonsági szabályzat csak általános alapelveket, előírásokat tartalmaz. A sikeres adatvédelmi tevékenységhez minden szervezeti egységnek, üzemeltető szervezetnek ki kell dolgoznia a saját helyi szabályait is.

A biztonsági szabályzatok az alábbi fejezetekből épülnek fel:

- Biztonsági feladatok
- Biztonsági minősítések
- Fizikai védelmi előírások
- Személyzeti védelmi előírások
- Szabályozási feladatok
- Hardver védelmi eszközök alkalmazása
- Szoftver védelmi eszközök alkalmazása
- Hálózati biztonsági előírások
- Biztonsági személyzet, hatáskörök
- Szoftver csomagok installálása

A továbbiakban az egyes fejezetekkel kapcsolatos fontosabb tudnivalókat ismertetjük.

3. Biztonsági feladatok

A szabályzatban nyilvánvalóan először meg kell adni a szabályzat célját, hatáskörét. Mi határozottan azt az álláspontot képviseltük, hogy szükség van külön felhasználói szabályzatra, külön üzemeltetési szabályzatra és biztonsági szabályzatra. Ezek között ugyan lehet némi átfedés, de így sokkal jobban kezelhető az alkalmazók számára. A szabályzat készítőjének viszont fokozottan kell ügyelnie az egyes részek közötti konzisztenciára.

A biztonsági feladatokat az üzemeltető személyzet számára fogalmazzuk meg a biztonsági szabályzatokban. Rögzíteni kell az elvárható gondosság fogalmát. A kártérítési felelősség megállapításának egy jó alapja lehet az, hogy a vizsgált személy betartotta-e a szabályzatban megadott előírásokat.

4. Biztonsági minősítések

A felhasználók érdekeinek védelmében az üzemeltető személyzetnek tájékoztatnia kell a felhasználókat az egyes informatikai rendszerek biztonsági lehetőségeiről, az elérhető adatvédelmi szintről. Ez egy igen kritikus feltétele annak, hogy a felhasználók be tudják tartani az információk kezelésére vonatkozó általános szabályokat.

4.1. Minősítési eljárás

Természetesen az informatikai rendszerek adatvédelmi szintjét egy nagyméretű, komplex hálózatban nem könnyű megállapítani. Az egyes rendszerek összehasonlíthatósága is fontos. Ezért létre kell hozni egy a belső igényeknek megfelelő minősítési eljárást. A minősítés komoly következményei miatt szabályozni kell az ezzel kapcsolatos hatásköröket és jogorvoslati lehetőségeket is.

4.2. Kategóriák

A BME-n az egyes számítógépes rendszerek minősítésére az ideiglenes szabályzat öt kategóriát állapít meg:

- I. védelmi rendszer nélküli gép
- II. részleges védelem
- III. privát anyagok védelme
- IV. bizalmas anyagok védelme
- V. titkos anyagok védelme

A kategóriák definiciója a rendelkezésre álló hardver és szoftver eszközökre, az alkalmazott fizikai és ügyviteli védelmi eljárásokra alapul. A szoftvereket a TCSEC kritériumok alapján kell besorolni.

4.3. Ügyviteli és fizikai védelem figyelembe vétele

A minősítési eljárásban figyelembe kell venni, hogy az ügyviteli védelem azonos szinten áll-e a fizikai ill. a szoftver védelmi eszközökkel. Ehhez megfelelő módon auditálni kell a rendszert üzemeltetők tevékenységét. A gyenge ügyviteli védelem megállapítása esetén alacsonyabb kategóriába kell sorolni a rendszert, nehogy a felhasználók hamis tudatban legyenek anyagaik biztonsága felől.

4.4. Informatikai tevékenységek és biztonsági kategóriák viszonya

Az informatikai rendszerek felhasználói számára meg kell fogalmazni a biztonsági kategóriák és a szokásos munkatevékenységek során keletkező információk közötti viszonyt. Ezen a téren lesznek a legnagyobb viták, itt lesz a legnehezebb betartatni az előírásokat. Fell kell hívni a figyelmét az ellenlábasoknak arra, hogy az adatvédelmi törvény és jogszabályok komoly kötelezettségeket rónak a felelős vezetőkre. A feladatok végrehajtása elképzelhetetlen a biztonsági rendszer szervezett minőségi kontrollja nélkül.

5. Fizikai védelmi előírások

A felhasználási módtól függően szabályozni kell a számítógépek fizikai védelmi szintjének minimális követelményeit. A kritikusabb alkalmazási területeken kötelezővé kell tenni a zárható helyiségben történő elhelyezést, a gépkulcs vagy más hozzáférést gátló eszköz használatát. Az előírások esetleges megsértése fontos minősítési szempont.

Két területen lesz még szükség a szabályozás részletezésére. Az egyik a szerver konzolok fokozott védelme. Ugyanis minden operációs rendszerben a konzolról megfelelő módszerekkel megkerülhető a szoftver védelmi rendszer. A másik kritikus fizikai védelmi terület, ami további megfontolásokat igényel, a hálózati kábelezés védelme. Jelenleg még nincs kialakult elképzelés ezen a téren.

6. Személyzeti védelmi előírások

Sokan meglepődtek azon, hogy személyzeti védelmi előírások is megjelentek a biztonsági szabályzatban. Nagyon nehéz lesz ezek érvényesítése a gyakorlatban, de véleményünk szerint mindenképpen jobb leírni a korrekt eljárásokat, mint a nehézségek miatt szönyeg alá söpörni a problémákat. Ez a rész azonban különösen megmutatja azt, hogy a biztonsági szabályzat alkalmazhatóságának egyik alapfeltétele az, hogy a lehető legmagasabb jogkörű testület hagyja jóvá azt és tegye kötelezővé a szervezeti egységek vezetői számára.

Nyilvánvalóan az első követelmény az üzemeltető személyzettel szemben a feddhetetlenség, hiszen bizalmi állást töltenek be, a kezükbe kerülő információkkal vissza tudnának élni. A feladatok ellátásának megkezdését meg kell előznie a megfelelő kioktatásnak. Jól megfogalmazott jogi nyilatkozatok aláírásával is alá kell támasztani az egyéni felelősség érvényesítésének lehetőségét. Az alkalmazott kilépéskor ügyelni kell a jogok törlésére, hiszen a mai globális hálózatokon könnyen hozzáférhető sok erőforrás, s az eltávozott alkalmazottal szemben nehéz érvényesíteni szankciókat.

A legnehezebben teljesíthető követelmény, de ugyanakkor mégis a legfontosabb, a motiváció megteremtése, az anyagi és erkölcsi megbecsülés biztosítása. Nagyon törkény az a rendszer amely csak a negatív elemekre, szankciókra épít. Sokkal robosztusabb egy olyan szisztéma, ahol a pozitív késztetések a meghatározók.

A biztonsági előírások érvényesítésekor nem szabad liberálisan eljárni. Ez rövid úton az egész rendszer összeomlásához vezet. A biztonsági szabályzat komolyabb megsértése esetén csak az elbocsátás lehet a hatékony védekezés alapeleme.

7. Szabályozási feladatok

Rengeteg olyan kérdés merül fel a gyakorlatban, amely további szabályozást igényel, de egy nagy intézményre vonatkozó általános szabályzatba nincs értelme foglalkozni vele. Ezért kötelezni kell a szervezeti egységek vezetőit a helyi biztonsági szabályzatok kidolgozására.

A helyi szabályzatnak rendelkeznie kell az adatvédelmi felelős kijelöléséről, a rendszer biztonsági ellenőrzések végzéséről, a biztonsági mentések és visszaállítások szervezéséről, a kockázat és kár elemzése, az elhárítási tervek készítése során követendő eljárásokról.

A helyi szabályzatoknak összhangban kell lennie a globális előírásokkal. Ezért a központi üzemeltető szervezetnek véleményeznie kell azt. Ez biztosítja a szakmai szinvonal kontrollját is.

8. Hardver védelmi eszközök alkalmazása

A legmagasabb biztonsági igényű kategóriákba sorolt gépek közötti kommunikáció védelme kiemelt fontosságú. Elő lehet írni hálózati forgalmat kódoló eszközök alkalmazását, vagy elkülönített optikai hálózat telepítését.

A nem megfelelően kiválasztott hardver védelmi eszközök alkalmazása komoly üzemltetési problémákat vethet fel. Ezért elő kell írni az ilyen berendezések kötelező bevizsgálását a központi üzemeltető szervezet számára. Ugyancsak a központi üzemeltető szervezet jogává kell tenni az ilyen berendezés engedélyezését az egyes szervezeti egységek számára. Ez egyrészt fontos a globális hálózat konzisztenciája szempontjából, másrészt előfeltétele a titkosítással kapcsolatos jogszabályi előírások teljesítésének.

9. Szoftver védelmi eszközök alkalmazása

A rendelkezésre álló szoftver védelmi eszközök alkalmazása sokban függ a helyi viszonyoktól, igényektől, de néhány alapelvet az általános szabályzatban is rögzíteni kell. Amennyiben egy rendszerben megvan a lehetőség a felhasználó azonosítási módszerek finomabb beállítására, akkor a következő minimális követelményeket célszerű megfogalmazni:

- jelszavak minimális hossza normáls és privilegizált témaszámokon
- könnyen kitalálható jelszavak visszautasítása
- kísérletezés kitiltása
- automatikus jelszó lejárat alkalmazása

Amennyire lehet automatizálni kell az eljárásokat, így például az időleges alkalmazottak, diákok, hallgatók esetén a témaszámokat automatikus lejárattal kell ellátni. Lehetőség szerint gondoskodni kell a kritikus fájlok felülírás védelméről és betörési kísérletek esetén a riasztásról. A tartósan távol levő felhasználóknál be kell vezetni a témaszámok ideiglenes letiltásának gyakorlatát. A felhasználók felelőségét csak akkor lehet érvényesíteni, ha ragaszkodunk a személyes témaszám átadáshoz. A rendszergazda kötelességévé kell tenni az operációs rendszer biztonsági lehetőségeinek tanulmányozását, a biztonsági minősítés megismertetését a felhasználókkal.

10. Hálózati biztonsági előírások

A hálózat kiváló táptalaja a betörési kísérleteknek, az illegális adatszerzési akcióknak. Néhány minimális követelmény előírása azonban nagy mértékben segítheti az üzemeltetők hibakeresési, nyomozási tevékenységét. Amennyiben azt az operációs rendszer lehetővé teszi, legalább a be- és kilépések naplózását elő kell írni. Rendelkezni kell a naplók megörzéséről és hozzáférhetőségéről.

A globális hálózatra új szolgáltatások felvétele csak szabályozott módon történhessen. A szolgáltatások nyújtásának biztonsági feltételei közé tartozik a minimális biztonsági minősítés megfogalmazása, egy kötelező regisztrációs ill. engedélyezési eljárás bevezetése.

A munkaállomások telepítésénél is meg kell követelni a központi regisztrációt és engedélyezést. A nagyméretű hálózatoknál ezzel kapcsolatban le lehet adni jogköröket alacsonyabb szintre, ha vannak leválasztott részhálózatok, de a nyilvántartásnak mindenképpen egységesnek kell lennie. Csak ekkor van lehetőség az eljárásra az illetéktelenül csatlakozók ellen. Az illegális csatlakozások felderítése és megkakadályozása alapvetően befolyásolja az elérhető biztonsági szinvonalat.

11. Biztonsági személyzet, hatáskörök

A biztonsági szabályok betartásának ellenőrzése, a biztonsági feladatok végrehajtása speciális szakértelmet és gyakorlatot igényel. Ezért a magasabb biztonsági kategóriákban elő kell írni adatvédelmi felelős kijelölését minden helyi rendszernél. Ezen túl az egyes nagyobb hálózati részekhez hálózati adatvédelmi felelőst is kell rendelni. (Elméletileg az adatvédelmi felelősi funkció összeférhetetlen más üzemeltetési funkcókkal, ezt azonban gyakorlatilag szinte lehetetlen megvalósítani.)

A hálózati adatvédelmi felelős feladatai közé tartozik a biztonsági minősítés megállapítása, a forgalom figyelés, a nyomozás, az adatvédelmi rendszerek ellenőrzése, a fejlesztési elképzelések kidolgozása, vészhelyzetben a hozzáférések korlátozása. A lokális adatvédelmi felelős feldatai közé tartozik a helyi szabályok kidol-

gozása, ellenőrzése, a felhasználói tevékenység figyelése, a vírus detektálás és irtás, vészhelyzetben a hozzáférések korlátozása.

12. Szoftver csomagok installálása

A szoftver csomagok installálására is elő kell írni bizonyos alapelveket. Ennek két fő célja van. Az egyik az értékes szoftverek integrítás védelme, a másik a vírusok terjedésének meggátolása.

Kötelezeően elő kell írni a biztonsági másolat készítését. Az installálást csak a munkapéldányról szabad végezni. Az eredeti példányt biztonságos helyen kell tárolni.

Az installálás előtt a rendszergazda kötelessége az összes lehetséges módszerrel a vírusellenőrzés elvégzése. Működési tesztekkel is ellenőrizni kell, hogy a szoftver valóban az aminek állítja magát. Feltétlenül szükséges az írásvédelem alkalmazása az archívumokban.

A különböző alkalmazások telepítését lehetőleg egy példányban a szervereken kell megtenni, majd írásvédelemmel kell ellátni a könyvtárakat és fájlokat. Ez a praxis nagy mértékben csökkenti a vírusveszélyt ahhoz az állapothoz képest, amikor minden alkalmazás TCSEC D kategóriájú gépeken (PC-k) van installálva.

A helyi szabályzatokban sok esetben meg lehet tiltani, hogy a felhasználók bármiféle programot saját kezűleg telepítsenek.

13. Összefoglalás

Az ismertett biztonsági szabályozás sok ember tevékenységét érinti, s több esetben a vezetők számára is komoly feladatokat fogalmaz meg. Ezért a bevezetése igen nehéz, hosszas diplomáciai, politikai előkészítést igényel. Jelenleg ideiglenes jelleggel az EIK elkezdte a szabályzat bevezetését, de még várat magára az illetékes szervezet, az Egyetemi Tanács döntése. A jóváhagyás esetén is hatalmas erőfeszítések kellenek majd az egyes emberek kiképzésére, a motivációk megteremtésére, a széleskörű elfogadtatásra. "Szerencsére" az utóbbi időben elszaporodó betörések, biztonsági problémák egyre több eddig ellenségesen viszonyuló rendszermenedzser számára megmutatják a szabályozás szükségességét.

A problémák ellenére is azonban megállapíthatjuk, hogy a kilencvenes évek elején megindult szabályozási kezdeményezések fontos szerepet töltöttek be az egyetemi hálózat üzemképességének fenntartásában.

Irodalomjegyzék

[1] Várkonyi Béla: "Számítógépes infrastruktúra szabályzatok", (tanulmány), BME EIK, 1992.

[2] Fekete László, Várkonyi Béla: "Hálózati szabályzatok - a BME hálózati szabályzata", Networkshop '94, Keszthely, NJSZT-IIF, 1994 (előadás)

Information and Communications Security

by CRYPTO AG

Legitimate users of EDP systems and networks have become highly vulnerable to tapping and changing of information elements by "leisure time hacking" or even well-aimed professional attack or sabotage. Considering that in this, the Information Age, we absolutely rely upon secure communication, this means that:

- in many cases, virtual channels do not allow control to be maintained on physical paths.
- usually, it is difficult to detect whether unwanted third parties have copied information.
- damage may originate from compromised information believed to be genuine.

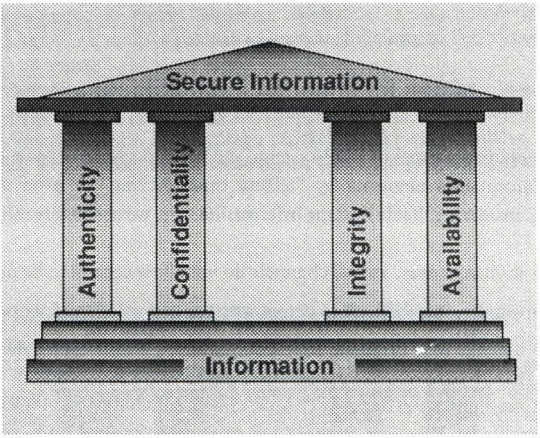
Communication Security (Comsec) with suitable crypto-logical measures will eliminate only some of these problems. However, in more and more cases integral Information Security – **Infosec** – is the way to go:

- End-to-end ciphering and integrity control bring a higher level of security *per se*.
- Access and boot control, as well as user-level differentiation is assimilated.
- Lower and higher layer security covers the entire system, not just dedicated elements.
- One all-encompassing security umbrella even for multivendor environments

The state-of-the-art approach to your security problem.

The strict requirement not to compromise on organisational, physical or logical measures in order to carry through and enforce security concepts should lead to these four basic elements of integral **Infosec:**

- **Authenticity**: To prevent illegal access to valuable data and EDP resources
- **Confidentiality**: To keep information secret – both in the system and during communication
- **Integrity**: To ensure the integrity of information
- **Availability**: To keep the system ready for legal users within their authority range



To cover all the above it needs no less than a tailor-made solution to let our customers resolve these problems in a way which is specific to their structure, organisation, personnel and security philosophy.

Accordingly, Crypto serves the security market with an exhaustive **Infosec** – package comprising analysis, planning, project management, and realisation which defines all the necessary ingredients for a customer-specific security solution.

Packages tailored for the needs of the respective organisation.

These are just a few examples on how
Governmental organisations may use **Infosec** effectively:

Every day Ministries of Foreign Affairs create, process and file information of national security, which is forwarded to their embassies all over the world.
Crypto's security solutions will protect this vital information - from the office of the Minister to the Ambassador's desk - against unauthorised access, alteration, deletion, and misuse.

The Armed Forces - Army, Navy, Air Force depend on well-functioning and secure command and control systems. Today's military have access to the most modern electronic systems - but so has the enemy.
Whether at a strategic or tactical level, Crypto has the solution to keep the electronic data processing and communication systems safe.

Information about the organisation, the administration, and the personnel files of Ministries and other governmental departments has to be kept confidential during generation, processing, communication and archiving. Keep your "inside" information "inside" through EDP-security systems from Crypto.

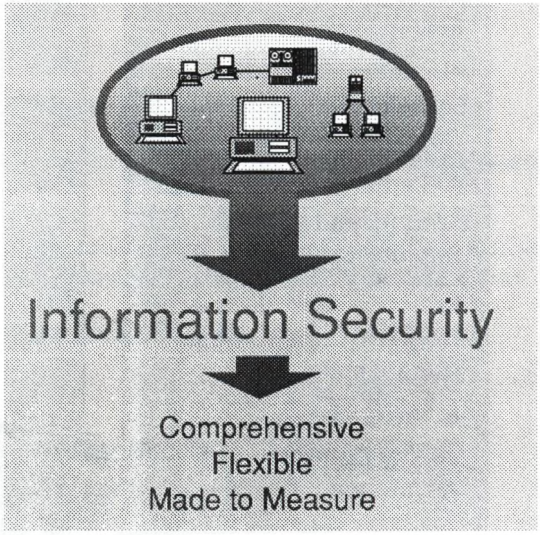
With all the data security tasks from one source.

Crypto's complete and accurate implementation of **Infosec** incorporates:

- Coverage under just one umbrella from local access to integrated solutions
- From one source – solutions for hardware, software, firmware, and brainware
- Integration of features like management, control, and auditing
- Powerful state-of-the-art algorithmic processing as for all of the systems
- Modular philosophy to support the evolutionary development of your networks

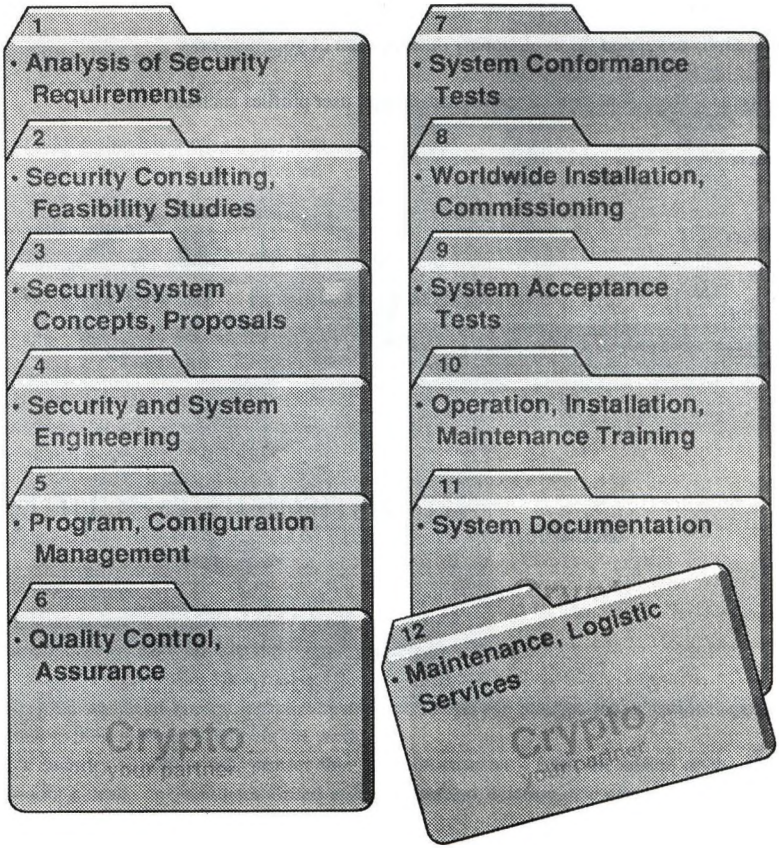
Crypto's **Infosec** packages adopt your structures and support user profiles such as:

- Individual users
- User groups
- System manager
- Administrator
- Internal Auditor
- External Auditor



From the very first planning session downstream to...

With its wide and global experience in managing large projects of integrated high security systems in over 120 countries Crypto is your partner for:



After-sales-service and maintenance; Crypto is at your disposal.

With experience accumulated over more than 40 years, Crypto continues to be at the forefront of developing and manufacturing information security products. It is today one of the world's leading manufacturers of ciphering systems built to the highest standards of cryptological technology.

Crypto, located in the heart of Switzerland, is an independent company with development, engineering, manufacturing, and support services all under one roof.

The use of the latest technology in the field of algorithms, security management, and integrated security engineering is the main focus of our activities.

Our engineers make sure that Total Quality Assurance meaures are kept in the centre of the entire development and manufacturing process. This is done by the exclusive implementation of high quality hardware and software elements into our products and systems.

In acknowledgement of this stringent dedication to quality, Crypto has earned:

The Swiss Quality Standard (SQS) Certificate in full compliance with ISO 9001/EN29001
(equivalent to NATO's AQAP-1)
Production Quality Assurance Approval Number 0490 of BABT meeting the EU Council Directive 91/263 EEC.

In its role as an experienced contractor Crypto has designed, developed, manufactured, installed, commissioned and maintained turnkey EDP and communications systems for various applications, such as:

- Secure client/server systems in a LAN/WAN environment
- Secure document archiving system
- Nationwide node authentication system
- Secure worldwide store and forward message handling system
- Secure radio data system for mobile access to computer networks
- Secure border patrol voice and data communication

Crypto, your partner in all fields of demanding Infosec today and tomorrow.

CRYPTO AG
P.O. Box 474
CH-6301 Zug/Switzerland
Phone +41 42/44 77 22
Fax +41 42/41 22 72
Telex 868 702 cry ch