HÁLÓZATBIZTONSÁGI TECHNIKÁK AZ EGÉSZSÉGÜGYBEN

Ködmön József, *h8628kod@ella.hu*
Takács Péter, *h8627tak@ella.hu*
DOTE Egészségügyi Fõiskolai Kar

Abstract

The lecture is about the controlling and realization of the data safety and data security, andis treating the special features of handling the data in the health care. It is analyzing the security functions of the Novell Netware, the Windows for Workgroups, Windows NT and UNIX operating systems. Is shows some security holes. It offers some rarely applied networking data safety technique, such as NCP packet signature, Kerberos system.

1. Bevezetés

Az egészségügy különbözõ területein egyre elterjedtebbek a számítógépek, a hagyományos ügyviteli, adminisztrációs rendszereket számítógépes szoftverek helyettesítik. Ezek egy jelentõs része, fõként a kórházakban, hálózatban mûködik. Ez a technikai váltás azonban nem hozott egyértelmû javulást az adatvédelem ter ületén.

Az egészségügyi hálózati alkalmazások használatánál is sok probléma jelenik meg, hiszen a hálózati operációs rendszerek által szolgáltatott adatvédelmi, biztonsági lehetõségeket általában igen kis mértékben használják ki. Gyakran fordul elõ, hogy egyforma belépési jelszót alkalmaz egy teljes kórházi osztály, több évig használhatók azonos jelszavak, nincsenek hierarchikus, a tevékenységi kompetenciának megfelelõ hozzáférési jogosultságok. Igen gyakori, hogy az egyébként számítógépekkel felszerelt, egészen jól mûködõ szoftvereket használó egészségügyi szervezeti egységnek nincs Informatikai biztonsági szabályzata, nincs kinevezett, egyértelmû munkaköri leírással rendelkezõ rendszergazdája és adatvédelmi fel elõse.

Mivel az egészségügyi intézmények nagyrészt személyes adatokat, sõt azon belül igen gya kran különleges adatokat kezelnek, alapvetõen fontos azok biztonsága és védelme.

Természetesen vannak az egészségügyben is olyan szervezeti egységek, amelyeknél az ada tvédelemmel, adatbiztonsággal kapcsolatos tevékenységek is jól mûködnek, de sajnos nem ez az általános, az ilyen intézmények száma elég k evés.

2. Az adatvédelem szabályozási szintjei

Az elsõ szinten lévõ általános adatvédelmi törvények az adatvédelmi rendszer kereteit hat ározzák meg. Mivel az informatikai rendszerek dinamikusan változnak, a konkrét szabályozás a rendszer változását követõ, szintén dinamikusan változó szabályhalmazt jelent. Magyarországon ezt az általános funkciót megvalósító törvény a személyes adatok védelmérõl és a közérdekû adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.

A második szint a mûszaki normák, szabványok, irányelvek, rendeletek szintje. Ide tartoznak az építésügyi, tûzvédelmi normák, szabványok és rendeletek; a beruházásokra, az általános és speciális iratkezelésre, a titokvédelemre vonatkozó jogszabályok és rendeletek. Meghatározó jelentõségûek az Európa Tanács és az OECD ajánlásai, valamint egyéb a témával foglalkozó nemzetközi szervezetek iránymutatásai.

Természetesen az adatvédelmi rendszer tervezésénél semmiképpen sem szabad figyelmen kívül hagyni a korábbi hagyományos adminisztrációs és ügyviteli rendet sem.

A harmadik szintet az ágazati, tárca szintû végrehajtási utasítások alkotják. Sajnos jelenleg ezen a területen csak egy régen elfogadásra váró tervezet létezik. Ez rögzíti az egészségügyi adatok kezelésének alapfogalmait és az adatkezelés lehetséges formáit. A tervezet kötelezõvé teszi az egészségügyi intézményekben az adatvédelmi felelõs kijelölését, valamint adatvédelmi szabályzat kidolgozását és használatát. Az egészségügyi adatok kezeléséröl szóló rendelet valószínûleg beépül a megújuló egészségügyi törvénybe és az így teljessé váló szab ályozás kerül majd elfogadásra.

A negyedik szint a helyi, intézményi szabályok halmaza. Minden egészségügyi adatok kezel ésével foglalkozó intézménynek kell készíteni egy Informatikai biztonsági szabályzatot. Ebben az elõzõekkel egyeztetve az alábbiakat kell szabályozni:

- a védelmet igénylõ adatok, eszközök és objektumok köre és azok védelmének szintje,
- az információs rendszer elemeinek védelme,
- az adatvédelmi felelõs tevékenysége, jogai és kötelezettségei,
- az adatokat kezelõ személyzet tevékenysége, jogai és kötelezettségei,
- a rendelkezéseket megszegõk szankciói.

Ebben a szabályzatban tehát olyan intézkedéseket kell tenni, amelyek illeszkednek az inté zmény egyéb szabályzataihoz és az informatikai rendszerre irányuló veszélyek, veszélyforrások hatásait elfogadható mértékûre csökkentik.

3. Az adatvédelem megvalósításának szintjei

A fizikai védelem szintje a számítógép, annak közvetlen környezete és az adathordozók v édelmét jelenti. A számítógépes helyiséget különféle beléptetõ rendszerekkel és mozgás, valamint hõérzékelõ berendezésekkel szokás védeni. A fontos adathordozókat tûzbiztos páncélszekrényben táro lják.

Az ügyviteli védelem az informatikai rendszert üzemeltetõ szervezet ügyme netébe épített biztonsági szabályok, tevékenységi formák együttese, amelyet az Informatikai biztonsági szabályzat ír le. Az ügyviteli védelem a fizikai védelemre épül, a teljes védelem egy következõ rétegét képezi. Míg a fizikai védelem a rendszerbe való engedélyezett belépési pontokat jelöli ki, addig az ügyviteli védelem a belépési pontok igénybevételének elfogadható, elvárt formáit rögzíti.

Az algoritmikus védelem azokból az eljárásokból áll, amelyek a rendszer szolgáltatásaival egyidejûleg, velük szorosan együttmûködve látják el a védelmi feladatokat. A magas szintû adatvédelem algoritmikus eszközei a következõk: adatok titkosítása, rejtjelezés, partner azonosítás, hitelesítés, digitális aláírás, idõpecsét és eseménynapló.

Ezek az eszközök ma már fõként számítógépes környezetben használhatók, mai fejlettségi szintjükön elvileg lehetõvé teszik a papírmentes adminisztráció megvalósítását. A papír alapú adminisztrációs rendszerek dátumának, pecsétjének és aláírásának számítógépes környezetben az idõpecsét és a digitális aláírás felel meg. Ezeket az informatikai eszközöket IC kártya alapú betegkártyával, biztosítási kártyával valamint orvosi kártyával kiegészítve, valóban megvalósítható egy nagykiterjedésû hálózatban mûködõ egészségügyi adminisztrációs rendszer, amelynek az adatvédelme és adatbi ztonsága megfelel az európai szintû elvárásoknak.

4. Az egészségügy speciális védelmi követelményei

Az orvos tudomására jutott adatok tárolása, kezelése a szakma évszázados hagyományai alapján, az orvosi titoktartás elõírásai szerint történik. Eddig egyedül az orvos volt felelõs az adatoknak a betege és a lakosság egészsége érdekében való felhasználásáért. Mára az orvostudomány és az információs technológia gyors fejlõdése miatt nem mindenben tarthatók az évszázados hagyományok. Megõrizve az összes bevált és

folytatandó gyakorlatot, föltétlenül szükséges felülvizsgálni, az európai elvárások szerint újragondolni ezt a nagyon összetett problémát.

Az egészségügyi adat (az érintett testi, lelki és értelmi állapotára, kóros szenvedélyére és szexuális szokásaira, valamint a megbetegedés körülményeire vonatkozó adat) a személyes adatokon belül a különleges adat kategóriájába tartozik, melynek kezelését az érintett, vagy egy törvény engedélyezheti. A különleges személyes adatok kezelésének fontosságát az Európa Tanács ajánlása is elismeri: Recommendation No. R(81) 1 on the Regulations for automated medical data banks (Ajánlás az automatizált gyógyászati adatbankokról).

A társadalombiztosítási célok érdekében használt személyes adatok védelmével a Recommendation No. R(86) 1 on protection of personal data used for social security purposes címû ajánlás foglalkozik.

Az Európa Tanács az adatkezelés és adatvédelem egy speciális részkérdésével, az írásos bizonyíték megkövetelésére vonatkozó jogszabályok harmonizációjáról és az iratmásolatok, illetve a számítástechnikai eszközökön rögzített adatok elfogadásáról szóló R(81) 20 számú ajánlásában foglalkozik. Az egészségügyi szféra számára is igen fontos, hogy a számítógépen rögzített adatok, iratok az igazságszolgáltatási eljárás során bizonyítékként elfogadhatók legyenek. Az ajánlás elõírja, hogy a fenti módon készült dokumentumoknak milyen biztonsági elvárásoknak kell eleget tenniük.

5. Hálózati operációs rendszerek adatvédelmi, biztonsági lehetõségei

5.1. Novell NetWare

Ez a legelterjedtebb hálózati operációs rendszer. Kelet-Európában, illetve Magyarországon különösen nagy a piaci részaránya. Gyakran olyan egészségügyi informatikai rendszerek is erre a platformra kerülnek, amelyek máshol alapvetõen a nagygépes világ speciális szolgáltatásaira épülnek.

A NetWare operációs rendszer 4.x verziójától teljesíti a C2 biztonsági osztály követelményeit. Ez az osztályozás az Egyesült államok védelmi minisztériuma által kidolgozott Megbízható Számítógép Rendszerek Kiértékelési Kritériumának Interpretálása Megbízható Hálózatokra (Trusted Network Interpretation of the Trusted Computer System Evaulation Criteria). A C2 a szabályozott hozzáférési védelemmel rendelkezõ rendszerek osztályát jelenti. Ez a hálózati operációs rendszer volt az elsõ, amely megkapta az NCSC (National Computer Security Center, USA) C2 minõsítését, illetve a közel azonos európai ITSEC által kiadott E2 minõsítést. Ismereteink szerint több külsõ cég foglalkozik a NetWare 4.x B1 illetve B2 kritériumoknak megfelelõ kiegészítések tervezésével, amelyeknek a rendszerhez való illesztésével egy lényegesen magasabb szintû adatvédelem és adatbiztonság valósítható meg.

A C2-es minõsítés a nagyvállalatok rendszereinél a szokásos szintet jelenti, a banki rendszereknél pedig a minimálszintet. Az egészségügyi intézmények által kezelt személyes és különleges adatok kezelésére is alkalmas.

Itt most a NetWare védelmi és biztonsági rendszerét nem részletezzük, hiszen számos publikáció és a rendszer dokumentációja is részletesen leírja azt. Felhívjuk azonban a figyelmet egy talán kevéssé alkalmazott, de igen fontos védelmi lehetõség használatára.

A hálózatoknál speciális problémát jelent az információt továbbító kábelrendszer hatékonyvédelmének megoldása. A hálózati kábel megcsapolása különösen veszélyes lehet, ha a támadó a különleges adatokat hallgatja le, vagy hamisított csomagok hálózatba juttatásával magas szintû jogosultságokat szerez. Ennek megakadályozására szolgál a NetWare 4.x csomag aláírási lehetõsége.

5.1.1. Az NCP csomag aláírása

Az NCP (NetWare Core Protocol) csomagok digitális aláírásával megelõzhetõ a hamisított csomagok hálózatba juttatása oly módon, hogy a csomagokat a szervernek és a munkaállomásoknak is lehetõsége van aláírással megjelölni. Amennyiben nem megfelelõen aláírt csomagot észlel a hálózat, azt azonnal lekönyveli a hibanaplóba (errorlog). A szerver konzol képernyõjére is érkezik egy üzenet, ami a problémás csomaggal összefüggésbe hozható munkaállomás címét és az ott bejelentkezett felhasználó LOGIN nevét is tartalmazza, így a rendszerbe való illetéktelen behatolás gyanúja azonnal fölmerül.

Ha a csomagok aláírása funkció telepítve van a rendszerben, akkor gyakorlatilag lehetetlen meghamisítani az NCP csomagokat. Ennek a magas szintû biztonságot eredményezõ funkciónak a használata mind a munkaállomáson, mind pedig a szerveren a processzort veszi igénybe, emiatt a hálózat mûködése lassul. Ezért nem is javasolt minden munkahelyre, nem ez a rendszer alapbeállítása. A munkafeladatok függvényében a hálózati rendszeradminisztrátorok dönthetik el, hogy alkalmazzák-e a csomagaláírást a szerverek és munkaállomások közötti kommunikáció biztonságának fokozására. Az alábbi esetekben **nem célszerû** az NCP csomagok aláírását használni:

- csak futtatható programok, állományok vannak a szerveren,
- az összes felhasználó személyesen ismeri egymást és a rendszergazda megbízhatónak tartja a felhasználókat,
- az adatok nem esnek valamely titkossági fokozatba, elvesztésük vagy sérülésük nem lesz végzetes kihatással az üzemelésre.

Az alábbi esetekben viszont **ajánlatos** a csomagok aláírásának használata a nagyobb biztonság érdekében:

- a hálózatban õrizetlen, nyilvánosan hozzáférhetõ munkaállomások is vannak,
- megbízhatatlan felhasználók is dolgoznak a hálózat munkaállomásainál,
- könnyû hozzáférni a hálózati kábelekhez,
- titkos, bizalmas információkat tárolnak a szerveren.

5.1.2. A csomagaláírás opciói

A szerveren és a munkaállomásokon külön-külön beállítható négy védelmi szint közül lehet választani. A 0. a legalacsonyabb szint, ez nem jelent védelmet, a 3. pedig a legmagasabb, ekkor a szerver és a kliens kizárólag aláírással megjelölt csomagokkal kommunikál. Az alapértelmezett NCP csomag aláírási szint az 1. Általában ez nyújtja a legtöbb rugalmasságot, a védelem és a mûködési sebesség megfelelõ kompromisszumát. A szerveren és a munkaállomáson beállított szintek együttesen döntik el az NCP csomagaláírás védelmi szintjét.

A kliens aláírási szintjét a **net.cfg** fájlban lehet beállítani a

SIGNATURE LEVEL = szintszám

parancssor beírásával. Az alábbi táblázatok mutatják az egyes beállítási szintek jelentését a kliens és a szerver esetére.

Szám	Kliens tevékenység
0	A kliens nem írja alá a csomagot.
1	A kliens csak akkor írja alá a csomagot, ha a szerver kéri azt (a szerver opciója 2, vagy annál magasabb).
2	A kliens csak akkor írja alá a csomagot, ha a szerver alkalmas az aláírásra (a szerver opciója 1, vagy magasabb).
3	A kliens aláírja a csomagot és a szervernek is alá kell írnia a csomagot, egyébként a bejelentkezés meghiúsul.

Szám	Szerver tevékenység
0	A szerver nem írja alá a csomagot (független a kliens aláírási szintjétõl).
1	A szerver csak akkor írja alá a csomagot, ha a kliens kéri azt (a kliens aláírási szintje 2, vagy annál mag asabb).
2	A szerver csak akkor írja alá a csomagot, ha a kliens alkalmas az aláírásra (a kliens aláírási szintje 1, vagy magasabb)
3	A szerver aláírja a csomagot és minden klienst kötelez az aláírásra, egyébként nem lehet bejelentkezni.

Az aláírási szintet a szerver konzolján a következõ paranccsal lehet beállítani:

SET NCP PACKET SIGNATURE OPTION = szintszám.

A szerveren és a munkaállomásokon beállított aláírási szintek együttesen határozzák meg a tén yleges csomagaláírást, vagyis azt, hogy a hálózat milyen biztonsági lehetõségekkel rendelkezik. A szerver és a kliens szintek szélsõséges kombinációja esetén a munkaállomásról be sem lehet jelentkezni a szerverre. A következõ táblázat a szerver és a kliens aláírási szintek közötti kapcsolatot m utatja:

Ha	Szerver=0	Szerver=1	Szerver=2	Szerver=3
Kliens=0	O	O	O	∅
Kliens=1	O	O	l	l
Kliens=2	O	l	l	l
Kliens=3	∅	l	l	l

Jelölések:

l: csomagaláírás O: nincs csomagaláírás ∅:nem lehet bejelentkezni

Természetesen a NetWare dokumentációk számos tanácsot adnak a védelmi, biztonsági leh etõségek beállítására, használatára. Nagyon fontos azonban, hogy sohasem feledkezzünk meg arról, hogy ezek a lehetõségek az ügyviteli és fizikai védelmi szint megfelelõ alkalmazása nélkül semmit sem érnek.

5.2. Windows for Workgroups, Windows NT

A Windows típusú grafikus felhasználói felületek igen népszerûek, hiszen kezelésük igen eg yszerû, sok jótulajdonsággal rendelkeznek. Az adatvédelmi, biztonsági funkciók azonban igen sokszínû képet mutatnak. A feladatok függvényében nagyon körültekintõen kell kiválasztani a használni k ívánt hálózati grafikus felületet.

Ha azonos projecten, hálózatban dolgozó, egymást jól ismerõ, megbízható munkatársak eg yszerû hálózathasználati igényeit akarjuk kielégíteni, valószínûleg elegendõ a Windows for Workgroups használata. Ez a rendszer nem önálló operációs rendszer, használja a DOS-t, többek között ez az oka annak, hogy a biztonsági, védelmi rendszere a korábban említett osztályozás szerint D szintû, azaz csak minimális védelmet biztosít.

Ha biztonsági, védelmi szempontból igényesebb hálózati feladatokat akarunk grafikus fe lhasználói felületet igénylõ szoftverekkel megoldani, akkor föltétlenül a Windows NT hálózati operációs rendszert célszerû választani, mivel ez teljesíti a C2 biztonsági osztály követelményeit, sõt a kõvetkezõ verziókban - az ígéretek szerint - a B2-es szintet fogja elérni. Ennek a rendszernek a biztonsági filozófiája hasonló a Novell NetWare 4.x operációs rendszeréhez, de a biztonsági, védelmi funkciók adminisztrálása, beállítása kevéssé kiforrott.

Egyes biztonsági szakértõk véleménye szerint [3] jobb, ha inkább külsõ gyártók biztonsági, védelmi rendszereit integráljuk és nem használjuk a Windows NT ilyen funkcióit.

A Windows 95 biztonsági, védelmi funkciói is sok szakértõ által vitatottak. Számos olyan t ámadási lehetõséget ad a betolakodóknak, amelyet csak külsõ cég által gyártott, a rendszerhez integrálható biztonsági rendszerekkel lehet megszüntetni.

5.3 Unix

Az egészségügy számos területén a feladatok nagysága indokolja a PC-nél nagyobb teljesí tményû számítógépek használatát, amelyek többnyire valamilyen UNIX operációs rendszert használnak. A UNIX rendszert alkotói teljesen nyílt rendszernek szánták, így a más rendszerekben (például VMS) megszokott védelmi módszerek csak kevéssé jellemzõek. Ha legalább C2 szintû biztonságra törekszünk, akkor be kell tömnünk a rendszer biztonsági lyukait.

5.3.1. Biztonsági lyukak a UNIX-ban

A teljesség igénye nélkül a legfo ntosabb biztonsági lyukakra (security hole) hívjuk fel a figyelmet. Ezen biztonsági Achilles-sarkak megszüntetésével a rendszer egészségügyi adatok kezelésére is alkalmassá válik. A legfontosabb teendõk a megbízható biztonsági szint eléréséhez:

- a jelszavak megfelelõ kezelése: a rendszerbe való belépés a rendszerbiztonság legkritikusabb pontja. Nagyon szigorúan be kell tartatni a jelszavak kezelésével és a belépési procedúrával kapcsolatos általános szabályokat. Ez csak szigorú szankciókat kilátásba helyezõ ügyviteli sz abályokkal együtt lehet hatásos.
- az Anonymus-szolgáltatások ellenõrzése: az **ftp** démont vagy teljesen le kell tiltani, vagy egy olyan változatát kell használni, amely az eredetinél lényegesen nagyobb ellenõrzési lehetõséget biztosít.
- az "R" szolgáltatások használata nem javasolt: az **rlogin**, **rcp** és hasonló parancsok segítségével távolról, esetleg jelszó ismerete nélkül illetéktelenek is bejelentkezhetnek gépünkre.
- az NFS használatának korlátozása: a fájlrendszer exportálásának engedélyezésénél igen óvatosan kell eljárni, célszerû például a SUN által bevezetett secure NFS használata.
- az elektronikus levelezés szigorú felügyelete: a betörõk kedvencei a **sendmail** és **finger** parancsok gyenge pontjai. Ezeket érdemes lecserélni biztonságosabb változatokra.
- az X-Windows rendszerek biztonsági funkcióinak kötelezõ használata: ne adjunk lehetõséget a betörõnek ahhoz, hogy egy X-terminált monitorozva felhasználói jelszavakhoz és egyéb fontos adatokhoz jusson.
- ne engedélyezzük hálózatmonitorozó programok futtatását: vannak public domain programok is, melyekkel a hálózati forgalom közvetlenül figyelhetõ, elemezhetõ, futtatásukhoz többnyire root jogosultságra van szükség, ezért igen veszélyesek lehetnek hálózatunk biztonságára.

Biztonsági, védelmi szempontból azonban a legjobb megoldás, ha egy külsõ gyártó ilyen célra készített megbízható termékét használjuk. Ilyen például a MIT (Massachusetts Institute of Technology) által az Athena project keretében kidolgozott Kerberos rendszer.

5.3.2. A Kerberos rendszer

A Kerberos olyan azonosító rendszer, amely fizikai védelem nélküli, bárki által hozzáférhetõ, nyílt hálózatban lévõ adatok és szolgáltatások hatékony védelmét szolgálja. Ez a rendszer a saját szerverén kívül a hálózati forgalomban résztvevõ egyetlen egységrõl sem tételez fel megbízhatóságot. Tehát nem kell megbízhatónak lenni a felhasználóknak és programjaiknak, sem a felhasználók munkaállomásainak és azok rendszerfelügyeletének. A rendszer képes kiszûrni az illegális hálózati tevékenységet, sõt fel tudja ismerni a rossz szándékú vagy illegális klienseket és szervereket.

A Kerberos mûködése azon alapul, hogy létezik a rendszerben egy **garantáltan megbízható** egység, ez a Kerberos szerver, amelynek az ítéletét mindenki elfogadja. Ez a szerver a kliensek azonosítója és jelszava

alapján egyértelmûen el tudja dönteni, hogy az adott kliens legális vagy illegális. A rendszer a következõ tulajdonságokkal rendelkezik:

- a kliensnek minden szerverkérésnél azonosítania kell magát, a felhasználónak azonban ezt csak egyszer, a hagyományos bejelentkezésnél kell megtennie,
- jelszó kódolatlan formában soha nem kerül a hálózatra, sõt a munkaállomás memóriájában sem tárolódik,
- minden felhasználónak és minden szerver szolgáltatásnak van azonosítója és van titkos jelsz ava,
- kizárólag a Kerberos szerver ismeri az összes azonosítót és jelszót,
- a Kerberos szerver magas szintû fizikai és ügyviteli védelme is biztosított.

A Kerberos rendszer a védelem három különbözõ szintjét biztosítja:

- a kommunikációban résztvevõk azonosítása a kapcsolatfelvételnél,
- partnerazonosítás minden egyes üzenetváltáskor,
- partnerazonosítás minden egyes üzenetváltáskor és az üzenetek tartalmának titkosítása.

Ez a rendszer alkalmas az egészségügy különleges adatainak védelmére ott is, ahol nagy k iterjedésû, komplex kórházi információs rendszereket UNIX környezetben üzemeltetnek.

6. Felhasznált irodalom

[1] Trusted Computer System Evaluation Criteria, Department of Defense Computer Security Center, USA, 1983.
[2] Dietz Gusztávné dr., Pap Márta: Adatvédelem, adatbiztonság, NOVORG, Bp. 1995.
[3] Winn Schwartau: Biztonsági funkciók a Windows NT-ben. Számítástechnika, 1995. 8. szám.
[4] Microsoft Windows NT System Guide, Microsoft Corporation
[5] Adatvédelem, adatbiztonság HISEC '93, NJSZT, Bp. 1993.
[6] Adatvédelem, adatbiztonság HISEC '94, NJSZT, Bp. 1994.
[7] H. Kersten, M. Weinand: Sicherheitsaspekte bei der Vernetzung von Unix-Systemen, Oldenburg Verlag, 1991.
[8] John T. Kohl: The Evolution of the Kerberos Authentikation Service, MIT, 1991.