Adat és információvédelmi kérdések a kórházi gyakorlatban I.

Nagy István, Gottsegen György Országos Kardiológiai Intézet (GOKI)

A technika folyamatos fejlődése révén a kórházi szakemberek (vezetők és beosztottak) a mindennapi munkájuk kapcsán elkerülhetetlen, hogy olyan informatikai eszközökkel és szoftverekkel kerüljenek kapcsolatba, amelyeknek az üzemeltetése az információvédelem szabályozási körébe tartozik.

Ha informatikai veszélyekről van szó, mindenkinek automatikusan a vírusok jutnak az eszébe. A lehetséges veszélyek, támadási formák azonban ennél sokkal sokrétűbbek, így a védekezésnek is annak kell lennie. A védelem árát, a ráfordítás mértékét az elfogadható kockázat határozza meg.

A biztonság akkor kielégítő mértékű, ha a védelemre akkora összeget és oly módon fordítunk, hogy ezzel egyidejűleg a támadások kárvonzata, illetve kockázata (kárérték*bekövetkezési gyakoriság) az elviselhető szint alá süllyed.

BEVEZETÉS

A kórházak egy része szakértőnek hitt cégekhez fordul adatvédelemmel kapcsolatos tanácsért, és komoly pénzt fizet a szabályzatok elkészítéséért. Előfordulnak olyan szabályzatok, amelynél megpróbálják az iratkezelési, archiválási, vírusvédelmi, betegjogi, számítástechnikai és minden egyéb kérdést egy anyagban rendezni.

Ezek az anyagok csak arra jók, hogy ki lehessen pipálni a szabályzatok meglétét, de arra semmiképp nem alkalmasak, hogy ezeket az elkerülhetetlenül fontos kérdéseket a törvény előírásainak, a mai kor színvonalának és a kezelt adatok értékének megfelelően védjék, és segítő módon meghatározzák az ezzel kapcsolatos tennivalókat a szakemberek és vezetők részére. (1. ábra)

A szabályozások keretében biztosítani kell az információk, illetve adatok

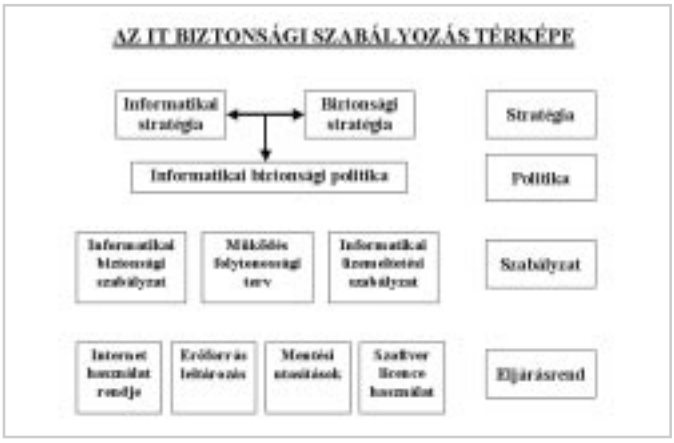
- rendelkezésre állását, elérhetőségét az arra jogosultak számára,
- sértetlenségét (sérthetetlenségét, valódiságát),
- az információk, illetve adatok jellegétől függő bizalmas kezelését,
- az információk, illetve adatok hitelességét, valamint
- a teljes informatikai, illetve információs rendszer működőképességét.

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

Az említett alapkövetelmények megvalósítása érdekében olyan intézkedésekre van szükség, amelyek az információk és adatok rendelkezésre állását, sértetlenségét, bizalmasságát, hitelességét és a rendszer működőképességét a lehető legkisebb kockázattal és egyenlő mértékben 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.

A továbbiakban a kórházi környezetben előforduló, az informatikai biztonsággal és információvédelemmel kapcsolatos eszközökről és kérdésekről számolok be, saját napi gyakorlatunk alapján.



1. ábra

TELEKOMMUNIKÁCIÓS VÉDELMEK

Telefon, fax

Ezt az eszközt, amelyet minden nap esetleg órákon keresztül használunk, teljesen mostohán kezeljük adatvédelmi és információvédelmi szempontból.

A telefonnal kapcsolatban maximum a telefonálási jogosultsági kérdések kerülnek szabályozásra

- helyi, távolsági, mobil, külföldi
- hivatalos, magán

Sok esetben nem definiálják előre, hogy mekkora értékű telefonszámla fogadható el még hivatalosként, mit értünk hivatalos beszélgetésen, mi a teendő a keret túllépése esetén (a központok szinte mindegyike rendelkezik, ún. kredit rendszerű kiegészítéssel, amely arra hivatott, hogy az előre engedélyezett keretösszeg elérése esetén letiltsa a telefonmellék vagy a személy hívási jogosultságát). Ilyen és ehhez hasonló apróságok (pl. rövidített hívószámok, híváscsoportok kialakítása stb.) előre történő szabályozása sok kellemetlenségtől kímélheti meg a vezetőket és a beosztottakat egyaránt.

Nem tisztázott a telefonközpontok által gyűjtött magán és hivatalos jellegű adatok (személyhez kapcsolható telefonszámok és telefonálási szokások) titkossága és hozzáférhetősége.

Nem használjuk ki a hívásirányok szerinti kimutatásokat (szolgáltatók szerint, árak szerint), illetve a top listák szerinti (leggyakrabban hívott számok, leghosszabb beszélgetések, legdrágább beszélgetések stb.) kimutatásokat.

Ezeknél a telekommunikációs eszközöknél nyilvános csatornán történő adatátvitelről beszélünk. Hátrányként kell említeni az erős hardver-függést, valamint azt, hogy a titkosítást alacsony védelmi szinten tudják csak biztosítani az ilyen elemek.

Modem

Az analóg és ISDN telefonvonalak másik legelterjedtebb felhasználási területe a modemes kapcsolat létesítése internetes kapcsolat, levelezés, help-desk szolgálat, adatátvitel és egyéb tevékenységek lebonyolítása érdekében. Nincs olyan magyar kórház, amelyben legalább egy ne üzemelne! Gondoljunk csak bele, és azonnal elborzadunk, hogy melyek a leggyakoribb területek, ahol ezek a védelem nélküli eszközök szinte biztosan előfordulnak:

- Bér és munkaügyi adatok hálózata
- Gazdasági rendszerek „help desk” szolgáltatása
- Klinikai rendszerek „help desk” szolgáltatása (általában közvetlenül a szerverre kötve)
- Klinikai mérési adatok, laboreredmények, képek, kísérletekkel kapcsolatos adatok stb. továbbítása érdekében
- Levelezés letöltése
- Tűzfal nélküli internetes kapcsolat

Ezek az eszközök általában vagy a szerverekhez biztosítanak direkt kapcsolatot az éjjel-nappali hibaelhárítás érdekében, vagy egyes éjjel nappal üzemelő hálózatba kapcsolt munkaállomáshoz csatlakoznak, amelyen keresztül a kórház teljes rendszere elérhető.

Egy ilyen eszköz már 5-10 ezer forintért megvásárolható és kb. 5 perc alatt telepíthető.

Hiába a drága tűzfallal védett rendszer, ha a hálózatba kötve működik PC, amely modemmel kapcsolódik az internetre. Ebben az esetben sajnos a védelmünkön kaput nyitottunk.

LOKÁLIS HÁLÓZAT (LAN) VÉDELME

A helyi hálózatok esetében az adattovábbítás ellenőrzött csatornán és általában egy épületen belül – UTP kábelen, üvegszálon keresztül – történik. Hálózatok összekapcsolására (protokoll konverterek, bridge-ek, rooter-ek) léteznek ugyan hardver applikációk (nagy sebességű kripto-berendezések), de ezeknél az eszközöknél is biztonság (titkosság) szempontjából a telekommunikációs célberendezéseknél tett kritikai megjegyzések érvényesek.

A belső hálózat (intranet) további elemekre bontható. Ha több telephely van, akkor azok összeköttetését általában nagy távolságú (WAN) hálózattal biztosíthatjuk. Ez működhet zártan az intézet tulajdonában lévő eszközökkel, kábelekkel, vagy lehet valamennyire nyilvános, a szolgáltatótól bérelt, de még mindig kizárólagosan használt, illetve teljesen nyílt, bárki által elérhető csatornákkal. Minden esetben érdemes elgondolkodni azon, hogy miket küldünk át a „dróton” illetve az éteren. Ha adataink nyílt formában közlekednek, úgy azok illetéktelen kezekbe kerülhetnek, és az adatvédelem – tekintettel arra, hogy egészségügyi adatokról van szó – nem mellőzhető. Az egészségügyi adatokat például a VPN (virtuális magánhálózat) szoftveres vagy hardveres megvalósítása védheti. A hardveres megoldást általában akkor alkalmazzuk, ha a kábel mindkét végén saját eszközeink üzemelnek (mellé telepítjük a titkosítást biztosító berendezést).

A szoftveres úton titkosított csatorna esetén el kell dönteni, hogy melyik szoftvert érdemes használni: nyílt forráskóddal rendelkezőt (Linux), vagy egyéb vásárolt szoftvert. A szoftveres kódolás rugalmasabban konfigurálható és eldönthetjük, hogy mely két eszköz között alkalmazzuk. Amennyiben a munkaállomáson történik a titkosítás, akkor az egész adatút biztonságban van, mivel a gépből kijövő adat már titkosított. Ha még az adattárolón is kódolt formában tároljuk az adatokat, akkor a teljes adatúttal biztonságosnak tekinthető a belső hálózaton.

Szerverek és munkaállomások szoftvereinek karbantartása

Rendszerünk aktív elemei, a különféle szerverek (Web, alkalmazás-, adatbázis) az útválasztók, a munkaállomások, operációs rendszerüktől függően más és másképpen ellenállóak a behatolásokkal szemben. Ismerünk olyan operációs rendszereket, alkalmazásokat, amelyek magukban is

meglehetősen ellenállóak, és olyanokat is, amelyekkel sok „baj" van.

A hardver- és szoftvergyártók rendszeresen publikálják termékeik ismert hibáit, amelyek egy-egy támadás alapjai lehetnek. Ezzel egy időben a javító csomagokat is kibocsátják.

Elengedhetetlenül fontosnak tartom e biztonsági hibajavító szoftverek (pech-ek) megjelenésének figyelését és rendszeres, előre tervezett, ütemezett módon történő telepítését minden munkaállomásra. A rendszereinknek ebből a szempontból is karbantartottnak kell lenniük, hiszen legalább a már ismert hiányosságok kihasználásának esélyét tagadjuk meg a crackerektől. Gondoljunk bele: elég ha csak 1 munkaállomásra nem kerül fel a hibajavítás és a rendszerünk ezen a ponton máris támadható.

Mivel egy-egy munkaállomáson, szerveren nem csak az operációs rendszer, hanem a telepített alkalmazások (pl. irodai alkalmazások stb.) hibajavítását is el kell végezni, ezért ez komoly előkészítő munkát és szakértelmet igényel.

A javításokat sokszor megelőzik a támadások, ezért rendszereinket többféleképpen is védenünk kell a webes veszélyektől. Az egyik legelterjedtebb védekezési eszköz a tűzfal.

Tűzfalépítés

A tűzfal (firewall) csak az általunk megengedett forgalmat engedi át a külső hálózatból a belső hálózatba és viszont. Úgy kell konfigurálni, hogy elhárítsa a kifelé irányuló szükségtelen kéréseket, és megakadályozza a kintről irányított támadásokat, közben ügyelve arra, hogy minden engedélyezett protokoll és adatcsomag – például a levelezés és a cég webszolgáltatása – átjusson rajta. Csak annyit mutasson meg a rendszerünkből, amennyit szükséges. Azokat a funkciókat tegye elérhetővé, amelyeket engedünk, valamint jelezze a támadásokat.

Törekedni kell arra, hogy minél kevesebb „kapu" legyen a rendszerünkön, és ezek se legyenek ellenőrizetlenek. Óvakodjunk ezért külső munkatársak részére történő védelem nélküli „kapu" nyitásától.

Proxy

A védelem további és sajátos lehetősége a proxy szerver üzemeltetése. Ennek alkalmazása nem mindenhol szükséges, de érdemes elgondolkodni az alkalmazásán. Olyankor érdemes üzemeltetni, ha sokan tudnak belülről kifelé http/ftp kéréseket indítani, anyagokat letölteni, a hálón böngészni. Minél nagyobb az ilyen forgalom, annál inkább szükség lehet egy jó proxy beállítására, mert ez

- egyrészt csökkenti a nem kis pénzbe kerülő sávszélesség igényt azáltal, hogy a már egyszer letöltésre került anyagok egy meghatározott ideig (a háttértároló kapacitásától függ, ami manapság nem túl drága) tárolásra kerülnek a proxy szerver merevlemezén. Az oldal ismételt „kérése" esetén már nem az internetről, hanem a szerver merevlemezéről töltődik le a kért weboldal tartalma,
- másrészt jó szűrési feltételekkel kordában lehet tartani az alkalmazottak Intenet használatát.

Egyetlen cégnek sem érdeke, hogy alkalmazottai munkaidőben pl. szexoldalakat látogassanak, de az sem cél, hogy a munkához szükséges információkat tartalmazó címeket kitiltsuk, és hasznos hozzáféréseket korlátozzuk. A szűrést is folyamatosan gondozni kell, hiszen címek tömege születik és szűnik meg naponta. Ma már szolgáltatásként megvehető a naponta frissített tiltási adatbázis.

Levelezés

Egyre több intézet alkalmaz belső levelezést, és ez általában nincs elválasztva az internetes levelezéstől sem, hiszen ma ez a leggyorsabb kapcsolattartási forma. Néhány fogalmat mindenféleképpen fontos tisztázni és megbeszélni.

Hitelesítés

A tárolt adatok vagy kommunikációs üzenetek tartalmára vonatkozó védelmi eljárás. Az adatokat védi hamisítás, manipulálás, üzenetkivonás vagy járulékos üzenet beiktatása ellen. A hitelesítés olyan ellenőrző számot generál, amely csak az adott biztonsági rendszerben készíthető és ellenőrizhető. Készítéséhez általában felhasználják azokat a kulcselemeket, amelyeket a rejtjelező algoritmusok is használnak.

Digitális aláírás, időpecsét

A digitális aláírás egy autentikáló és identifikáló üzenet összeállítását és különleges rejtjelezését jelenti. Az aláírás általában tartalmazza az „aláírandó" adatállomány megnevezését, hitelesítő karaktersorozatát, az aláírás idejét, helyét és az aláírást. A rejtjelezés abban különleges, hogy az aláírás megfejtése csak az aláírót egyértelműen azonosító kulcs felhasználásával lehetséges. A megfejtéshez felhasznált kulcs akár publikus is lehet. Szintén a nyilvános kulcsú rendszerekben terjedt el az alkalmazása.

Az elküldött levelek titkosítása és a digitális azonosítás lehetősége

Soha ne feledjük, hogy az internet egy nyilvános hálózat. A neten továbbított leveleink és adataink véletlen (vagy szándékos) hiba vagy hibaelhárítás folytán illetéktelen kezekbe kerülhetnek, ezért olyan anyagot, amelynek tartalma bizalmas, vagy csak egyszerűen kellemetlen lenne ha illetéktelenek is elolvasnák, érdemes a titkosítva eljuttatni. Erre számos jó programot találhatunk a helyi levélkódolástól a hálózati átvitel titkosításáig. Az eleve titkosítás olyan szempontból is szerencsésebb, hogy ezáltal a levél tárolásának biztonsága is megoldódik. Amennyiben sok felhasználónk folytat levelezést, abban az esetben indokolt egy központi WEB-mail üzemeltetése. Ebben az esetben a levelek egy jól védett (és rendszeresen mentett!) központi szerveren kerülnek tárolásra. Az üzeneteink a hálózat bármely pontjáról (bármely gépről) mindig elérhetők. Az elolvasott levelek nem töltődnek le a kliens gépre.

A digitális azonosítás (aláírás) pedig azért fontos, mert ebben a közegben semmi más nem hitelesíti a feladót. A digitális aláírás hitelességének ellenőrzéséhez nem feltétlenül szükségesek nagy országos hitelesítő szervezetek. Megfelelő programokkal házon belül illetve a partnerekkel egymás között ugyanúgy lehet rendezni a hitelességet.

Vírusvédelem

A vírusvédelem önmagában is olyan szerteágazó téma, hogy számos publikációt igényelne tárgyalása. E helyen ezért csak röviden összefoglalom, hogy melyek az alapvető követelmények a jó vírusvédelemmel kapcsolatban (a teljesség igénye kizárt):

- Minden beviteli és csillagponton védő, automatikusan frissülő, központilag felügyelhető, egységes, automatikus naplózással és riasztással rendelkezik
- A hatékonyság maximalizálása érdekében kellő gyakorisággal (különös tekintettel a kelet európai vírusmintákra) aktualizáltnak (aktualizálhatónak) kell lennie
- A rendszert illetve annak frissítéseit lehetőleg saját eljárásaival központi helyről kell telepíteni (lehet az informatikai menedzsment rendszer segítségével is)
- Minden potenciális támadási ponton aktívan üzemelnie kell, összhangban az adott intézmény informatikai biztonsági stratégiájával.
- Többféle konfiguráción és platformon kell működnie.
- Többféle keresési menedzsment technológiát kell ismernie és alkalmaznia (ismert minták keresése, heurisztikus keresés, virtuálisgép módszer, karantén technológia stb.)
- A frissítéssel és a vírusokkal kapcsolatos eseményekről a vírusvédelemért felelős informatikusok és a felhasználók számára is értesítést kell küldeni a feltételezett vírusveszélyről

Mindenképpen indokolt az alábbi pontok kiemelt vírusvédelme:

- A hálózatban működő munkaállomások
- A rendszer állomány és alkalmazás kiszolgálói
- Tűzfal(ak) és a levelezőszerver(ek)

Az interneten keresztüli vírusfertőzés után a második legjelentősebb fertőzési forrás az otthonról behozott lemezek, CD-k amelyek intézeti gépeken kerülnek megtekintésre.

Léteznek olyan vírusvédelmi szoftverek, amely megvásárlása esetén a szoftvert nem csak az intézeti, hanem a saját otthoni gépeken is lehet használni díjmentesen és persze jogtisztán.

A RENDSZEREK ÉS AZ ADATBÁZISOK VÉDELME

A felhasználói azonosítás és hitelesítés az informatikai rendszerek biztonságának alapeleme, hiszen minden egyéb biztonsági funkció (jogosultság kezelés, naplózás stb.) azon alapul, hogy az azonosításnak és hitelesítésnek meg kell előznie a felhasználó és a rendszer közötti minden egyéb kapcsolatot.

A hitelesítő rendszerek feltételezik, hogy az azonosítandó személynek:

- „valamit tudnia”,
- „valamit birtokolnia” vagy
- „valakinek lennie” kell.

Ezekből, illetve ezek kombinációjából állapítható meg egy felhasználóról, hogy jogosult-e az adott szolgáltatás elérésére.

Ha a felhasználói rendszerekben nem kellő körültekintéssel, részletességgel és a valóság figyelembevételével alakítjuk ki a jogosultságokat, paraméterezzük a hozzáférés védelmet, akkor a felhasználók bizonyos jogok átruházása érdekében a magasabb prioritással bíró jelszavukat megadják a beosztottjaiknak, munkatársaiknak.

Fontos tehát a valóságnak megfelelő kellő mértékig és módon szabályozott hozzáférés védelem.

A jogosultságok kiadásának, módosításának és megszüntetésének a módját rendszerenként pontosan szabályozni kell! A kilépő és a hosszasan távol lévő felhasználók esetében pontosan szabályozni kell az eljárásrendet, ügyelve arra, hogy minden rendszerből és funkcióból szükség esetén ki legyenek ideiglenesen vagy véglegesen tiltva.

A napi korrekt jogosultság karbantartás mellett évente legalább egyszer ellenőrizni kell a jogosult felhasználók személyét és a munkaköri feladatok változásának megfelelően szükség szerint korrigálni kell a felhasználói jogokat.

A munkahelyi hálózatokban és a személyi számítógépeken a hozzáférést sokáig csak jelszóval védték annak ellenére, hogy a jelszavas hozzáférés védelem számítógépes környezetben kevés védelmet nyújt és könnyen támadható. Az informatikai piac az elmúlt évtized számos kutatási és fejlesztési eredménye alapján keresi a megfelelő technikát a biometriai azonosítás automatizálására. A többféle egyedi testi jelhordozó (ujj, hang, írisz, kézalak, arc stb.) közül leggyorsabban az ujjlenyomat azonosításán alapuló eszközök terjednek, míg a nem biometriás azonosítási lehetőségek esetében még mindig a személyazonosító kártyák vezetik a piacot, de erőteljesen kezdenek elterjedni az intelligens chipkártyák is. A chipkártya technológia biztonságának alapja, hogy a memóriacellák tartalmát nem lehet értelmezhető formában kiolvasni. A ma korszerűnek tekinthető biztonsági rendszerekben az algoritmus szervesen összeépül egy „kulcskészlettel", amelynek ismerete nélkül a kódolt üzenet megfejtése – a rejtjelezés „feltörése" – reménytelen vállalkozás.

A kulcskészlet, vagy annak egyes elemei úgy épülnek be a rejtjelezett anyagba, hogy a kulcsok egyetlen bitjének megváltoztatása is a teljes rejtjelezett üzenet megváltozását vonja maga után. Az algoritmus erősségét a megfejtési idővel (gépidővel) is szokták jellemezni

E rendszerek lelke a fejlett titkosító programokon alapul. A kliens gépekbe épített olvasók segítségével megoldható a felhasználók és a rendszergazdák azon régi vágya, hogy

minden rendszerbe egyetlen bejelentkezés legyen csak szükséges, de ahhoz erős szerveroldali hitelesítés kapcsolódjon még azoknál az alkalmazásoknál is, amelyek ezt nem támogatják. Ezzel a módszerrel nem csak a felhasználók hitelesítése, hanem az egyre többet emlegetett digitális aláírás előállítása is megoldható.

Az egészségügyi ellátások során a használt beteg adatbázisok, az ehhez kapcsolódó vizsgálati eredmények és dokumentumok esetében már most is elengedhetetlen az adatmanipulációt (megnyitás, adatbevitel, módosítás, törlés és minden egyéb tranzakciót) végző személyzet azonosítása és naplózása.

A tranzakciók naplózása már a gazdasági rendszerek esetében is egyre inkább elvárásként jelentkezik!

ADATHORDOZÓK TITKOSÍTÁSSAL TÖRTÉNŐ VÉDELME

Az intézetek életében elengedhetetlen az adatok különböző típusú adathordozóra történő mentése adattovábbítási illetve adatmentési célból. Az adathordozó készítése esetén az elsődlegesen eldöntendő kérdés, hogy nyílttá kívánjuk-e tenni a médián tárolt adatokat. 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 előírásoknak, ill. utasításoknak kell szabályozni. A kulcskialakítással a konkrét feladatnak megfelelően biztosítani lehet, hogy

- A rejtjelezett adathordozó a hálózat valamennyi állomásán „leolvasható" legyen
- A rejtjelezett adathordozó csak azon az állomáson legyen leolvasható, ahol készült (archiválási, mentési feladat);
- A rejtjelezett adathordozó a hálózat valamennyi állomásán, de csak meghatározott felhasználói körben legyen leolvasható (szelektív, jelszavas rejtjelezés);
- Az adathordozó rejtjelezése egységes vagy „track-sector függő" legyen;
- A rejtjelezett adathordozót az időszakos kulcs-csere alkalmával frissíteni (átrejtjelezni) kell.

AZ ADATOK KIKERÜLÉSE MÁS EGYÉB MÓDON

Lopás

Gyakran és megdöbbenve halljuk, hogy egészségügyi intézményekből számítógépek tűnnek el. Számomra megdöbbentő, hogy ezekben a nyilatkozatokban szinte mindig csak a hardverpótlás nehézségeiről esik szó. Holott az adatok pótlása olykor lehetetlen, vagy rendkívüli erőfeszítéseket igényel. A személyiségi adatok védelmén esett csorbáról szinte alig esik szó.

Fontos tehát, hogy a klinikai, gazdasági, kontrolling és egyéb fontos adatokat tartalmazó szervereket jól biztosított szerverszobában tároljuk.

Ugyanez az előírás vonatkozik a mentett adatokra is. Persze a mentésnek csak 1 példányát kell a szerverszobában őrizni, a másodpéldányt egy másik épületben, kell tűzbiztos és jól zárható helyen tárolni.

Ez a kérdés még inkább előtérbe került a mobil eszközök elterjedésével. Ebben az esetben elengedhetetlenül fontos, hogy a hordozható számítógépünk bejelentkezése illetve a rajta tárolt anyagok is jelszóval védettek legyenek. Ez esetben a legjobb megoldásnak tűnik az „USB-pen"-hez hasonló (pl: e-token) eszköz használata (persze ezt nem illik a hordozható eszközzel egy helyen tárolni).

Szerviz

A meghibásodott számítógépeket az esetek nagy részében szakszervizbe szállítják javításra. A szervizbe szállítás előtt meg kell arról győződni, hogy milyen adatok találhatók az adott gép merevlemezén. Szükség esetén menteni, majd törölni kell a diszkről, illetve gondoskodni kell arról, hogy ezek az adatok ne legyenek helyreállíthatók. Amennyiben központi eszköz javításáról van szó, ragaszkodjunk a helyszíni javításhoz.

Nyomtatás

- A munkavégzés egyes fázisaiban elkerülhetetlen, hogy bizonyos adatokat kinyomtassunk. Ezeken a nyomtatott anyagokon sok esetben személyes adatok (pl: betegadatok) és azonosítók találhatók
- Egyes vezetők vagy idősebb munkatársak még manapság is idegenkednek a számítógépek használatától, ezért azt kérik, hogy számukra nyomtatásban adjuk meg a kért adatokat

Számos példát lehetne még hozni, amellyel alá lehetne támasztani azt a tényt, hogy hányszor kerülnek fontos adatokat tartalmazó anyagok a papírkosárba.

Azokat a munkahelyeket, amelyeken bizalmas jellegű adatok képződnek, minden esetben el kell látni iratmegsemmisítő berendezéssel és a dolgozókat a munkaköri leírásukban kötelezni kell ezen anyagok rendszeres és folyamatos megsemmisítésére.

Számítógépes lopás – Belső „ellenség"

Számítógépes lopásról beszélünk akkor, amikor a támadó pénzszerzés vagy adatlopás szándékával, esetleg bizonyos erőforrások jogosulatlan használatának szándékával támadja meg a kiszemelt informatikai rendszert. Ekkor a támadónak elemi érdeke, hogy tettére egyáltalán ne derüljön fény (ellentétben a weboldalak feltörésével). Az ilyen támadások elkövetéséhez alapos szakmai felkészültségre és gyakorlatra, általában jó helyismeretre van szükség. A támadások általában, vagy az operációs rendszer, vagy vala-

melyik telepített program hibáját, vagy rossz konfigurációját használja ki.

Az informatikai biztonsággal foglalkozó szakirodalom az egyik legnagyobb veszélyforrásként említi a belülről jövő támadást. Ez az a támadási típus, amely ellen a legnehezebb védekezni. Ennek ellenére a munkáltatók a munkaköri leírásban nem élnek a törvény adta lehetőségeikkel. Emlékeztetőül néhány fontos jogi formula a munkavállalói, közalkalmazotti kötelezettségek jogszabályi hátterével kapcsolatban:

1992. évi XXII. törvény a Munka Törvénykönyvéről

3. § (3) A munkavállaló a munkaviszony fennállása alatt – kivéve, ha erre jogszabály feljogosítja – nem tanúsíthat olyan magatartást, amellyel munkáltatója jogos gazdasági érdekeit veszélyeztetné.

103. § (3) A munkavállaló köteles a munkája során tudomására jutott üzemi (üzleti) titkot, valamint a munkáltatóra, illetve a tevékenységére vonatkozó alapvető fontosságú információkat megőrizni. Ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely munkaköre betöltésével összefüggésben jutott tudomására, és amelynek közlése a munkáltatóra vagy más személyre hátrányos következménnyel járna.

1992. évi XXXIII. törvény a közalkalmazottak jogállásáról

81. § Gondatlan károkozás esetén a közalkalmazott háromhavi illetménye erejéig felel, amennyiben

a) a munkáltató gazdálkodására vonatkozó szabályok súlyos megsértésével,

b) az ellenőrzési kötelezettség elmulasztásával, illetve hiányos teljesítésével okozta a kárt, vagy

c) a kár olyan – jogszabályba ütköző – utasítása teljesítéséből keletkezett, amelynek várható következményeire az utasított közalkalmazott előzőleg a figyelmét felhívta.

ÖSSZEFOGLALÁS

Az informatikai biztonságon esett csorba után lehet a kártevőt (betörőt, tolvajt, vírust, hackert stb.) szidni, rendőrt is lehet hívni, és elkezdhetünk pereskedni (ha van kivel), de mindez már csak pótcselekvés, a védelem hiányosságainak látványos kompenzálása.

A biztonsági rendszer kialakítása évekre szóló feladat. A napi üzemeltetés mellett, tanulmányozni kell mások tapasztalatait, és ne reméljük, hogy valójában valaha is készen leszünk, mivel a támadók egy-két lépéssel mindig előttünk járnak.

Örömmel vennénk, ha olvasóink (egészségügyi informatikával foglalkozó cégek és az egészségügyben tevőlegesen résztvevő szakemberek) megjegyzéseikkel, kiegészítéseikkel, helyesbítéseikkel pontosítanák a szerző által leírtakat.

Jó lenne, ha az egészségügyi informatikai biztonságnak fórumot tudnánk adni e lap hasábjain. Kérem, ragadjanak tollat és írják meg tapasztalataikat, elképzeléseiket, ajánljanak irodalmat és az EU-s egyesülés idejére váljanak Önök is szakértőjévé ennek a fiatal szakterületnek.

(Szerk.)

IRODALOMJEGYZÉK

[1] Informatikai biztonsági módszertani kézikönyv (Informatikai tárcaközi bizottság ajánlásai), Miniszterelnöki hivatal Informatikai Koordinációs Iroda. 8. sz. ajánlás

[2] Sándor Gábor: A vállalati adatok védelme, új alaplap 2000/8

[3] Szentpály Miklós: Integrált védelem, Új Alaplap 2000/8

[4] Kürti Sándor–Papp Attila: Vírusvédelem, IT- Busines I. évfolyam 37. szám

A SZERZŐ BEMUTATÁSA

Nagy István A Kandó Kálmán Villamosipari Műszaki Főiskolán végzett villamos üzemmérnökként, majd számítástechnikai szakmérnöki képesítést szerzett. Korábban a gyöngyösi Bugát Pál Kórházban dolgozott az informatikai és dokumentációs osztály vezetőjeként. 1997–1999-ben a Világbanki Kórházinformatikai Programiroda projektmenedzsere az Országos Korányi TBC és Pulmonológiai Intézetben.

1999 óta az Országos Kardiológiai Intézetnél bevezetésre kerülő integrált informatikai rendszer projektmenedzsere és a számítástechnikai osztály vezetője.

Nagy tapasztalatot szerzett a nemzetközi mércéjű projektek menedzsmentjében, amelyet mindennapi munkájában jelenleg is alkalmaz tanácsadóként, számítógépes hálózatok és rendszerek tervezésében, kivitelezésében, menedzsmentjében, üzemeltetésében, illetve a modern telefonrendszerek kialakításában. 2001-től a Magyar Egészségügyi Informatikai Társaság vezetőségi tagja.