Biztonságban vannak a betegadatok az informatikai rendszerekben és a világhálón?

Baross Szabolcs, Qualiprod Kft., Balog Géza, IT-IQ Informatikai Bt.

A cikk a hamarosan aktuálissá váló (2005-2006) elektronikusan tárolt betegadat-biztonsági kérdéseket taglalja. Kitér az intézményen belüli és az intézmények közötti várhatóan felgyorsuló adatcsere biztonsági kérdéseire. Fokozatosan halad a populárisan értelmezhető biztonsági intézkedésektől a szigorúbb szakmai értelmezésig és szabályrendszer bemutatásáig. Könnyed stílussal és hangvétellel, példákkal jól illusztráltan mutatja be a címben megjelölt témát. A hazai egészségügyi informatikában uralkodó állapotokat jól illeszti a nemzetközi helyzetbe, és javaslatokat tesz az első lépések megtételére a sajnos eléggé sanyarú helyzet megszűntetése érdekében.

BEVEZETÉS

A cikk inkább szól orvosoknak, mint egészségügyi informatikusoknak és ez nem véletlen. Terminológiájában próbál a népszerűsítés szintjén maradni. Szántszándékkal nem alkalmaz nagyon elvont számítástechnikai fogalmakat. Miért? Azért, mert a számítástechnika/informatika és vele együtt a biztonsága is csak olyan lesz, amilyennek hagyjuk, hogy legyen, és ez nemcsak az egészségügyben van így. A biztonság nem csak a portáson és a tűzrendészen múlik. Az informatikai biztonság sem az operátorok és rendszergazdák kizárólagos felelőssége, hanem olyasvalami, amit jobb, ha mi vezetők (orvosok és hajdan volt orvosok) nem is értünk, mert csak beleszédülünk. (Szándékos a többes szám első személy, habár mi a szerzők, sosem voltunk orvosok!)

Mint, ahogy a saját lakásunk biztonságát sem egy lakatosmester szakértelmére bízzuk, hanem alaposan felkészülünk. Megnézzük milyen riasztók vannak a piacon? Milyen távőrző szolgáltatások vannak a környéken? Ugyanúgy kell a kórházakban, szakrendelőkben, gondozókban és a házi orvosi rendelőkben keletkező betegadatok biztonságáról is gondoskodni!

Mik a veszélyek? Néhány eset a világhálóról

Az előző néhány évben számos cikk jelent meg, ami arra figyelmeztet, hogy a hackerek (vagy crackerek, ha így jobb) hogyan használják ki az internetes böngészők keresőmotorját arra, hogy olyan információkat szerezzenek meg, amihez eredetileg nem férnének hozzá.

A Wired magazin munkatársa így talált rá például az Apple-lel kapcsolatban álló több száz tanár részletes életrajzára, címére és telefonszámára. Ráadásul a lista tartalmazta a tanárok felhasználóneveit és jelszavait is. Az adatbázis teljesen védtelen volt. Egy másik találat a Drexel orvosi egyetem egy adatbázisára mutatott, ahol 5500 idegsebészeti beavatkozáson átesett beteg adatai voltak elérhetők.

Az egészségügyi adatfeldolgozás két alapvető biztonsági követelménye

Világosan kell látni, hogy teljesen átfogó értelmezésben két szálon kell vizsgálódnia annak, aki az egészségügyben használatos elektronikusan tárolt adatok biztonsági problémáival szeretne foglalkozni.

A beteg biztonsága:
- Hiteles adatokat adó és megbízhatóan működő rendszerek
- Szoftver minőségbiztosítás működtetése

Orvosi betegadatok védelme:
- Politikai, jogi, adminisztratív, és technikai problémák

A jelenlegi kaotikus papír alapú működés hordoz magában valamiféle „természetes védettséget”, mert elég nehezen megközelíthető az információ. Az elektronikus média fejlődésének tükrében, a jövőben már nem tolerálható az adatok továbbra is hasonló „könnyed kezelése”.

Ma az egészségügyi ellátó rendszer egyes intézményei a betegadatok szempontjából szigetként működnek. Az egyes helyeken keletkező és/vagy felhalmozódó információk hozzáférése, átadása más intézmények részére nem automatikus. Az eseti átadás papíron történik (pl. kórházi zárójelentések), vagy bemondás alapján (pl. szedett gyógyszerek).

Az emberi életmód változásának egyik jellemzője az országban és a világban való utazás mértékének (távolság és gyakoriság) megnövekedése.

Az egyes intézményeknek önálló adatbázisuk van, az adatbázisok között on-line kapcsolat nincs kiépítve, a használatos adatok intézményenként újbóli adatbevitelre kerülnek (pl.: személyi adatok).

Nem informatikai, hanem felszereltségi probléma, hogy a diagnosztikai adatok egy része eltérő műszerezettség és mérési mód miatt korlátozottan használható fel más intézményeknél. Így ott ismételt vizsgálatokra és újabb informá-

ciók születésére kerül sor, amelyek együttes felhasználása nehézséget okozhat. Ez sok idő, sok-sok pénz és sokszor késedelem a gyógyító munka megkezdésében.

Milyen formában várható az orvosi adatok internetre kerülése

A turista forgalom szélesebb, a hivatásforgalom szűkebb, de jelentős rétegeket érint. Ezen rétegek megjelenése és növekedése már rövid távon is felveti a betegadatok korszerű mozgatásának igényét. Erre az informatika különböző megoldásokat ajánl, melyek közül leginkább kézenfekvő megoldás az internet. Nyilván a magyar egészségügy ettől ma még elég távol áll, de a hosszú távú gondolkodást a stratégia kialakítói nem mellőzhetik! Nem kell túl messzire mennie Magyarországtól annak, aki látni akarja mi vár ránk.

Világ vagy nemzeti szintű elérés megjelenése a betegek személyes kórtörténeti adataihoz

- Maga a beteg kéri le adatait elektronikusan saját számítógépére
- A háziorvosa kéri le az adatokat.
- A kórház kéri le az adatokat.
- A közegészségügyi szakemberek informálódnak.
- Kutató közösségek.
- Távoli szakértői konzultáció során.
- Sürgősségi beavatkozás előkészítése során.
- Távgyógyítás folyamán a beteg és orvosa együttműködésének során.

Mindez felveti azt a kérdést, hogy az adatok védelme az informatikai eszközök, a szervezet működése, a személyek felkészültsége oldaláról hogyan biztosítható, továbbá, hogy az adatvédelmi törvény hogyan foglal állást ebben a kérdésben.

A bizalmas adatok eltulajdonításának, gondatlan kezelésének következményei

Kis ízelítőt adunk a törvénykezési háttérből. A 2002. április 1-jén hatályba lépett adatvédelmi törvény szerint Számítástechnikai rendszer és adatok elleni bűncselekmény a 300/C.§ által van szabályozva, amelyben a jogosulatlan belépés, a tárolt, feldolgozott, kezelt vagy továbbított adatok jogosulatlan megváltoztatása, törlése vagy hozzáférés, számítástechnikai rendszerbe történő adatok bevitele az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztatása, törlése vagy hozzáférhetetlenné tétele mind nevesítetten szerepel és a szankcionálása egy évtől öt évig, két évtől nyolc évig, öt évtől tíz évig tartományba eshet.

Látható hogy nagy a tét. Az egészségügyi információk (betegadatok) kezelése „veszélyes üzem” az adatok védelmét komolyan kell venni.

AZ ADATOK VÉDELME

Biztonság fogalma a hétköznapi értelmezésben

A biztonság, mint fogalom nagy változáson ment és megy keresztül napjainkban, mely az információs rendszerekben több oldalról is megközelíthető. Mint minden – nem csak – információs rendszerben, itt is annyi biztonságra van szükség, amennyinek ott értelme van.

Ezt a fenyegetések valószínűségével és a védeni kívánt objektum fontosságával (értékével) szokták összhangba állítani. Profitorientált szervezetekben ez eléggé egyértelmű. Azonban a költségvetési intézményeknél (ha csak nem védelmi vagy hadiipari létesítményről van szó) szintén világos szokott lenni, hogy milyen erős védelemre van szükség? Fegyveres őröket nem látunk kórházak előtt, de katonai kórházak előtt már igen. Magán kórházak fizikai védelme minden bizonnyal erősebb, mint az állami kórházaké. Saját jól felfogott érdekük fűződik, ahhoz, hogy amiből élnek, ami a profitjukat adja, azt megvédik.

Tehát a biztonsági szint (és annak költségei) előzetesen kockázatfelméréssel kezdődnek, mint bármely (nem feltétlenül egészségügyi) intézmény esetében. Ez egy hangolási folyamat, ahol a felmért várható biztonsági sérülések bekövetkezési valószínűségét és az általuk okozott kár mértékét illesztik egymáshoz.

Nyilván a védendő „objektumok” leltározása során a mi esetünkben nem a műtők, a gyógyszeres szekrények, hanem, az információ lelőhelyei állnak a fókuszban.

Az első nagy meglepetés akkor érhetne minket, ha esetleg kiderülne, milyen komolysággal őrizzük a papír alapú információkat? A nagybetűs INFORMATIKAI BIZTONSÁGI KULTÚRA kisbetűsnél a papír alapú információ biztonságánál kezdődik.

Tehát páncélszekrényekben tartjuk a beteg-kartonokat? Ha nem, akkor a kartonokat tároló egyszerűbb szerkénynek helyet adó helyiség zárhatósága (pl. vasrácsozott nyílászárása) megoldott-e? Ezek csak villanásnyi keresztkérdések voltak a folytatás kellő megalapozása érdekében.

Nos tegyük fel, hogy a papír alapú adatok teljes biztonságban vannak. Itt a fizikai védelmi rendszerek szakértőinek hagyjuk meg a helyet a bővebb kifejtésre. A mágneskártyás és egyéb csalafinta módszerek kialakítása az ő asztaluk.

Nekünk a számítógépes rendszerek biztonságát kell elemeznünk, mégpedig speciálisan a magyar egészségügyben. Egy adott probléma tisztességes megtárgyalásakor nem árt a képbe-helyezéssel is foglalkozni.

Biztonságra helyezett hangsúly az egyes ágazatokban

Mi a helyzet más ágazatokban? Az ágazati biztonsági besorolásokat a következőképpen állíthatjuk össze. Első helyen a biztonság terén az állambiztonság, második helyen a hírszerzés, harmadikon a hadsereg, negyediken a hadiipar áll.

Ötödik helyen az államigazgatási hierarchia felső és középszintjei következnek. Az üzleti szféra csak ezután következik. Itt se mindegyik. Csak ahol fontos gyártási vagy egyéb technológiákat őriznek, pl. egy gyógyszergyár biztonsági szintje sokkal magasabb, mint egy konzervgyáré. (A neves német sörgyárnak mégis ellopták a több mint 100 éve sikerrel őrzött nagy értéket képviselő sörkészítési receptjét.)

Az üzleti szférát az állami intézmények alacsonyabb költségvetésből működő szintjei követik.

Az egészségügyi intézmények biztonsági védettségét talán csak a közoktatási intézmények követik, de rögtön felvetődik bennünk a kérdés. Jól van ez így? Tényleg az őt megillető helyen szerepel az egészségügy informatikai biztonság területén?

Mit kell védeni?

Az adatbiztonság, mert hogy erről lesz szó, vizsgálatát több szempontból is elvégezhetnénk, jelen esetben először a tárolt adatokat fajtájuk és rendeltetésük szerint vesszük végig.

Ezután, mivel a felhasználásuk során „nyúlunk" hozzájuk, a folyamatokban érintett adatbeviteli és adatvételezési (szebben szólva adathozzáférési) helyek szerint csoportosítjuk őket.

A vizsgálódásból nyilván nem lehet kifelejteni az adat manipulátorokat (ami/aki papír esetén az asszisztens, orvos, toll, ceruza röntgen gép stb.).

Nem lehet kifelejteni az adattároló helyeket sem (szekrény, számítógép, hajlékonylemez, merevlemez, pen-drive, CD, DVD, e-mail csatolmány, illetve maga az e-mail). Sőt még lehet elmélkedni a gépből kinyomtatott papírokról, a FAX gépekről, a PC-kben lévő FAX-szoftverekről, mint potenciális „biztonsági lyuk"-akról.

Az informatikai szakma abban egyetért, hogy az információ digitalizálódásával egy időben az információrobbanás nyomán az információ „elfolyásának" („data leakage") sokkal szélesebb tere nyílott meg, mint amekkora az a hagyományos papír alapú tárolás esetében volt. A papírnak meg van az a hátránya, hogy „m-tömegű testét" át kell vinni valamilyen fürkésző tekintet előtt. A behálózott glóbuszon ezt egy e-mail-el, már jóval nehezebb megtenni.

Egészségügyi adatok csoportosítása

- Beteg adatok (azon belül is demográfiai adatok, és egészségi állapotleíró adatok
- Vizsgálati /diagnosztikai adatok, kórképek
- Beavatkozási adatok (műtéti jegyzőkönyvek / ha végeznek az adott intézményben műtétet)
- Gyógymód adatok, kezelések, gyógyszerezési adatok,
- Kórtörténeti / beteg történeti adatok, zárójelentések,

Az adatok kezelésénél azok tartalmi elemeinek tisztázása mellett

- a felhasználáshoz szükséges azonosíthatóságot,
- a változások nyomon követhetőségéhez szükséges visszakereshetőséget egyaránt biztosítani kell.

Pl.: egy diagnosztikai adat a mérési mód (esetenként eszköz) és mérési körülmények együttes ismertetésével használható. Ugyanígy a különböző helyen és időben végzett, megfelelően azonosított adatok nagyobb valószínűségű hipotézisek felállítására adnak lehetőséget.

Fentieken kívül lehetne még szót ejteni az intézményi szintű, statisztikai adatokról, kimutatásokról, jelentésekről, vezetői információkról.

Mint adat jelen van, habár nem mindegyikben jelennek meg személyes adatok (ezekkel nem foglakozunk most).

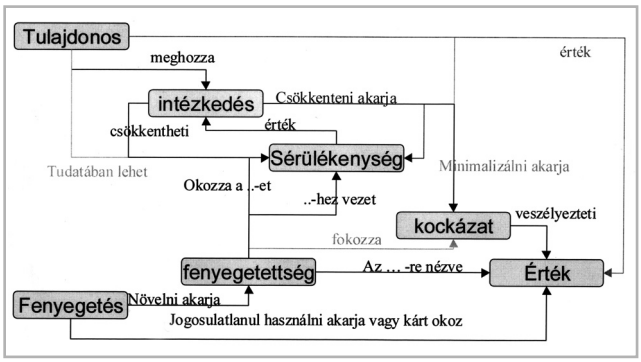
Minden biztonsági rendszer kialakításakor meg kell határozni a célértékeket. Eldöntendő, hogy az egészségügyi intézményekben melyek legyenek ezek. Egy lehetséges minta:

- komplett kórházi információs rendszerleállás miatt előálló, tömeges megbetegedést /ellátatlanságot okozó estek száma kisebb, mint: xxx?
- Évente országosan (információ-biztonsági előírások megsértéséből származó)
  - 1 műhiba (halálesettel járó) – tragikus kimenetelű?
  - 10 közepes következménnyel járó – maradandó szövődményeket okozó?
  - 100 könnyű sérüléssel járó – kis-kockázatú?

MIT LEHET TENNI?

Az informatikai biztonsági rendszer kialakításának kérdéseivel egy később következő cikkünkben foglalkozunk. A helyzet elemzéséhez kitűnő segítséget ad az 1. sz. ábra. Annak keretében az alábbi kérdéseket taglaljuk:

- Kockázatelemzés
- Érzékenység meghatározása
- Rendszerelemek gyenge pontjai és fenyegető tényezői
  - Környezeti infrastruktúra
  - Hardver
  - Adathordozó
  - Adatok
  - Kommunikáció
  - Személyek



1. ábra
A biztonság elemeinek kapcsolata a CC (Common Criteria) szerint

Mit vár el az Unió a tagországoktól?

Az európai Parlament és az Európai Bizottság 2002. szeptember 23-án hozott, No. 1786/2002/EC számú döntése a közegészségügy területére vonatkozó 2003-2008-as közösségi akcióprogramjának elfogadásáról

A népegészségügyi célkitűzéseken és kezdeményezéseken kívül a járványok terjedésének gyors jelzőrendszerének kiépítésén túl a lakosság társadalmi szintű egészségügyi információkhoz való hozzáférésének elősegítése a cél. Az európai polgárok egészségügyi személyes adatainak biztonságát az alábbi passzus (3-as cikkely) fejti ki.

A program végrehajtása során a bizottságnak a tagállamokkal közösen olyan mechanizmusokat kell bevezetnie, amelyek igazodnak a megfelelő személyes adatok védelméről szóló rendelkezésekhez, és amelyek biztosítják az ilyen adatok bizalmasságát és biztonságát.

Az általános helyzet Magyarországon

Az egészségügyről eddig még nem készült speciálisan informatikai helyzetet taglaló összefoglaló, viszont rendelkezésre áll egy 2 éves, a Bell Research által készített jelentés. Ez így fogalmaz AZ ELEKTRONIKUS BIZTONSÁG HELYZETE MAGYARORSZÁGON című tanulmányban.

Ajánlások, sztenderdek kidolgozása a költségvetési intézmények számára magában foglalhatja a fentieken túlmenően egyrészt az intézmények IT-biztonsági kockázat szerinti besorolását és az egyes kockázati szinteken és területeken alkalmazandó IT- biztonsági eszközök körét, másrészt ajánlásokat fogalmazhat meg az alkalmazható, minősített eszközök körére és az igénybe vehet ő gyártók, forgalmazók, tanácsadók csoportjára vonatkozóan.

Az intézmények közötti együttműködések felélénkítése mellett központi iránymutatással nagymértékben lehetne támogatni az intézmények munkáját, amely során az alábbi területeken várnak segítséget:

Minimálisan elvárható IT-biztonsági megoldások körének meghatározása, ajánlások megfogalmazása terén is.

Az ajánlások kidolgozásához hozzátartozik annak felülvizsgálata is, hogy a közbeszerzésben eddig nem jelentek meg külön kategóriaként a biztonsági termékek az antivírus szoftver termékek kivételével, ezért tűzfal megoldást vagy IT-biztonsági tanácsadást hivatalos eljárás keretében nem vásárolhattak az intézmények.

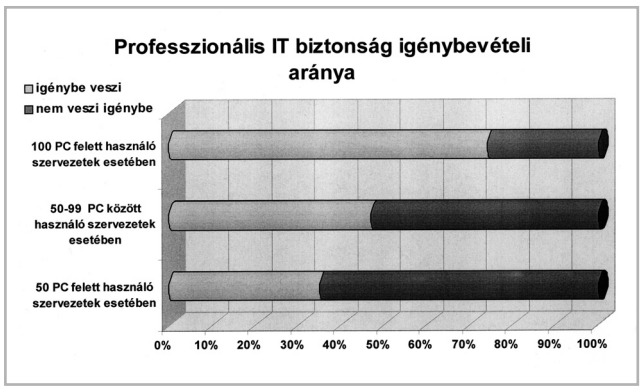
Biztonsági megoldások

A kutatás során vizsgált intézmények jelenlegi informatikai helyzete szélsőséges képet mutat, míg egyik oldalon a hardver problémákkal küzdő elmaradott intézmények, például egészségügyi intézmények állnak, addig a másik oldalon a távoli hozzáférés biztonságát is körültekintően kialakító szervek (pl. közigazgatási intézmények) helyezkednek el.

A költségvetési intézmények hozzávetőleg egyharmada rendkívül súlyos IT-biztonsági gondokkal küzd, míg a szervezetek fele csak a megfelelő szoftvereszközöket hiányolja a védelemhez. Minden intézménynél kritikus kérdésként jelenik meg a gazdasági és a személyi adatok biztonságos tárolása. Legfőbb veszélyforrásnak a vírustámadásokat, a hacker behatolásokat, a hardvereszközök meghibásodásából fakadó adatvesztést és a felhasználói tudatlanságot érzékelik az informatikai vezetők, melyek közül az első hármat leginkább az anyagi erőforrások és a vezetői akarat határoznak meg, míg a felhasználói tudást nehezebb csupán a belső informatikai csapat által fejleszteni.

Az IT-biztonságot szolgáló eszközök közül legfontosabbnak a vírusvédelmet, a tűzfalak alkalmazását, a felhasználó azonosítást, a fájlok jelszavas védelmét és az eseménynaplózást tartották a szakemberek, amelyeket alapkövetelményként, követendő gyakorlatként határoztak meg a költségvetési intézmények számára.

Professzionális IT-biztonsági szolgáltatást a szervezetek kevesebb, mint harmada vett igénybe [30%], az 50+ PC-s körben azonban ennél nagyobb arányban terjedt el az alvállalkozó bevonása [50-99 PC: 47%, 100+ PC: 74%]. (Lásd 2. sz. ábra.) A biztonsági szolgáltatások közül leginkább az egyszeri alkalmat jelentő megoldásokat választották eddig a vállalatok [pl. a biztonsági rendszer kiépítése – 67%, ill. tanácsadás ezen a területen – 45%], emellett a biztonsági rendszerek felügyelete, karbantartása fordul elő számottevő mértékben [43%].



2. sz. ábra
A biztonsági beruházások aránya

MI A FEJLESZTŐK FELELŐSSÉGE?

A jövő esélyei a kórházakban

Ha azt akarjuk, hogy a betegadatok biztonságban legyenek az egyre jelentősebb mértékben alkalmazni kívánt világhálón, akkor az nemcsak az üzemeltetők felelőssége lesz, hanem a rendszer-architektoroké is. Az idejekorán a fejlesz-

tés legelső szakaszában (már a rendszer-követelménytámasztáskor) a biztonsági elvárásoknak és követelményeknek pontosan szerepelniük kell a követelmények között.

Mint mindenhol az informatikai megoldáskészítők és az őket felkérő üzleti (itt kórházi) megrendelők együttműködésében az informatikusokat hibáztatják az egyes rendszerhibák hiányosságok miatt. A helyzet mint általában, itt is kétoldalú. Egyértelműen nem lehet csak az informatikusok nyakába varrni a keletkező problémákat.

Az együttműködő partnereknek egyformán nagyobb affinitást kell mutatniuk a „másik féllel" szemben. Ez véleményem szerint képzési probléma. Sok informatikus nem ássa bele magát elég mélyen az adott üzleti probléma megértésébe és ezzel egy időben sok üzleti megrendelő nem hajlandó megfelelő mélységben elmélyedni a megoldandó probléma körültekintő tálalásában. A süketek párbeszéde nem szokott jó megoldásokat teremni. A kivezető út mindkét fél nyitásában rejlik, az üzleti oldalnak jóval jelentősebb informatikai érzékenységgel kell rendelkeznie, míg a másik fél számára is kötelező elmélyedni a megoldásra váró adott üzleti terület törvényszerűségeiben. A „kicsit orvos-nagyon informatikus" szakember és a „kicsit informatikus de nagyon orvos" szakemberek párosa lesznek a jövőben a „nyerőpárosok".

Ez színtisztán képzési kérdés. Jelenleg a kívánt eredmény kaotikusan képződő, alkalmas tudású általában pályaelhagyók „fejében", gondolkodásában jön létre, „orvos-informatikus" és „informatikai orvos" (egészségügyet értő informatikai szakember) szakképzés híján.

Az új rendszerek kialakítása során felügyeleti szervek minősítési rendszere lehetne a garancia arra, hogy megbízható információs rendszerek terjedjenek el az egészségügyben, melyekből az információlopás erősen meg van nehezítve.

Biztonsági szintek definiálása az egészségügyben

Nemzetközi téren az 1970-as évek végén indult meg az Egyesült Államokban az informatikai biztonság követelményrendszere kidolgozása. Első nyilvánosságra hozott eredménye a Trusted Computer System Evaluation Criteria (magyarul: Biztonságos Számítógépes Rendszerek Értékelési Kritériumai, röviden: TCSEC), mely a következő 4 csoportra bontja a biztonsági osztályokat, egyre szigorúbb követelményekkel :

- D csoport: minimális védelem
- C csoport: szelektív és ellenőrzött védelem
- B csoport: kötelező és ellenőrzött védelem
- A csoport: bizonyított védelem

A TCSEC a D csoportot érdemtelennek tekinti az informatikai biztonság szempontjából, az A csoport esetében pedig matematikailag (formálisan) bizonyítható előírásokat, specifikációkat követel meg, amelyek a gyakorlatban csak nagyon nagy rá fordításokkal lehet megvalósítani.

Az előzőekben ismertetett szabványban lévő besorolási sémát követve, ha neki akarnánk kezdeni az egészségügy reformján belül az informatikai biztonság növelésének valamiféle saját magyar egészségügyi területen betartandó minimum szintet kellene definiálni, amit ahogy a lehetőségek engedik, egyre magasabb és magasabb szintre kell majd emelni, de mindig csak racionálisan a lehetőségek figyelembe vételével.

MI AZ ÜZEMELTETŐK FELELŐSSÉGE?

Ragadjuk meg az alkalmat és tekintsük kezdésnek a „D" szint elérését. Itt a magyar egészségügyi minimum szint kijelölését értem alatta. Ha a rendszer kiépült és működik, akkor onnan a továbblépés már könnyebb lesz.

Tehát a javaslat arra nézve, mik a legalapvetőbb és legsürgősebb tennivalók ott, ahol az információ biztonságra még nem tudtak különösebb figyelmet fordítani, öt pontban:

- A betegadatok demográfiai részéhez csak olyanok férhessenek hozzá, akiknek a munkaköri leírásában ez szerepel.
- Zárhatóvá tenni minden olyan papír alapú információtárolót (szekrényt, iratrendezőt, helyiséget), amely betegek demográfiai adatait tárolja.
- Üzembe állítani az adatmegsemmisítést minden olyan eszközre nézve, ahol betegek üzemszerűen már fel nem használt demográfiai adatai megjelenhetnek.
  - Papírok esetén (számítógép-nyomtatókból származó iratokra is) iratmegsemmisítőt üzembe állítani és használatát elrendelni.
  - Mágneses adathordozók formattálás (totális törlés) nélkül intézményen kívülre jutását megtiltani és rendszeresen ellenőrizni.
  - PC-k leselejtezett lemezeit előzetesen formattálni,
  - floppykat formattálni, vagy használhatatlanná tenni, átmágnesezni,
  - szalagokat, használaton kívüli mágneskazettákat használhatatlanná, olvashatatlanná tenni,
  - CD-ket, DVD-ket szintén olvashatatlanná tenni!
  - Betegek érzékeny adatait a WEB-en csak az átvitel idejére elérhetővé tenni.
  - WEB szerverek operációs rendszereit rendszeresen frissíteni a kiadott patch-ekkel, melyek általában biztonsági réseket „tömnek be".
  - Érzékeny betegadatokat különálló adatbázis szerveren és nem WEB szerveren tartani.
  - Az adatbázis szervert szeparált (és tűzfal mögötti) LAN szegmensre fűzni.
  - Az adatbázis szerverhez való hozzáférést fizikailag is és logikailag is korlátozni:
- Az érzékeny beteg adatokhoz történő számítógépes (logikai) hozzáférést authentifikációs ellenőrzésen keresztül végezni.

- Rendszeresen ellenőrizni kell a felhasználói hozzáférések kiosztását, megszűntetését illetve áthelyezések miatti változtatását:
  - Háttérellenőrzéseket tartani azoknál a dolgozóknál, akiknek az érzékeny betegadatokhoz hozzáférésük van.
  - A kritikus rendszerekhez mindenhol életbe léptetni (megszigorítani) a bejelentkeztetést.
  - Rendszeresen ellenőrizni a szokatlan eseteket a rendszer log-okban.

Tudjuk, hogy a fenti öt alapintézkedés nem old meg mindent, de most nem is ez volt a cél, ezek együttes alkalmazása jelentősen csökkenti az informatikai biztonsági kockázatot az érzékenynek minősített betegadatokkal kapcsolatosan. Ezek az intézkedések elsősorban az identitás lopás megelőzésében játszanak kulcs szerepet, de előnyös hatásuk megmutatkozik az adatvédelem egyéb területein is.

ÖSSZEFOGLALÁS

Szóval biztonságban vannak-e adataink a világhálón? Jelenleg még nem túl gyakran kerül oda. Később várató az egészségügyi reformok hatására, melynek előhírnöke a HEFOP 4.4-es projekt lesz 2005–2007-ben. Amikor majd az intézményközi rendszerek elindulnak, akkor már interneten keresztül fognak az eAdatok áramlani intézménytől intézményig. Annak a rendszernek mindenképpen része lesz egy erőteljes titkosítási és aláírás-hitelesítési mechanizmus.

Konklúziók:

- Az egészségügyi ellátó rendszerek felülvizsgálata és újraszervezése a világ legtöbb országában napirenden van. Valószínűsíthető, hogy az intézményrendszer egyes elemei inkább tarkaság, semmint az egysíkúság irányában változnak. A különbözőség elsődleges látható tartalmi jegyei a vele szemben támasztott követelmények és azok teljesítése között lesz. A szelektív igények között az intézmények egy részével szemben felerősödhet
  - az általános biztonság és ezen belül az információ védelem, valamint
  - az egyes ellátó intézmények közötti, betegközpontú adatáramlás és kezelés igénye.
- Az EU-s pályázatoknál már ma is, és a jövőben is – vélhetően – fokozott mértékben fog hangsúlyt kapni az adatbiztonság, a titkosság, a sérthetetlenség és a rendelkezésre állás.
- Az e helyzetre felkészülni kívánó intézményeknél meg kell határozni védendő egységenként, azon belül adatfajtánként
  - a kívánatos biztonsági szintet
  - a szükséges technikai és működési feltételeket,
  - ezek forrásigényét.
- A biztonságnak és azon belül a betegadatok azon szegmensének, mely a személyi adatok biztonságát védi, megfelelő helyet kell kapnia a finanszírozás felhasználási tételei között.
- Fel kell készíteni a szervezetet és a személyzet teljes állományát szabályozásokkal és képzésekkel a biztonságos működés és ennek keretében az információ biztonság megteremtése, fenntartása, valamint az ehhez tartozó fegyelem szükségességének felismerése és gyakorlása kérdéseire.

IRODALOMJEGYZÉK

[1] Medical Requirements for Data Protection
[2] Klaus Pommerening, Institut für Medizinische Statistik und Dokumentation der Johannes-Gutenberg-Universität D-55101 Mainz
[3] www.sap.com: Health Care Success Story, SAP kiadvány.
[4] How to prevent identity theft? News Story by Marne Gordan, FEBRUARY 26, 2003. (COMPUTERWORLD
[5] Szabványok és ajánlások az informatikai biztonság területén,
Muha Lajos, Előadás CIO Hungary konferencia
[6] Decision No 1786/2002/EC of the European Parliament and of the Council of 23 September 2002 adopting a programme of Community action in the field of public health (2003-2008) – Commission Statements
[7] Az elektronikus biztonság helyzete és az állami szerepvállalás lehetséges területei, Bell Research , Vezetői összefoglaló a Hírközlési Felügyelet részére 2003. Augusztus
[8] Budapesti Műszaki és Gazdaságtudományi Egyetem, Méréstechnika és Információs Rendszerek Tanszék 8/54 SEARCH Laboratory
[9] Budapesti Műszaki és Gazdaságtudományi Eegyetem Méréstechnikai és Információs Rendszerek Tanszék, Informatikai biztonság az internetes támadások tükrében, 2003.01.

A SZERZŐK BEMUTATÁSA

Dr. Baross Szabolcs A Miskolci Egyetem Gépészmérnöki Karán végzett. Első munkahelye az Ipargazdaságtani Tanszék volt, ahol munkaszervezéssel és költségtannal foglalkozott. Ezt követően a Hungalu Rt-ben a csoporthoz tartozó cégek szervezését fogta össze, irányította a működésfejlesztési munkákat. 1982-től vezetési tanácsadóként dolgozik, vezeti saját tanácsadó cégét. Főbb szakmai területei a stratégiakészítés, szervezetfejlesztés, cégcsoporti modellek kialakítása, szervezetszabályozás, vezetésszervezés, projekt menedzsment.
Az egészségügy területén részt vett: a háziorvosok vállalkozóvá válásának előkészítő munkáiban, a gyógyszerészek vállalkozóvá válásának felkészítő képzésében, vezetett több intézményátvilágítást, részt vett egyházi intézmény visszaadásának előkészítésében.
Oktatási tevékenységet végzett, illetve végez több hazai egyetemen, főiskolán, vezetőképző intézetben. A CEU, illetve a jogelőd IMC menedzser képzési programjaiban oktatóként 10 éve vesz részt.

Balog Géza a főként egészségügyi és banki területen működő, informatikai biztonsági szaktanácsadással és informatikai minőségbiztosítással foglalkozó IT-IQ informatikai társaság ügyvezetőjeként dolgozik.
Tanulmányait Moszkvában végezte, ahol 1979-ben szerzett jeles diplomát. Eddigi munkahelyei: Struktúra Szervezési Vállalat, (termelésirányítási szoftverek), ING Biztosító, (számítóközpont üzemeltetés, fejlesztés, üzleti rendszerek fejlesztésének minőségbiztosítása), ABN-AMRO Bank (Informatikai üzemeltetés), K&H Bank (Informatikai Minőségbiztosítás).
Főbb szakterületei az informatikai biztonság, informatikai szervezet átalakítás, projektmenedzsment és informatikai minőségbiztosítás. Jártasságot szerzett az informatikai fejlesztés különféle fejlesztési életciklus modellekben, konfiguráció menedzsmentben, komplex projektek irányításában és a nagy megbízhatóságú rendszerek kialakításában.

PROJECT HOPE – Projektek 2004.

Folytatás a 23. oldalról

13. Szeged Megyei Jogú város Önkormányzata Kórháza
    Dr. Demeter Ildikó, Dr. Tari Róbert, Dr. Temesváry Beáta
    Pszichiátriai és Addiktológiai Osztály strukturális és funkcionális átszervezése. (Rekonstrukcióból minőségfejlesztés)"

14. Szent Borbála Kórház, Tatabánya
    Dr. Bányász Zsolt, Kecskeméti Csilla, Dr. Molnár László
    „A központi műtő új munkarendje, délutáni műszak bevezetése, költségracionalizálása a Komárom-Esztergom Megyei Szent Borbála Kórházban"

15. Szent Lázár Megyei Kórház, Salgótarján
    Korbáss Diána, Varga Roland, Dr. Vekszlerné Vukovics Éva
    „A takarítás hatékonyságának növelése, gazdaságosabbát tétele"

16. Szent Pantaleon Kórház, Dunaújváros
    Dr. Fedor László, Horváthné Kósa Edit, Stipkovits Gabriella
    „Egyéni teljesítményértékelő rendszer bevezetése a Szent Pantaleon Kórházban"

17. Területi Kórház, Szentes
    Dr. Ábrahám Ágota, Dr. Kiss Andrea, Dr. Tóth Edit
    „Műtétes Mátrix Osztály és Központi Műtő működésének kialakítása"

18. Vasútegészségügyi Közhasznú Társaság Egészségügyi Központ, Balatonfüred
    Dr. Bors József, Horgas Mária, Turcsányi Lilla Márta
    „Balatoni Időskorúak Otthona"

19. Városi Kórház, Nagykanizsa
    Dr. Nagy Éva, Németh Rita, Soós Ferenc
    „MRI berendezés telepítése és gazdaságos működtetése a nagykanizsai kórházban"

20. Városi Kórház Rendelőintézet, Várpalota
    Dr. Beleznay Gábor, Hegyi Zoltánné, Dr. Tollas Árpád
    „Kontrolling rendszer kiépítése a Várpalotai Kórházban"