HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Baráth Artur
magicman@mail.duf.hu

AZ ISO 27799:2008 SZABVÁNY AZ INFORMATIKAI BIZTONSÁG KEZELÉSE AZ EGÉSZSÉGÜGYBEN

I. RÉSZ

Absztrakt

Az informatikai rendszerek biztonságos, hatékony, megbízható működéshez elengedhetetlen a vonatkozó törvényi rendelkezések és szakmai normák beható ismerete. Ezen tudás elsajátításához ad segítséget jelen munkám, amelyben, a címben szereplő szabvány részletes ismertetésének első része olvasható.

The knowledge of professional norms and related laws are indispensable for the safe, reliable and effective work of informatics systems.For acquiring this knowledge my work provides help, in which the first part of the detailed presentation of the title standard is readable.

Kulcsszavak: *egészségügy, informatika, biztonság, ISO 27799:2008, szabvány ~ healthcare, informatics, safety, ISO 27799:2008 standard*

BEVEZETÉS

Ezen cikk első darabja egy háromrészes cikksorozatnak, melyben az ISO 27799:2008 számú szabványt dolgozom fel annak érdekében, hogy segítsek azoknak, akik Magyarországon kívánnak a témában dolgozni vagy kutatni. A vizsgált szabvány az egészségügyi informatikai rendszerek egységesítését és minőségének javítását hivatott segíteni, azáltal, hogy pontosan deklarált és megszabott környezetet biztosít a működéshez.

Magyarországon a napokban lehetett hallani az országos egészségügyi rendszerek átfogó modernizációjáról, egységesítéséről, a köztük szükséges átjárhatóságok megvalósításáról. A törekvés üdvözlendő és természetesen megkésett, ennek ellenére bizakodásra ad okot, hogy foglalkoznak a témával.

Egy biztonságos és nemzetközi szinten is kompatibilis, elismert rendszer kialakításához elengedhetetlen a vonatkozó szabványok és jogszabályok ismerete. Magyarországon sajnos még igen kezdetleges állapotok uralkodnak az egészségügyi informatikai rendszerek biztonsága területén, amit rövid időn belül orvosolni kell, hisz a társadalom és az ország érdeke egy stabil, hatékony, biztonságos ellátórendszer létesítése. Ezen folyamat elindulásához nyújt fontos segítséget cikksorozatom.

AZ ISO 27799:2008 SZABVÁNY

Az ISO 27799:2008 nemzetközi szabvány az egészségügyi informatika működését támogató iránymutatásokat határoz meg. A szabvány meghatározza egy sor részletes ellenőrzés irányítását az egészségügyi információs biztonság vizsgálatára, és a legjobb gyakorlati iránymutatásokat. Megvalósításával az egészségügyi szervezeteknek és egyéb egészségügyi információk kezelőinek képes biztosítani a minimálisan szükséges biztonsági szintet, amely megfelel saját szervezeti körülményeik között, és amely fenntartja a személyes egészségügyi adatok bizalmasságának, sértetlenségének és rendelkezésre állásának körülményeit. A szabvány minden egészségügyi információ vonatkozik, függetlenül a tárolásra használt eszközöktől és függetlenül a továbbítási csatornától.

Az ISO 27799:2008 nemzetközi szabvány az ISO/IEC 27002 nemzetközi szabvánnyal együtt alkalmazandó, és együtt határozzák meg, mire van szükség a biztonságos tájékoztatáshoz az egészségügyi ellátásban.

A szabvány technológia-semleges, mert a biztonsági technológiák gyorsan fejlődnek, miközben a szabvány előírásai hosszú távon is érvényben maradnak.

A szabvány szakkifejezései és meghatározásai

Jelen szabvány alkalmazásában az alábbi fogalom-meghatározásokat kell alkalmazni:

Az egészségügyi informatika egy tudományág, amely érinti a kognitív, az információ-feldolgozó és a kommunikációs feladatait az egészségügyi gyakorlatnak, oktatás és kutatás, beleértve az információs tudomány és a technológia támogatását.

Ennek kiszolgálására szolgál az egészségügyi információs rendszer, ami lényegében egészségügyi ellátással kapcsolatos információk tárolása számítógéppel feldolgozható formában, feladata kezelni és biztonságosan tárolni az adatokat, továbbá hozzáférést biztosítani azokhoz jogosult felhasználónak. E kettő terület összehangolt munkája is kell az egészségügyi ellátás működéséhez, ami bármilyen típusú szolgáltatás szakemberek részéről, akár paraprofessionálisan[1] rendszerben is.

Az egészségügyi ellátás működését biztosítja az egészségügyi szervezet, ami általános kifejező leírása többféle típusú szervezetnek, amelyek az egészségügyi szolgáltatásokat

[1] Állapot, mikor a professzionális képzettség és tudás a személy birtokában van, viszont a cím és jogosultság nincs. Mindig supervisori felügyeletet kíván meg a működése.

biztosítják. Ezen szervezeteken belül végeznek munkát az egészségügyi szakemberek, akik jogosult személyek, melyek hivatalos testület által elismert minősítéssel végeznek bizonyos egészségügyi feladatokat. Az egészségügyi szolgáltató, ami bármely személy vagy szervezet, aki részt vesz a nyújtott vagy kapcsolódó egészségügyi szolgáltatásokban az ügyfél részére, vagy jóléti gondozó biztosítja a körülményeket a munkavégzéshez

A felelősségre vonhatóság érdekében definiálni kell többek között azonosítható személyt, aki az a személy, aki azonosítható, közvetlen vagy közvetett módon. Különösen egy azonosító szám vagy több egyedi tényező és a személy fizikai, fiziológiai, mentális, gazdasági, kulturális vagy társadalmi jellemzői alapján.

Személyes egészségügyi adatok: Tájékoztatás az azonosítható személy részére, amely kapcsolódik az egyén fizikai vagy mentális egészségi állapotához, továbbá azon egészségügyi szolgáltatások adatai, amiket az egyénnek nyújtottak. Ezen adatok az alábbiak lehetnek:

- a) tájékoztatás a nyilvántartásba vételről az egyén számára;
- b) információ a kifizetések vagy jogosultság az egészségügyi ellátás tekintetében az egyén részére;
- c) egy számot, szimbólumot vagy különleges egyedi jelet, mely azonosítja az egyes egészségügyi célokra;
- d) származó információi vizsgálatnak, egy testrésznek vagy testi anyagnak;
- e) azonosítása egy személy (pl. egy egészségügyi szakember), mint az egészségügyi szolgáltató, az egyén számára.

További meghatározandó fogalom az ellátás tárgya: ez, egy vagy több személy beütemezése fogadására, illetve egészségügyi szolgáltatás nyújtására. Eközben szükséges használni vagyontárgyakat, ami bármi lehet, ami értéket jelent a szervezet részére. Ezen szolgáltatások biztosítóját és tárgyak felhasználóját felelősségre vonhatóvá kell tenni, ami egy tulajdonság, amely biztosítja, hogy a végrehajtott intézkedések hatásai egyénekhez legyenek köthetőek a gazdálkodó egység vezetői által. Szorosan ide kapcsolódik a biztosíték, ami egy sor megfelelési folyamat eredményein keresztül a szervezet részéről megvalósítja a bizalom státuszát az információbiztonsági irányítás területén. Mindezek mellett elérhetőséget is biztosítani kell, ami azon tulajdonság, hogy hozzáférhető és használható igény által a felhatalmazott szervezet vagy személy által.

Az egészségügyi informatikai biztonság

Az egészségügyi informatikai biztonság célja a szabvány szerint, hogy fenntartsa az információk titkosságát, hozzáférhetőségének és épségének állapotát, beleértve a hitelesség, elszámoltathatóság és auditálhatóság2 [1] területét is.

Titoktartási intézkedéseket kell tenni, hogy fennmaradjon az adatok integritása, ha másért nem, hogy ne férjenek hozzá a vezérlési adatokhoz, ellenőrzési nyomvonalakhoz és a rendszer egyéb adataihoz, oly módon, hogy lehetővé teszik a titoktartás sérülését. Ezen túlmenően, a betegbiztonság függ a titoktartás fenntartásától, a személyes egészségügyi adatok integritásától, ezek sérülése eredményezhet betegséget, sérülést vagy akár halált.

Hasonlóképpen, a magas szintű rendelkezésre állás különösen fontos tulajdonság az egészségügyi rendszereknél, ahol a kezelés gyakran idő-kritikus. Katasztrófahelyzetet jelenthet, amikor nem egészségügyi vonatkozású informatikai rendszerek megbénulnak, éppen akkor, amikor az érintett információkra az egészségügyi rendszernek a leginkább szüksége volna.

[2] vizsgálhatóság, ellenőrizhetőség, mérhetőség, minősíthetőség

Veszélyek az egészségügyi informatikai biztonságra nézve

Jelen részben sorra veszem azon eseményeket, állapotokat, melyek veszélyt jelenthetnek az egészségügyi informatikai rendszerekre. A legtöbb esetben konkrét nevet hordoz a probléma, de néha csak magát a jelenséget, eseményt írom le, egyfajta gyűjtőfogalomként.

Kezdjük az alapvető fogalmakkal. Az egészségügyi ellátást végző személyek rendszer-hozzáférési eljárásokat sértenek, amikor egymás autentikációs[3] adatait, rosszabb esetben egymás felhasználói profiljait használják a kijelentkezés-bejelentkezés vesződségének elkerülésére. A felelősségre vonást is ez nagyban megnehezíti. További gondokat okozhatnak a Masquerade szolgáltatók (ideértve a szerződött karbantartó személyzetet, a rendszer szoftvermérnökét, hardver javító személyzetet, akik lehet, hogy pro forma jogon hozzáférnek rendszerekhez és adatokhoz). Masquerade szolgáltatók szerződéses személyzet segítségével a kiváltságos hozzáférést igénylő rendszereknél (például a helyszíni vizsgálatok és berendezések üzemzavarának elhárítása során) illetéktelenek hozzáférhetnek az adatokhoz.

Mint ilyen, ez egy megsértése a biztonságos kiszervezési megállapodásoknak. Bár ritkább, de a bennfentesek is lehetnek forrása a súlyos szabályszegéseknek, amik veszélyeztetik a személyes egészségügyi adatok titkosságát. Léteznek még masquerade kívülállók (beleértve a hackerek-et is), akik kívülállók és masquerade esete akkor jelentkezik, ha illetéktelen harmadik fél hozzáfér a rendszer adatokhoz vagy erőforrásokhoz, akár felhatalmazott felhasználó megszemélyesítése módján. Az alábbi esetek a leggyakoribbak ezen területen:

- a felhasználó azonosítása;
- a felhasználói hitelesítést;
- a származási hitelesítés;
- beléptető és kiváltság irányítását.

Meglepően könnyű lehet hozzájutni jogosulatlanul egy egészségügyi információs rendszer hozzáféréséhez (például egy séta során egy felügyelet nélküli hagyott munkaállomás mellett).

Jogosult felhasználók is végezhetnek jogosulatlan műveleteket, mint rosszindulatú megváltoztatása az adatoknak. Kritikus fontosságú a helyesen azonosított ellátási témák, hogy az egészségügyi nyilvántartásokat vezető egészségügyi szervezetek részletes azonosító jellegű információkkal kezeljék betegeiket. Ezt azonosító adatok használatára való kötelezéssel érhetjük el. Általában véve, az egészségügyi információk jogosulatlan használata a következő esetekben lépnek életbe:

- munkacsoport beléptető hibás, jogtalan használata
- az elszámoltathatóság és pénzügyi ellenőrzés hibái esetén
- személyi biztonsági megsértése

Káros vagy romboló szoftverek bevezetésével (köztük a vírusok, férgek és egyéb "malware[4]" [2] programok) is érhetik a rendszert támadások. A legtöbb IT biztonsági esemény számítógépes vírusok által keletkezik. A káros és zavaró szoftverek rendszerint a vírusvédelm vagy a szoftver változás-frissítés rendszer működésének kudarcából adódik. A káros programok terjedésének megakadályozásának akadályai általában a védelmi rendszerek hatáskörein belül az e-mail férgek és vírusok működése és a szerver szoftverek hiányosságai. További gondot okozhat a rendszer erőforrásaival való visszaélés. Ez a fenyegetés magában a felhasználókkal él, jellemzően akkor, amikor az egészségügyi dolgozó nem rendeltetés-szerűen használja az egészségügyi informatikai rendszer eszközeit, adatbázisait, személyes adatait. Például munkaidő alatt az őt foglalkoztató szervezet számítógépein zenét, filmeket, videókat hallgat és néz, rosszabb esetben az egészségügyi adatbázisokat használja személyes célokra. Kommunikációs beszivárgással végrehajtott támadásról beszélünk, amikor a normál

[3] Autentikáció: egy adott személy, eljárás hitelesítése különböző adatok által.

[4] Rosszindulatú szoftverek, melyek zavarják vagy akadályozzák a működést eközben esetlegesen illegális adatgyűjtést folytatnak.

adatáramlás folyamába egy kívülálló személy vagy szervezet becsatlakozik. A leggyakoribb esemény egy denial-of-service[5] támadás, amelyben szervert vagy hálózati erőforrásokat

hatékonyan off-line állapotba taszítják. Más beszűrődési kommunikációs formák is lehetségesek (például visszajátszás támadás, amelyben egy érvényes, de out-of-date üzenetet újraadnak egy valamilyen módon, ami normálisnak tűnik. Kommunikációs beszűrődésnek minősül a behatolásjelző károsítása és / vagy a hálózati hozzáférés-vezérlés károsítása.

Kommunikációs lehallgatás az, amikor nem titkosított a csatorna az átvitel alatt, a bizalmas információkat igen könnyen lehallgathatják. Ez egyszerűbb, mint amilyennek hangzik, bárki a helyi hálózatban potenciálisan telepíthet egy úgynevezett "csomag szippantás" alkalmazást,ami nyomon követi a hálózati forgalmat a saját helyi hálózaton, beleértve az olvasott e-maileket is az átvitel során. Erre szolgáló hacker eszközök könnyen hozzáférhetőek, amik automatizálják és egyszerűsítik ezt a folyamatot. Kommunikációs lehallgatásnak minősülő hiba, ha egy rendszer nem biztosítja a biztonságos kommunikációt.

Utóbbi támadás kapcsán fordul elő leginkább a megtagadás, amely fenyegetés az, amikor a felhasználók tagadják, hogy küldtek egy üzenetet (elállás eredet) vagy kaptak egy üzenetet (elállás kézhezvétel). Megtagadás jelenthet az ellenőrző alkalmazások használatának elmulasztását, mint például a digitális aláírás az e-receptek esetében (például: eredetmegjelölés), vagy az e-mail üzenetek olvasási visszaigazolásainak elhagyását.

Eltérő gondot okozhat a csatlakozási hiba, ami a következő: minden hálózatnak van egy rendelkezésre állási szintje, amikor ez nem elégséges és nem teljesíti a kívánt szintet, csatlakozási hibát eredményezhet. Ezen hiba előidézhető a hálózati rendszereszközök – elsősorban forgalomirányítók – káros befolyásolásával, vagy az autentikációs eljárások megzavarásával. Eredménye, hogy a felhasználók kevésbé biztonságos rendszereken kénytelenek kommunikálni, ami könnyűvé teszi a lehallgatást. Kiterelésnek is szokták nevezni, a biztonságos hálózatból való kiterelés nyomán. Ezen állapot egyik kivitelezési módja, a rosszindulatú kódok beágyazása. Ez a fenyegetés magában foglalja az e-mail vírusokat és a rosszindulatú mobil kódokat. A vezeték nélküli és mobil technológiák egészségügyi szolgáltatók általi növekvő használata emeli ennek a fenyegetésnek a potenciálját. A rosszindulatú kód beágyazása eredményezheti az antivírus szoftver alkalmazásának elmulasztását vagy bénítását, vagy a behatolásvédelmi ellenőrzések elmaradását, vagy elégtelen működését.,

A hálózati hibák sorában az első, amit sorra veszünk a véletlen misrouting[6]. Ez a fenyegetés magában foglalja annak lehetőségét, hogy az információ egy hibás címre kerül kézbesítésre a hálózaton keresztül. Véletlen misrouting hiba adódhat a felhasználó oktatásának hiányából, vagy az integritás fönntartásának elmulasztásából. További ilyen területű gond a műszaki hiba a fogadó, tároló és hálózati infrastruktúrában. Ezen fenyegetések közé tartoznak hardverhibák, hálózati meghibásodások vagy adattároló létesítmények hibái. Sajnos egyáltalán nem egyedi az egészségügyi információs rendszereknél, hogy ezen hibáknak életveszélyes következményei vannak a betegek számára. További speciális hiba a környezetvédelmi támogatás hiánya (beleértve áramkimaradás és hálózati zavarok, szolgáltatásból származó természetes vagy ember által okozott katasztrófák). Egészségügyi információs rendszerek működése kritikus lehet a természeti katasztrófák közben és egyéb események ideje alatt. A megfelelő veszély-és kockázatértékelést az egészségügyi információk tartalmazzák. Annak felmérése, hogy természeti katasztrófák idején létfontosságúak-e az ilyen rendszerek működése elengedhetetlen.

Továbblépünk a szoftveres érintettségű hibákra. Az első értelemszerűen a rendszer vagy hálózati szoftver hiba. Denial-of-service támadásokat nagyban elősegítik ezen hiányosságok,

[5] Denial-of-service: informatikai szolgáltatás temporális használhatatlansága valamely ártó beavatkozás eredményeként.
[6] Téves irányítás

vagy a helytelen működésű operációs rendszer vagy hálózati operációs rendszer szoftver. A rendszer vagy hálózati szoftver hiba megelőzésének minősül a szoftver integritásának ellenőrzése, a rendszer tesztelése, illetve szoftver-karbantartásának ellenőrzése. Magyarországon sajnos roppant gyakori a szoftver hibás alkalmazása (pl. egy egészségügyi információs alkalmazás), amikor egy szoftvert nem a rendeltetésének vagy céljának megfelelő módon használunk. További gyakori gond az operátor hiba. Ez azon anomáliák összessége, mely az informatikai rendszer felhasználójának hibájából adódnak. Jellemzően az alábbi hiányosságokból adódhatnak: [3]

- műveletek ellenőrzései
- személyi biztonság (beleértve a hatékony képzés)
- a katasztrófa-elhárítás (beleértve az adatok biztonsági mentését és visszaállítását.)

További emberi mulasztásra visszavezethető probléma a karbantartási hiba. Minden olyan hiba, mely megelőzhető lett volna azon tevékenységek elvégzésével, amik az informatikai-rendszer karbantartására irányulnak és a karbantartási terv előír. Lehet ez szoftver oldali (például: frissítések elmulasztása) vagy hardwer oldali (hibás eszközök javításának vagy cseréjének elmulasztása)

Egyik leggyakoribb eset - az egész világ tekintetében is - a felhasználói hiba: Jelen anomália akkor állhat fenn, ha a felhasználó követ el hibát, például figyelmetlenségből rossz címzettnek küld bizalmas információkat. Felhasználói hibát eredményezhet:

- a felhasználói kezelőszervek rossz kialakítása
- személyi biztonság hiánya (hiányos képzés)

Speciális – e Magyarországon gyakori gond – a személyzet alacsony száma. A személyzet hiányból adódó fenyegetés lehetőségét tartalmazza, ha a kulcsfontosságú személyzet hiányos, vagy létszáma szűken szabott. E fenyegetés nagysága attól függ, hogy milyen mértékben küzdenek munkaerőhiánnyal az üzleti folyamatok. Az egészségügyi járvány nagymértékben növeli a keresletet a szakszemélyzetre.

Nagyon sötét terület a bennfentesek általi lopás (ideértve a berendezések vagy adatok eltulajdonítását). Bennfentesek általában jobban hozzáférnek a bizalmas információkhoz, mint a kívülállók, ezért kedvező helyzetben vannak, hogy ellopjanak információkat annak érdekében, hogy eladják vagy nyilvánosságra hozzák azt másoknak.

Egy fokkal kevésbé kellemetlen és szégyenteljes ügy a kívülállók általi lopás (ideértve a berendezések vagy adatok eltulajdonítását). Kívülállók általi adatok és berendezések eltulajdonítása egy komoly probléma egyes kórházakban. Sok ellenőrzés, beleértve a mobil számítástechnika ellenőrzések, biztonságos média szállítás, incidenskezelés, compliance[7] ellenőrzések vagy fizikai lopás elleni védelem segíthet megelőzni ezen eseményeket.

Jellemzően elégedetlen alkalmazottak követi kel a szándékos károkozás bennfentesek által nevű cselekményt. Akkor beszélhetünk ilyen eseményről, ha az alkalmazott személyzet szánt szándékkal károsítja a reá bízott, vagy használatra átadott eszközöket. Ez vonatkozik mind hardware, mind software eszközökre. Ennek is van külsős párja, a Szándékos károkozás külsősök által kategória. Akkor beszélhetünk ilyen eseményről, ha kívülálló személyek (nem a szolgáltató vagy annak megbízott alvállalkozóinak szerződéses munkavállalói) kárt okoznak azon rendszerekben vagy eszközökben, amelyekhez hozzáféréshez jutnak.

Kórházaknál, klinikáknál és egyéb egészségügyi szervezeteknél sokkal nehezebb megakadályozni, mint a legtöbb más működési környezetekben, elsősorban a nagyszámú rokonok, látogatók, barátok, járó betegek által generált embermennyiség miatt.

Sok magyarázatot nem kíván a terrorizmus által jelentett veszély. A terrorizmus fenyegetése, hogy szélsőséges csoportok szándékosan károsítják vagy megzavarják egészségügyi szervezetek munkáját vagy veszélyeztetik az egészségügyi szolgáltatók

[7] Szolgáltatás-készség

működését az egészségügyi információs rendszerek zavarása által. Az egészségügyi rendszerek tervezésénél komoly figyelmet kell fordítani a terrorizmus elleni védelemre, mert egyre komolyabb fenyegetést jelent. [4]

Mint az látható, elég száraz és nehézkes egy szabvány olvasata, értelmezése. Ennek ellenére igyekeztem minél inkább olvasó és felhasználóbaráttá tenni. A forma természetesen eltér a megszokott cikkek kinézetétől, de sajnos egy szabvány lényegében meghatározásokból áll, így azok formája erősen köti a lehetőségeket. Esetünkben a funkcionalitás elsőbbséget élvezett a külalaknál, remélem elnézi nekem a Tisztelt olvasó ezt a kompromisszumot.

ÖSSZEGZÉS

Jól látható, hogy elsősorban az emberi eredetű hiányosságokkal foglalkozik a szabvány eddigi része. Az egész világon nagy probléma, hogy a munkáját végző egészségügyi személyt nehéz rábírni a felelős adminisztrációs tevékenységre. Ennek érdekében olyan rendszereket kell kifejleszteni, amik nem teszik lehetővé a hanyagságot és minimalizálják a lehetséges hibákat.

Másik fontos terület, a fizikai környezet biztosítása. Hisz hiába érjük el, hogy mindenki tartsa be a biztonsági előírásokat, ha rendszerünk sebezhető és könnyen korrumpálható.

Az eddig taglalt ismeretek alapján ezen két fontos területen szükséges a mielőbbi előrelépés, hisz ezek alapokat képezhetnek egy további, magas színvonalú rendszer felépítéséhez.

Felhasznált irodalom

[1] Angol-Magyar Műszaki és tudományos szótár könyv és CD - Akadémiai Kiadó 1993.

[2] Webster's Encyclopedic Unabridged Dictionary of the English Language. – Gramercy Books, New Work/Avenel, 1996.

[3] Útmutató az IT biztonsági szintek meghatározásához BME IK, 2008

[4] Európai Bizottság, Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról, COM(2005) 576, 2005. november 17. (Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final

A cikk alapjául szolgáló szabvány:

Az ISO 27799:2008 szabvány angol nyelvű kiadása – ICS: 35.240.80 Első kiadás 1998.