Az információ biztonság követelményrendszere

Fazekas Tibor, QUALIPROD Minőségi és Műszaki Tanácsadó Kft.

Az információ védelme korunk alapvető igénye, nemcsak a felhasználók munkáját segíti, hanem az egészségügyi szolgáltatás magas szintű, minőségi színvonalát eredményezi. Az egészségügyben használt információk, adatok hitelessége, bizalmassága, sértetlensége és rendelkezésre állása feltétele a korszerű betegellátásnak. A cikk ennek megvalósítására kidolgozott BS 7799 szabvány szerinti információbiztonsági irányítási rendszer bevezetését ismerteti.

BEVEZETÉS

Az információ hatalom. A gazdasági és társadalmi élet legfontosabb értéke, vagyon, amely egyben a működés alapja. A működést meghatározza mennyire biztonságos, védett és megbízható az információ és milyen gyorsan jut el a megfelelő helyre.

Az információ védelme régóta fontos kérdés, – számítógéppel teli világunkban ennek védelme új értelmet kap.

Az első információ védelemmel foglalkozó BS 7799 számú információbiztonsági szabványt a Brit Szabványügyi Hivatal (British Standard Institute) adta ki 1995-ben. Ezzel az információbiztonság menedzsment rendszerek értékelésének hatékony eszköze jött létre, ami gyorsan elterjedt az egész világon és ma több, mint 11 nyelven hozzáférhető, többek közt magyarul is.

A BS 7799-1:1995 tartalmazta az információvédelem kezelésének azt az optimális gyakorlatát, amely segíti a hatékony információvédelmi irányítási rendszerek kialakítását, bevezetését és ellenőrzését.

A BS 7799 2. része „Az információbiztonság menedzsment rendszerének specifikációja” (Specification for Information Security Management Systems) címmel került kiadásra 1998-ban az első rész kiegészítéseként. A szabványok kiadása után világossá vált, hogy szükséges e rendszerek megbízható felülvizsgálata, a követelményeknek való megfelelőségük tanúsítása, így garantált a bizalom a szervezetek illetve partnereik közötti információvédelem biztosítására.

A Nemzetközi Szabványügyi Szervezet 2000 augusztusában a BS 7799 1. részét változatlan szerkezetben és gyakorlatilag változatlan tartalommal nemzetközi szabványnak fogadta el ISO/IEC 17799 néven. Az 1987 májusában alapított brit DTI/CCSC feladata a nemzetközi szinten is elfogadható informatikai biztonság értékelési és tanúsítási kritériumok és mechanizmus kidolgozása, dolgozik a BS 7799 2. rész nemzetközi szabványként történő elfogadáshoz szükséges kiegészítéseken.

Sajnos a magyar szabvány címe félrevezető, az eredeti „Code of practice for information security management” magyarul az „Informatikai biztonság menedzselésének eljárás rendje” lett a hivatalos szabvány cím, így leszűkítve a témakört az informatikára. Maga a szabvány minden típusú információvédelemhez ad útmutatót.

Ezeknek a szabványoknak és rendszereknek a célja az információ védelme kiszivárgás, lopás, illetéktelenek betekintése, vagy bármely más visszaélés ellen, továbbá az információ megőrzése gép- és egyéb problémák esetén.

AZ EGÉSZSÉGÜGYI INFORMÁCIÓ BIZTONSÁGA

Az információbiztonsági irányítási rendszer (IBR) bevezetése különösen fontos az egészségügyi intézményekben a következők miatt:

- a szolgáltatás az információ pontosságán alapszik
- az adatok áramlása elektronikus úton történik
- a betegek adatainak feldolgozása történik
- az információ biztonságának megőrzése
- személyes információkkal kezelése

Az egészségügyi szolgáltatás a bizalmon alapul, az információhoz csak az férjen hozzá, akinek erre felhatalmazása van.

A rendszerekben feldolgozott adatok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell.

A sértetlenség jelenti, hogy az erőforrás az eredeti állapotot tükrözze, a forrás eredetisége ne legyen megkérdőjelezhető.

A rendelkezésre állás feltétele a működőképességnek, hogy bármikor, ha szükség van rá előkereshető legyen.

Ebből adódóan az információ következő fajtái számítanak kiemelt területeknek:

- az egészségügyi ellátásban részesülőkkel kapcsolatos információk,
- ápolásra, gyógyításra és betegellátásra vonatkozó információk,
- az egészségügyi dolgozók bérezésével kapcsolatos adatok,
- stratégiai információk,
- kutatások, fejlesztések publikációja előtti eredmények.

A rendszer a megelőzésre helyezi a hangsúlyt az információ és adatbiztonság érdekében. Az információvesztésből adódó károk lehetnek közvetett és közvetlen veszteségek.

A közvetlen veszteségek (pl. hardver, szoftver károk) tulajdonképpen elhanyagolhatóak a közvetett veszteségekhez képest.

A közvetett veszteségek, mint a rendszer felállításának költségei, adatvesztés esetén a rendszer visszaállításának költségei, nem beszélve arról az időről, amire a tevékenységet szüneteltetni kell (kórházi ellátás) és nem utolsó sorban a betegek bizalmának elvesztése az egészségügyi szolgáltatóval szemben.

A technikai háttér pótlása lényegesen kisebb veszteség a tárolt adatok értékeihez képest.

Ezen veszteségek elkerüléséhez, a modell kidolgozásához és alkalmazásához ad útmutatást a BS 7799-es szabvány.

A BS 7799 szabvány szerinti információbiztonsági irányítási rendszer követelményei

Az információvédelmi irányítási rendszer követelményei:

- Biztonságpolitika (3. pont)
  A vezetőségnek biztonságpolitikát kell megfogalmaznia.
- Biztonsági szervezet (4. pont)
  Az információbiztonsági infrastruktúra meghatározása, felépítése, megtervezése.
  Információbiztonsági megbízott kinevezése.
- Az eszközök biztonsági besorolása és ellenőrzése (5. pont)
  Berendezések és állomány leltározása.
  Megfelelő védettségi szint meghatározása és kimutatása.
- Személyi biztonság (6. pont)
  Követelmények figyelembe vétele a munkaköri leírásoknál és a dolgozók alkalmazásánál.
  Felhasználók oktatása.
  Reagálás biztonsági esetekre és hibás funkciókra.
- Fizikai és környezeti biztonság (7. pont)
  Biztonsági tartományok meghatározása.
  Berendezések biztonsága.
  Általános utasítások.
- Számítógépes és hálózati szolgáltatások és üzemeltetés menedzsmentje (8. pont)
  Üzemviteli eljárások és felelősségek.
  Rendszer tervezése és átvétele.
  Vírusos szoftver elleni védelem, hálózatirányítás.
- Hozzáférés menedzsment (9. pont)
  Felhasználók hozzáférésének adminisztrációja, csoportok meghatározása.
  Hálózat hozzáférés felügyelet, operációs rendszer hozzáférésének felügyelete, alkalmazási hozzáférés felügyelete.
  Mobil munka és távműködtetés.
- Az IT rendszerek fejlesztése és karbantartása (10. pont)
  Biztonság az alkalmazási rendszerekben.
  Titkosítás felügyelete, adatállomány biztonsága.
  Fejlesztési és karbantartási folyamatok biztonsága.
- Üzletmenet-folytonosság menedzsment (11. pont)
  Folyamatosság biztosítása, tervezése, összeállítása és frissítése, felügyeletük a fennmaradás biztosítására, elvesztésük esetére.
- Megfelelés a jogszabályoknak és a belső biztonsági szabályzatoknak (12. pont)
  Törvényi követelmények betartása, törvényes adatvédelem és szoftver másolásvédelem tervezett feltételeinek figyelembe vétele.
  Biztonságpolitika átvizsgálása és műszaki követelmények betartása.
  Belső előírások, biztonságpolitika, rendszer-audit, alapelvek és célkitűzések megvalósítása.

Az eljárások és az előírások meghatározásra kerülnek az IBR kidolgozásakor. A vezetőség elkötelezettsége, érdekeltsége elengedhetetlen. Az irányítási rendszer révén, az információ biztonságba fektetett pénz sokszorosan megtérül a prevenció által.

Az információbiztonsági irányítási rendszer bevezetése

A bevezetés fázisai a következők:

- Helyzetfelmérés, a meglévő intézkedések felmérése, a felelősségi körök kijelölése.
- Felső- és középvezetői képzés során a rendszerszabvány, valamint az információ védelem folyamatának és gyakorlatának megismerése.
- Kockázatértékelés. Fő veszélyek, kockázatok és azok hatásainak értékelése és ennek eredményének dokumentálása.
- Információbiztonsági kézikönyv elkészítése, mely tartalmazza a szabvány követelményeinek való megfelelést.
- Eljárások és egyéb szabályozó dokumentumok elkészítése.
- Információvédelmi belső auditorok képzése.
- Rendszer bevezetése, oktatás.
- Rendszer belső felülvizsgálata.
- Elő-audit, tanúsító audit (BS 7799-2 szerint) külső független akkreditált tanúsító szervezet által.
- Folyamatos karbantartás és szabályozó módosítás az auditálások alkalmával.

Az egészségügyi szervezetek elsőrendű érdeke a betegellátás folyamatosságának biztosítása és a mielőbbi helyreállítás az esetlegesen bekövetkezett információ- és adatvesztések után. A BS 7799 szerinti információbiztonsági irányítási rendszer biztosítja a hatékony védekezést az információvesztés, illetve annak következményei ellen. Javul a szervezet megítélése, elismertsége, nő a bizalom a szolgáltatást igénybe vevők részéről.

A SZERZŐ BEMUTATÁSA

Fazekas Tibor A QUALIPROD Minőségi és Műszaki Tanácsadó Kft. kereskedelmi igazgatója. Közlekedésmérnök, gazdasági mérnök, menedzser. Az ÖVQ/MSZT által szervezett „Minőségirányítás" és „Auditor" tanfolyamokon vett részt, amelyeken eredményes vizsgát tett. Az Európai Minőségügyi Szervezet igazolása alapján az EOQ MINŐSÉGÜGYI RENDSZERMENEDZSER és az EOQ AUDITOR cím használatára jogosult. Az EARA által regisztrált KIR-auditortanfolyamok bejegyzett oktatója. Az SGS által szervezett képzésen Környezetközpontú Irányítási Rendszer vezető auditor címet szerzett (EARA). 1996 óta foglalkozik minőség-és környezetközpontú irányítási rendszerek, valamint integrált irányítási rendszerek bevezetésével.

Sajtóközlemény

Egyedülálló internetes szolgáltatás az orvosok és a betegek érdekében

Hazánkban a HáziPatika.com jóvoltából egyedülálló kezdeményezés indult „Orvosok a hálón" címmel. A www.hazipatika.com/doctors internetes oldal lehetőséget biztosít minden orvos számára saját bemutatkozó weboldal létrehozására, a betegek pedig szabadon tájékozódhatnak az Interneten és válogathatnak a lakhelyükhöz közel eső, vagy épp a betegségüknek megfelelő szakorvosok között. A szolgáltatás mindkét fél, azaz az orvosok és a betegek részére is ingyenes.

A HáziPatikai.com és a Magyar Orvos Kamara (MOK) a **www.hazipatika.com/doctors** oldalon lévő összes orvos és az újonnan feliratkozók esetében is ellenőrzi, hogy rendelkeznek-e az orvosi tevékenységhez szükséges MOK tagsággal. Az oldal látogatói így leinformált hálózatban kereshetnek a szakemberek között név, szakterület vagy földrajzi elhelyezkedés szerint. Az orvosok számára a program különlegességét az adja, hogy minimális számítástechnikai tudással megszerkeszthetik „virtuális rendelőjüket" az Interneten keresztül. Az eDoktoroknak lehetőségük van továbbá arra is, hogy fotókat tegyenek fel az Internetre tevékenységükről, szakrendelőjükről valamint tudományos publikációikat is az érdeklődő betegek rendelkezésére bocsáthatják.

A szakember oldalán a betegek nemcsak a rendelési címet és telefonszámot találják meg, de lehetőségük nyílik arra is, hogy kéréseiket e-mail-ben tegyék fel a kiválasztott orvosnak. A betegeknek ezen túlmenően lehetőségük van az orvos szakmai életútjába és különleges szolgáltatásaiba való betekintésre is.
Az Internet használók száma 2002-ben világszerte elérte a 600 milliót, 2004-re pedig várhatóan 900 millióra nő. Egy tavalyi felmérés kimutatta, hogy Kanadában az Internet hozzáféréssel rendelkezők kétharmada keresett egészségügyi tartalmat a világhálón, és az egészségügy volt az Interneten leggyakrabban keresett téma. Amerikában naponta átlag 6 millió ember kapcsolódik az Internetre csak azért, hogy egészségügyi információkhoz jusson.

Amint azt Kocsis Gábor az **„Orvosok a hálón"** program vezetője elmondta, a beteg és orvos közötti virtuális kommunikáció hazánkban még újdonságnak számít. Szeretnék azonban elérni, hogy ezzel a módszerrel megkönnyítsék a betegek szabad orvosválasztását, valamint az újszerű és ingyenes megoldás segítségével lehetővé kívánják tenni, hogy a szolgáltatással beteg és orvos a lehető leggyorsabban és legolcsóbban találják meg egymást."
„Jelenlegi ismereteink szerint a magyar orvostársadalom az átlagosnál nagyobb mértékben rendelkezik Internet hozzáféréssel." – hangsúlyozza Kocsis Gábor „Az átlagosnál nagyobb arányú hozzáférés mellett azonban igen alacsony a használati gyakoriság, így jelentős növekedésre számíthatunk az elkövetkező néhány évben. Szolgáltatásunkkal pontosan ezt a növekvő igényt és mindemellett az orvos-beteg kommunikáció újszerű, költséghatékony módszerét kívánjuk megvalósítani." – teszi hozzá a szakember.