Adat és információvédelemi kérdések a kórházi gyakorlatban II.

Nagy István, Gottsegen György Országos Kardiológiai Intézet

A Gartner Group elemzői által használt és általánosan elfogadott besorolás szerint öt szintet különböztetnek meg az informatikai infrastruktúra felügyeletének, védelmének színvonala szempontjából: kaotikus (chaotic, Level 0), követő (reactive, Level 1), megelőző (proactive, Level 2), szolgáltató (service-oriented, Level 3), értéktermelő (value creation, Level 4). Az Európai Uniós csatlakozás küszöbén ideje felmérni azt, hogy az intézetünk melyik kategóriába tartozik és azt is, hogy milyen tennivalóink vannak, amivel az „értéktermelő" kategóriába kerülhetünk.

BEVEZETÉS

A két részes cikk első részben áttekintést adtam – a kórházi környezetben előforduló, az informatikai biztonsággal és információvédelemmel kapcsolatos eszközökről és kérdésekről a saját napi gyakorlatunk alapján.

Az informatikai biztonság nem csak az informatikával foglalkozik, hiszen más szakterületek is egyre inkább szervesen kapcsolódnak hozzá. Ilyen például a jogtudomány, a minőségbiztosítás és a „hagyományos" biztonsággal foglalkozó „védelem" tudomány.

A jogtudományhoz az informatikai biztonság az adminisztratív védelem területén kapcsolódik egyrészt az érvényben lévő jogszabályok (állami, szolgálati, üzleti titok, illetve a személyes adatok védelme) szabályzatokba történő beillesztésével és alkalmazásával, másrészt a szervezetek helyi szabályozási rendszerének kialakításával.

A „védelemtudomány" elemei az informatikai rendszerek védelmében, mint a „hagyományos biztonság" megteremtői jelennek meg.

A minőségbiztosítás elsősorban az informatikai rendszerek részéről elvárhatóan az adatminőség biztosítása, az adatok sértetlenségének, hitelességének, rendelkezésre állásának és funkcionalitásának területén jelentkezik a tervezéstől az üzemeltetésig.

A kórházakban működő informatikai rendszereknek és az ehhez kapcsolódó szabályozóknak számtalan elvárásnak kell megfelelniük. Ezek közül kiemelhető a folyamatosság igénye, az erőforrások korlátozottsága és egyéb szabályokból (pl. jogszabályból) adódó korlátosság. A feltételeknek megfelelni csak jó infrastruktúrával, kimagasló infrastruktúra felügyelettel, képzett személyzettel és jó szabályozó rendszerrel lehet. Az infrastruktúra néhány elemét az előző részben tárgyaltuk. Az alábbiakban az infrastruktúra felügyelettel és az informatikai stratégiai és biztonsági tervezéssel foglalkozunk.

AZ INFORMATIKAI INFRASTRUKTÚRA FELÜGYELETÉNEK OSZTÁLYOZÁSA

Az alábbi besorolást valószínűleg többen szubjektívnek fogják tartani. Kétségtelen, hogy a magyar kórházak informatikai szervezetei és struktúrája nehezen sorolható be fehéren feketén egy-egy kategóriába. Természetesen szervezeti egységenként, alkalmazásonként, működési platformonként, illetve a menedzsment szervezetétől függően is alapvetően eltérő kép alakulhat ki. Ha bátrak vagyunk és vállaljuk a szembesülést saját infrastruktúra felügyeletünkkel, akkor érdemes időt szentelni az intézetünk egyes informatikai szakterületeinek besorolására.

Kaotikus

Ez a szint egyértelműen magán viseli az informatikai evolúciós fejlődés szinte minden jegyét. Az informatikai szervezet a legnagyobb jóindulat és szakmai hozzáértés ellenére (és itt senkit sem akarok megbántani!) az adottságok, lehetőségek és az anyagiak közös hatására nem tekinthető tudatosnak. Az informatikusok nincsenek birtokában azoknak az eszközöknek, szoftvereknek és rendszereknek (néhol az ismereteknek) amelyek segítségével a felügyeletükre bízott rendszerek és az azt kiszolgáló infrastruktúra pillanatnyi állapotát, legkritikusabb mutatóit ellenőrizni tudnák. Ritkán hálózati vagy szerver-felügyeleti elemek előfordulnak. A hálózat felügyeleti szoftverek alkalmazásánál előre el kell dönteni, hogy milyen szintig akarjuk a hálózati eszközöket menedzselni (fizikai és logikai hálózati szegmens, aktív eszköz, hálózati végpont vagy kliens szinten). Szerver felügyelet esetén melyek azok a paraméterek, amelyek állapotát, értékét mindig tudni szeretnénk, vagy mely szerverrel kapcsolatos folyamatok elkészüléséről (pl. mentés sikeres, mentési hibaüzenet,…) vagy megtörténtéről (pl. szerver leállás, újraindulás,…) szeretnénk azonnal tudomást szerezni.

Szinte kizárólag a végfelhasználóktól jövő hibajelentések alapján javítják, ellenőrzik, felügyelik, esetleg tartják karban a rendszereiket. A bejelentésekről nem készül feljegyzés, nem üzemel központi hibabejelentő (ún. hiba-logoló), amelyen nyilván lehetne tartani a bejelentett hibákat és nyomon lehetne követni a megoldás pillanatnyi állapotát.

Ezen a szinten gyakori a párhuzamos funkciókat ellátó modulok üzemeltetése. Sűrűn megtalálhatók olyan hardver és szoftver komponensek, amelyek már régen nem támogatottak. Sokszor találkozunk olyan modulokkal, rendszerekkel, amelyeknek programnyelve, adatbázis kezelője elavult, programozója már nem elérhető, ezért nem beszélhetünk rend-

szerfelügyeletről sem. Az esetleges „help-desk” szolgáltatásra még gondolni sem lehet.

Az adatvédelem megvalósíthatatlan abban az esetben is, ha az alkalmazás a rendszerek olyan egyvelegén fut amelyek közös alkalmazásakor a rendszerek adatvédelmi szempontból nem védhetők (pl. adatbázis kezelő – Clipper; munkaállomáson alkalmazott operációs rendszer – Windows 98; hálózati operációs rendszer – Novell 4.2).

Az üzemeltetési felelősség – ha definiált – a rendszerek telepítőié, ami a gyakorlatban elég nehezen érvényesíthető. Ezért aztán nem ritka, hogy a különböző rendszerek hibaelhárítása érdekében az intézet több pontján éjjel-nappal üzemelő, felügyelet nélküli (mindig bekapcsolt) modemek találhatók. Kitárva így az informatikai biztonság elvei szerint oly lelkesen becsukott számtalan kiskaput, mint azt az előző részben részletesen megbeszéltük. Ebből következőleg nincs érvényesíthető, számon kérhető felügyeleti koncepció és üzemeltetői felelősség.

Az eszközök nyilvántartása (és az adott kliensen folyó tevékenység) sok esetben nem pontos és sokszor redundáns, jogilag nem mindig tisztázott (pl. idegen tulajdonú eszközök).

Ezen a szinten még nem általánosan elfogadott és nem mindenhol elérhető az elektronikus levelezés. A felhasználók a levelezésüket és egyéb feladataikat különböző nem központilag menedzselt jogtiszta vagy nem jogtiszta szoftverek segítségével valósítják meg melyek működése és rendszerbe illesztése nem mindig egyszerű feladat a kórház informatikusai részére. A jogtisztaság megvizsgálása a BSA egyre aktívabb ellenőrző tevékenysége miatt egyre inkább aktuálissá válik.

Ez az a szint, amely valószínűleg a leggyakoribb és – ez az esetek nagy többségében – nem csak a kórházak anyagi lehetőségei miatt van így. Magyarországon fiatal még az egészségügyi informatika. Érdekes szimbiózisban találhatók meg a:

- számítógépek 386-os (esetleg 286-os!) számítógépektől kezdve a Pentium 4-ig,
- hálózatok Arcnet és Ethernet topológiával,
- koax, UTP és az optikai kábelek,
- vezetékes és vezeték nélküli adatkapcsolatok,
- 64kbit-es és 100 Gigabites hálózati adatátviteli eszközök,
- egyedi és hálózatos munkaállomások,
- csöves és digitális képalkotó eszközök,
- mobil és helyhez kötött adatbeviteli eszközök, adatgyűjtők,
- cikkszámos és vonalkódos azonosítás és adatbevitel,
- papír alapú adattárak és a DVD adatboxok,
- floppylemezes és Internetes adattovábbítás,
- papíralapú és digitális aláírás és levelezés,
- egyedi mátrix és hálózatos színes laser nyomtatók.

Követő

Ezen a szinten már megjelennek a felügyeleti eszközök (esemény és hibalogolás). A hibajelek és üzenetek megelőzik a végfelhasználói hívásokat vagy bekövetkezésük időpontjában észlelhetők. Az e-mail vagy az SMS – esetleg mindkettő együttes – alkalmazása esetén maximális mobilitás biztosítható. Ennek viszont alapvető követelménye a kiemelt szerverfunkciók és azok eredményének szabványos formában történő továbbítása a levelező szerver vagy a telefonközpont részére, amelynek mobil adapterrel kell rendelkeznie. Kiemelt rendszereknél már „help-desk” szolgálatot vesz igénybe az intézet. Kórházak esetében az outsourcing szerződések kapcsán telepített klinikai vagy gazdasági rendszerekhez ez a szolgáltatás szinte minden esetben biztosított. A rendelkezésre állás a szolgáltatási díjtól függ. A hibaelhárítás folyamatát profi szakember segíti. A hibakezelés folyamata kezd kialakulni (ki mit tesz, vagy ki kit hív, ha…?). Az elektronikus levelezés elfogadott kommunikációs eszközzé válik az intézeten belül. Az elektronikus levelezés általában rövid időn belül magával hozza a belső elektronikus információs rendszerek (ún. Intranetek) kialakulását. Mentési és helyreállítási eszközök, illetve eljárások kialakulnak elfogadottá válnak.

Az Intézeten belül az egyedi igények szerint kialakított speciális rendszerek, kereskedelmi és a szabad szoftverek sokszigetes, elszigetelt kavalkádja üzemel.

Ez talán a legveszélyesebb állapot. A „Követő” szint hajlamos többnek mutatni és érezni magát, mint amilyen valójában. Mivel a felhasználók egyre inkább biztonságban érzik magukat és a megelőzés feltételei ezen a szinten még nem adottak, ezért ilyenkor szoktak a legkomolyabb adatvesztések és vírusfertőzések bekövetkezni.

Megelőző

Ezen a szinten már folyamatközpontúan történik az informatikai rendszerek működtetése. A készültség túllép az „öncélú informatika” korlátain. Integrált hálózati alkalmazásról és rendszerfelügyeletről beszélhetünk, természetesen mindegyikhez speciális tudást és rendelkezésre állást biztosító „help-desk” szolgáltatással. A tudatosan átgondolt és megszervezett folyamatokkal párhuzamosan a rendszerek is konszolidálódnak, azaz működésük, működtetésük és kapcsolatrendszerük is letisztul. Az alapvető üzemeltetési folyamatokkal kapcsolatos feladatok specifikálásra kerülnek, és konkrét gazdákhoz, felelősökhöz (személyhez) kötődnek, például: problémakezelés, hibabejelentés, rendelkezésre állás, ügyelet, teljesítmény felügyelet, változáskezelés, konfigurációkezelés és menedzsment.

Definiálásra és beállításra kerülnek a végfelhasználói feladatok végrehajtásához szükséges szoftverek és azok funkciói. A folyamatok, feladatok és a funkciók ismeretében kialakításra kerülnek a hozzáférési szintek és kellőképpen árnyalt jogosultságok. A tevékenységek végrehajtása során fontos az elektronikus és a papíralapú dokumentációs rend kialakítása.

Ezek azok a pontok a rendszereinkben, ahol az ISO vagy a TQM elindítása már elképzelhető, és a rendszerek működése, működtetése szempontjából ezen a szinten már jól áttekinthető és ellenőrizhető.

Jól megfigyelhető, hogy az eddig tárgyalt szintektől eltérően a platform és alkalmazás centrikus tagozódást felváltja a folyamat és üzemeltetési centrikus elkülönülés.

Szolgáltató

Az Intézet többi egységével közös megállapodás alapján kerülnek definiálásra és monitorozásra az informatikai szolgáltatások. Itt már az egyes egységek jó teljesítése, gazdaságossága elképzelhetetlen a két fél együttműködését szerződéses alapokra helyező szolgáltatásszint-megállapodások SLA-k (SLA: Service Level Agreement = Szolgáltatásszint megállapodás) nélkül. Az SLA-kat nem csak az informatika és az informatikai szolgáltatásokat igénybe vevő felhasználók között érdemes megfogalmazni, fontos, hogy az IT beszállítók között is legyen ilyen megállapodás (internet szolgáltató, számítógép szerviz, telefontársaságok, informatikai outsourcing szerződések beszállítói stb.).

A szolgáltatásszint megállapodásokat minél részletesebben kell összeállítani és az adott szakterület munkamódszereit, munkarendjét és a munkavégzéssel kapcsolatos valós elvárásokat minden esetben figyelembe kell venni. A kórházi gyakorlatban különböző rendelkezésre állási elvárások merülnek fel, például a klinikai és gazdasági terület szerverei és munkaállomásai tekintetében. Olyan kórházi környezetben, ahol teljes, vagy igen nagy mértékű az informatikai függőség, indokolt a kritikus minősítésű eszközök és szoftverek listájának elkészítése. Ezen eszközöknél minél magasabb rendelkezésre állás biztosítása indokolt.

A „help-desk”-et felváltja a minden kritikus infrastruktúraterületre és -elemre kiterjedő „service desk”.

Értékteremtő

Ezen a szinten már nem az infrastruktúra felügyelet és fenntartás a cél, hanem az, hogy olyan informatikai infrastruktúrát üzemeltessünk, ami az intézet céljainak elérését biztosítja az előző szinteken kialakított folyamatok és azok hatékonyságának monitorozása kapcsán. Az üzleti és az informatikai mérőszámok összekapcsolásával az információtechnológia mindennapi működése üzleti alapon mérhető, kontrollálható.

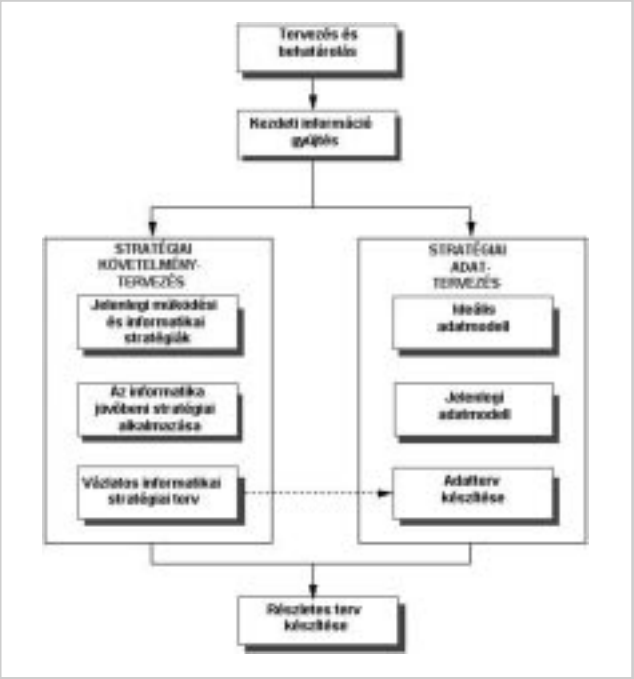
Mint minden másnak a kórházban az informatikai szolgáltatásoknak is ára van! El kell dönteni azt, hogy egy informatikai kiszolgáló pont szolgáltatásait hány személy milyen célból és milyen sűrűn veszi igénybe. Pontosan definiálni kell, hogy milyen feladatok elvégzésére kell alkalmasnak lennie a telepített eszköznek, milyen szoftverek és egyéb perifériák (pld: nyomtató, vonalkód olvasó, kártyaolvasó stb.) szükségesek a hatékony munkavégzéshez. Az intézet tevékenysége szempontjából kategorizálni (priorizálni) kell az adott munkahelyet. Az alkalmazások ismeretében biztosítani kell a munkavégzéssel kapcsolatos feladatokhoz szükséges adatátviteli szempontjából szükséges és elégséges hálózati sávszélességet.

Amennyiben a fenti adatok rendelkezésre állnak, pontosan megadható a kiszolgáló pont telepítésének és fenntartásának a költsége. Ezt a költséget kell szembeállítani az „értéktermelő” képességgel vagy a működési folyamatok szempontjából megállapított fontossággal.

Rendszeres időközönként felülvizsgálattal kell megállapítani, hogy a kiszolgáló pontnak változtak-e a funkciói, vagy van-e rá szükség, illetve azt, hogy indokolt-e a hardveres vagy a szoftveres bővítés.

AZ INFORMATIKA STRATÉGIA ÉS BIZTONSÁG TERVEZÉSE

A stratégia (hadviselés művészete) szót kezdetben kizárólag katonai területen értelmezték. A múlt század második felétől a gazdasági élet mindinkább élet-halál kérdésévé vált, ezzel együtt a stratégia szót a különböző intézmények és szervezetek működésére alkalmazzák. Abban az esetben beszélünk stratégiai döntésről, ha az hosszú távon határozza meg a sorsunkat abban a témában, amivel kapcsolatban a döntést meghozzuk. A stratégiai megközelítés nem csodaszer, hanem egy nélkülözhetetlen vezetési eszköz.



1. ábra
Az informatikai stratégiai tervezés folyamata (MTA alapján)

Az informatikai stratégia kialakításának lépései kapcsán az informatikai biztonság tervezését is ismertetni kívánom az alábbiakban:

Tervezés

Stratégia

A tervezési szakasz feladata a szervezeti szempontból érintett területek, témakörök behatárolása az elkészítendő dokumentumok és azok kapcsolatrendszerének megfogalmazása. Az ehhez kapcsolódó megvalósulási projektterv készítése (célok pontosítása, a projekt kapcsán érintett területek, személyek és informatikai feladatok felsorolása, felelősök, megvalósulási határidők, a megvalósulás során alkalmazandó technikák, dokumentációs rend, részletes tevékenységterv meghatározása stb.).

Biztonságpolitika

Meg kell határozni az informatikai rendszerhez kapcsolódó védendő értékek és a lehetséges fenyegetések körét, illetve a fenyegetettség elkerülése érdekében szükséges alapvető védelmi eszközöket (pl.: tűzfal).

Definiálni kell a biztonsági osztályokat és az osztályba sorolás lehetőségét és annak árnyalhatóságát.

Alapadatok gyűjtése

Stratégia

Az intézet azon szervezeti részeinek feltérképezése, melyekre a tervezés kiterjed. Az alábbi adatokról szoktunk információt gyűjteni szervezeti egységenként

- működési terület,
- funkciók és tevékenységek,
- létező és fejlesztés alatt álló informatikai rendszerek,
- rendszerek/tevékenységek/működési területek közötti kapcsolatrendszerek,
- kulcsemberek és szerepük,
- dokumentumok, stb.

Biztonságpolitika

Pontosan fel kell mérni a jelenlegi rendszerek veszélyeztetettségét és az eddig bekövetkezett adatvédelemmel kapcsolatos valós vészhelyzeteket.

Követelménytervezés

Stratégia

A projekt indulásakor az informatika használatának és az információtechnológia jelenlegi hasznosulásának elemzését feltétlenül meg kell vizsgálni a stratégiai tervkészítésbe bevont szervezeti egységen belül.

Biztonságpolitika

A kialakításra kerülő új pro-aktív (megelőzésre törekvő) informatikai biztonságpolitikának illeszkednie kell az intézmény teljes egészére kiterjedő informatikai biztonságpolitikához és filozófiához (ha van ilyen).

Az informatika jelenlegi felhasználásának elemzése

Stratégia

Ezen a felmérés kapcsán egyrészt a szervezetet vizsgáljuk. Megismerjük és értékeljük a működési területeket, a végzett tevékenységeket, a jelenleg érvényes működési stratégiákat, a működési területek fontosságát a szervezet számára. Másrészt vizsgáljuk a jelenlegi rendszerek szerepét és hatékonyságát, azt a módot, ahogyan a vezetés kezeli az informatikát. Összefoglaljuk, azokat a tevékenységeket, amelyekre érdemes informatikai támogatást biztosítani. A célok elérése érdekében megtörténnek az informatikai feladat kitűzések.

Biztonságpolitika

Vizsgálni kell, hogy a jelenlegi rendszerek informatikai biztonsági megoldásai milyen módon illeszkednek a tervezett rendszerbe.

Az informatika jövőbeli szerepének tervezése

Stratégia

A szervezet jelenlegi működési módjának, stratégiájának ismeretében a kritikus sikertényezőket és feltételezéseket egyeztetni kell a felső vezetéssel. Az átalakítandó területen elemzést kell végezni, hogy az információtechnológiát hol és hogyan lehetne használni úgy, hogy ebből a lehető legnagyobb haszon származzon. Meg kell határozni az információtechnológia költséghatékony alkalmazási módját a működési területre.

Megállapításra kerülnek a szervezeti célkitűzések a hatékonyság javítása érdekében, azok az elképzelések a jövőről, melyek mérhető és valós célokat fednek és azok az informatikai tevékenységek, melyek szükségesek a célok eléréséhez. Olyan tevékenységekre kell koncentrálnunk, melyek informatikával történő támogatásából a szervezet leginkább előnyt fog élvezni. A feladattól függően a célokat feladatkitűzésekké kell formálnunk, amely leggyakoribb formái: fejlesztési terv, megvalósíthatósági tanulmány, műszaki értékelés, technológia bevezetés, szervezeti változás stb.

Biztonságpolitika

Az informatikai biztonságpolitikának írásos formában pontosan meg kell fogalmaznia az informatikai biztonság megteremtéséhez szükséges vezetői elkötelezettséget, valamint a hazai és a nemzetközi biztonsággal kapcsolatos szabványoknak való megfelelőséget.

Kezdeti terv elkészítése

Stratégia

A feladatkitűzéseket rangsorolt projekttervé alakítjuk át, mely tartalmazza a felmerülő költségeket és ezek ütemezését, előnyöket, határidőket, felelősöket és fejlesztési erőforrásigényeket (humán, műszaki, eszköz stb.). Ezeket a projektspecifikációkat a projektmenedzsment szabályainak megfelelően önállóan működőképes és megvalósítható rész projektterveket állítjuk össze melyek, tartalmazzák a felmerülő költségek, előnyök, határidők és fejlesztési erőforrásigények részleteit. A projektterveken belül a projektspecifikációknál a megvalósítás szempontjából alapvető fázisokat (milestone) iktatunk be.

Biztonságpolitika

Meg kell határozni az informatikai rendszerek megvalósításának mikéntjét és a biztonsági rendszerek működésének, működtetésének általános kereteit. Olyan védelmi eljárásokat kell alkalmazni, amelyek garantálják, hogy az intézmény akkor is megőrzi alapműködését, ha egy szervezeti egységet katasztrófa ér. Ebből következik, hogy a terveket az intézeti informatikai mentési katasztrófa-elhárítási tervvel is össze kell hangolni.

Adattervezés

Stratégia

Az adattervezés a szervezet ideális adatmodelljének (Ideal Data Model – IDM) felállításával indul, melyet a jelenlegi

implementációkból adódó megszorítások figyelmen kívül hagyásával készíthetünk el. Az IDM a stratégiai tervben szereplő összes rendszer adatának kizárólag logikai leírását tartalmazza. Nincs benne redundancia és a fizikai megvalósítás megszorításaitól mentes. Elkészítése során különböző adatmodellezési technikákat lehet használni. Az adattervezési folyamat kapcsán megfelelő kompromisszumok árán elkészül a fizikai adatmodell. Törekedni kell arra, hogy az intézetben működő összes rendszer összes adata együtt kerüljön kezelésre, ne legyen benne redundancia, tartalmazza a szervezet meghatározó, generikus adategyedeinek a meghatározását.

Biztonságpolitika

Az adatokra vonatkozóan olyan védelmi eljárásokat kell kidolgozni, amelyek ellenőrizhetővé teszik a tranzakciókat, lehetővé teszik a naplózást és a visszakereshetőséget a például a HISA szabványban definiáltaknak megfelelően.

Részletes tervkészítés

Stratégia

A fejlesztési terv (kulcsdokumentum), amely tartalmazza mind a stratégiához, mind az informatikához kapcsolódó, rangsorba rendezett projektek leírásait is. A kritikus sikertényezők folyamatos ellenőrzésével a projekt megvalósítás ellenőrizhető.

Biztonságpolitika

Meg kell határozni az informatikai rendszerek megvalósításának mikéntjét. Rögzíteni kell, hogy kik, mely gépekről, mely protokollal jelentkezhetnek fel a belső és külső hálózatba. Kik és milyen külső gépekkel léphetnek kapcsolatba, és hogyan cserélhetnek adatot a külvilággal és a belső hálózatban lévő szerverekkel és munkaállomásokkal.

ÖSSZEFOGLALÁS

Egy-egy intézet informatikai érettségének egyik mutatója az, hogy milyen hardvereket és szoftvereket használ. Ám ennél sokkal árnyaltabb képet ad az, ha megnézzük, hogy a rendelkezésre álló technológiák miképp kerülnek felhasználásra.

A legtöbb informatikai beruházás esetében nem szoktak teljes körű, több évre előre szóló informatikai stratégiai tervet készíteni (vagy a meglévőt felülvizsgálni), inkább a konkrét informatikai feladat és projektmegvalósításra szoktak hangsúlyt fektetni. A stratégiai terv hiánya néhány év múlva a későbbi fejlesztés és bővítés esetén okoz problémát. Többek között ez is lehet az oka annak, hogy olyan döntések születnek, amelyek kapcsán az intézet „követő” vagy „megelőző” infrastruktúra felügyelettel rendelkező rendszere ismét „kaotikussá” válik.

IRODALOMJEGYZÉK

[1] Informatikai stratégiai tervezés a gyakorlatban (MTA Információtechnológiai Alapítvány),
[2] Az informatikai stratégia kialakításának és megvalósításának irányelvei (MTA Információtechnológiai Alapítvány)
[3] Miniszterelnöki Hivatal Informatikai Koordinációs Iroda. 8. sz. ajánlás
[4] Learmonth & Burchett Management Systems: LBMS Strategic Planning for Information Technology
[5] Kürt Computer Rendszerház Rt: Informatikai biztonsági rendszerek kialakítása Magyarországon
[6] Bartók Nagy János: Informatikai érettség és felügyeleti technológiák.
IT-Busines I. évfolyam, 19. 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 a Gottsegen György 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.