Gondolatok az információbiztonságról

Olvasói levél

Az IME utóbbi számaiban az informatika alkalmazásából fakadó biztonsági kockázatokkal, illetve az azok kezelésével foglalkozó témakörről több szerző, értékes gondolatokat tartalmazó publikációja is megjelent. A 2003/8-as számban a szerkesztőség felhívást tett közzé, amelyben észrevételekre, megjegyzésekre, nyilvános vitára invitálta az olvasókat és az érintetteket. E felhívás apropóján fejtenék ki röviden, két gondolatot.

TERMINOLÓGIAI ÉS MEGKÖZELÍTÉSI KÉRDÉSEK

Az egyik, a terminológiában tapasztalható, – akár bábelinek is nevezhető – zűrzavarral foglalkozik. Ez a kérdés érinti mind a téma megnevezésének, mind a problémák megfogalmazásának, mind pedig a megoldás egyes eszközeinek fogalomkészletét és azok jelentéseit, összefüggéseit.

Ha fellapozzuk akár az IME korábbi számait, akár más, hasonló tárgyú publikációkat, akkor a tárgykör azonosítására az alábbi fogalmakat találjuk – meghatározással vagy anélkül:

- adatbiztonság
- adatvédelem
- információbiztonság
- információvédelem

A megjelent publikációk egy része e fogalmakat nagyjából szinonimaként használja, míg mások különböző jelentéstartalmat tulajdonítanak nekik. Az utóbbira példa az adatbiztonság és adatvédelem fogalmára adott egyik definíció, amely szerint az adatvédelem az információ elvesztése (megsemmisülése) elleni, míg az adatbiztonság az információ illetéktelen kézbe kerülése elleni védekezés. Megjegyzendő ugyanakkor, hogy az adatvédelem fogalom mára a köznyelvben igen erősen kapcsolódik a személyes adatok védelméhez (lásd: „adatvédelmi törvény”) és az információs önrendelkezési joghoz.

A szakmai publikációkban és egyes szakértő-tanácsadó cégek kereskedelmi célú anyagaiban a fenti fogalmak egy másik tipikus definíciója szerint az adat- vagy információbiztonság jelenti magát az elérni kívánt állapotot (tehát, hogy az információk biztonságban vannak), míg az adat- vagy információvédelem jelenti az e cél elérése érdekében megtett óvintézkedések összességét. További értelmezések szerint az informatikai biztonság az informatikai rendszerekkel szorosabban összefüggő biztonsági kérdéseket jelenti, míg az információbiztonság ennél tágabb fogalom; az információnak a „teljes”, azaz az informatikai rendszereken kívüli biztonságát is magában foglalja.

Hasonló jelenség figyelhető meg a terminológia egy másik részterületén is. Egyes szabványok, szakmai irányzatok az alapfenyegetések három típusát különböztetik meg (bizalmasság, sértetlenség, rendelkezésre állás), mások ezeken felül külön is azonosítanak továbbiakat (tipikusan: hitelesség, funkcionalitás). A terminológia egységének hiánya tapasztalható a megoldási módszerek egyes elemeit illetően is: többek között a stratégia, politika, szabályzat, eljárás, kontrol, audit fogalmak számos értelemben és jelentéstartalommal használatosak.

A nem egységes és sokszor egymásnak is ellentmondó terminológia leginkább a felhasználó szervezeteknek, jelen esetben tehát az egészségügyi intézményeknek okoz gondot, hiszen egyrészt nem tudják világosan értelmezni a külvilágból e tárgykörben hozzájuk érkező üzeneteket – legyen az egy szakcikk, egy üzleti ajánlat vagy egy szabvány –, másrészt a külvilág – auditor, felügyeletei szerv, leendő befektető – sem képes kellő megbízhatósággal értelmezni a szervezet által kibocsátott dokumentumokat.

Az előzőekben bemutatott terminológiai problémák több okra vezethetők vissza. Az egyik fő ok az, hogy még a nemzetközi terminológia sem teljesen egységes, ráadásul így a már ab ovo létező eltéréseket tovább nagyítják a fordítási anomáliák.

A másik fő okot abban látom, hogy az információbiztonsággal foglalkozók (az egyes személyek éppúgy, mint a szakmai, illetve a profitorientált szervezetek) különböző szakmai előélettel, az azokból következő különböző nézőpontokból, illetve értelmezési szinteken fogalmaznak és értelmeznek.

Az egyik jellemző, bottom-up megközelítésnek tekinthető nézőpont az egyes informatikai eszközök, rendszerek biztonságából indul ki, ebből vezeti „fel” a biztonságot a struktúra magasabb szintjeire, a folyamatokra. Ebből a nézőpontból az információbiztonság kulcskérdése általában az informatikai eszköz (rendszer, szerver stb.) biztonsága, módszerei általában részletesen kidolgozottak az eszközök, esetleg a rendszerek biztonságának megteremtésére, ugyanakkor a biztonság szervezeti, szabályozási, adminisztratív, üzemeltetési és egyéb kérdéseit általában nagy-

vonalúan az adott eszköz működési környezetével szemben támasztott biztonsági követelménynek tekintik, anélkül, hogy annak részletes értelmezését megadnák. Ezáltal gyakorlatilag trivialitásként kezelik e kérdéseket.

A másik, top-down megközelítésnek tekinthető nézőpont a szervezet információs alrendszerével szemben támasztott biztonsági követelményekből indul ki, az információbiztonságért viselt felelősséget a szervezeti hierarchia magas szintjére helyezi és az információbiztonság – mint önálló szervezeti cél elérése – érdekében a releváns folyamatokat szabályozó irányítási rendszer létrehozásában és működtetésében látja a megoldást.

Természetesen e két megközelítés a gyakorlatban általában keveredik, de legtöbbször érzékelhető, hogy tendencia szintjén egy adott esetben melyik érvényesül. Talán jó példa erre az alapfenyegetések megfogalmazása: míg a top-down megközelítésben a rendelkezésre állás alatt az informatikai rendszer által az üzleti folyamat számára nyújtott funkciónak, az elvárt helyen, időben és módon történő szolgáltatását értjük, addig a bottom-up megközelítésben ez kettéválik: a rendelkezésre állás általában az eszköz elérhetőségét jelenti, és önálló fogalomként jelenik meg a funkcionalitás vagy működőképesség. További példaként említhető, hogy a bottom-up megközelítés a hangsúlyt azokra a tevékenységekre helyezi, amelyek szorosabban kötődnek az informatikai rendszerek üzemeltetési feladataihoz (hálózatokkal kapcsolatos biztonsági kérdések, vírusvédelem, tűzfal stb.). Ezzel szemben a top-down megközelítés elsősorban a folyamatok szabályozatlan működését tekinti a fő kockázati tényezőnek; beleértve az informatikai üzemeltetési tevékenységeket csakúgy, mint az ahhoz szorosan nem kötődő, de az információbiztonság szempontjából lényeges területeket is. (Ilyenek például az intézmény területére, egyes épületekbe, helyiségekbe való bejutás lehetősége és annak szabályozása, vagy a munkavégzésre irányuló jogviszony bármilyen okból való megszűnése esetén alkalmazandó eljárás a hozzáférési jogosultságok azonnali visszavonásáról.)

A sort még hosszasan lehetne folytatni a két megközelítés szemléletmódjának jellemző tulajdonságairól, ehelyett inkább térjünk át másik témánkra: az eddigiekben bemutatott két megközelítésnek – megítélésem szerint – van egy közös problémája: a scope kérdése, vagyis hogy mit is szabályozzunk, ha a cél az információbiztonság szabályozottsága.

MIT SZABÁLYOZZUNK?

A bevezetőben említett másik érintett terület a „Mit szabályozzunk?” kérdése, vagyis annak boncolgatása, hogy mennyire választható el az információbiztonság szabályozása a szervezet (az egészségügyi intézmény) információs rendszerét illető egyéb szabályozásától.

Amint azt néhány előző példán már láthattuk, az információbiztonság kérdései csak részben kapcsolódnak szorosan az informatikai rendszerek üzemeltetésének tevékenységeihez, az üzemletetés felelősségi körébe tartozó eszközökhöz. Az információbiztonság kihívásai és az azokra adott válaszok ugyanis nem önállóan, a „levegőben lógva” léteznek, hanem egyrészt át- és átszövik az informatikát alkalmazó folyamatokat, másrészt e folyamatokban más, nem biztonsági jellegű követelményekkel (pl. eredményesség, hatékonyság stb.) együtt, sokszor azokkal konfrontálódva szerepelnek.

Az információbiztonság megteremtésének és fenntartásának további szükséges feltétele tehát, hogy speciális szempontjai beépüljenek azokba a folyamatokba, amelyek alapvetően nem információbiztonsági, (sőt, egyes esetekben nem is kifejezetten informatikai) jellegű cél elérése érdekében működnek. Ebből pedig az következik, hogy az információbiztonság megteremtése és fenntartása sem képzelhető el anélkül, hogy a biztonság szempontjait és követelményeit a többi szemponttal és követelménnyel egységesen kezeljük: egyszerre lássuk az adott folyamat, tevékenység szervezeti célját és a releváns peremfeltételeket (pl. biztonság, jogszabályoknak való megfelelőség).

E feladatot viszont csak akkor tudjuk megoldani, ha az információbiztonság megteremtését célzó kontrollrendszer és szabályzatok kialakítása során olyan megoldásra törekszünk, amelyik képes az érintett folyamatokat egységesen szabályozni.

Mit szabályozzunk tehát? Az intézmény információs alrendszerét érintő folyamatok egészét, figyelemmel azok elsődleges céljára és a peremfeltételként megjelenő – például biztonsági – követelményekre. Fontosnak tartom megjegyezni, hogy a kockázatelemzés önmagában nem oldja meg ezt a problémát, hiszen az leginkább arra ad választ, hogy mennyit érdemes költeni egy adott veszélyforrás elhárítására (kockázatarányosság), illetve hogy adott óvintézkedés becsült költsége arányban áll-e a kockázattal. Ha ezek az információk nem párosulnak olyan nézőponttal, ami a kontrollok meghatározásánál, a szabályok kidolgozásánál is folyamatosan érzékelni képes a kiválasztott óvintézkedésnek a nem biztonsági követelmények teljesülésére gyakorolt hatását, akkor jó eséllyel várható, hogy a figyelembe nem vett szempontok a mindennapi gyakorlat során erősebbnek bizonyulnak.

Mindezekből következően az információbiztonság megteremtésének kiemelt és kritikus sikertényezőjének tartom az egészségügyi intézmények esetében is, hogy az információs alrendszer egészére, az azzal szemben támasztott minden releváns követelményre kiterjedő egységes szabályozási rendszer jöjjön létre, amelyik nem csak egyszerűen illeszkedik a szervezet egészének szabályozási rendszerébe, de annak felső szintjéből egyenesen következik.

Róth Dénes