

Biztonság

Az elmúlt évtizedekben bekövetkezett egyik legszokatlanabb gazdasági-társadalmi változás az, hogy egyrészt a legkülönbözőbb szervezetek működésében – mind üzleti, mind közszolgálati területen –, másrészt az egyének szintjén is eddig nem látott mértékben megnövekedett a *függés az információtól* és különösen az azt kezelő informatikai rendszerektől. Nem meglepő ezért, hogy előtérbe került az információ-biztonság, amelynek célja – a szervezetek információellátásában zavarokra vezető *gyenge pontok és veszélyek* meghatározása mellett – olyan *védintézkedések* meghozatala és megvalósítása, amelyek a fellépő kockázatok kezelésével és egyéb követelmények teljesítésével az *információellátás folyamatos működését* biztosítják összhangban a szervezet általános biztonsági és működési céljaival. De nem lehet meglepő az sem, hogy az egyéneknél a *magánélet* (privacy) védelme fokozott jelentőséget kap a megnövekedett veszélyek miatt.

A biztonság témakör két, az IKT-k iránti bizalom megeremtését szolgáló területet fog össze. Az egyik az *információbiztonság*, a másik pedig a *magánélet-védelem*. Ez utóbbi terület európai viszonyok között leginkább a személyes adatok védelmének kérdéseként értelmezhető a gyakorlatban. Az információbiztonság a szervezeti értelemben vett biztonság megeremtésének eszköze, míg a *személyesadat-védelem* a felhasználóknak és az ügyfeleknek az egyre növekvő kiszolgáltatottsággal szembeni biztonságérzetének megőrzését elősegítő eszköz.

Az információbiztonság egyik meghatározó pillére az *informatikabiztonság*, amely alatt az informatikai rendszerek és eszközök (szoftver, hardver vagy ezek együttese) elvárt működését (biztonságos működését) akadályozó vagy veszélyeztető kockázatok (cselekmények, külső hatások vagy ezek következményeként előálló állapotok) elleni *védetség* értendő. Az informatikabiztonság (biztonságos működés) – definíció szerint – csak a konkrét használati cél alapján *egyedileg meghatározható minőség*, ami ugyanakkor azonban nem zárja ki a tipizálás lehetőségét. Az „informatikai rendszer és termék” kifejezés az üzemeltetést és használatot is átfogó széles értelemben használatos, ahol az informatikai rendszerekbe az internetes alkalmazások és szolgáltatások növekvő szerepére való tekintettel beleértendők az adatátviteli-távközlési hálózatok is. Nem tekintendő ugyanakkor – szűkebb értelemben – az informatikabiztonsági kérdések közé tartozónak azon fejlesztéshez és üzemeltetéshez kapcsolódó minőségbiztosítási kérdések, amelyek ugyan hatással vannak az informatikai termékek és rendszerek biztonságára, de biztonsági kockázatok hiányában nem okoznak problémát.

Az információbiztonság és a személyes adatok védelme az IKT világában szorosan összekapcsolódik. A két terület egyszerre van *egymást kiegészítő és egymásnak ellentmondó* viszonyban. A kiegészítő viszony annak köszönhető, hogy a személyes adatok kezelése során az adatok védelme információbiztonsági megoldások nélkül elképzelhetetlen. A kezelt személyes adatok védelmének nézőpontjából az információbiztonság egyike azon kérdéseknek, amelyek megfelelő kezelése *elengedhetetlen tényező* a személyes adatok védelmében.

A magánélet védelmének azon aspektusa azonban, amely a személyes adatok kezeléséhez való jogosultság megszerzéséhez kapcsolódik már ellentmondásokhoz vezet a két terület között. Az információbiztonság megeremtésében ugyanis rendkívül fontos szerepet

játszik a felhasználók megfelelő azonosítása, valamint a felhasználókról történő kiterjedt adatgyűjtés az egyes biztonsági eseményekért való felelősségnek a későbbi megállapíthatósága érdekében. Az információbiztonság megteremtésének nézőpontjából ezért a személyes adatok védelme az információbiztonság megteremtését *akadályozó tényező*ként is jelentkezik a gyakorlatban.

1. A biztonság területének főbb változásai

A biztonság területén várható átfogó, legfontosabb tendenciák a következők:

- a kockázatok növekedése,
- a proaktív kockázatkezelés előtérbe kerülése,
- a polgári célú kriptográfia szerepének erősödése,
- az információbiztonság és az adatvédelem között feszülő ellentmondás csökkenése.

Az IKT használati körének kiterjedésével egyidejűleg folyamatosan nőttek a *biztonsági kockázatok* az információbiztonság és magánélet-védelem területén is. Ez az elkövetkező évtizednek is általános trendjeként fog megmaradni.

Az IKT használatát érintő biztonsági kockázatok kezelése az elmúlt időszakban elsősorban *reaktív* volt. Az ok, hogy a biztonsági szempontokat – a legtöbb esetben – a *fejlesztés fázisában* nem érvényesítik. Az információbiztonsági és adatvédelmi kockázatok ezért növekednek automatikusan az IKT-eszközök intenzívebb használata következtében. A biztonsági szempontok érvényesítésének elmaradása a fejlesztés fázisában azt eredményezi, hogy a biztonsági kockázatok csak utólagos, reaktív eszközökkel kezelhetők. Ennek a helyzetnek elsődlegesen az az oka, hogy a biztonságos IKT előállítására hosszabb időt igényel és többletköltségekkel jár, amit a piac rövidtávon nem nagyon honorál. Emellett azonban fontos szerepet játszik az a tény is, hogy a kellő biztonsági szintet garantálni tudó *termék- és rendszerfejlesztési módszertanok* nem voltak eddig használatban.

A következő évtizedben nagy előrelépés várható ezen a területen. A biztonsági kockázatok csökkentését és kezelését szolgáló technológiák, értékelő és auditmódszertanok, gyakorlatok, valamint szabályozási eljárások gyakorlati alkalmazásának általánossá válása a következő évtizedben elkerülhetetlenül be fog következni. Ennek eredményeként a biztonsági kockázatok kezelésében a hangsúly a reaktív megoldásokról a *proaktív megoldások irányába* tolódik el.

Ezt erősíti az is, hogy – ha egy évtizednyi vajúdas után is, de – 2005 végén megegyezés született az az információbiztonság-menedzsment (Information Security Management, ISM) nemzetközi szabványában (ISO/IEC 27001). Nemzetközi szinten is egyértelművé vált, hogy az információbiztonság legmagasabb, menedzsment szintjén milyen követelményekkel kell szembe nézniük azon szervezeteknek, amelyek ISM-rendszereik kiválóságára törekednek, és ezen belül a proaktivitást helyezik előtérbe. Jól alátámasztja ezt a várakozást az is, hogy ennek a proaktivitásnak és a fejlesztésre – sőt a termékek, rendszerek és szolgáltatások *teljes életciklusára* – kiterjedő *biztonságtudatosságnak* a jegyében született meg az IT-szolgáltatásmenedzsment nemzetközi szabványának (ISO/IEC 20000) követelményrendszere, majd 2007-ben az ITIL v3 ajánlásgyűjteménye is.

A *kriptográfiai technológiák* a bizalmasság, az azonosítás és hitelesítés megvalósításának legfontosabb eszközei, és ebből adódóan kiemelt szerepet játszanak az

információbiztonság és a magánélet-védelem területén is. Az információbiztonság és az adatvédelem számára is nélkülözhetetlenek ezért a polgári célú kriptográfiai technológiák, amelyeknek a folyamatos felértékelődése várható. Emellett a hitelesítés céljára használt kriptográfiai megoldásoknak a bővülő számítási kapacitások és a javuló teljesítmény miatti avulása azt eredményezi, hogy a kizárólag kriptográfiaiak mellett előtérbe kerülnek a *hitelességmegőrzési eljárások és szolgáltatások*.

A jelenleg használt kriptográfiai megoldások avulásának ütemében nem várható nagy változás, bár matematikai felfedezések bármikor eredményezhetik az éppen használt kriptográfiai eszközpark lecserélését. Ha azonban a technológiai fejlődés oldaláról nézzük a kérdést, akkor nem várható az avulás ütemének felgyorsulása. Például a *kvantumszámítástechnika* megjelenése a *nyilvános kulcsú kriptográfián* alapuló biztonsági és hitelesítési megoldásokat elavulttá teheti, ugyanakkor gyakorlatban használható kvantumszámítógépek megjelenése a következő évtizedben még nem várható.

Az IKT világában az elmúlt húsz évben az információbiztonság és az adatvédelem ellentmondásos viszonya jellemezte a biztonság átfogó területét. A jelenlegi ellentmondásos helyzet várhatóan a következő évtizedben is fennmarad, azonban az ellentmondások kiélezettsége csökkenni fog. Ennek a háttérben az áll, hogy a biztonsági kockázatok kezelésében a reaktív megoldások szerepe háttérbe szorul, ezáltal pedig csökken az információbiztonság területén a *személyes adatok gyűjtése és hosszú idejű tárolása* iránti igény.

Várható továbbá, hogy a következő évtizedben az informatika szolgáltatása és védelme *még szorosabban egymásba fonódik*, és szabványos, ugyanakkor (a biztonságra is) különböző garanciaszinteket biztosítani tudó *információszoftvertámasztás* alakul át.

2. Információbiztonság

2.1 Kockázatok

Az információbiztonsági kockázatok könnyen számszerűsíthetők, mivel az információ, egy-egy dokumentum illetéktelenek kezébe vagy nyilvánosságra kerüléséből, továbbá informatikai rendszerek rosszindulatú támadások eredményeként előálló időleges vagy végleges *működésképtelenségéből* potenciálisan származó kár mértéke elég jól meghatározható.

Az információbiztonsági kockázatok változása ezért szorosan összefügg az informatikai eszközök és rendszerek *üzleti értékével*, sőt megállapítható, hogy az IKT üzleti folyamatokban betöltött szerepének növekedésével együtt nőnek az információbiztonsági kockázatok. Tekintettel arra, hogy az üzleti folyamatok IKT-függősége folyamatosan nőni fog a következő évtizedben, az információbiztonsági kockázatok tartós növekedésére lehet számítani.

Az információbiztonsági kockázatok jövőbeli alakulása azonban a technológiai változások mellett a *potenciális támadók* körének jövőbeli alakulásától is függ. Az informatika korai időszakát jellemző individuális elkövetők helyébe az elmúlt időszakban egyre inkább a professzionális, jól szervezett, elkövetői csoportok léptek. Ez a folyamat várhatóan tovább fog erősödni.

2.2 Információbiztonsági technológiák

Az információbiztonsági technológiák köre igen széles. Ide sorolhatók mindazok a hardver- és szoftvereszközök, amelyek az információbiztonsági kockázatok csökkentését segítik. Egyes *reaktív információbiztonsági eszközök* (például vírusirtó, tűzfal) használata mára már általánossá vált. Az azonosítási megoldások is sokat fejlődtek az elmúlt évtizedben. Ennek a területnek a következő évtizedben tapasztalható nagy változása lesz, hogy az egyfázisú azonosítást fokozatosan és általánosan kiváltják a *kétfázisú azonosítási megoldások*.

A biztonsági kockázatok elleni proaktív védekezés előtérbe kerülése a technológiák szintjén elsősorban a szoftverfejlesztés átalakulásában ragadható meg. Ennek a változásnak egyik legfontosabb eredménye az lesz, hogy a következő évtized második felére általánossá válik az információbiztonsági szempontok figyelembe vétele a *termékek és rendszerek tervezése* során is. Néhány jellemző példája ennek a folyamatnak a Microsoft Trustable Computing Platform-jának megjelenése, valamint az olyan tervezési módszerek, specifikációk kialakulása és használatának általánossá válása, mint a USA CERT Survivable Systems Engineering kutatásainak eredményeként előálló módszertanok, a Trustable Computing Group biztonsági specifikációi, valamint az internetprotokolljainak biztonsági igényeket is figyelembe vevő változatának gyakorlati elterjedése (IPv6-ra történő átállás).

Az egysíkú, csupán néhány fenyegetettségre koncentráló megelőző típusú védekezést felváltja a többszintű, *átfogó behatolást megelőző* rendszerek használata.

2.3 Üzemeltetés

Az információbiztonság fenntartásában kiemelkedő és meghatározó szerepe van az IT-üzemeltetés során végzendő *megfigyelési és mérési tevékenységnek*. A paradox helyzetet az adja, hogy ezek megfelelő szinten történő végrehajtására csak akkor van esély, ha az IT-rendszerekbe eleve bele lettek tervezve az ehhez szükséges megfigyelési és mérőpontok a fejlesztés során, valamint ki lettek alakítva, és be lettek vezetve a szükséges eszközök. Erre épülhet rá aztán egy olyan *eseménymenedzsment* tevékenység, amely a megfigyelési információkat összevetve és értékelve – a lehetőség szerinti legnagyobb mértékben automatizálva – kellő időben való reagálást tesz lehetővé a várhatóan bekövetkező, kisebb-nagyobb üzemzavarok különböző szintű kezeléséhez (*incidens-, probléma és folytonosságmenedzsment*).

Az üzemeltetés során biztonsági szempontból kiemelt szerepet kap a *hozzáférésellenőrzés* a személyazonosság ellenőrzésében és a jogosultságok kiosztásában. Komplexitása miatt (sok rendszer, sok felhasználó, összetett jogosultsági viszonyok, áttekinthetőség igénye) ma már jellemzően specifikus szoftvereszközöket használnak erre a célra. Végül az információbiztonsággal kapcsolatos fenti tevékenységek alapját szerteágazó, *napi szintű feladatok végrehajtása* képezi az *adatmentésektől* a *különböző rendszer- és adatbázisadminisztrációs munkákig*.

Az ezen tevékenységekhez és eszközökhöz szükséges, egyre specifikusabb IKT-szaktudás és -kapacitás miatt a kis- és közepes méretű vállalkozások körében fokozatosan általánossá válik a *biztonságrendszer-felügyelet* külső szolgáltatáson keresztül történő biztosítása. A nagyobb vállalatoknál a belső IT-szervezetnek kell végeznie vagy legalábbis koordinálnia az üzemeltetést, amelynek megvalósításánál a következő évtizedben még feltétlenül meghatározó szerepe lesz az ITIL vonatkozó ajánlásainak. Emellett azonban itt is egyre növekvő mértékben vannak be külső szolgáltatókat, ami az

évtized második felében már jellemzően *közműszerű IT-szolgáltatás formájában* valósul meg.

2.4 Információbiztonsági értékelés és tanúsítás

A különböző értékelési és tanúsítási megközelítések egyre fontosabb szerepet játszanak az IKT biztonsága és megbízhatósága tekintetében, amelyeket részben *állami szabályozás* ír elő, részben bizonyos gazdasági szektorok, területek *ön szabályozása* révén válik kötelező előírássá. Ilyen a NATO-beszállítók előzetes értékelése és tanúsítása, a pénzügyi szektort érintő követelmények megjelenése (Basel II), vagy a New York-i tőzsde cégeire vonatkozó Sarbanes-Oxley törvény (2002).

További konszolidáció várható a jelenleg versengő biztonsági szabványok és tanúsítási rendszerek között (ISO/IEC 27001, a COBIT és az ISO/IEC 15408 – Common Criteria), és egyre inkább a piacon maradás feltétele lesz a megfelelő tanúsítvány megléte. E megközelítések közös jellemzője, hogy *komplex átfogó megoldásokat* kínálnak az információbiztonsági problémák kezelésére. Fontos azonban azt is látni, hogy az egyes megközelítések esetében a hangsúlyok eltérnek. Így például a Common Criteria az IKT-rendszerek és -eszközök *biztonsági értékelésére* használatos, az ISO/IEC 27001 elsősorban az *információbiztonság menedzsmentfolyamatainak* megítélésére, a COBIT-ot pedig a felelős, számonkérhető és *átlátható IT-irányítás* vizsgálatánál alkalmazzák. Várható, hogy ez a *munkamegosztás tovább erősödik*, ugyanakkor az egyes elemek jobban fognak egymáshoz illeszkedni. A jelenleginél is határozottabban elválnak a menedzsmentjellegű, a rendszer- és eszközszintű biztonsági szabványok, és az ezekre épülő értékelési és tanúsítási rendszerek, valamint az egyes szinteken történő értékelést és tanúsítást támogató technológiák. Ezzel párhuzamosan általánossá válik a biztonsági követelményeknek való megfelelést vizsgáló és ellenőrző, a biztonsági előírások kikényszerítését támogató *IT-alkalmazások használata*.

3. Magánélet, személyes adatok védelme

3.1 Adatvédelmi kockázatok

A személyes adatok kiterjedt használatában rejlő kockázatok – az információbiztonsági kockázatokkal ellentétben – nehezen fejezhető ki pénzügyi vagy más könnyen mérhető mutatókkal. Az adatvédelmi kockázat ugyanis az *egyének kiszolgáltatottságának mértékében* ragadható meg. A kiszolgáltatottság azonban nagyon relatív érték: kultúránként, életkoronként, de akár élethelyzetenként is eltérő lehet, hogy mikor érzi valaki magát kiszolgáltatottnak. Ettől a szubjektív megítélésből adódó bizonytalanságtól eltekintve kijelenthető, hogy: *minél több egyénre vonatkozó adat* érhető el mások számára, annál inkább növekszik a kiszolgáltatottság kockázata, és ez független attól, hogy hol található az a pont, amit valaki esetleg konkrétan problémásnak talál.

A számítási, adattárolási és adatátviteli kapacitások bővülését eredményező új technológiák megjelenése általánosságban növeli az adatvédelmi kockázatok szintjét. Az IKT-eszközök és -szolgáltatások használatának növekedésével egyidejűleg nő az ezen eszközök által gyűjtött és kezelt adatok mennyisége. Különösen a *személyazonosítást* is lehetővé tevő technológiák (például RFID, mobiltelefon-, internethasználat) megjelenése, elterjedése és általánossá válása járult hozzá eddig a kezelt *személyes adatok mennyiségének* – és ezáltal az adatvédelmi kockázatoknak – a növekedéséhez. Az elmúlt évtizedben az adatvédelmi kockázatok növekedéséhez leginkább a *federált (azaz*

kombinált) személyazonosság-kezelési rendszerek megjelenése és elterjedése, valamint a közösségi oldalak használatának növekedése járult hozzá.

A következő évtizedben az adatvédelmi kockázatok növekedésének – a kezelt adatok mennyiségnek növekedése mellett – egy másik fontos oka lesz a *fejlett adatbányászati eszközök* megjelenése és használatuk elterjedése. Ezen belül különösen a *kép- és mozgókép-elemzési technológiák* megjelenése és elterjedése hoz be új dimenziókat, és növeli látványosan e kockázatokat.

3.2 Adatvédelmi technológiák

Adatvédelmi technológiák közé azok a technológiák sorolhatók, amelyek lehetővé teszik vagy elősegítik az adatvédelmi kockázatok csökkentését. Ezeket a technológiákat szokás *magánszféra-erősítő technológiáknak* (Privacy Enhancing Technologies, PET) nevezni. A PET-ek jelentősége növekvőben van. A következő évtizedben elsősorban nem újabb megoldások kifejlesztése várható, hanem a PET-ek *integrálása a személyazonosság-kezelésbe*, továbbá komoly törekvések várhatók, e technológiák *szabványos réteggént* való beépítésére az informatikai alkalmazásokba, például a federált személyazonosság-kezelésbe.

A szűk értelemben vett technológiai oldal mellett az adatvédelem megteremtésében fontos szerepe lehet az adatvédelmi kockázatok csökkentésében az adatvédelmi szempontokat figyelembe vevő *adatgyűjtési és -kezelési üzletviteli gyakorlat* megjelenésének és elterjedésének. Ezt a folyamatot jelentősen segítheti az adatvédelmi előírások megfelelő *szankciórendszerének* kialakulása.

3.3 Adatvédelmi átvilágítás és audit

Az adatvédelmi elvárásoknak való megfelelés előzetes vizsgálatának és utólagos ellenőrzésének eredményességét növeli az adatvédelmi átvilágítás és az adatvédelmi audit. Hasonlóan az információbiztonsági értékeléshez és tanúsításhoz, az adatvédelmi auditot megkövetelő előírások megjelenése, *adatvédelmi auditszabványok* és *szabványos gyakorlatok* alkalmazásának elterjedése prognosztizálható.