



4 ÁTFOGÓ TÉMAKÖRÖK

4.1 BIZTONSÁG

INFORMATIKA-BIZTONSÁG 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 védettséget értjük. Az informatika biztonság (biztonságos működés) – definíciónk szerint – csak a használati cél alapján egyedileg meghatározható minőség, ami ugyanakkor nem zárja ki a tipizálás lehetőségét. Az „informatikai rendszer és termék” kifejezést az üzemeltetést és használatot is átfogó széles értelemben használjuk, az informatikai rendszerekbe a várható fejlődésre tekintettel beleértjük az adatátviteli-távközlési hálózatokat is. Nem tekintjük a biztonsági kérdések közé tartozónak azon fejlesztéshez és üzemeltetéshez kapcsolódó minőségbiztosítási kérdéseket, amelyek ugyan hatással vannak az informatikai termékek és rendszerek biztonságára, de biztonsági kockázatok hiányában nem okoznak problémát.⁷

A biztonság mellett a két kérdéskör szoros összefüggésére tekintettel e témakör keretében kerül sor az INFORMÁCIÓS ÖNRENDELKEZÉST támogató ADATVÉDELMI technológiák fejlődésének, valamint az INFORMATIKA-BIZTONSÁGI és ADATVÉDELMI TECHNOLÓGIÁK számára is nélkülözhetetlen polgári célú kriptográfiai technológiák fejlődésének bemutatására.

A 2007-2013-as időszak általános trendje a biztonsági és ADATVÉDELMI kockázatok növekedése, valamint ezen kockázatok csökkentését és kezelését szolgáló technológiák, értékelő és audit módszertanok, gyakorlatok, valamint szabályozási elvárások (követelmények) megjelenése és általánossá válása.

⁷ Saját biztonság meghatározásunk kialakításának oka az volt, hogy az elemzés céljait leginkább szolgáló biztonság fogalom használata révén elkerülhessük a versengő biztonság koncepciók közti kényeszerű választás terhét.



Részterületek fejlődése

4.1.1 Informatika-biztonsági technológiák

A biztonsági kockázatok elleni utólagos védekezéstről a hangsúly az informatikai rendszerek és termékek vonatkozásában eltolódik a megelőzés irányába. 2015-ig a biztonsági megoldások fokozatosan beépülnek az informatikai rendszerekbe és termékekbe, valamint a szervezeti folyamatok részévé válnak. Ennek a folyamatnak egyik legfontosabb eredménye az lesz, hogy a biztonsági elvárások és szempontok figyelembe vétele 2015-re általánossá válik termékek és rendszerek tervezése során is. Néhány jellemző példája ennek a folyamatnak a Microsoft Trustable Computing Platform-jának megjelenése, valamint az olyan – ma még intenzív kutatás tárgyát képező – tervezési módszerek, specifikációk kialakulása és használatának általánossá válása, mint a USA CERT (Computer Emergency Response Team) Survivable Systems Engineering kutatásainak eredményeként előálló módszertanok, a Trustable Computing Group biztonsági specifikációi, valamint az Internet protokolljainak biztonsági igényeket is figyelembe vevő átalakítása.

2008-ra a hálózat biztonsági fenyegetettségek csökkentése érdekében alkalmazott tűzfalak, vírus- és spyware védelem használata általánossá válik mind a szerverek mind a desktopok szintjén. Ezzel párhuzamosan 2010-re az egysíkú, néhány fenyegetettségre koncentrálnó megelőző típusú védekezést felváltja a többszintű, átfogó behatolást megelőző rendszerek használata.

Rendszerek tekintetében az egyre specifikusabb szaktudás és kapacitás iránti igény miatt a kis és közepes méretű vállalkozások körében 2015-ig fokozatosan általánossá válik a felderítést célzó biztonsági rendszer felügyeletnek külső szolgáltatások igénybevételén keresztül történő biztosítása.

4.1.2 Biztonsági értékelés és tanúsítás

A különböző értékelési és tanúsítási rezsimek (pl.: BS 7799, COBIT, Common Criteria) egyre fontosabb szerepet játszanak az IKT-k biztonsága és megbízhatósága tekintetében. 2015-re az informatikai termékek és rendszerek biztonsági értékelésének és tanúsításának megkövetelése egyes területeken általánossá válik. Az értékelés és tanúsítás részben állami szabályozói előírások, részben egyéb globális szolgáltatási rendszerek önszabályozása révén válik kötelező előírássá. Ennek a változásnak az előfutárai a NATO beszállítók előzetes értékelése



és tanúsítása, valamint a Payment Card Industry Data Security Standard-je.

Konzolidáció várható a jelenleg versengő biztonsági szabványok és tanúsítási rendszerek között. 2010-re határozottan elválnak a menedzsment jellegű, a rendszer szintű és az eszköz szintű biztonsági szabványok, értékelési és tanúsítási rendszerek, valamint az egyes szinteken történő értékelést és tanúsítást támogató technológiák. Ezzel párhuzamosan 2010-re általánossá válik a biztonsági követelményeknek való megfelelést vizsgáló és ellenőrző, a biztonsági előírások kikényszerítését támogató alkalmazások használata.

4.1.3 Adatvédelmi kockázatok

A számítási, adattárolási és adatátviteli kapacitások bővülését eredményező új technológiák megjelenése általánosságban növeli az ADATVÉDELMI kockázatok szintjét. Egyes specifikus személyazonosítást is lehetővé tevő technológiák (pl. RFID, mobil telefon használat) megjelenése, elterjedése és használatuk általánossá válása a kezelt személyes adatok mennyiségének növekedését eredményezik, és ezáltal jelentősen hozzájárulnak az ADATVÉDELMI kockázatok növekedéséhez.

4.1.4 Adatvédelmi elvárások teljesülését támogató technológiák

Az ADATVÉDELMI kockázatok robbanásszerű növekedése következtében elterjednek az ADATVÉDELMI elvárások teljesítését támogató technológiák. Ezen technológiák két csoportra oszthatók. Az egyikbe azok a technológiák tartoznak, amelyek az adatkezelői oldalon segítik az ADATVÉDELMI elvárások teljesülését. (pl. közvetítő szolgáltatások, valamint ADATVÉDELMI szempontokat figyelembe vevő adatgyűjtési és adatkezelési üzletviteli gyakorlatok megjelenése) A másik csoportba azok a technológiák sorolhatók, amelyek a felhasználói oldalon teszik lehetővé vagy segítik elő az ADATVÉDELMI kockázatok csökkentését (PRIVACY ENHANCING TECHNOLOGIES – PRIVÁT SZFÉRÁT ERŐSÍTŐ TECHNOLÓGIÁK, PET-EK). A PET-ek jelentősége növekvőben van, s a vizsgált időszakban elsősorban nem újabb megoldások kifejlesztése várható, hanem a PET-ek integrálása az identitás-menedzselésbe, illetve szabványos réteggént való beépülésük az informatikai alkalmazásokba.

4.1.5 Adatvédelmi audit

Az ADATVÉDELMI elvárásoknak való megfelelés előzetes vizsgálatának és utólagos ellenőrzésének eredményességét növeli az ADATVÉDELMI audit. Hasonlóan az INFORMATIKA-BIZTONSÁGI értékeléshez és tanúsításhoz, az ADATVÉDELMI auditot megkövetelő előírások



megjelenése, ADATVÉDELMI audit szabványok és szabványos gyakorlatok alkalmazásának elterjedése prognosztizálható.

4.1.6 Kriptográfia polgári célú felhasználása

2010-ig általánossá válik a kriptográfia polgári célú használata mint a biztonsági és az azzal szorosan összefüggő azonosítás és hitelesítés legfontosabb eszköze. A kvantum számítástechnika fejlődése elavulttá teheti a nyilvános kulcsú kriptográfián alapuló biztonsági és hitelesítési megoldásokat, a kvantum számítógépek használatának elterjedése azonban a vizsgált időszakban még nem várható. A hitelesítés céljára használt kriptográfiai megoldásoknak a bővülő számítási kapacitások és teljesítmény miatti gyorsuló avulása a kizárólag kriptográfiai alapú hitelesítési megoldások mellett felértékeli a hitelesség megőrzési eljárások és szolgáltatások szerepét.