

20. BIZTONSÁG-TUDATOS FEJLESZTÉS, ÜZEMELTETÉS

Rátai Balázs

A biztonságos rendszerek és alkalmazások fejlesztését lehetővé tevő technológiák és módszerek használata, valamint a biztonság-tudatos fejlesztést és üzemeltetést megkövetelő szabályozás elterjed és általánossá válik.

1. Megnevezés és rövid leírás

AZ INFORMATIKA-BIZTONSÁGI⁶² problémák egyik legfontosabb oka, hogy a termékek és rendszerek fejlesztése során nem fordítanak kellő figyelmet a biztonsági kockázatok csökkentésére. Ez a gyakorlat az utóbbi években változóban van, nem utolsósorban annak köszönhetően, hogy ma már rendelkezésre állnak olyan – korábban nem létező – fejlesztési és üzemeltetési gyakorlatok, amelyek támogatják a biztonság-tudatos fejlesztést és üzemeltetést.

Az elemzés áttekintést nyújt ezen gyakorlatok várható fejlődéséről, és a jelenlegi fontosabb kutatási irányokról. Emellett vizsgálja azt is, hogy a szabályozás milyen szerepet játszhat a biztonság-tudatos fejlesztés és üzemeltetés kialakulásában.

2. Jelenlegi helyzet

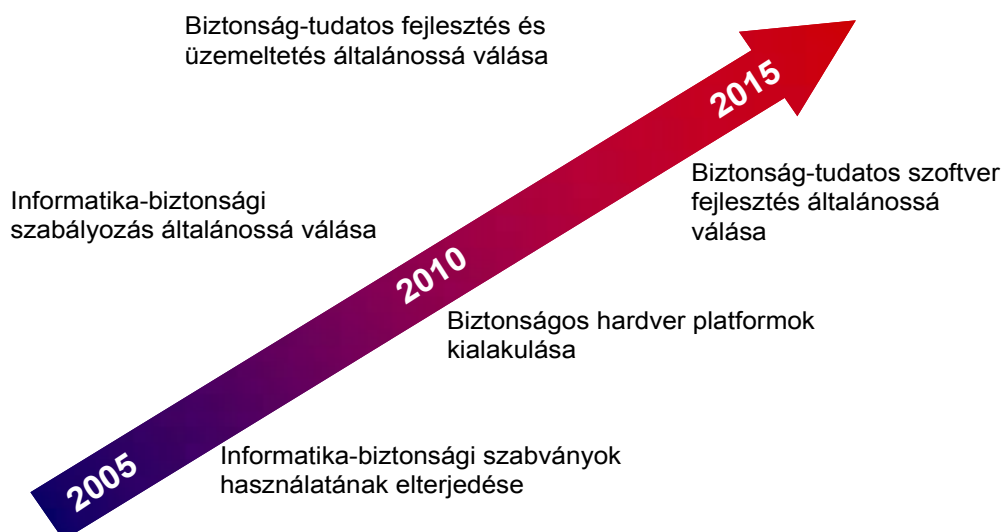
A jelenlegi PC-k architektúráis alapjai mintegy húsz évre nyúlnak vissza mind hardver, mind operációs rendszer tekintetében. Ekkoriban pedig nem számoltak még a PC-k nyílt hálózatokra való kapcsolásával. Emellett a jelenlegi architektúrán a biztonságos és nem biztonságos programok együttes futtatása sem megoldott. Mindezért a nyílt hálózatok által felvetett biztonsági problémák megoldása utólagos biztonsági kérdésként jelentkezik és a reaktív megoldások dominálnak. A biztonsági problémák kezelése továbbá kilépett abból a korszakból, amikor pusztán IT technológiai kérdésként volt kezelendő, mivel az IT eszközök alkalmazása ma már szervesen illeszkedik ügyviteli folyamatokba, és emiatt a technológiai védelem mellett az információ kezelési folyamatok védelme is elengedhetetlen.

⁶³ Saját biztonság meghatározásunk kialakításának oka az volt, hogy az elemzés céljait leginkább szolgáló biztonság fogalom használata révén elkerülhessük a versengő biztonság koncepciók közti kényszerű választás terhét.

Jellemző továbbá a mai helyzetre a biztonsági megoldások költségként való felfogása, az újabb kutatások azonban rámutatnak arra, hogy a biztonság elsősorban befektetés. A vállaltok és szervezetek többsége még ma is informatikai üzemeltetési kérdésnek tekinti az INFORMATIKA-BIZTONSÁGOT és gyakran alulértékelik a kockázatokat, holott az INFORMATIKA-BIZTONSÁGI problémák ma már a legtöbb esetben az egész szervezet működésre közvetve vagy közvetlenül kihatnak. Emellett sok esetben hiányoznak a biztonság-tudatos fejlesztéshez és üzemeltetéshez a megfelelő szintű alkalmazói, felhasználó ismeretek is.

3. A várható fejlődés eredményének jellemzése

A biztonság-tudatos fejlesztési, üzemeltetési módszerek fokozatos megjelenése és használatuk általánossá válása elősegíti a proaktív (és nem reaktív) védekezési módok előtérbe kerülését. Ma már számos olyan módszertan létezik, amely lehetővé teszi, hogy az eszközök, alkalmazások és rendszerek tervezése során megfelelő figyelmet fordítsanak a felmerülő biztonsági problémák kezelésére. Ilyen módszertan például a Survivable Systems Engineering, amely elősegíti, hogy a rendszerek minden esetben biztosítsák a létfontosságú szolgáltatások ellátását és a létfontosságú adatok védelmét, vagy a Survivable Systems Analysis, amely a meglévő rendszerek túlélésének biztosítását segíti elő. Hasonló jellegű, a biztonság szempontjából is előremutató kezdeményezés a Trustable Computing Platforms létrehozása is, amelynek lényege, hogy létrehozzanak egy, a rendszeren belül fizikailag is elválasztott környezetet (a saját biztonságos periféria- és rendszerhozzáférésekkel, memóriával), ahol digitális aláírás-technológia biztosítja a nem megbízható programok futásának kizárását.



1. ábra A biztonság-tudatos fejlesztés és üzemeltetés fejlődése 2005-2015.

Az elkövetkező 5-10 év során lényegében kialakulnak és elterjednek azok a szoftverfejlesztési módszertanok, architektúrális megoldások, és üzemeltetési gyakorlatok, amelyek lehetővé teszik az informatikai eszközök és rendszerek biztonságosabb használatát. Az általános biztonsági szint növekedésére különösen nagy hatása lesz a biztonságosabb szoftverfejlesztést lehetővé tevő módszertanok megjelenésének.

A technológiai feltételek kialakulása mellett azonban fontos, hogy megfelelő ösztönző és előíró szabályozási környezet is kialakuljon, mivel a jelenleginél biztonságosabb eszközök előállítása és üzemeltetése egyértelműen többletköltségekkel jár.

4. Szükséges technológiai előfeltételek

A biztonsági problémák többsége a szoftverfejlesztés problémáira vezethető vissza. Jelenleg nem állnak rendelkezésre olyan módszertanok és eszközök, amelyek lehetővé tennék, hogy a piac által megkövetelt gyorsaság mellett is biztosítható legyen a biztonságos szoftver fejlesztése. Fontos látni, hogy a megfelelő funkcionalitással működő szoftver még nem feltétlenül biztonságos. A minőségi szoftver fejlesztés segíti ugyan a biztonsági problémák kiküszöbölését, ugyanakkor biztonságos szoftver előállítása mindig többletköltséggel jár. A biztonságos szoftverfejlesztést lehetővé tevő módszertanok használatának általánossá válása a 2010-es évek első felére várható.

| OWASP Top Ten Most Critical Web Application Security Vulnerabilities⁶³ | |
|--|--|
| 1. | Unvalidated Input |
| 2. | Broken Access Control |
| 3. | Broken Authentication and Session Management |
| 4. | Cross Site Scripting (XSS) Flaws |
| 5. | Buffer Overflows |
| 6. | Injection Flaws |
| 7. | Improper Error Handling |
| 8. | Insecure Storage |
| 9. | Denial of Service |
| 10. | Insecure Configuration Management |

Mivel az informatikai eszközök és rendszerek biztonsága jelentősen függ az üzemeltetők és felhasználók felkészültségétől is, ezért az előfeltételek közé kell sorolnunk a biztonsági kockázatok csökkentését elősegítő felhasználói és üzemeltetői

⁶⁴ forrás: The Open Web Application Security Project – <http://www.owasp.org/documentation/top10.html>

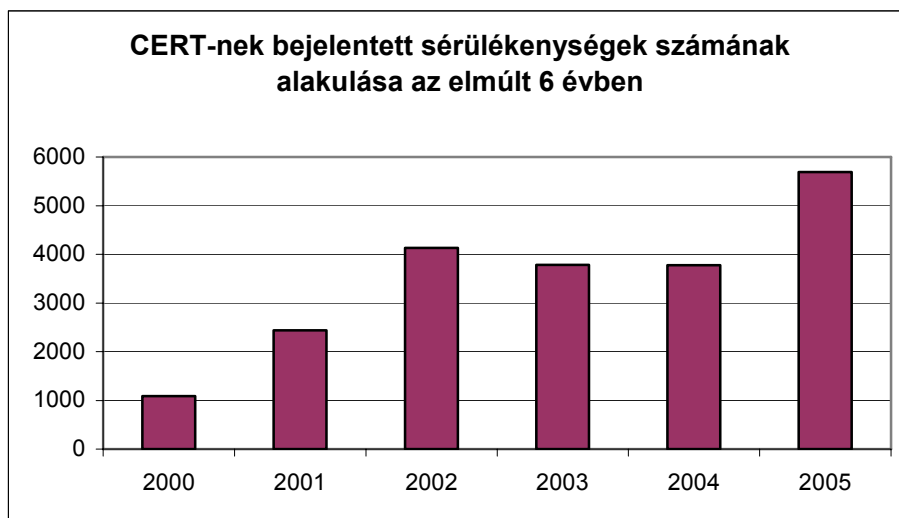
ismereteket kialakulását is. A biztonság-tudatos felhasználói és üzemeltetői magatartás megteremtése elsősorban oktatás kérdése.

A nem megfelelő biztonságból eredő károk egy része nem ott jelentkezik, ahol az adott biztonsági kockázat keletkezik. Például egy banki rendszer nem megfelelő biztonsága elsősorban a bank ügyfeleinek okoz kárt és csak másodsorban a banknak. Ezért ilyen területeken szükséges olyan szabályozás, amely visszahárítja a kockázatból eredő kárért való felelősséget arra a félre, amely a kockázat keletkezéséért felelős.

A szabályozásnak való megfelelés igazolása és a piaci bizalom megőrzése miatt egyre fontosabbá válik a termékeknek és rendszereknek harmadik független fél által történő biztonsági vizsgálata és tanúsítása. A jelenleg létező értékelési és tanúsítási tevékenység stabilizálódása, az értékelési és tanúsítási rendszerek konszolidációja ezért elengedhetetlen feltétele a biztonságos fejlesztés és üzemeltetés kialakulásának.

5. Folyamatban lévő kutatások, fejlesztések

A biztonság területén a technológiai fejlesztés egyik jelentős műhelye az USA CERT (USA COMPUTER EMERGENCY RESPONSE TEAM), amely jelenleg olyan új módszertanok kifejlesztésén dolgozik, amelyek jelentősen elősegíthetik a biztonság-tudatos rendszerfejlesztést és üzemeltetést.



Az alábbiakban néhány olyan kiemelt USA CERT kutatási projekt kerül bemutatásra⁶⁴ a jövő szoftvereinek és hálózatainak fejlesztése köréből, amelyek vélhetően iparilag is alkalmazható eredményekre vezetnek. A bemutatásra kerülő módszertanok elsődleges szerepe a jövő biztonságosabb IKT eszközeinek és hálózatainak fejlesztéséhez szükséges eszközök biztosításában van. A módszertanok

⁶⁴ Természetesen más fontos műhelyek eredményeit is megemlíthetnénk. Választásunk azért esett a USA CERT kutatási projektjeinek ismertetésére, mert megítélésünk szerint a kutatási projektek jól reprezentálják azokat a kutatási irányokat, amelyek a biztonság-tudatos fejlesztés és üzemeltetés szempontjából a legfontosabbak.

fejlesztése folyamatos, bizonyos eredményeket, mint pl. a korábban említett Survivable Systems Analysis, már ezidáig is fel tud mutatni. A USA CERT évente teszi közzé jelentését a projektek aktuális állásáról.⁶⁵

Flow Service Quality

Elsősorban fejlesztési módszerek meghatározását jelenti komplex hálózati alkalmazások számára, amelyeket változó felhasználók, felhasználási módok, bizonytalan funkcionalitás és biztonság kereskedelmi szoftverek esetén, előre láthatatlan hibák és az átláthatóság és ellenőrzés hiánya jellemeznek.

FX (Function Extraction)

A mai méretes programok esetén nem mérhető fel előre a programok tevékenysége, ami a szoftverek fenntarthatósági és biztonsági problémáinak jelentős részét okozza. Az FX projekt célja a program összes funkciójának, automatikus felmérési lehetőségeinek meghatározása. Jelenleg az FX technológia első alkalmazásának, a rosszindulatú szoftverek funkcionalitását felderítő Function Extraction for Malicious Code (FX/MC) rendszernek a fejlesztése folyik.

Intrusion-Aware Design

A projekt célja, hogy a tervezés során figyelemmel kísérjék az architektúrák reagálását a biztonsági problémákra és elősegítsék annak javulását.

LEVANT (LEvels of ANonimity and Traceability)

Az internet protokolljai (eljárásai) nem felelnek meg a mai biztonsági elvárásoknak. A Levant projekt célja, hogy lehetővé tegye a névtelenség és a követhetőség közötti finom változtatásokat az egyes folyamatok számára.

MAAP (Mission Assurance Analysis Protocol)

A MAAP projekt célja, hogy a szervezeti határokon átívelő feladatok, folyamatok esetére dolgozzon ki megfelelő biztonsági megoldásokat. Ma az ilyen feladatok, folyamatok létrejötte igen gyakori (pl. az outsourcing miatt), és a fellépő biztonsági kockázatok kezelése nem lehetséges a szervezetek közötti együttműködés nélkül.

NSE (Next Generation Software Engineering)

A jövő nagy és komplex szoftvereinek kifejlesztésére elégtelennek látszanak a mai módszerek. A projekt célja az újabb módszerek kidolgozása, először az elvi alapokat, majd a gyakorlati megoldásokat illetően, a számítási automatizmusok bevonásával.

SQUARE (System Quality Requirements)

A szoftverek minőségének elméleti meghatározása már megtörtént, ám a gyakorlat hiánya miatt a felhasználás előtt nem állapítható meg a minőség. A projekt célja a gyakorlati módszerek meghatározása, amely az iparági szereplők és a kormányzat bevonásával történik. Különös hangsúlyt kap a biztonság.

Threat Dynamics

A projekt célja olyan módszerek és eszközök kidolgozása, amelyek lehetővé teszik egy szervezet veszély dinamikáinak felmérését, modellezését, és az eredmény fényében javítják a biztonságát és fennmaradási esélyeit.

⁶⁵ Az áttekintés a 2004-es beszámoló alapján készült.

V-RATE (Vendor Risk Assessment and Evaluation)

A beszállítói termékek beépítése kritikus rendszerekbe gyakori, azonban sem a kódhoz nincs hozzáférés, sem a fejlesztésekbe nem lehet belelátani. A fenti projekt célja értékelési módszerek kidolgozása a beszállítói termékekre. Ez egyrészt a beszállítói kockázatok besorolásán, másrészt a beszerző kockázatkezelési képességén alapul.

Egy szintén jellegzetes és előremutató projekt a Trustable Computing Platforms létrehozása, amely a PC architektúra területén hozhat jelentős előrelépést, mivel a személyi számítógépek szintjén teremti meg a biztonságos üzemeltetés alapfeltételeit. A Trustable Computing Platforms specialitása több szemponton alapszik: egyrészt a hardver és szoftver együttes szerepén a kialakításában (amelynek előfeltétele természetesen az érintett cégek együttműködése), másrészt a projekt előrehaladottságán. Nem mellékes az a szempont sem, hogy nem kizárólag a PC-k területén bír jelentőséggel.

A jelenleg használt PC környezet tervezésekor senki nem számított, hogy a gépek jelentős része hálózati alkalmazásban kerül majd használatra. Ezért a jelenlegi hardver- és szoftver architektúra nem tudja biztosítani egyidejűleg megbízható (trusted) programok futását, amennyiben nem megbízható programok is futnak. Gyakorlatilag már ma is elérhető egy közel megbízható környezet a konfigurációk lezárásával, kizárólag digitálisan aláírt programok futtatásával, a tároló hardveres védelmével és a felhasználók adminisztrációs jogainak letiltásával, ám számos felhasználónak szüksége van bizonyos rugalmasságra, nem is beszélve a fentiek költségéről. Ezért valamilyen más, a megbízható programok védelmét biztosító megoldásra van szükség.

A Trusted Computing Platform Alliance romjain 2003 áprilisában hozta létre az AMD, a Hewlett Packard, az IBM, az Intel és a Microsoft a Trusted Computing Group-ot (továbbiakban: TCG), amely együttműködés a Trustable Computing Platforms célkitűzéseit kívánja megvalósítani. Felismerve a PC világon túlnyúló jelentőséget, csatlakozott a Nokia, az Amtel és a Sony is.

Ahhoz, hogy megakadályozzák a megbízhatónak minősített programokhoz való hozzáférést, azokat el kell különíteni a többi alkalmazástól. Ennek megoldásához pedig a hardverek megfelelő átalakítása is szükséges, amelynek szabványát adhatja az Intel LeGrande technológiája. A szoftvermegoldást pedig a Microsoft Next Generation Secure Computing Base (korábban Palladium) biztosíthatja. A megbízható programok elkülönítése digitális aláírási technológia alkalmazásával valósul meg. A digitális aláírással ellátott programok nem futhatnak azonos helyen az azzal nem bírókkal. Ez nem csak a jelszavak, kulcsok, stb. biztonságos kezelését, de a digitális jogvédelmet is biztosíthatják a szellemi tulajdonnak. A fenti rendszernek azonban mindenképpen megbízhatónak, kiszámíthatónak és biztonságosnak kell lennie, aminek a stabil alapjait a korábban említett szoftver, hardver és rendszerfejlesztéssel kapcsolatos módszertanok teremthetik meg. A szükséges technológia azonban már ma is lényegében rendelkezésre áll. Első bevezetése a Windows új operációs rendszerével (Vista, korábban Longhorn) várható.⁶⁶ Ennek ellenére a Gartner elemzői 2008-ra teszik, hogy a fenti technológia elérje a kritikus tömeget a PC-k területén, és legalább 2010-ig tart, hogy az egyéb felhasználói elektronikus eszközök területén elérjék azt.

⁶⁶ Jelenleg a Vistával kapcsolatosan nem említik a terméket. Forrás: www.microsoft.hu

Mindenesetre a fentiek piaci alkalmazásának feltétele a tartalomszolgáltatók gyakorlatának megváltozása. A Gartner kutatói három scenáriót vázoltak fel a fentiek alapján, azaz közel sem biztos a termék átütő sikere. Azonban a törekvés egyértelmű: egy módszer a védelmet igénylő adatok beépített elkülönítésére, nem pedig a jogosulatlan hozzáférések szoftveres megoldású kizárására.

6. Az IKT más területeire való hatások bemutatása

A biztonság szempontjának fejlesztés során való figyelembe vétele várhatóan biztonságosabb szoftvereket eredményez, és ráirányítja a figyelmet ezek biztonságos használatára is. A különböző értékelési és tanúsítási standardok szerepe folyamatosan növekszik, hiszen az ezeket alkalmazó cégek, párhuzamosan a szükséges technológiai megoldásokkal, biztosíthatják ügyfeleik számára az elvárt biztonsági szintet, mégpedig jól követhető és dokumentált módon. Ez a jelenség is jól jelzi a biztonság kérdéskörének átértékelését.⁶⁷ A biztonsági követelményeket úgy kell teljesíteni, hogy közben hozzáférhetőek maradjanak a védeni kívánt adatok és eljárások. Ezért a biztonság egy komplex, az egész szervezetet érintő kérdéskörre vált, amelynek központi fogalma a kockázat.

A tanúsítási rendszerek, amellet, hogy egy kipróbált és már bevezetett rendszert nyújtanak a felhasználóiknak, biztosítják üzletfeleiket, hogy partnerük lépéseket tesz közös érdekeltségeik védelmére. A jelentősebb tanúsítási rezsimek (BS 7799, a COBIT és a COMMON CRITERIA) mára már mind kinőtték gyerekbetegségeiket és egyre szélesebb körben nyernek alkalmazást. Ezek közös jellemzője, hogy komplex átfogó megoldásokat kínálnak az INFORMATIKA-BIZTONSÁGI problémák kezelésére. Fontos azt is látni, hogy az egyes tanúsítási rezsimek esetében a hangsúlyok eltérőek. Így például a COMMON CRITERIA az IKT eszközök biztonsági tanúsítása terén nyert teret, a BS 7799 elsősorban információkezelési folyamatok biztonságának megítélésére, a COBIT-ot pedig elsősorban az általános IT üzemeltetés biztonságának vizsgálatánál alkalmazzák.

7. Társadalmi-gazdasági hatások elemzése

A biztonságtudatosabb fejlesztés és üzemeltetés legfontosabb hatása, hogy csökkenti, vagy megszünteti az informatikai eszközök használatából adódó biztonsági kockázatokat, az utólagos kockázatkezelésről a megelőzésre helyezi át a hangsúlyt.

A biztonságosabb eszközök és rendszerek okozta változás elsősorban infrastrukturális jellegű közvetett hatásként jelentkezik, közvetlen eredményekben ezért nehezen kimutatható. A biztonságosabb informatikai környezet összességében jelentősen befolyásolja az informatikai eszközök, alkalmazások és szolgáltatások iránti bizalmat,

⁶⁷ Richard A. Caralli és William R. Wilson: The Challenges of Security Management.

és hosszú távon ezért egész iparágak fejlődésére lehet hatással, valamint befolyásolja az emberek általános közérzetét és viszonyulását az informatikai eszközökhöz.

A technológiai fejlődés mellett fontos szerep hárul a szabályozásra is. Mivel az INFORMATIKA-BIZTONSÁGI kockázatokból eredő károk nem mindig az üzemeltetőnél vagy a gyártónál csapódnak le, ezért a drágább biztonság-tudatos fejlesztés és üzemeltetés kizárólag piaci folyamatok eredményeként nem fog megvalósulni, ezért feltétlenül szükséges a biztonság-tudatos fejlesztést és üzemeltetést ösztönző vagy adott esetben megkövetelő szabályozási környezet kialakítása. Ezen szabályozási környezetnek a kialakulása már elkezdődött. A szabályozási környezet elemei direkt követelményekből, felelősségi szabályokból, és a tanúsítási rezsimek állami elismerését biztosító szabályrendszerekből áll majd össze.

8. Magyar vonatkozások

A nemzetközileg elismert értékelési és tanúsítási rezsimek már Magyarországon is megjelentek, és egyre jelentősebb figyelmet kapnak. A COMMON CRITERIA egyezményhez Magyarország 2003-ban csatlakozott, a csatlakozással egyidejűleg pedig elindult a hazai CC tanúsítási rezsimek kialakítása, amely jelenleg a MIBÉTS (Magyar Informatika Biztonsági Értékelési és Tanúsítási Séma) nevet viseli. Emellett természetesen vannak magyar szakértők és cégek is, amelyek foglalkoznak BS 7799 szerinti tanúsítással is. Tanúsítási körben mindenképpen említést érdemel az is, hogy a több, mint 100 országban működő és 30.000-nél is több tagot számláló Information Systems Audit and Control Association (ISACA) magyar tagozata, amely elkészítette és könyv formában is megjelentette a COBIT magyar verzióját. A COBIT módszertan szerinti értékelések elsősorban a pénzügyi szektorban terjedtek el, nem kis részben annak köszönhetően, hogy a PSZÁF is ezt a módszertant alkalmazza a pénzügyi intézmények ellenőrzése során. Az ISACA magyar tagozata a legaktívabb magyar informatika biztonsági szakértői közösség.

A CERT-nek (COMPUTER EMERGENCY RESPONSE TEAM) is működik magyar tagozata, az MTA SZTAKI-n belül. A Hun-CERT elsősorban internetes hálózat-biztonsági incidensek felderítésében és a megelőzésében nyújt segítséget. Jelenlegi legnagyobb, az IHM által támogatott kutatási projektjük célja „Az informatikai hálózati infrastruktúra biztonsági kockázatainak és kontrolljainak c. ajánlás kidolgozása.

Hazánkban is kezd megjelenni az INFORMATIKA-BIZTONSÁGI szabályozás. Figyelemre méltó a hitelintézetekről és pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény 2004-es módosítása, amely a 13/B. § keretében szabályozza a törvény hatálya alá eső vállalkozások kötelezettségeit az informatikai rendszerük védelmével kapcsolatban. Emellett még az adatvédelmi törvénynek az adatkezelések biztonságra vonatkozó rendelkezéseit érdemes kiemelni.

9. Következtetések

A biztonság-tudatos fejlesztés és üzemeltetés technológiai feltételeinek kialakulása az elkövetkező 5-10 év egyik legfontosabb változása. Hatása számokban nehezen kimutatható, jelentősége az általános infrastrukturális beruházások hatásával vetekszik. Az INFORMATIKA-BIZTONSÁG megteremtése azonban nem kizárólag műszaki és üzleti feladat, hanem komoly állami szerepvállalást igényel, többek között az INFORMATIKA-BIZTONSÁG megteremtését segítő ösztönző szabályozás kialakítása révén.