AZ INFORMATIKAI BIZTONSÁG MÉRÉSE

Muha Lajos
tanszékvezető főiskolai tanár
ZMNE Bolyai János Katonai Műszaki Kar Informatikai Tanszék
E-mail: muha.lajos@zmne.hu

Összefoglalás: A biztonság mérése az informatikai biztonság egy területe. Ez nem egy új téma, de még csak szórványos figyelmet kapott. Ez a cikk az informatikai biztonság mérése területének egy áttekintése.

Kulcsszavak: informatikai biztonság, mérés, auditálás, ellenőrzés

Abstract: Security measurement an area of information security. It is not the new topic, but one which receives focused interest sporadically. This paper provides an overview of the information security measurement area

Keywords: information security, measurement, audit, control

1. Bevezetés

Napjainkban divatos lett az informatikai biztonság méréséről beszélni. Sokan sokfélét értenek ez alatt. Mérnöki szemmel vizsgálva jó néhány esetben kiderül, hogy nem beszélhetünk mérésről. Néha nem az informatikai biztonság méréséről van szó, hanem valamilyen informatikai auditról.
Vegyük például a nemrégiben frissített NIST szabványt, az SP800-55 új változatát. A *Teljesítménymérési útmutató az informatikai biztonsághoz* [1] létrehozásának elsődleges oka az amerikai szövetségi informatikai biztonsági törvény[1] [2] volt. A szabványosított metrikakészlet alkalmas az informatikai biztonság egységes elvek alapján való mérésére a különböző ügynökségeknél.
A dokumentum előírja, hogy az „információbiztonsági mérési program fejlesztése és implementációja során:

- a méréseknek mennyiségi információt kell nyújtaniuk (százalékok, átlagok, és számok);
- a mérések alapjául szolgáló adatoknak könnyen használhatónak lenniük;
- csak megismételhető informatikai biztonsági eljárások vehetők figyelembe a mérések során;
  és
- a méréseknek hasznosítható kell lenniük a teljesítmény értékeléséhez és az erőforrások kezelésében.

[1] Federal Information Security Management Act, röviden: FISMA

2. Az ISO/IEC 27004

2.1. Az ISO/IEC 27000 szabványsorozat

Az ISO/IEC 27000 szabványsorozatot – bár kritikák is érik – a világ, és különösen az Európai Unió mind több országában fogadják el a különböző szervezetek informatikai rendszerük biztonságának alapjaként. A szabványsorozat nemcsak azért kiemelt fontosságú, mert a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelmények és védelmi intézkedések mellett az azok implementálásához, auditálásához, kockázatelemzéséhez szükséges előírásokat tartalmazza, de a különböző dokumentumok közül ez vált nemzetközi szabvánnyá, és emellett a nemzetközi szabvánnyá vált ITIL (ISO/IEC 20000) is ezt használja hivatkozási alapként.
A szabványsorozat célja valamennyi, az informatikai és kommunikációs rendszerek biztonságirányításával (menedzselésével) foglalkozó szabvány egyetlen sorozatba gyűjtése. A szabványcsalád jelenlegi és tervezett tagjai közül néhány[2]:

- **ISO/IEC 27000:2009** Information technology – Security techniques – Information security management systems – Overview and vocabulary (definíciók a sorozat összes szabványához);
- **ISO/IEC 27001:2005** Information technology – Security techniques – Information security management systems – Requirements;
- **ISO/IEC 27002:2005** – Information technology – Security techniques – Code of practice for information security management;
- **ISO/IEC FDIS 27003** – Information technology – Security techniques – Information security management system implementation guidance (terv: ez a szabvány az ISO/IEC 27001 szabvány implementálásához szükséges tanácsokat és útmutatókat fogja tartalmazni);
- **ISO/IEC FDIS 27004** – Information technology – Security techniques – Information security management – Measurement (terv);
- **ISO/IEC 27005:2008** – Information technology – Security techniques – Information security risk management;
- **ISO/IEC 27006:2007** – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems;
- **ISO/IEC CD 27007** – Information technology – Security techniques – Guidelines for information security management systems auditing (terv).

2.2. A tervezett ISO/IEC 27004 szabvány

Az informatikai biztonság méréséről szóló nemzetközi szabvány, az ISO/IEC 27004 még csak terv. A szabvány fejlesztése már négy évvel ezelőtt elindult, és 2009 végére várható a kiadása. A szándékok szerint az informatikai biztonsági irányítási rendszerek tekintetében nagyon sokféle szervezetre alkalmazható lenne.
Az ISO/IEC 27004 egy új szabvány lesz, amely az informatikai biztonság mérésével fog foglalkozni, abból a célból, hogy az informatikai biztonság irányítási rendszerének hatékonyságát mérni tudjuk. A szabványtól azt várják, hogy lefedi mind az ISO/IEC 27001 szabványban meghatározott menedzsment eljárásokat, mind az ISO/IEC 27002 szabványban meghatározott biztonsági követelményeket. A szabvány várhatóan a mérési módszerek

[2] A sorozat 35 tagura van (jelenleg) tervezve, ebből a 27033 például 7 részből áll.

részletes leírását és az azok használatára vonatkozó útmutatót fog tartalmazni. Célja az informatikai biztonsági menedzsment rendszerek hatékonyságát növelni.
A szabvány várhatóan nagyon részletes lesz a mérési eljárások tekintetében. Le fogja írni annak a módszereit, hogy az alap és a származtatott védelmi intézkedésekről hogyan gyűjtsünk adatokat és hogyan elemezzük azokat. Ebben a körben magasabb szintű absztrakciók megvalósítását is lehetővé kívánják a használatával tenni.

3. A hazai helyzet

3.1. A MIBA

Hazánkban az informatikai biztonságról szóló törvény már egy éve vár tárgyalásra, de a Közigazgatási Informatikai Bizottság 25. ajánlásában[3] az informatikai biztonság méréséhez is felhasználható dokumentumok vannak.
A Magyar Informatikai Biztonsági Ajánlások (MIBA) című ajánlássorozat fő célja, hogy biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő.
A nemzetközi szabványokhoz és ajánlásokhoz igazodva a MIBA három fő részből áll [3]:

- A **Magyar Informatikai Biztonsági Keretrendszer (MIBIK)** szervezeti szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBIK a biztonságos informatikai rendszerek irányításáért, menedzseléséért felelős vezetőknek, illetve a szervezet egészére vonatkozó követelmények teljesülését értékelő szakembereknek szól.
- A **Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)** technológiai szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBÉTS célközönsége az informatikai rendszer kialakításáért, fejlesztéséért felelős vezetők, valamint az informatikai termékek és rendszerek biztonsági értékelését és tanúsítását végző szakemberek köre.
- Az **Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)** olyan szervezeteknek nyújt segítséget biztonságos informatikai rendszereik kialakításához, amelyek nem rendelkeznek jelentősebb informatikai rendszerrel, illetve ehhez elkülönült informatikai személyzettel.

A **MIBIK** az ISO/IEC 27001:2005, ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. A MIBIK része az Informatikai Biztonsági Irányítási Rendszer (IBIR)**,** amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK), amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányítás Vizsgálata (IBIV), amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget. [3]
A **MIBÉTS** az ISO/IEC 15408:2005 és ISO/IEC 18045:2005 nemzetközi szabványokon, illetve a nemzetközi legjobb gyakorlatokon és nemzeti sémákon alapul. Keretet biztosít arra, hogy az informatikai termékek és rendszerek tekintetében a biztonsági funkciók teljessége és hatásossága értékelésre kerüljön. Értékelési módszertana alkalmas az operációs rendszerek, hardverek (pl. hálózati eszközök, tűzfalak, behatolás észlelők, intelligens kártyák), szoftver-alkalmazások (pl. különböző programnyelveken megírt kritikus alkalmazások) speciális biztonsági szempontjainak értékelésére. Ezzel a MIBÉTS a megbízható harmadik felek által végzett biztonsági ellenőrzés és audit egységes szempontrendszerét alkotja meg. [3]

[3] Magyar Informatikai Biztonsági Ajánlások, röviden: MIBA

Az **IBIX** elsődleges célja, hogy segítséget nyújtson az informatikai biztonság megfelelő szintjének kialakításához önkormányzati és más informatikai szempontból kis méretű környezetben. Javasolt az anyag azon szervezetek számára, ahol a szervezet méreténél fogva nem áll rendelkezésre külön emberi és egyéb erőforrás az informatikai rendszerek biztonságának kialakítására és üzemeltetésére, hanem ezt „házon belül" kell megoldani. [3]

3.2. A MIBIK

A **MIBIK** az ISO/IEC 27001:2005, ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. A MIBIK része az Informatikai Biztonsági Irányítási Rendszer (IBIR)**,** amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK), amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányítás Vizsgálata (IBIV), amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget." [4]

3.3. Az IBIV

Az **Informatikai Biztonság Irányításának Vizsgálata** (**IBIV**) egy olyan módszertani segédlet, amely a szervezetek vezetése és belső ellenőrző szervei által végrehajtott ellenőrzések mellett az nemzetközi, de már a hazai gyakorlatban is egyre jobban terjedő ISO/IEC 27001:2005 szabványnak való megfelelést bizonyító – megfelelő felkészülés utáni – audit elvégzéséhez is segítséget nyújt.
Az IBIV célja az informatikai rendszereinek biztonsági vizsgálatához egységes módszertan biztosítása, amely alkalmazásával a szervezet vezetése bizonyosságot szerezhet arról, hogy a szervezet informatikai rendszere kielégíti saját biztonsági céljait, illetve az érdekelt külső felek meggyőződhetnek arról, hogy az őket is érintő biztonsági fenyegetéseket kellően figyelembe veszik. Ez a módszertan részletes előírásokat ad az informatikai biztonság irányításának vizsgálatához és tanúsításához a vizsgálatot végzőknek és az arra felkészülőknek egyaránt. Az Informatikai Biztonság Irányítási Rendszer folyamatainak vizsgálata (1. rész) és a biztonsági intézkedések vizsgálata (2. rész) lefedi az ISO/IEC 27001 szabvány szerinti tanúsításhoz szükséges vizsgálati eljárás (audit) során vizsgálandó kérdéseket. [5]
Az IBIV tartalmi felépítése:

1. Az Informatikai Biztonság Irányítási Rendszer folyamatainak vizsgálata
   A vizsgálat lefedi az Informatikai Biztonság Irányítási Rendszer (IBIR) folyamatait. Ezek a folyamatok lefedik a teljes tevékenységi ciklust, megcélozva az informatikai biztonság hatékony irányítását egy folytonos fejlesztési programon keresztül. A vizsgálati eljárás az Informatikai Biztonság Irányítási Rendszer (IBIR) a folyamatainak vizsgálatához ad részletes segítséget.
2. Biztonsági intézkedések vizsgálata
   Itt az úgynevezett *Gap analysis* kerül felhasználásra, amely a biztonsági rések feltárásához ad részletes és teljes körű kérdőíveket. Az összeállított kérdőívek feladata az informatikai biztonsági intézkedések részletes vizsgálata, azaz segítségükkel részletesen meghatározhatjuk, hogy az IBIK követelményei mennyiben kerültek megvalósításra. A kérdések az IBIK pontjait követve a teljes követelményrendszert vizsgálják.

3. Az informatikai rendszer biztonságának vizsgálata (kockázatelemzés)
   A kockázatelemzés elvégzését az IBIK előírja, ugyanakkor annak megtörténte feltétel az ISO/IEC 27001 szabvány szerinti audit eredményességéhez is. Az informatikai rendszer biztonságának kockázatelemzés alapú vizsgálatához két különböző módszertant ír le.
   Az első eljárásrend a NIST SP 800-30[4] és a FIPS 199[5] dokumentumokon alapuló módszertan. Ez a módszertan viszonylag egyszerű, kis idő- és erőforrás igényű kockázatbecslést tesz lehetővé.
   A másik bemutatott eljárásrend egy CRAMM[6] alapú módszertan, amely MeH ITB 8. számú ajánlása (Informatikai biztonsági módszertani kézikönyv) alapján, annak aktualizálásával készült kockázatelemzési módszertan. A CRAMM módszertan egy részletes, az egyes fenyegetések kockázatait feltáró eljárás, azonban idő- és erőforrás igénye nagy – ezért költséges.

Az 1. és 2. részben a kérdőívek a következőkre térnek ki:

- a vizsgálat tárgya;
- a vizsgálati szempontok;
- értékelés (megfelel a követelménynek, részben megfelel a követelménynek és nem felel meg a követelménynek kategóriákkal).

4. Összegzés

Az informatikai biztonság mérése még kialakulóban van. A szakma sem teljesen egységes az értelmezésében, kezelésében.
A kialakulóban lévő mérési módszereknek garantálni kell az informatikai biztonság megvalósítása hatékonyságának mérését. Mindemellett le kell írnia annak a módszereit, hogy hogyan gyűjtsünk adatokat az informatikai rendszerek biztonságáról és azok elemezéséről.
Az informatikai biztonsági mérések során mennyiségi információkat kell feldozgozni, úgy, hogy a mérések megismételhetőek legyenek ellenőrzés céljából.

Irodalomjegyzék

[1] Chew, E.; Swanson, M.; Stine, K; Bartol, N.; Brown, A.; Robinson, W.: *NIST Special Publication 800-55 Revision 1 : Performance Measurement Guide for Information Security*, National Institute of Standards and Technlogy, Gaithersburg, USA, 2008., http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

[2] *E-Government Act of 2002 (Title III. – Information Security : Federal Information Security Management Act)*, House of Representatives, Washington D.C., USA, 2002., csrc.nist.gov/drivers/documents/FISMA-final.pdf

[4] NIST Special Publication 800-30, *Risk Management Guide*, 2001 – Kockázatkezelési Útmutató. NIST – National Institute of Standard and Technology, USA
[5] FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*, 2004 – . FIPS – Federal Information Processing Standards Publication, USA
[6] *CCTA Risk Analysis and Management Method* – CCTA Kockázatelemzési és Kezelési Módszertan. CCTA –Central Computer and Telecommunications Agency (Központi Számítógép és Távközlési Ügynökség)

[3] *Közigazgatási Informatikai Bizottság 25. ajánlása : Magyar Informatikai Biztonsági Ajánlások (MIBA)*, Közigazgatási Informatikai Bizottság, Budapest, 2008., http://www.ekk.gov.hu/hu/kib/KIB-25-0_MIBA_v1_vegl.pdf

[4] Muha L.: *Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK)*, Közigazgatási Informatikai Bizottság, Budapest, 2008., http://www.ekk.gov.hu/hu/kib/KIB-25-1-0_MIBIK_V1_0_vegl.pdf

[5] Balázs I.; Déri Z.; Lobogós K.; Muha L.; Nyíry G.; Sneé P.; Váncsa J..: *Az Informatikai Biztonság Irányításának Vizsgálata (IBIV)*, Közigazgatási Informatikai Bizottság, Budapest, 2008., http://www.ekk.gov.hu/hu/kib/KIB-25-1-0_MIBIK_V1_0_vegl.pdf