KÖZIGAZGATÁSI INFORMATIKAI BIZOTTSÁG

25. számú Ajánlása

Magyar Informatikai Biztonsági Ajánlások (MIBA)

25/1.

Magyar Informatikai Biztonsági Keretrendszer (MIBIK)

1.0 verzió

2008. június

Közigazgatási Informatikai Bizottság
25. számú Ajánlása

Készült a

Miniszterelnöki Hivatal megbízásából

K é s z í t e t t e :

Muha Lajos PhD, CISM

Az ajánlás a Közigazgatási Informatikai Bizottság (KIB)
Jogi és Műszaki Szabályozási Albizottsága észrevételei alapján véglegesített tartalommal
a KIB tagjainak 2008. május-júniusi elektronikus távszavazása alapján
került elfogadásra

TARTALOMJEGYZÉK

1. BEVEZETÉS

Az informatikai rendszerek egyre átfogóbb alkalmazása érinti a társadalom minden rétegét (az államigazgatást, a kritikus infrastruktúrákat, a gazdasági és a civil szférát) és ezek kapcsolatát. Ebből következően egyre nagyobb értéket képvisel az információ-technológiai eszközökben feldolgozott adat, melynek megsérülése vagy szándékos veszélyeztetése (beleértve az információval történő visszaéléseket és az adatok meghamisítását is) mérhetetlen károkat okoz(hat). Az informatikai rendszereket üzemeltető vezetők és üzemeltetők felelőssége kiterjed az informatikai adatvagyon, az adatokhoz kapcsolódó személyiségi jogok védelmére is, melyet a társadalmi, szervezeti érdekeken túlmutatóan jogszabályi előírások is elvárnak. Mindezek miatt kiemelt igény mutatkozik az informatikai biztonság garantálására.

Az informatikai biztonság – mely tartalmazza az információk és az informatikai eszközök és szolgáltatások védelmét is - sokrétű fogalom, fejlesztése, folyamatos fenntartása minden résztvevő felelőssége, egyúttal szerteágazó szaktudást igényel.

A szervezetek hatékony vezetése és rendeltetés szerinti működtetése csak a szükséges információ birtokában valósítható meg. Jelentős anyagi és erkölcsi károkat okozhat, ha az információ nem hozzáférhető, megsérül, vagy illetéktelen kezekbe jut, ezért kiemelten fontos feladat egy **informatikai biztonsági irányítási rendszer működtetése.**

Információs rendszereink és hálózataink egyre gyakrabban érintettek különböző forrásból származó biztonsági fenyegetésekkel, többek között a számítógépes csalással és a bizalmas információk illetéktelen megszerzési törekvéssel szemben. A szándékos károkozások technikai lehetőségeinek széles skálája áll a rosszindulatú támadók rendelkezésére. Ismeretes, hogy a védelmi rendszerek fejlődésével – annak ellenére, hogy a támadó rendszerek kifejlesztése egyre több szaktudást igényel – jelentős károkat okozó támadások végrehajtása minimális felkészültséggel is eredményt hozhat, mivel a támadó rendszerek (hacker- és kémprogramok, vírusok, …) jelentős eszközparkja az interneten szabadon hozzáférhető. Ezért a szervezeti szinten megtett védelmi intézkedések hatékonysága érdekében szükség van az **informatikai termékekre és rendszerekre előírt technológiai biztonsági követelmények**re**,** valamint **az ezek teljesítését igazoló garanciák**ra is.

A fentieknek megfelelően az informatikai biztonság közvetlenül és alapvetően függ:

- mind az informatikai rendszert üzemeltető szervezet folyamataitól, biztonságot menedzselő szervezeti struktúrájától, hozzáértő humán erőforrásaitól, szabályozási rendszerszerétől, a szabályok betartásának ellenőrzésétől;

- mind a szoftver és hardver termékek, valamint az ezekből integrált komplex informatikai rendszerek és alkalmazások biztonsági megfelelőségétől;
- valamint e két terület egymásra ható kapcsolatától.

A Miniszterelnöki Hivatal Elektronikuskormányzat-központ megrendelésére elkészült a Magyar Informatikai Biztonsági Ajánlások (MIBA) című ajánlássorozat. A MIBA fő célja, hogy biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő.

A nemzetközi szabványokhoz és ajánlásokhoz igazodva a MIBA három fő részből áll:

- 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.

Ez a dokumentum a MIBIK ajánlást tartalmazza.

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)[1]**,** amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelményei (IBIK), amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányításának Vizsgálata (IBIV), amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

[1] előkészületben!

2. A MIBIK CÉLJA ÉS CÉLKÖZÖNSÉGE

2.1. A MIBIK CÉLJA

A MIBIK célja az informatikai biztonság szervezeti szintű kezeléséhez nemzetközi szabványokhoz (elsősorban az ISO/IEC 27001, 27002) és módszertanok és ajánlásokhoz igazodó hazai előírások biztosítása az egységes elvárásokon alapuló informatikai biztonságának megteremtéséhez.

Informatikai irányítási oldalról a MIBIK segítséget ad az informatikai rendszer-menedzselés biztonságos kialakításához, de ezen túlmenően ennek értékeléséhez is, akár belső, a szervezet által végzett értékelés útján, akár feljogosított külső értékelő szervezet igénybe vételével.

2.2 AZ AJÁNLÁS CÉLKÖZÖNSÉGE

A MIBIK ajánlásai egyrészt az informatikai rendszerek kialakításáért és működtetéséért felelős vezetők és szakemberek munkáját igyekszik segíteni, akiknek mind az új informatikai rendszerek kialakításánál, mind a már működő rendszerek megújítása, fejlesztése során az szervezeti szintű biztonsági szempontokat figyelembe kell venni.

Az ajánlás másik célközönsége az informatikai rendszerek vizsgálatát, auditálását végző belső és külső szakemberek.

3. A MIBIK RÉSZEI ÉS ALKALMAZÁSUK

Az információvédelem hatékonyabbá tétele érdekében szükség van a nemzeti, NATO és EU követelmények és feladatok szakmailag egységes kezelésére, a jelenlegi helyzet áttekintése alapján jogszabályi szintű elektronikus információvédelmi szabályozás kiadására, ennek bevezetése érdekében a szervezeti struktúrát érintő változtatásokra, a bevezetés lehetséges ütemezésére, valamint a személyzet felkészítésére vonatkozó feladatokra, amelyek bizalmat teremthetnek a különböző szervezetek között az informatikai rendszerek biztonságát illetően.

A fentieket figyelembe véve a szervezeti szintű informatikai biztonság követelményei és a vizsgálat rendje az I**SO/IEC 27001:2005**, **ISO/IEC 27002:2005** nemzetközi szabványok alapján, az **ISO/IEC TR 13335** szabvány, továbbá a **NATO** (**C-M(2002)49)** és az **Európai Unió** (**2001/264/EK**) releváns szabályozásai figyelembe vételével készültek.

Az ISO/IEC 27000 szabványok nem csak azért kiemelt fontosságú, mert a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelményeket és védelmi intézkedéseket tartalmazzák, de a különböző nemzeti dokumentumok közül ez vált nemzetközi szabvánnyá, és emellett a „de facto" nemzetközi szabvánnyá vált ITIL is ezt használja hivatkozási alapként. A szabványsorozatot – bár kritikák is érik – a világ, és különösen az Európai Unió mind több országában fogadják el a különböző szervezetek informatikai rendszerük biztonságának alapjaként.

3.1. INFORMATIKAI BIZTONSÁG IRÁNYÍTÁSI RENDSZER (IBIR)

A jól irányított informatikai biztonság a sikeres üzleti tevékenység egyik alapfeltétele. Egyetlen szervezet sem tud napjainkban sikeres lenni informatikai rendszereinek biztonsága nélkül.

Az **Informatikai Biztonsági Irányítási Rendszer**[2] **(IBIR)** egy általános irányítási rendszer, amely megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja a szervezet informatikai biztonságát. Az irányítási rendszer magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat.

[2] Information Security Management System – **ISMS**

Az IBIR a szervezet működési és üzleti kultúrájának szerves része kell, hogy legyen. A technikai megoldásokkal szemben ez elsődlegesen vezetői kérdés, bár vannak nem elhanyagolható technikai problémák is, különösen az informatika használatától való általános függőség.

3.2. INFORMATIKAI BIZTONSÁG IRÁNYÍTÁSI KÖVETELMÉNYEK (IBIK)

Az **Informatikai Biztonság Irányítási Követelmények** (**IBIK**) azoknak ad segítséget az informatikai biztonság szervezeti szintű kezeléséhez, akik saját szervezetükben a biztonság kezdeményezéséért, megvalósításáért és megtartásáért felelnek. A követelményrendszer átfogó tájékoztatást ad a szervezetek vezetésének és szakembereinek az informatikai biztonsággal kapcsolatos követelményekről.

Az IBIK célja a szervezetek részére egységes elveken nyugvó, a nemzetközi szabványokhoz és ajánlásokhoz igazodó olyan hazai előírások biztosítása az informatikai biztonságának megteremtéséhez. Az IBIK szerkezetében pontosan követi az ISO/IEC 27002:2005 nemzetközi szabványét, és tartalmában is többnyire erre épül, a már fent említett további anyagok felhasználásával. Ezzel a megoldással azt biztonság alapelvet követi, miszerint a védelmi intézkedéseknek a rendszer összes elemére ki kell, hogy terjednek (teljes körűség), és valamennyi releváns fenyegetést figyelembe kell venniük (zártság).

Az IBIK alapján elkészíthetők az informatikai biztonság alapdokumentumai (az informatikai biztonságpolitika, az informatikai biztonsági stratégia és az Informatikai Biztonsági Szabályzat), segítséget ad a biztonságos működéshez szükséges szervezeti struktúra, a személyi, a fizikai és az elektronikus információvédelem kialakításához.

3.3. INFORMATIKAI BIZTONSÁG IRÁNYÍTÁSÁNAK VIZSGÁLATA (IBIV)

Az **Informatikai Biztonság Irányításának Vizsgálata** (**IBIV**) – módszertan, a szervezetek vezetése és belső ellenőrző szervei által végrehajtott ellenőrzések mellett a 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.

Az IBIV tartalmi felépítése:

1. Az Informatikai Biztonság Irányítási Rendszer folyamatainak vizsgálata

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[3] és a FIPS 199[4] dokumentumokon alapuló módszertan. Ez a módszertan viszonylag egyszerű, kis idő- és erőforrás igényű kockázatbecslést tesz lehetővé.

A másik bemutatott eljárásrend egy CRAMM[5] alapú módszertan, amely MeH ITB 8. számú ajánlása (Informatikai biztonsági módszertani kézikönyv) alapján, annak aktualizálásával készült kockázatelemzési módszertan. A CRAMM módszertan egy

[3] NIST Special Publication 800-30, *Risk Management Guide*, 2001 – Kockázatkezelési Útmutató. NIST – National Institute of Standard and Technology, USA

[4] FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*, 2004 – . FIPS – Federal Information Processing Standards Publication, USA

[5] *CCTA Risk Analysis and Management Method* – CCTA Kockázatelemzési és Kezelési Módszertan. CCTA – Central Computer and Telecommunications Agency (Központi Számítógép és Távközlési Ügynökség)

részletes, az egyes fenyegetések kockázatait feltáró eljárás, azonban idő- és erőforrás igénye nagy – ezért költséges.

4. AJÁNLÁS A MIBIK FELHASZNÁLÁSÁRA

A MIBIK keretében kidolgozásra került az informatikai biztonság irányításának, követelményeinek és vizsgálatának hazai keretrendszere, amely az ISO/IEC 27000 szabványsorozatra épül.

Jelen ajánlás az alábbi, a MIBIK keretén belül kidolgozott dokumentumokra épül:

A dokumentum címe	A dokumentum tartalma
1. számú kiadvány: **Informatikai Biztonsági Irányítási Rendszer**[6] **(IBIR)**	Egy általánosan használható irányítási rendszer, amely megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja a szervezet informatikai biztonságát. Az irányítási rendszer magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat.
2. számú kiadvány: **Informatikai Biztonság Irányítási Követelményei** (**IBIK**)	Egységes elveken nyugvó, a nemzetközi szabványokhoz és ajánlásokhoz igazodó olyan hazai előírások biztosítása az informatikai biztonságának megteremtéséhez. Az IBIK alapján elkészíthetők az informatikai biztonság alapdokumentumai (az informatikai biztonságpolitika, az informatikai biztonsági stratégia és az Informatikai Biztonsági Szabályzat), segítséget ad a biztonságos működéshez szükséges szervezeti struktúra, a személyi, a fizikai és az elektronikus információvédelem kialakításához.
3. számú kiadvány: **Informatikai Biztonság Irányításának Vizsgálata** (**IBIV**)	Vizsgálati módszertan a szervezetek vezetése és belső ellenőrző szervei által végrehajtott informatikai biztonsági ellenőrzésekhez, belső auditokhoz, amellyel a szervezet vezetése bizonyosságot szerezhet arról, hogy a szervezet informatikai rendszere kielégíti saját biztonsági céljait. Segítséget nyújt az ISO/IEC 27001:2005 szabványnak való megfelelést bizonyító audit megrendeléséhez, elvégzéséhez és elfogadásához.

[6] előkészületben

FELHASZNÁLT AJÁNLÁSOK ÉS SZABVÁNYOK

[1] Az Európai Unió Tanácsának Biztonsági Szabályzata (2001/264/EK)

[2] ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

[3] ISO/IEC TR 13335-2:1997 Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security

[4] ISO/IEC TR 13335-3:1998 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security

[5] ISO/IEC TR 13335-4:2000 Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards

[6] ISO/IEC TR 13335-5:2001 Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security

[7] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[8] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management

[9] ISO/IEC 27006:2007 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

[10] ISO/IEC 20000-1:2005 Information technology – Service management – Part 1: Specification

[11] ISO/IEC 20000-2:2005 Information technology – Service management – Part 2: Code of practice

[12] Control Objectives for Information and related Technology (COBIT), http://www.isaca.org/cobit