ROBOTHADVISELÉS 2010

ADATBÁZISOK BIZTONSÁGÁNAK KEZELÉSE A KÖZIGAZGATÁSBAN

Fleiner Rita

ZMNE KMDI doktorandusz hallgató

Muha Lajos PhD, CISM

tanszékvezető főiskolai tanár

ZMNE BJKMK IHI Informatikai Tanszék

Miért kell?

Lényeges kérdés az adatbázis-biztonság megvalósítása és ennek szabályozása, támogatása.

A KIB 25. és 28. ajánlások mellett szükség van az informatika egyes részterületeinek védelmét is elősegíteni, hasonlóan az USA DoD részletes szabályozó dokumentumokaihoz, különös tekintettel az Adatbázis-biztonság Technikai Megvalósítási Útmutatóra.

Hazai szabályozás

A Magyar Informatikai Biztonsági Ajánlás, a KIB 25. és a 28. számú ajánlás nemzetközi szabványok alapján készült.

KIB 25. számú ajánlás

MIBA:

- MIBIK
- MIBÉTS
- IBIX

MIBIK

A Magyar Informatikai Biztonság Irányítási Keretrendszere (MIBIK)

Az ISO 27000, az ISO/IEC TR 13335 szabványok, továbbá a *Security within the North Atlantic Treaty Organisation* és az Európai Unió (*Európai Unió Tanácsának Biztonsági Szabályzata* figyelembe vételével készült.

25/1-1. IBIR

Az Informatikai Biztonsági Irányítási Rendszer a **TVEB** (PDCA = Plan-Do-Check-Act, Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás) modellen alapul. Ezek a folyamatok lefedik a teljes tevékenységi ciklust, megcélozva az effektív informatikai biztonság irányítását egy folytonos fejlesztési programon keresztül.

25/1-2 IBIK

Az Informatikai Biztonsági Irányítási Követelmények alapját az ISO/IEC 27002:2005, az ISO/IEC TR 13335 nemzetközi szabványok, továbbá a NATO és az Európai Unió releváns szabályozásai képezik.

25/1-3 IBIV

Az Informatikai Biztonság Irányításának Vizsgálata c. vizsgálati módszertan alapját a MeH ITB 8. számú ajánlás, a BS 7799-2:2002 szabvány, és az ehhez kapcsolódó PD 3001 – PD 3005 munkadokumentumok képzik, továbbá az IFIP 199/200 (USA) előírások.

MIBÉTS

Magyar Informatika Biztonság Értékelési és Tanúsítási Séma

A Common Critéria egyezményhez (2003. október) való csatlakozás után kezdődött meg egy magyar „lite CC” kidolgozása

Adatbázis-biztonság?

Az Informatikai Biztonsági Szabályzatokban lehetlenne helye az adatbázis-biztonságnak, de ehhez nincs segítség, „Útmutató”.

Az amerikai modell

A USA DoD a haderő informatikai rendszerei adatbázisainak védelme érdekében adatbázis-biztonság megvalósítását szabályozó dokumentumokat dolgozott ki. A dokumentumok nyilvánosak és bármely szervezet számára hasznosíthatóak, így a civil szféra is profitál belőle.

Szabályozsi struktúra

Az adatbázis-biztonsággal foglalkozó szabályozás egy nagyobb egységnek, az **Informatikai Védelmi Direktívának** és az erre épülő **Informatikai Védelmi Megvalósítási Utasításnak** a része.

Célok alapján!

Meghatározzák az informatikai biztonság alapvető szintjét, a megvalósítandó vezetési célok együttese formájában.

Az előírt vezetési célok a rendszerek működésbiztonsági kategóriáitól és bizalmassági szintjeitől függően kerülnek meghatározásra.

Működésbiztonság

A **működésbiztonsági kategória** az informatikai rendszerek által kezelt információknak a DoD célkitűzéseinek, különösen a harci küldetéseknek megvalósításában betöltött jelentőségét tükrözi. A szabályozóban három működésbiztonsági kategória van meghatározva.

bizalmasság

Az informatikai rendszerek elfogadható hozzáférési követelményeinek (személyi biztonsági ellenőrzések és háttérvizsgálatok, hozzáférési engedélyek, „tudnia-kell” szabályozások, összekapcsolási ellenőrzések és engedélyek) és felhasználói hozzáférési módszereinek (intranet, Internet, vezeték nélküli kapcsolat) meghatározására szolgál.

Biztonsági területek

1. Biztonság tervezése és konfigurálása
2. Azonosítás és hitelesítés
3. Alrendszer és eszközrendszer
4. Alrendszer határvédelem
5. Fizikai és környezeti biztonság
6. Személyi biztonság
7. Működésfolytonosság
8. Sebezhetőség és incidenskezelés

DBS Technikai Megvalósítási Útmutató

Az adatbázis-kezelő rendszerek biztonságára vonatkozóan nyújt általános útmutatást gyártófüggetlen és a DoD informatikai rendszerének részét képező adatbázis rendszerekre fogalmaz meg kötelezően betartandó biztonsági követelményeket.

Az adatbázis-biztonság területei

1. Biztonság tervezése és konfigurálása
2. Azonosítás és hitelesítés
3. Alrendszer és eszközrendszer
4. Alrendszer határvédelme
5. Működésfolytonosság
6. Sebezhetőség és incidenskezelés.

Biztonsági szerepkörök

1. informatikai biztonsági menedzser
2. informatikai biztonsági munkatárs
3. adatbázis adminisztrátor
4. adatbázis-szerver operációs rendszer adminisztrátor

Sérülékenységi kategória 1.

olyan sérülékenységet jelent, ami a támadónak közvetlen hozzáférést ad az adatbázis rendszerhez, ott superuser hozzáférést eredményez

Sérülékenységi kategória 2.

olyan sérülékenységet jelent, ami olyan információt nyújt a támadó számára, ami nagy valószínűséggel az adatbázis rendszerhez történő hozzáférés megszerzéséhez vezethet

Sérülékenységi kategória 3.

olyan sérülékenységet jelent, ami olyan információt nyújt a támadó számára, ami az adatbázis rendszer megsértésének lehetőségét hordozza magában.

Adatbázis-biztonsági Ellenőrző Lista

GYÁRTÓ SPECIFIKUS!

Az Útmutató általános követelményeihez az egyes adatbázis-kezelőrendszerektől (Oracle, MS SQL, DB2) függő, konkrét követelmények, továbbá egy platform független követelménylista.

Megvalósítás

Az adatbázis rendszerek automatikusan megvalósítható biztonsági auditját szkriptek segítségével is támogatják.

Csak a DoD szervei számára elérhetőek!

Javaslat

A jelenleginél szigorúbb és részletesebb hazai központi szabályozás szükséges az informatika egyes részterületeinek védelme tekintetében (különös tekintettel a működés kritikus területeken), ezen belül az adatbázis rendszerek védelmére.
Ehhez egy hazai ***Adatbázis Biztonsági Útmutató***ra lenne szükség!

Adatbázis-kezelő rendszer

- Adatbázis-kezelő rendszer konfigurációs követelményei
- Operációs rendszer biztonsága
- Hálózati biztonság
- Adatbázist elérő alkalmazások biztonsági beállításai

Operációs rendszer biztonsága

- Adatbázis-kezelő rendszer program könyvtárának és fájljainak védelme
- Adatbázis adatfájljainak védelme
- Adatbázis rendszerrel kapcsolatos operációs rendszer szintű felhasználók beállításai

Hálózati biztonság

- Listener védelme
- Port védelem
- Az adatbázis-kezelő rendszer külső interfészeinek és ezeken áramló információknak a védelme
- Külső objektumok elérése és külső eljáráshívás
- Tükrözés, elosztott rendszerek, database link
- Távoli hozzáférés adminisztrációs feladatok elvégzésekor

Az adatbázisban tárolt adatok biztonsága

- Adatbázis objektumok védelme hozzáférés szabályozással
- Adatbázis szerepkörök
- Adatok védelme rejtjelzéssel
  - Hálózaton
  - Adatbázisban

Adatbázis objektumok védelme

- Általános elvek
- Objektum privilégiumok
- Rendszer privilégiumok

Adatbázis szerepkörök

- Adatbázis adminisztrátori szerepkör
- Alkalmazás fejlesztői szerepkör
- Adatbázis alkalmazás felhasználói szerepkör
- Adatbázis alkalmazás adminisztrátori szerepkör

Működtetési folyamatok, eljárások

- Ügyrendi, biztonsági és egyéb eljárások szabályzatok
- Adatbázis-kezelő rendszer telepítése és biztonsági frissítése
- Felhasználók azonosítása, hitelesítése, bejelentkezése
- Adatbázis audit, logelemzés
- Éles és teszt környezetek szétválasztása
- Adatbázismentés és helyreállítás

Adatbázis-kezelő telepítése, frissítése

- Adatbázis-kezelő rendszer telepítésének és frissítésének tesztelése
- Az adatbázis-kezelő rendszer frissítése
- Az adatbázis-kezelő rendszer elkülönítése, a nem használt komponensek eltávolítása

Felhasználók azonosítása, hitelesítése

- Adatbázis felhasználók
- Csoportos azonosítás és hitelesítés
- Egyéni azonosítás és hitelesítés
- Inaktív felhasználók
- Jelszavak tárolása és tulajdonságai
- Tokenekre és tanúsítványokra vonatkozó szabványok
- Adatbázis rendszerekbe történő belépések

Adatbázis audit, logelemzés

- Általános követelmények
- Az audit tartalma
- Audit nyomvonal, monitorozás, elemzés és jelentés

ROBOTHADVISELÉS 2010

Köszönöm a figyelmet!

Fleiner Rita

Muha Lajos PhD, CISM