TANÚSÍTÁSI JELENTÉS

az

ELEKTRONIKUS BESZÁMOLÓ RENDSZER

elektronikus közszolgáltatás biztonságáról szóló 223/2009 (X. 14.) Korm. Rendeletnek megfelelőségi vizsgálatáról

HUNG-TJ-223-01/2011

Verzió: 1.0
Fájl: **HUNG-TJ-223-01/2011**_v1.0.doc
Minősítés: Nyilvános

Oldalak:

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2011.11.15.	A szerkezet felállítása
v0.9	2011.12.12.	A tanúsítás eredményeit tartalmazó teljes változat
v1.0	**2011.08.15**	**Végleges verzió**

A tanúsítási jelentést készítette:

Sillye Ferenc
Hunguard Kft.
Tanúsítási divízió

A tanúsítási jelentést ellenőrizte:

Staub Klára
Hunguard Kft.
Minőségbiztosítási vezető

Tartalomjegyzék

1. A tanúsítás (és az értékelés, amelyen a tanúsítás alapul) jellemzői

Azonosító adatok

A rendszer elnevezése:	Elektronikus beszámoló rendszer (eBESZ rendszer)
Az IBSZ kiadási dátuma:	
A technológiai értékelés alapja:	2011. 09. 24-i állapot
Rendszer integrátor:	Atigris Informatika Zrt.
Rendszerműködtető:	Közigazgatási és Igazságügyi Minisztérium
Rendszerüzemeltető:	Közigazgatási és Igazságügyi Minisztérium
Tanúsító:	HunGuard Kft.

A tanúsítás tárgya, a rendszer biztonsági környezete és határai

A tanúsítás tárgya az eBESZ rendszer, amely egy elektronikus közszolgáltatást megvalósító informatikai rendszer.

A vizsgálandó rendszer környezetét, funkcióit és határait az *Elektronikus beszámoló rendszer - rendszerbiztonsági előirányzat* (SST: System Security Target) [D3] dokumentum részletesen azonosítja.

1.2.1 Az eBESZ rendszer szolgáltatásai

Az eBESZ rendszer két fő közszolgáltatása az alábbi:

- **Beküldés**: Kettős könyvvitelt vezető vállalkozók (az adózás rendjéről szóló 2003. évi XCII. törvény 7. §-ának (2) bekezdése szerinti) képviselői számára biztosítja, hogy eleget tehessenek a számvitelről szóló 2000. évi C. törvényben meghatározott, éves beszámoló letétbe helyezésére és közzétételére vonatkozó kötelezettségüknek. Ezen ügyfeleknek (a továbbiakban **beküldők**) az eBESZ rendszer lehetővé teszi, hogy a kormányzati portál útján a céginformációs szolgálatnak elektronikusan beküldhessék a cégükre vonatkozó mérleget, eredmény-kimutatást és a jogszabály által előírt egyéb kötelezően benyújtandó céges dokumentumokat (pl. kiegészítő melléklet, könyvvizsgálói jelentés), a [2] törvény szerinti elektronikus űrlappal együtt.
- **Nyilvános lekérdezés**: Bárki számára biztosítja, hogy a közzététel céljából megküldött beszámolókat haladéktalanul és ingyenesen megismerhesse. Ezen ügyfelek (a továbbiakban **lekérdezők**) az eBESZ rendszer honlapján cégnév, cégjegyzékszám vagy adószám alapján megkereshetik és megtekinthetik a beszámolókat.

Az eBESZ rendszer két kiegészítő közszolgáltatása az alábbi:

- **Letöltés**: Bárki (a továbbiakban **letöltők**) számára biztosítja a szolgáltatások igénybe vételéhez szükséges tájékoztató és egyéb nyilvános információk (Nyomtatvány kitöltő program, Elektronikus űrlap, Beszámolóséma, stb.) letölthetőségét az eBESZ rendszer honlapjáról.

- **Elektronikus számla ellenőrzés**: Bárki (a továbbiakban **ellenőrzők**) számára biztosítja az eBESZ rendszer által küldött elektronikus számlák webes felületen történő ellenőrzési lehetőségét.

Az eBESZ rendszer a közszolgáltatásain kívül az alábbi háttérszolgáltatásokat is biztosítja, melyek funkcióit és rendszerkapcsolatait szintén figyelembe kell venni a biztonsági tanúsításnál:

- **Belső lekérdezés**: Az eBESZ rendszert működtető KIM egyes munkatársai (a továbbiakban **belső felhasználók**) számára egy külön alkalmazáson keresztül speciális lekérdezési lehetőséget biztosít az adatbázisba szervezett cégadatokról.
- **Zárt külső lekérdezés**: A [2] törvény által meghatározott szervek/szervezetek az eBESZ rendszert működtető KIM egyes munkatársainak (a továbbiakban **külső felhasználók**) számára egy külön alkalmazáson keresztül speciális lekérdezési lehetőséget biztosít az adatbázisba szervezett cégadatokról.
- **NAV kapcsolat**: Az eBESZ a fogadott űrlapok és csatolmányok egy részét továbbítja a NAV informatikai rendszere számára, illetve fogadja és feldolgozza a válaszokat.
- **CKT kapcsolat**: Az eBESZ számlázási adatokat továbbít a Cégközzétételi rendszer számára, illetve fogadja az elkészült elektronikusan aláírt számlákat és az ezekhez tartozó kiegészítő adatokat.
- **Microsec kapcsolat**: 2001-2008 közötti beszámolókra vonatkozó kérésekre az eBESZ saját adatbázisából megadja a választ.

1.2.2 Az informatikai rendszer főbb jellemzői

Az informatikai rendszer jól dokumentált, a hatalmas számú dokumentációja a biztonsági előirányzatban került részletesen összegzésre. A legfontosabb elemek tanúsítási szempontból:

- Az eBESZ rendszer két központi telephellyel rendelkezik, melyek védett (VPN) és nagysebességű (300 Mbps) kapcsolattal folyamatos összeköttetésben állnak egymással;
- Mindkét telephelyen nagy számban kereskedelmi termékek a rendszerhez fejlesztett alkalmazások, szolgáltatások integrált rendszere működik (nagy teljesítményű hardver elemek: szerverek, mentési rendszerek stb., szoftverek: operációs rendszerek, adatbázis-kezelők, vírusvédelmi és tűzfal rendszerek, felügyeleti rendszer stb.).

1.2.3 Az eBESZ rendszer legfontosabb biztonsági tulajdonságai

A biztonsági probléma leírása első lépésben az alábbiak meghatározásán alapul:

- Azon **fenyegetések**, melyeket a rendszernek ki kel védeni,
- Azon **szervezeti biztonsági szabályok**, melyeket a rendszernek érvényre kell juttatnia,
- A rendszer üzemeltetési környezetére vonatkozó (fizikai, személyi és kapcsolódási) **feltételezések**, melyek teljesülésére a rendszer építhet.

Az eBESZ rendszer *biztonsági céljai* teljes mértékben levezethetők jogszabályban megfogalmazott szervezeti biztonsági szabályokból és üzemeltetési környezetre vonatkozó

feltételezésekből. Ezért az SST *fenyegetések*et nem fogalmaz meg (a jogszabályok a releváns fenyegetések felmérése alapján fogalmazta meg kötelező elvárásait).

> Megjegyzés: Ugyanakkor az eBESZ rendszer Rendszerszintű Informatikai Biztonsági Szabályzat (eBESZ-RIBSZ) *4.2 Biztonsági fenyegetések* c. fejezete és a kapcsolódó *M-3 Biztonsági fenyegetések* c. melléklete ismertetik a rendszerre érvényes, különböző (emberi és természeti eredetű, illetve műszaki jelegű) fenyegetéseket első sorban a rendszer külső és belső felhasználói számára.

Az SST 3.1 alfejezete a jogszabályokban meghatározott elvárásokat tükröző szervezeti biztonsági *szabályok*at, a 3.2 alfejezete pedig az eBESZ rendszer üzemeltetési környezetére vonatkozó feltételezéseket határozza meg.
A biztonsági probléma meghatározásának másik lépése az eBESZ rendszer biztonsági kategorizálása, ezzel az SST 3.3 alfejezete foglalkozik.
Az SST 4. fejezete a biztonsági célokat és azok indokolását, az 5. fejezete pedig a részletes biztonsági követelményeket rendszerezi

Összefoglalva a biztonsági követelmények és intézkedések a következők:

Magas rendelkezésre állás:

- Az eBESZ rendszer valamennyi szolgáltatásához folyamatosan biztosítja a hozzáférést.

Integritás védelem:

- Az eBESZ rendszer megőrzi és megvédi az általa kezelt felhasználói adatok sértetlenségét.
- Az eBESZ rendszer garantálja a szolgáltatások nyújtásához szükséges rendszer adatok és szoftver elemek sértetlenségét.

Hozzáférés védelem:

- Az eBESZ rendszer a *Beküldés* szolgáltatás biztosításánál elfogadja a *beküldők* Ügyfélkapu által végrehajtott azonosítását és hitelesítését.
- Az eBESZ rendszer a *Nyilvános lekérdezés* szolgáltatást a *lekérdezők* azonosítása és hitelesítése nélkül biztosítja.
- Az eBESZ rendszer a *Belső lekérdezés* szolgáltatást csak azonosított és hitelesített *belső felhasználók* számára biztosítja.
- Az eBESZ rendszer a *Zárt külső lekérdezés* szolgáltatást csak azonosított és hitelesített végpontokról bejelentkezett *külső felhasználók* számára biztosítja.

Bizalmasság:

- Az eBESZ rendszerben a kezelt ügyféladatok nyilvánosak, erre vonatkozóan bizalmassági követelmény nincs.

Hitelesség:

- A jogszabályok ilyen követelményt nem fogalmaznak meg.

.

A tanúsítás jellemzése

1.3.1 A tanúsítás fókusza

A jogszabályok alapján meghatározott funkcionális elvárások (ld. fentebb) és az [1] kormányrendelet összevetése alapján a rendszer biztonsági előirányzat foglalja össze a rendszer biztonsági céljait, a biztonsági célok elérését eredményező biztonsági követelményeket, és annak meghatározását, hogy az értékelés és tanúsítás során:

- Mely követelmények teljesülését kell igazolni a szervezeti biztonsági szabályzatok és a rendszer üzemeltetésére vonatkozó biztonsági elvárások teljesülésének vizsgálatával és
- Melyeket kell igazolni az SST-ben meghatározott garanciális szinten elvégzett technológiai értékelés alapján.

1.3.2 Jogszabályi hivatkozások

[1]: 223/2009. (X. 14.) Korm. Rendelet az elektronikus közszolgáltatás biztonságáról

[2]: 2006. évi V. törvény a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról (2009. december 27-től hatályos változat)

1.3.3 Az alkalmazott értékelési és tanúsítási módszer

A jogszabályi megfelelőség tanúsítása eljárásrendjének részét képezik az alábbiak:

a) A tanúsítandó rendszerre vonatkozó jogszabályok előírásainak vizsgálata
   Ld. 1.3.2 fejezet,
b) Előzetes szervezeti- szabályozási auditálás és technológiai értékelés
   - A szolgáltató rendszer általános és biztonsági dokumentumainak vizsgálata;
   - A szükséges kiegészítő dokumentumok bekérése, illetve elkészítése: IBSZ, Kérdőív, Rendszer biztonsági előirányzat stb.
   - A szervezeti- és szabályozási audit elvégzése és értékelői tanúsítói részjelentés elkészítése.

     Megjegyzés: A szervezeti- és szabályozási audit során figyelemmel kellett lenni arra, hogy a szolgáltató szervezet nem rendelkezik az ISO/IEC 27001-es tanúsítással.

c) A Tanúsítvány kiállítása,
   amely a Tanúsítási Jelentésen alapul, és amely egységes szerkezetben tartalmazza az összes vizsgált dokumentum megfelelőségi következtetéseit, esetleges javaslatait.
d) A rendszer használati ideje során rendszeres és szükség szerint független értékelési és auditálási eljárások.

   Jelen tanúsítás során a rendszer elsődleges tanúsítása történt meg, a későbbi felülvizsgálati auditok az első audit eredményei, valamint a változások és üzemeltetési vizsgálatán fognak alapulni.

A szervezeti auditálás során az információvédelmi irányítási rendszerek (ISMS) közül az MSZ ISO/IEC 27001:2006 *Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények* c. szabvány ajánlásait vettük figyelembe.

A technológiai értékelés során a MIBÉTS 2009 /Magyar Informatikai Értékelési és Tanúsítási Séma/ módszertanát használtuk, mely a KIB (Közigazgatási Informatikai Bizottság) 25. és 28. számú ajánlásában szerepel (és amely módszertan az ISO/IEC 15408 és a Common Criteria követelményrendszer honosított verziója).

Mindkét módszertan megfelel az elektronikus közszolgáltatás biztonságáról szóló 223/2009 (X. 14.) Kormányrendelet 13.§ (2), 11. § (1), valamint 30. § (1) pontok követelményeinek, illetve az értelmező 2.§ b), c) pontjában meghatározott szabványoknak, ajánlásoknak, követelményrendszereknek.

Az alábbiakban a technológiai értékelés és tanúsítás során alkalmazott értékelési módszereket, technikákat és szabványokat dokumentáljuk.

MIBÉTS termékértékelési és tanúsítási módszertan

Az eBESZ értékelése és tanúsítása során az informatikai termékek technológia szempontú biztonsági értékelésére és tanúsítására kidolgozott MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) módszertant használtuk. A MIBÉTS módszertana néhány, a módszertan szempontjából kisebb eltéréstől eltekintve /pl. a MIBÉTS a CC EAL 1-7 szintje helyett csak a 2-4 szintekre lett honosítva, magyar akkreditáció is szerezhető a MIBÉTS-re, stb./ pontosan megfelel a Common Criteria módszertannak.

A MIBÉTS értékelési és tanúsítási módszertana a KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlásának (Az E-közigazgatási Keretrendszer követelménytár, 2009) részét képezi az alábbi címen: „Termékekre vonatkozó értékelési módszertan”, illetve „Útmutató tanúsítók számára” /ld. http://kovetelmenytar.complex.hu/.

[M1]: IT biztonsági műszaki követelmények a különböző biztonsági szintekre - Követelmény előírás (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v1.01, 2008.08.22) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M2]: Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v4 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M3]: Útmutató az IT biztonsági szintek meghatározásához (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v1.01, 2008.08.22) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

A MIBÉTS módszertana az alábbi nemzetközi mértékadó dokumentumok honosított változata (CC: [1]- [3], CEM: [4])

[CC1]: Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 1: Introduction and general model
[CC2]: Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 2: Security functional components
[CC3]: Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 3: Security assurance components
[CC4]: Common Methodology for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2)

Az [1] - [4] dokumentumokat az alábbi nemzetközi szabványként is elfogadták:

[I1]: ISO/IEC 15408-1: 2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
[I2]: ISO/IEC 15408-2: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components
[I3]: ISO/IEC 15408-3: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
[I4]: ISO/IEC 18045: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Methodology for IT Security Evaluation

A technológiai értékelés garanciaszintje **MIBÉTS kiemelt**, mely a CC (Common Criteria, MSZ ISO/IEC 15408) szerinti **EAL4**-es szintnek felel meg.

További figyelembe vett módszertani dokumentum:
[NI1]: National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, December 2007

1.3.4 A tanúsítást előkészítő értékelések mérföldkövei

A technológiai értékelés /TÉ/ előkészítési szakasz kezdési dátuma:	2011.05.11.
A TÉ előkészítési szakasz befejezési dátuma:	2011.06.18.
A TÉ szakasz kezdés dátuma:	2011.06.18.
A meglévő szabályozási dokumentumok vizsgálata	2011.07.11.
A szabályozási dokumentumok előzetes véleményezése	2011.09.05.
A TÉ értékelési szakasz befejezési dátuma:	2011.09.24.
A fejlesztés/integrálás helyszín látogatásának dátuma:	2011.08.09.
Az üzemeltetési helyszín látogatásának dátumai:	2011.06.28.
	2011.07.07.
	2011.08.23.
	2011.09.20.
A rendszer biztonsági tesztelésének dátumai:	2011.08.15.
	2011.08.23.
A behatolás tesztelés dátumai:	2011.07.01.
	2011.07.07.
Rendszer értékelési jelentés tervezet elkészítésének dátuma:	2011.10.14.
Rendszer értékelési jelentés (végleges) elkészítésének dátuma:	2011.10.31.
Az előzetes eBESZ-RIBSZ dokumentum áttekintése:	2011.11.02.
A kitöltött Kérdőív (VI-BIZT/17/6 /2011) átvétele:	2011.11.03.
A jóváhagyott eBESZ-RIBSZ dokumentum elemzése:	2011.11.10.
A szabályozási tanúsítói részjelentés (első verzió) elkészítése:	2011.11.15.
A szabályozási tanúsítói részjelentés véglegesítése:	2011.11.30.

1.3.5 A tanúsításhoz felhasznált főbb dokumentumok és megalapozó értékelési jelentések azonosítása

Főbb dokumentumok:

[D1]: **Kérdőív** A 223/2009. (X. 14.), az elektronikus közszolgáltatás biztonságáról szóló kormányrendeletnek való megfelelőség tanúsítás (VI-BIZT/17/6 /2011), aláíró: Misák István, Közigazgatási és Igazságügyi Minisztérium informatikai biztonsági vezető /79-55-130/, 2011. november 3.

[D2]: **eBESZ-RIBSZ**: A Közigazgatási és Igazságügyi Minisztérium elektronikus beszámoló rendszerének Rendszerszintű Informatikai Biztonsági Szabályzata, kiadó: Fekete Gábor, a Közigazgatási és Igazságügyi Minisztérium e-Közigazgatásért Felelős Helyettes Államtitkár, 2011. október

[D3]: Elektronikus beszámoló rendszer - **Rendszerbiztonsági előirányzat (SST v1.0)**, Készítette: Hunguard Kft Értékelési Divízió, 2011. 12.20.

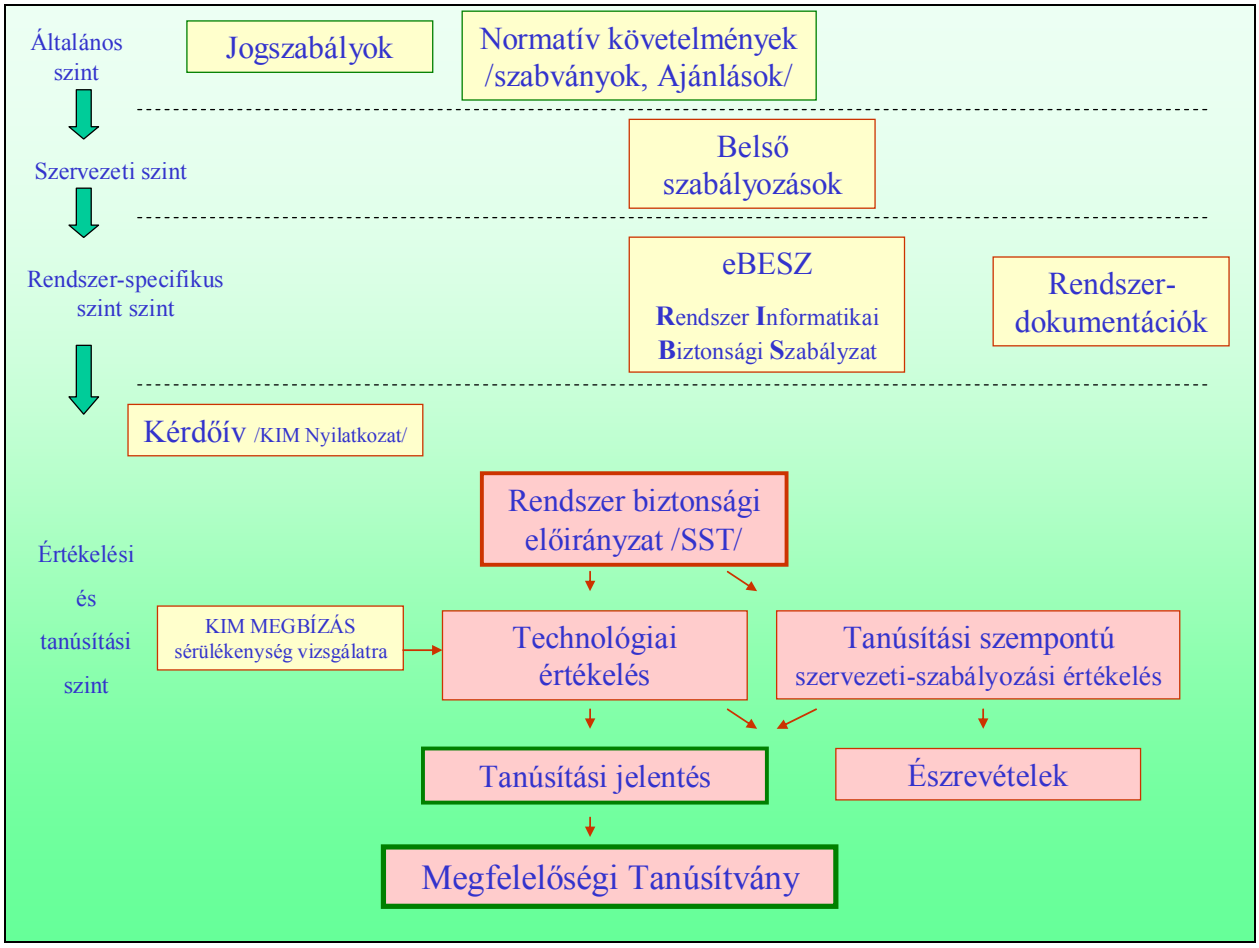
[D4]: MEGBÍZÁS /technikai sérülékenység-vizsgálathoz/, aláíró: Fekete Gábor, a Közigazgatási és Igazságügyi Minisztérium e- Közigazgatásért Felelős Helyettes Államtitkár, 2011.június 30.

Értékelési jelentések:

[É1]: ELEKTRONIKUS BESZÁMOLÓ RENDSZER **Technológiai Rendszer értékelési jelentés**

[É2]: **TANÚSÍTÓI RÉSZJELENTÉS** a Közigazgatási és Igazságügyi Minisztérium által üzemeltetett Elektronikus beszámoló Rendszer (eBESZ) az elektronikus közszolgáltatások biztonságáról szóló 223/2009 (X.14.) Kormányrendelet szabályozási és minőségirányítási követelményeinek megfelelőségéről

A tanúsítási folyamatot és felhasznált főbb dokumentumokat a következő szemlélteti:



Megjegyzések az ábrához:

- zöld kerettel a nyilvános dokumentumokat jelöltük
- sárga alapon a tanúsításhoz külső forrásból kapott dokumentumokat jelöltük;
- a felsőbb szinteken található dokumentumok felhasználásra kerültek az alsóbb szintek dokumentumaiban.

2. Az értékelési jelentések főbb megállapításai

2.1 A technológiai értékelés főbb megállapításai

A technológiai rendszer-értékelés az SST-ben részletesen meghatározott technológiai biztonsági követelmények / **Azonosítás és hitelesítés, Hozzáférés ellenőrzés, Naplózás és elszámoltathatóság, Rendszer és kommunikáció védelem, Rendszer és információ sértetlenség, Folyamatos működés (üzletmenet folytonosság), Konfigurációkezelés /** érvényre juttatását értékeli az SST-ben meghatározott garanciális szinten.

A rendszer értékelés keretében elvégzett fő feladat-csoportok az alábbiak voltak:

a) a rendszer biztonsági előirányzat értékelése,
b) a rendszer biztonsági architektúrájának értékelése,
c) a rendszer telepítési és üzemeltetési útmutatóinak a vizsgálata,
d) a rendszer konfiguráció vizsgálata,
e) a rendszer biztonsági tesztelése,
f) a rendszer sebezhetőség vizsgálata.

2.1.1 A rendszer biztonsági előirányzat értékelése

A rendszer biztonsági előirányzat (SST) értékelésének kitüntetett szerepe van, hiszen ez biztosítja a teljes rendszer-értékelés kiindulópontját.

Az SST legfontosabb célja az eBESZ rendszer megvalósított biztonsági képességeinek meghatározása. E biztonsági képességeket a rendszer adott üzemeltetési környezetében alkalmazzák a felmért kockázatok kivédésére és a megfogalmazott szervezeti biztonsági szabályzatok érvényre juttatására, annak érdekében, hogy a maradványkockázat elfogadható szintjét érjék el.

Az értékelés főbb megállapításai:

- Az SST felépítése megfelel az elvárásoknak:
- Az SST tartalma megfelel az elvárásoknak:

Az SST értékelése alapján megállapítható, hogy az a jogszabályi elvárásokból ([1] és [2]) **egy belső ellentmondásoktól mentes, teljes és egymást erősítő biztonsági követelményrendszert határoz meg, egyúttal magas szinten át is tekinti, hogy az eBESZ rendszer hogyan teljesíti a biztonsági követelményeket.**

2.1.2 Az eBESZ rendszer biztonsági architektúrájának értékelése

Az eBESZ rendszer különböző tervezési dokumentációinak átvizsgálása az értékelt rendszer biztonsági szerkezetének értékelése mellett a tesztelés és a sebezhetőség vizsgálat előkészítéseként is szolgált.

A tervezési dokumentációk elemzése kiemelten az alábbiakra koncentrált:

- a rendszer integrátor úgy tervezte és úgy valósította-e meg a rendszer biztonsági funkcionalitását, hogy az képes legyen megvédeni magát a nem-megbízható aktív egyedek hamisításaitól (***önvédelem***), illetve

- a rendszer integrátor úgy tervezte és úgy valósította-e meg az eBESZ rendszert, hogy annak biztonsági funkcionalitását ne lehessen megkerülni (***megkerülhetetlenség***).

A tervezési dokumentációk értékelése alapján összességében megállapítható, hogy az eBESZ rendszer egy jól átgondolt, a biztonságot kitüntetett szempontként kezelt fejlesztés, illetve integrálás eredménye.

2.1.3 A rendszer telepítési, konfigurálási és üzemeltetési útmutatóinak a vizsgálata

Az értékelés megállapította, hogy útmutató dokumentációk egyaránt tartalmazzák az alábbiakat:

- a telepítéshez szükséges előfeltételek,
- a telepítés lépései,
- a telepítés sikerességének ellenőrzési módja,
- az elvárt eredmények,
- nem várt események bekövetkezése esetén a visszaállás lépései.

A telepítési, konfigurálási és üzemeltetési dokumentációk értékelésének eredménye, hogy az eBESZ rendszer biztonságosan lett kialakítva és konfigurálva, valamint biztonságosan üzemeltethető.

2.1.4 A rendszer biztonsági tesztelése

Az értékelés elemezte a különböző alrendszerekre vonatkozó

- Tesztelési koncepciókat, teszttterveket,
- A végrehajtott tesztelések dokumentációit.

Az értékelők pozitívan értékelték a rendszer integrátor tesztelési munkáját.

Az értékelők független, saját vizsgálatokkal igazolták biztonsági funkciók helyes működését.

A biztonsági tesztelés értékelése az alábbiakat állapította meg:

- **A rendszer integrátor tesztelte az eBESZ biztonsági funkcionalitását.**
- **A tesztelés érintette a rendszer összes külső interfészét és összes alrendszerét.**
- **A teszteredmények és az éles üzemeltetés eredményei megfelelnek az elvárásoknak.**
- **Az értékelő részleges, független teszteléssel megerősítette a helyes működést.**

2.1.5 A rendszer sebezhetőség vizsgálata

Az eBESZ rendszerre vonatkozó sebezhetőség vizsgálatokat három egymástól elkülönülő, egymásra épülő ütemben hajtotta végre az értékelő:

- 1. ütem: külső, internetes munkaállomásról
- 2. ütem: az eBESZ rendszert működtető tartományon belül

- 3. ütem: a KIM informatikai hálózatán belül, de az eBESZ rendszert működtető tartományon kívül eső hálózati szegmensből

A sebezhetőség-vizsgálat kockázatokat nem tárt fel.

A vizsgálatok és eredmények részletesen dokumentálásra kerültek az „ELEKTRONIKUS BESZÁMOLÓ RENDSZER Technológiai Rendszer értékelési jelentés" c. dokumentumban /ld. [É1]/.

A sebezhetőség vizsgálatot kiegészítette a helyszíni, automatizált szoftver és hardver leltár, szoftver-sértetlenség ellenőrzése.

Az alkalmazott IT elemek helyszíni vizsgálatának fő megállapításai az alábbiak:

- **az egyes kiszolgálók csak a szükséges szoftver elemeket tartalmazzák,**
- **az aláírt szoftver elemek sértetlenek.**

2.2 A szabályozási értékelés főbb megállapításai

Az eBESZ-RIBSZ értékelése során az értékelés a kitöltött Kérdőívből indult ki (ld [D1]), majd a 223/2009 (X.14.) Kormányrendelet előírásait §-ról §-ra ellenőrizte a dokumentumokban, a rendszer üzemeltetéséről rendelkezésre álló információk (elsősorban Kérdőív, és konzultációk) alapján.

2.2.1 Az informatikai biztonság irányítása (II. Fejezet)

Megállapítás: a rendszer és szabályozása megfelel az irányítási követelményeknek.

2.2.2 A biztonságos működés alátámasztása, minőségirányítási követelmények (III. Fejezet)

A fejezet követelményeinek jelentős része a technológiai értékelés hatókörébe tartozik (pl. a folyamatok naplózása, mentési követelmények stb.), annak pozitív megállapításai egészítik ki a szabályozási értékelés megállapításait.

Megállapítás: a rendszer és szabályozása megfelel az irányítási követelményeknek.

2.2.3 Biztonsági követelmények (IV. Fejezet)

A fejezet követelményeinek jelentős része a technológiai értékelés hatókörébe tartozik (pl. hozzáférési és fizikai biztonsági követelmények stb.), vagy az adott rendszerre nem releváns (pl. az adattovábbítás bizalmasságának támogatási követelményei stb.), a technológiai értékelés pozitív megállapításai egészítik ki a szabályozási értékelés megállapításait.

Megállapítás: a rendszer és szabályozása megfelel az irányítási követelményeknek.

2.2.4 Szabályozási és ellenőrzési követelmények (V. Fejezet)

Megállapítás: a rendszer és szabályozása megfelel az V. fejezet követelményeinek.

Kiegészítés: Néhány követelmény a tanúsítás után elvégzendő feladatokra vonatkozik (pl. a tanúsítás nyilvántartási bejelentése, regisztrálása, informatikai biztonsági felügyelő tájékoztatása stb.), amelyek ellenőrzése a következő audit feladata lesz.

A szervezeti és szabályozási szempontú értékelés eredményei részletesen megtalálhatóak a „TANÚSÍTÓI RÉSZJELENTÉS a Közigazgatási és Igazságügyi Minisztérium által üzemeltetett Elektronikus beszámoló Rendszer (eBESZ) az elektronikus közszolgáltatások biztonságáról szóló 223/2009 (X.14.) Kormányrendelet szabályozási és minőségirányítási követelményeinek megfelelőségéről” c. 21. oldal terjedelmű dokumentumban /ld. [É2]/.

3 A biztonság érvényre juttatásához szükséges – rendszeren kívüli – feltételek

Az értékelések következtetései a rendszer biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak. Ezen feltételeket (melyek teljesítése nem műszaki, hanem menedzsment és üzemeltetési ellenintézkedéseket igényel, és a szabályozási értékelés a megfelelőséget megállapította) a folyamatos működtetés során biztosítani szükséges.

F1_Kockázatfelmérés
A rendszer működtetője rendszeres időnként, illetve jelentős változások alkalmával felméri a szervezeti működés során jelen lévő, a rendszer működéséből és kapcsolódó információ feldolgozó, tároló vagy átviteli műveletekből származó biztonsági kockázatokat és a rendszer értékeit.

F2_Biztonsági_értékelés_és_auditálás
A rendszer működtetője:

a) rendszeres időközönként értékeli az IT rendszer biztonsági intézkedéseit, annak megállapításához, hogy az intézkedéseket hatékonyan alkalmazzák-e;
b) intézkedési tervet készít és hajt végre a hiányosságok korrigálására, a rendszerekben meglévő sebezhetőségek csökkentésére vagy kiküszöbölésére;
c) engedélyezteti (akkreditáltatja) az informatikai rendszer működését és bármilyen rendszerkapcsolatot, kapcsolódást;
d) folyamatosan felügyeli, ellenőrizi a biztonsági intézkedések betartását a hatékonyság folytonosságának biztosítása érdekében.

F3_Fizikai_biztonság
Az eBESZ rendszer működtetője és üzemeltetője:

a) a jogosult felhasználókra korlátozza az eBESZ rendszerhez, berendezéseihez és kapcsolódó üzemeltetési környezetéhez való fizikai hozzáférést;
b) védi a fizikai létesítményt, biztosítja az eBESZ rendszerhez szükséges infrastruktúrát;
c) biztosítja az eBESZ rendszerhez szükséges háttér és kiegészítő szolgáltatásokat;
d) védi az eBESZ informatikai rendszert a környezeti veszélyektől;
e) megfelelő környezeti intézkedésekről gondoskodik az eBESZ rendszernek helyt adó létesítményekben.

F4_Adathordozók_védelme
Az eBESZ rendszer működtetője és üzemeltetője:

a) védi a rendszer papír alapú vagy digitális adathordozóin lévő információit;
b) jogosult felhasználókra korlátozza a hozzáférést a nyomtatott vagy digitális információkhoz;
c) a digitális adathordozóról biztonságosan törli a rajtuk lévő információt azok eltávolítása vagy újra használata előtt.

F5_Üzletmenet_folytonosság_tervezése
Az eBESZ rendszer működtetője és üzemeltetője terveket készít, ezeket karbantartja és hatékonyan megvalósítja a rendkívüli helyzetekre való reagálásra, a mentési műveletekre és a katasztrófák utáni helyreállításra, annak biztosítása érdekében, hogy a kritikus információs erőforrások rendelkezésre álljanak és rendkívüli helyzetekben is megvalósuljon a folyamatos működés követelménye.

F6_Reagálás_biztonsági_eseményekre
Az eBESZ rendszer működtetője és üzemeltetője

a) biztonsági események kezelésére alkalmas képességet alakít ki az eBESZ rendszerre,
b) nyomon követi, dokumentálja és jelenti az eseményeket a szervezetben erre kijelölt illetékes személynek és/vagy szervezetnek, hatóságnak.

4. Megfelelőségi összegzés

Minden informatikai rendszerben természetesen keletkeznek és maradnak is nem kivédett kockázatok a kialakítás, használat, továbbfejlesztés és üzemeltetés során.

Az informatikai biztonság az informatikai rendszer olyan – a szervezet számára kielégítő mértékű – állapota, amelyben a rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása védelme szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos /KIB 25-ös Ajánlás/.

Ennek megfelelően a fenti definícióba nem beleértendő azon kockázatokat tekintjük maradvány kockázatoknak, amely az adott rendszerben sem technológiai eszközökkel, sem szervezési, szabályozási eszközökkel nincsenek kivédve, de a veszélyek kockázatai, károkozásai, az esetleges támadók motivációi oldaláról – bár kis valószínűségű események – mégis kivédendő kockázatoknak minősíthetőek.

> A technológiai értékelés is feltárhat ilyen, ki nem védett maradvány kockázatokat.
>
> Általában a szervezet biztonságért felelős vezetőségének felelőssége, hogy milyen szintű kockázatot vállalnak fel.
>
> A döntések leggyakrabban (leírt, vagy csak átgondolt) költség-haszon elemzésen, valamint kockázatbecslésen alapulnak. /Lehet a maradványkockázatokat áthárítani is (pl. biztosításokkal), vagy tudatosan, megfelelő elemzések alapján felvállalni./

A jogszabályi előírások (pl. a 223/2009 (X.14.) kormányrendelet előírásai) már feltételezhetően egy kockázatelemzés utáni szükséges intézkedés-sorozatot írnak elő. A jogszabályi megfelelőség tanúsítása során az előírásoktól való eltérést – még kis valószínűségű, vagy kis kárértékű esetekben is - már enyhe nem megfelelőségnek kell minősíteni, amelyek ha nem nagy kockázati szintűnek is minősíthetőek, akkor is javító intézkedéseket egy soron következő változtatásig (pl. az informatikai rendszer továbbfejlesztése, a jóváhagyott szabályzatokban történő változtatás), de mindenképpen a következő audit időpontjáig célszerű megtenni.

Ilyen minőségi javító intézkedések szerepelnek „az ÉSZREVÉTELEK, Feltárt maradványkockázatok a Közigazgatási és Igazságügyi Minisztérium által üzemeltetett Elektronikus beszámoló Rendszer (eBESZ) biztonsági értékelése során” c. 7 oldal terjedelmű, nem nyilvános dokumentumban

A fenti dokumentumokban szereplő észrevételek értékelésének ellenőrzése a következő auditon kerülhet sorra.

A fent idézett észrevételek mellett is a tanúsítás megállapítása a következő:

Az eBESZ rendszer és dokumentációja megfelel a 223/2009 (X.14.) kormányrendelet előírásainak, az abban kitűzött biztonsági célok, elvárások teljesülnek, a rendszer biztonságosan üzemeltethető.

Az eBESZ rendszer 223/2009 kormányrendeletnek megfelelőségére a Tanúsítvány kiállítható.