Hunguard Kft. Tanúsítási Divízió
1123 Budapest, Kékgolyó u. 6. 5. em. 4.
Honlap: http://www.hunguard.hu
Telefon: (+36) 1 225-87-96
Telefax: (+36) 1 225-87-97
E-mail: iroda@hunguard.hu

HIVATALOS LAPKIADÁSI RENDSZER
2013. március 26-i rendszerverzió

TANÚSÍTÁSI JELENTÉS

HUNG-TJ-MIBÉTS-006-2013

Fájlnév: Hung-TJ-MIBETS-006-2013
Verzió: 1.0
Minősítés: Bizalmas
Oldalak: 16

A Tanúsítási jelentés a Hunguard Kft. Tanúsítási Divíziójának, mint a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezetnek a vizsgálatai alapján készült.

Változáskezelés

Verzió	Dátum	A változás leírása
v0.01	2013.03.07.	A szerkezet felállítása
v0.02	2013.03.22.	A tanúsítás eredményeit tartalmazó első teljes változat
v0.05	2013.03.26.	Egyeztetett változat
v1.0	**2013.03.29.**	**Végleges verzió**

A tanúsítási jelentést készítette:

dr. Szabó István
Hunguard Kft
Tanúsítási Divízió

Tartalomjegyzék

1 Összefoglaló

1.1 A tanúsítás (és az értékelés, melyen a tanúsítás alapul) jellemzői

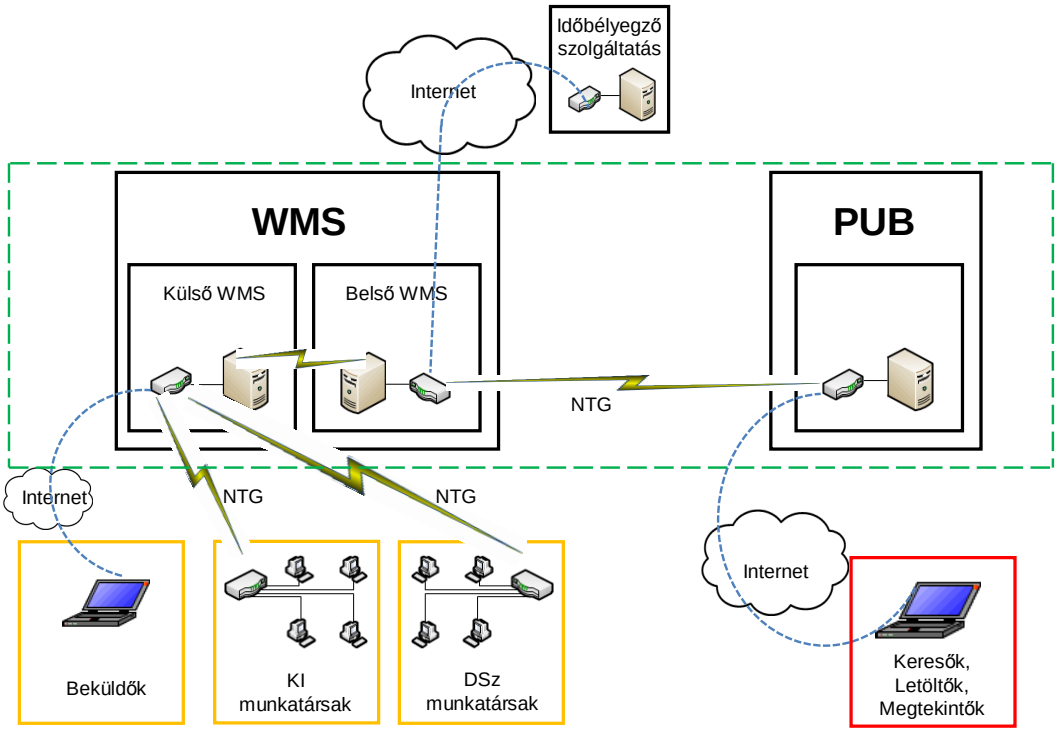
Az értékelt rendszer:	Hivatalos Lapkiadás Rendszer (rövidítve: WMS+PUB)
verziója:	(2013.03.26-án telepített rendszer)
Rendszer működtető:	KIM (Közigazgatási és Igazságügyi Minisztérium)
Rendszer üzemeltetők:	Publikációs alrendszer: KEKKH (Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala), Külső és belső WMS alrendszer: MHK (Magyar Közlöny Lap- és Könyvkiadó) A telephelyek közötti NTG hálózat: NISZ Zrt.
Rendszer értékelő:	Hunguard Kft. Értékelési Divízió
Az értékelés megkezdése:	2012.10.08.
Az értékelés lezárása:	2013.03.28.

1.2 A tanúsítás tárgya, biztonsági környezete és határai

A Hivatalos Lapkiadás Rendszer a Magyar Közlöny és a Hivatalos Értesítő (továbbiakban: hivatalos lapok) elektronikus megjelentetésének teljes munkafolyamatát támogató informatikai rendszer. A három alrendszer által támogatott teljes munkafolyamat kiterjed az alábbiakra:

- a hivatalos lapok kiadásának szerkesztési folyamatának zárt rendszerben történő elhelyezése (belső WMS alrendszer),
- a hivatalos lapok kiadásához szükséges külső kapcsolatok (külső feltöltés) lehetőségének biztosítása (külső WMS alrendszer),
- a hivatalos lapok egységes és zavartalan megjelenését támogató publikálási felület, (publikációs alrendszer),
- a rendszer adatainak mentése (a publikációs alrendszer tartalmazza az adatmentő szervert is).

Az 1. ábra a Hivatalos Lapkiadás Rendszer (WMS+PUB) három alrendszerét, külső (és legfontosabb belső) interfészeit, valamint az általuk biztosított szolgáltatások igénybe vevőit szemlélteti (az ábrán DSz a digitális szerkesztőséget, KI a Kormányiroda lapkiadással foglalkozó területét jelöli, míg NTG a Nemzeti Távközlési Gerinchálózat rövidítése).



1. ábra: Rendszer áttekintés

A belső és külső WMS alrendszerek egy telephelyen működő, tűzfallal elválasztott szeparált hálózatok.
A két WMS alrendszer, illetve a publikációs alrendszer földrajzilag is szeparált hálózatok.

A rendszer publikációs (PUB) alrendszere az alábbi közszolgáltatásokat biztosítja

1. **Keresés**: a közzétett hivatalos lapok között kereső állampolgárok számára biztosítja, hogy évszám, hónap, közlönyszám és keresett szó vagy szótöredék alapján ingyenesen megkereshessen közzétett hivatalos lapokat.
2. **Megtekintés**: a közzétett hivatalos lapokat kijelölő személyek számára biztosítja a közzétett hivatalos lapok ingyenes megtekintését a publikálási felület saját megjelenítőjén keresztül.
3. **Letöltés**: a közzétett hivatalos lapokat letöltő állampolgárok számára biztosítja a közzétett hivatalos lapok ingyenes letöltését, valamint a letöltött dokumentumok hitelességének ellenőrzési lehetőségét.

Mindhárom fenti közszolgáltatást a publikációs alrendszer biztosítja, egy hivatalos publikációs weboldal /www.magyarkozlony.hu/ böngészésén keresztül.

A rendszer több kiegészítő- és háttér szolgáltatással rendelkezik, ilyenek:

- tartalom szerkesztés;
- tartalomjegyzék készítés;
- tartalomjegyzék elfogadás;

- digitális szerkesztés;
- hitelesítés aláírással, automatikus közzététel;
- kézi közzététel;
- külső feltöltés;
- jóváhagyás; időbélyegzés;
- adatmentés.

A kiegészítő- és háttér szolgáltatások, a rendszer szereplői, az elkülönülő biztonsági tartományok részletesen ismertetésre kerülnek a Rendszer biztonsági előirányzatban /az SST-ben [D1]/ .

A tanúsítási folyamatban felhasználásra kerültek az SST-ben részletesen elemzett

- a szervezeti biztonsági szabályok;
- a rendszer üzemeltetési környezetére vonatkozó feltételezések;
- a biztonsági kategorizálás (és indokolása);
- a biztonsági célok.

2 A tanúsítás jellemzése

2.1 Az alkalmazott értékelési és tanúsítási módszer

A WMS+PUB rendszer műszaki szempontú értékelésére az [M1]-ben és [M2]-ben meghatározott, rendszerekre vonatkozó értékelési módszertant alkalmazta az akkreditált értékelő szervezet, az alábbi pontosításokkal:

- a rendszer értékelés típusa[1]: kezdeti
- a rendszer értékelés garanciaszintje[2]: MIBÉTS fokozott (SAP-F)
- a rendszer értékelés megközelítése[3]: kombinált

A fenti értékelési jellemzők részletesen kifejtésre kerültek a [D2] számú Értékelési jelentés 3. fejezetében.

Az alkalmazott módszertan szerinti Rendszer biztonsági előirányzat értékelésének fő célja annak megerősítése, hogy nincsenek következetlenségek vagy hiányosságok a biztonsági követelmények és a megvalósított intézkedések között.

A rendszer technológiai értékelése a célfeladatokra fejlesztett, továbbá a megvásárolt rendszerkomponensekből integrált, telepített, tesztműködésben vizsgált rendszer SST-ben megfogalmazott követelményeinek teljesítését vizsgálta.

A Rendszer értékelési jelentés [D2] 4. fejezete összefoglalja a legfontosabb megállapításokat az alábbi területeken:

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.

A Rendszer értékelési jelentés következtetéseket tartalmazó fejezete a Rendszer biztonsági előirányzatnak megfelelés feltételekkel való megfelelését állítja, valamint biztonságnövelő javaslatokat fogalmaz meg a maradványkockázatok csökkentésére vagy kiküszöbölésére.

A tanúsítás a MIBÉTS módszertan szerinti rendszerértékelés elvégzésére NAT-1-1578/2013 számon akkreditált Hunguard Kft. vizsgáló laboratóriuma által kiállított Rendszer értékelési jelentés megállapításain alapul.

A tanúsítás az értékelési folyamat elfogadott értékelési módszertan szerinti kontrollját biztosítja és igazolja.

Minden informatikai rendszerben természetesen maradnak nem kivédett kockázatok. A technológiai rendszerértékelés feltárta, hogy mely informatikai fenyegetettségeket védi ki műszaki biztonsági intézkedésekkel az informatikai rendszer, és milyen maradványkockázatok vannak, amelyek részben felvállalhatóak, részben menedzsment és üzemeltetési intézkedésekkel, eljárásokkal kell azokat kivédeni.

[1] A rendszer értékelés típusai: kezdeti, tervezett felülvizsgálati, rendkívüli felülvizsgálati, megismételt kezdeti.

[2] A rendszer értékelés lehetséges garanciaszintjei: MIBÉTS alap (SAP-A), MIBÉTS fokozott (SAP-F) és MIBÉTS kiemelt (SAP-K) rendszer értékelési garanciacsomag.

[3] A rendszer értékelés lehetséges megközelítés módjai: lineáris, sebezhetőség vizsgálatra koncentráló, kombinált.

3 A Hivatalos Lapkiadás Rendszer (WMS+PUB) legfontosabb biztonsági céljai és tulajdonságai

Az SST részletesen áttekinti a rendszer- és tartomány szintű fenyegetettségeket, szabályokat feltételezéseket, biztonsági kategorizálást, biztonsági célokat, funkcionális és garanciális biztonsági követelményeket, melyeknek a Hivatalos lapkiadás rendszer megfelel.

Az értékelt rendszerre vonatkozó **műszaki biztonsági célok**:

3.1 Rendszer szintű biztonsági célok

O[4].Individual accountability
Egyéni felelősségre vonhatóságot kell biztosítani a naplózott események vonatkozásában. A naplóeseményeknek tartalmazniuk kell az alábbiakat: az esemény dátuma és időpontja, az eseményért felelős entitás. A naplórekordokat védeni kell a jogosulatlan hozzáféréssel, módosítással vagy törléssel szemben abból a célból, hogy biztosítva legyen a felelősségre vonhatóság a felhasználói tevékenységekért.

O.Fault_Tolerance
A rendszer kritikus komponensei számára hibatűrő eszközöket és megoldásokat kell biztosítani a folyamatos működés fenntartása érdekében.

O.Secure_State
A folyamatos működés (rendszerhiba vagy katasztrófa következtében történő) megszakadása esetére biztosítani kell a helyreállítás lehetőségét, a biztonság megőrzése mellett.

O.Apply_Code_Fixes
A rendszer valamennyi szoftver komponensére biztosítani kell a feltárt, jogosulatlan hozzáférést lehetővé tevő biztonsági hibákat kiküszöbölő javítások beépítését.

3.2 Az 1. tartomány (PUB) biztonsági céljai

O.Confidentiality_PUB
Meg kell védeni a PUB-ban kezelt egyes felhasználói adatok (még nem közzétett, de már feltöltött hivatalos lapok) bizalmasságát.

O.Integrity_PUB
Meg kell védeni a PUB-ban kezelt felhasználói adatok (feltöltött hivatalos lapok), valamint a közszolgáltatások nyújtásához szükséges rendszer adatok és szoftver elemek sértetlenségét.

O.Availability_PUB
Biztosítani kell a Publikációs alrendszer közszolgáltatásaihoz való hozzáférést, folyamatosan (24/7/365), magas rendelkezésre állással.

[4] O: Objects for the evaluated system (az értékelt rendszerre vonatkozó biztonsági célok)

3.3 A 2. tartomány (WMS) biztonsági céljai

O.Confidentiality_WMS
Meg kell védeni a WMS-ben kezelt felhasználói adatok (még nem közzétett státuszú hivatalos lapok, illetve külső és belső ügyek) bizalmasságát, a 3. szintnek megfelelő módon.

O.Integrity_WMS
Meg kell védeni a WMS-ben kezelt felhasználói adatok (még nem közzétett státuszú hivatalos lapok, illetve külső és belső ügyek), valamint a kiegészítő szolgáltatások nyújtásához szükséges rendszer adatok és szoftver elemek sértetlenségét, a 4. szintnek megfelelő módon.

O.Availability_WMS
Biztosítani kell a belső és a külső WMS alrendszer kiegészítő szolgáltatásaihoz való hozzáférést, munkaidőben, magas rendelkezésre állással.

A Hivatalos lapkiadás rendszer **legfontosabb biztonsági tulajdonságai** a klasszikus IT biztonsági fogalmakkal:

Rendelkezésre állás

- A WMS+PUB rendszer közszolgáltatásaihoz (Keresés, Letöltés, Megtekintés) folyamatosan, magas rendelkezésre állással (24/7/365) biztosítja a hozzáférést.
- A WMS+PUB rendszer kiegészítő szolgáltatásaihoz munkaidőben, magas rendelkezésre állással biztosítja a hozzáférést.

Integritás védelem

- A WMS+PUB rendszer megőrzi és megvédi az általa kezelt felhasználói adatok (különböző státuszú hivatalos lapok, illetve ügyek) sértetlenségét.
- A WMS+PUB rendszer garantálja a szolgáltatások nyújtásához szükséges rendszer adatok és szoftver elemek sértetlenségét.

Hozzáférés védelem

- A WMS+PUB rendszer közszolgáltatásait (Keresés, Letöltés, Megtekintés) a keresők, letöltők és megtekintők azonosítása és hitelesítése nélkül biztosítja.
- A WMS+PUB rendszer a hivatalos lapok belső szerkesztését és a hivatalos lapok közzétételét támogató kiegészítő szolgáltatásait csak azonosított és hitelesített belső felhasználók számára biztosítja.
- A WMS+PUB rendszer a hivatalos lapokban megjelentetendő dokumentumok külső feltöltését támogató kiegészítő szolgáltatásait csak azonosított és hitelesített külső felhasználók számára biztosítja.
- A WMS+PUB rendszer az időbélyegzés háttérszolgáltatást azonosított és hitelesített (minősített) időbélyeg-szolgáltatótól veszi igénybe.

Bizalmasság

- A belső és a külső WMS alrendszer megőrzi és megvédi az általa kezelt felhasználói adatok (még nem közzétett státuszú hivatalos lapok, illetve külső és belső ügyek) bizalmasságát.
- A PUB alrendszerben közzétett felhasználói adatok (közzétett hivatalos lapok) nyilvánosak, erre vonatkozóan bizalmassági követelmény nincs. Ugyanakkor a még nem közzétett, de kis idővel a közzététel előtt már feltöltött hivatalos lapok bizalmasságát is meg kell őrizni.

Hitelesség

- A WMS+PUB rendszer minősített elektronikus aláírással és minősített szolgáltatótól származó időbélyeggel igazolja a közzétett hivatalos lapok hitelességét (sértetlenségét, eredet hitelességét, az időbélyegben szereplő időpont előtti létrehozását).
- A WMS+PUB rendszer hardvereszközben tárolt magánkulcson alapuló, fokozott biztonságú elektronikus aláírással igazolja a rendszerben tárolt felhasználói adatok státuszváltozással járó módosításának hitelességét (a módosító személyének letagadhatatlanságát, a módosított adatok sértetlenségét).

4 Az értékeléshez felhasznált értékelési bizonyítékok

A Rendszer értékelési jelentés [D2] részletesen felsorolja az értékeléshez rendelkezésre álló fejlesztői és értékelői bizonyítékokat (hivatkozással, verziószámokkal) a következő csoportosításban:

- Terv dokumentációk

  Közöttük:

  - Rendszer biztonsági előirányzat
  - Rendszer interfészek
  - Kiviteli terv - Publikálási felület
  - A4 – Authentication, Authorization, Accounting and Audit - általános leírás
  - Hozzáférési mátrix
  - Logolási mátrix
  - Jogosultságok – szerepek
  - stb., (összesen 13 dokumentum).

- Útmutató dokumentációk (20 dokumentum)

  Közöttük:

  - Telepítési kézikönyvek,
  - üzemeltetési kézikönyvek,
  - konfigurációs file-leírások, alkalmazás-frissítési kézikönyv,
  - stb., (összesen 20 dokumentum)

- Tesztelési dokumentációk
  - fejlesztői,
  - auditterv,
  - független teszteléshez
    - backbox, white boksz értékelői tesztelés
    - [D3]: WEB alkalmazás biztonság vizsgálati tesztelés

5 Javaslat a Tanúsítvány szövegezésére

5.1 Javaslat a Tanúsítvány főlapjának szövegezésére

A HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft,
mint a Nemzeti Akkreditációs Testület által NAT-6-0048/2011 számon akkreditált
terméktanúsító szervezet tanúsítja,
hogy a

Közigazgatási és Igazságügyi Minisztérium
E-Közigazgatásért Felelős Helyettes Államtitkárság által fejlesztetett

„Hivatalos Lapkiadás Rendszer”

2013. március 26-i rendszer verziója

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vételével

a KIB 28-as Ajánlásban szereplő MIBÉTS módszertan alapján
fokozott garanciaszinten értékelve, tanúsítva

alkalmas

a Rendszerbiztonsági előirányzatban meghatározott
azonosítás és hitelesítés, folyamatos működés, hozzáférés ellenőrzés, naplózás és elszámoltathatóság, rendszer- és információ sértetlenség, rendszer és kommunikáció védelem műszaki biztonsági követelményeinek az érvényesítésére.

Értékelve és tanúsítva a KIB 28-as Ajánlásban szereplő MIBÉTS módszertan szerinti fokozott (SAP-F) garanciaszinten.

Jelen tanúsítvány a HUNG-TJ-MIBÉTS-06-2013 számú Tanúsítási jelentés alapján került kiadásra.

Készült a Közigazgatási és Igazságügyi Minisztérium e-közigazgatásért Felelős Helyettes Államtitkárság megbízásából.

A tanúsítvány regisztrációs száma: HUNG-T-MIBÉTS-06-2013.

A tanúsítás kelte: 2013. március 29.

A tanúsítvány érvényességi ideje /évenkénti felülvizsgálat mellett/: 2016. március 29.

5.2 Javaslat a Tanúsítvány mellékleteire

Javasoljuk, hogy a Tanúsítvány mellékleteiben a következők szerepeljenek:

- A tanúsított rendszer azonosító adatai és főbb funkciója
- A biztonságos felhasználás feltételei (az SST és a Rendszer értékelési jelentés alapján)
- A tanúsítással és értékeléssel kapcsolatos hivatkozások.

5.3 Javaslat a biztonságos felhasználás feltételeire

Az alábbiakban összefoglaljuk azokat a betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a Hivatalos lapkiadás rendszer biztonságához.

Az értékelés – a Rendszer biztonsági előirányzatban meghatározott – üzemeltetési környezetre vonatkozó biztonsági feltételrendszer teljesülése esetén ad garanciákat a rendszer biztonsági tulajdonságainak érvényesülésére.

A. Risk_Assessment[5]

A rendszer működtetője rendszeres időnként felméri a működés során tapasztalt biztonsági eseményeket, értékeli a rendszer működéséből és kapcsolódó információ feldolgozó, tároló vagy átviteli műveletekből származó biztonsági kockázatokat, a kockázatok csökkentési lehetőségeit, szükség esetén megteszi a kellő szervezeti védelmi intézkedéseket.

Indokolás:

A rendszer fejlesztésének befejezéséhez képest nem volt még kellő tapasztalat a rendszer folyamatos működtetésében, előjöhetnek még nem feltárt, biztonságot veszélyeztető hibák.

A.Physical_Protection

A rendszer működtetője és üzemeltetője

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

Indokolás:

A műszaki biztonsági intézkedések csak akkor hatásosak, ha kiegészülnek megfelelő menedzsment és üzemeltetési intézkedésekkel.

[5] A: Assumptions (feltételezések), a jelölések megfelelnek a MIBÉTS módszertan alapját képező Common Criteria nemzetközi értékelési módszertan jelöléseinek.

A.Personnel_Security

A rendszer működtetője és üzemeltetője

a) biztosítja, hogy a szervezeten belül felelősségi körrel, feladattal rendelkező személyek megbízhatóak és megfelelnek az adott pozícióra vonatkozó biztonsági kritériumoknak;
b) biztosítja, hogy a rendszer üzemeltetői, belső felhasználói betartják a szervezeti biztonsági szabályokat, követik az érvényben lévő eljárásokat;
c) biztosítja, hogy a szervezeti információk és informatikai rendszerek védve legyenek a személyzeti mozgások esetére, így például egy felhasználó munkaköréből való eltávolítása vagy áthelyezése esetén.

Indokolás:

A műszaki biztonsági intézkedések csak akkor hatásosak, ha kiegészülnek megfelelő menedzsment és üzemeltetési intézkedésekkel. Például nem megbízható rendszergazda ellen egyes műszaki biztonsági intézkedések nem hatásosak.

A.Awareness_and_Training

A rendszer működtetője és üzemeltetője

a) biztosítja hogy az informatikai rendszer irányítói és a nem publikus alkalmazások felhasználói tudatában legyenek a tevékenységeikkel kapcsolatos biztonsági kockázatokkal, valamint az informatikai rendszerre vonatkozó törvényekkel, jogszabályi előírásokkal, szabványokkal, szabályzatokkal és eljárásokkal;
b) biztosítja, hogy a szervezet személyi állománya megfelelő képzésben részesüljön a számukra kijelölt, biztonsággal kapcsolatos feladatok és felelősségek teljesítése érdekében, továbbá amíg az üzemeltetés nem rendelkezik kellő gyakorlattal, ismerettel, (a biztonsági szabályok adta kereteken belül) az éles rendszer üzemeltetését támogassák a fejlesztők/integrátorok.

Indokolás:

A műszaki biztonsági intézkedések csak akkor hatásosak, ha kiegészülnek megfelelő menedzsment és üzemeltetési intézkedésekkel. Például ha a rendszer üzemeltetői nem kellően gyakorlottak, akkor a rendelkezésre álló műszaki intézkedési lehetőségek esetén sem garantálható pl. az elvárt rendelkezésre állási paraméterek tartása.

A.Media Protection

A rendszer működtetője és üzemeltetője a biztonsági szempontból érzékeny rendszerelemek, információk tekintetében

a) védi a szervezetnél fellelhető nyomtatott formájú vagy digitális adathordozón lévő információit;
b) jogosult felhasználókra korlátozza a célrendszerből kivett nyomtatott vagy digitális információkhoz való hozzáférést;
c) törli a digitális adathordozókat azok eltávolítása vagy újra használata előtt.

Indokolás:

A rendszerrel kapcsolatos adat- és programhordozó médiákat a rendszeren kívül is védeni kell, pl. vírusos adathordozó ne kerüljön a rendszerbe, a rendszer jelszavait védeni kell, a rendszer mentéseit védeni kell az illetéktelen módosítás, megismerés és megsemmisítés ellen, stb.

A rendszer életciklusában a biztonsági elvárások teljesítésének folyamatos fenntartásához szükséges, hogy rendszer működtetője és üzemeltetője

- a szükséges változtatások során fenntartsa a rendszer értékelés idején fennálló biztonsági szintjét, az üzemeltetési dokumentációkat aktualizálja;
- fejlessze a biztonsági megoldásokat az Értékelési jelentésben szereplő biztonságnövelő javaslatok figyelembe vételével;
- időszakosan vizsgáltassa felül a rendszer biztonságát.

Indokolás:

A működő rendszerben bizonyos változások folyamatosan szükségessé válnak, egyes változtatások pedig a biztonság fenntartása érdekében is elengedhetetlenek. Ilyenek pl. a frissítések (operációs rendszer, vírusvédelem stb.), de ilyenek lehetnek a működtetésből származó tapasztalatok, újabb funkcionális igények, jogszabályi változások által generált igények is.

Amennyiben ezek nem érintik alapvetően a biztonsági funkciókat, a legközelebbi éves felülvizsgálat során kerülhetnek ellenőrzésre.

Természetesen jelentős változások a tanúsítvány érvényességét megszüntethetik.

Az értékelési jelentésben szereplő biztonságnövelő javaslatok beépítése ajánlatos a következő továbbfejlesztett verzióba, melyek annak a verziónak az értékelése során kerülnek felülvizsgálatra.

6 A tanúsítással és értékeléssel kapcsolatos hivatkozások

Módszertani hivatkozások:

[M1]: 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)

[M2]: Útmutató rendszer értékelőknek (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v3 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M3]: Útmutató rendszer tanúsítóknak (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v3 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M4]: 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)

[M5]: NIST SP 800-53: National Institute of Standard and Technology U.S. Department of Commerce Specila Publications 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, February 2012

A tanúsításhoz felhasznált főbb dokumentumok és megalapozó értékelési jelentések azonosítása

Főbb dokumentumok:

[D1]: Hivatalos lapkiadási rendszer (WMS+PUB v1.0) - Rendszerbiztonsági előirányzat (SST v1.0)

[D2]: Hivatalos lapkiadási rendszer (WMS+PUB) Rendszer értékelési jelentés (PUB_SETR_v04)

[D3]: Hivatalos lapkiadási rendszer (WMS+PUB) WEB alkalmazás biztonság vizsgálati jelentés