Tanúsítási jelentés

Transzreklám - TRFlow rendszer

2016. június 17-i állapot

HUNG-TJ-MIBÉTS-010-2016

Verzió:	1.0
Fájl:	HUNG-TJ-MIBÉTS-010-2016_v10.pdf
Minősítés:	Nyilvános
Oldalak:	27

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2016.06.07.	A szerkezet felállítása
v0.2	2016.06.26.	Belső egyeztetésre kiadott verzió
v0.9	2016.06.27.	Külső egyeztetésre kiadott verzió
v1.0	**2016.06.28.**	**Végleges verzió**

A tanúsítási jelentést készítette:

dr. Szabó István
Hunguard Kft.
Tanúsítási divízió

Tartalom

I. Összefoglaló

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

TOE név:	**Transzreklám – TRFlow rendszer**
TOE rövid neve:	TRFlow
TOE verzió:	2016.06.17.
Értékelő:	Hunguard Kft. Értékelési Divízió 1123. Budapest, Kékgolyó u. 6.
Értékelés befejezése:	2016. június 17.
Az értékelés módszere:	MIBÉTS rendszerértékelés
Az értékelés garanciaszintje:	Fokozott (SAP-F)

I.2. A tanúsítás tárgya

A TRFlow egy olyan rendszer, amely lehetővé teszi, hogy

- az érintett szervezetek
  - elérjék, illetve
  - engedélyezni tudják a szállítók által feltöltött hozzájuk tartozó kommunikációs kampányhoz tartozó tervet és az ezekhez kapcsolódó
  - teljesítési igazolásokat, illetve
  - a teljesítési igazolásokhoz tartozó számlákat tudjanak megtekinteni
  - és a hozzá tartozó kampányokból kimutatásokat készíteni;
- a szállító
  - a hozzá tartozó kampányokhoz tervsorokat
  - a tervsorokhoz teljesítési igazolásokat,
  - az érintett szervezet által elfogadott teljesítési igazolásokhoz számlákat tud rögzíteni
  - és a hozzá tartozó kampányokból kimutatásokat készíteni;
- az NKOH
  - lehetősége van a kampányok során keletkezett adatokba betekintést nyerni
  - és ezekből kimutatásokat készíteni.

Szállító

- A szállító a Nemzeti Kommunikációs Hivatal által kihirdetett nyertes pályázóként a kampány tervét elkészíti és a terv engedélyeztetését igényli.

- Az engedélyezett kampány terveket a terveknek megfelelően az alvállalkozóktól megrendeli, és annak teljesítését felügyeli.
- Az alvállalkozói teljesítést követően a teljesítés igazolást engedélyezésre az érintett intézmény és hivatal számára átadja.
- Az engedélyezett teljesítés igazolásokat a beszállítók számára számla adásához csatolja.
- A kiállított számlákat a rendszerben rögzíti.
- A szállító által érintett kampányok mindenkori aktuális állapotáról a szállító részletes riportokat érhet el, amelyeket akár Excel-ben is lekérdezhet.

Nemzeti Kommunikációs Hivatal

- A közbeszerzési eljárás lefolytatását követően előállt kampányokat és azok műszaki és jogi tartalmát a rendszer számára elérhetővé teszi.
- Az engedélyeztetési folyamatokban (terv és teljesítés igazolás) a Hivatal a szükséges engedélyeztetést elvégezheti – de ez a hivatal számára opcionális.
- A rendszeren belül kezelt kampányok mindenkori állapotáról a Hivatal részletes riportokat érhet el, amiket akár Excel-ben is lekérdezhet.
- A Hivatal a közbeszerzési eljárás során meghatározott cikktörzset a rendszer rendelkezésére bocsájtja.
- A Hivatal a mindenkori érvényes szállítói és intézményi alap adatokat a rendszer számára elérhetővé teszi.

Intézmény (érintett szervezet)

- Az Intézmény a szállító által létrehozott kampány tervet engedélyezi.
- Az Intézmény a kampány végrehajtása során előállt teljesítés igazolásokat engedélyezi a kifizetés engedélyezése céljából.
- Az Intézmény az érintett kampányokról részletes kimutatásokat érhet el, amiket akár Excel-ben is lekérdezhet.

A rendszer biztonságát a https (SSL) alapú kommunikáció és az erőforrásokhoz való hozzáférés ellenőrzése garantálja.

A rendszer használatához érvényes felhasználónév, jelszó pár megadása szükséges, amely azonosíthatja a felhasználót.

A rendszer mind szerepkör, mind pedig szereplő szerint biztosítja a hozzáférést.

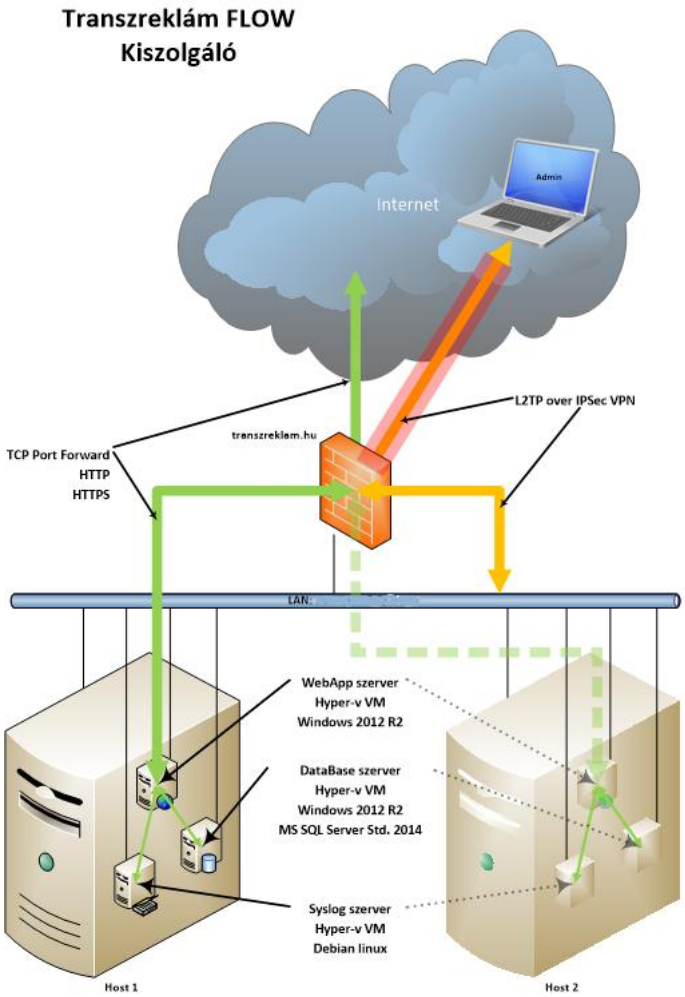
A szerepkör meghatározza az elérhető funkcionalitásokat, míg a szereplő meghatározza a funkciókon belül elérhető adatok halmazát.

A rendszerben alkalmazott felhasználói azonosítási eljárás az Oauth2 szabványban lefektetett implicit bejelentkezési folyamat szerint kerül megvalósításra. A bejelentkezéshez szükséges a bejelentkezés helyének (CORS) ellenőrzését követően – a login szerver által - biztosított felületen bevitt felhasználó név és jelszó megadása. Sikeres bejelentkezést követően a loginserver JWT authentikációs ticketeket állít ki, amelynek eredetiségének igazolásáért a JWT szabványnak megfelelően aláírja. A későbbiekben

a ticket felhasználása során a hitelesítést igénylő komponensek és folyamatok a ticketben szereplő adatok helyességét a login szerver által megadott publikus kulcs felhasználásával ellenőrzik. A rendszer által felhasználható ticket előállítása ily módon csak a login szerver megfelelő azonosítást követően lehetséges.

A rendszerben alkalmazott alkalmazás integrációs kapcsolatok megfelelő előkészítést – jogi és technikai feltételek – követően az alkalmazás és a partner között megosztott és adott időszakra érvényes jelszó felhasználásával lehetséges. Azonban ebben az esetben nem személyeket, hanem például a Hivatal rendszerével közvetlenül kommunikáló integrációs alkalmazásokat azonosítják és hitelesítik.

I.3. A TOE biztonsági környezete és határai



1. ábra: A rendszer fizikai határai, belső felépítése és struktúrája.

I.4. A rendszer főbb komponenseinek azonosítása

Az alap funkcionalitást megvalósító szoftverkomponensek és SHA256 lenyomataik:

"Smart.Cloud.Contracts.dll",

"A1DFD1372FAFD44737FD5AF2E7FB0AB82478E161D9F0F0B8A3CF22CD48221570"

"Smart.Cloud.Db.dll"

"A27B8076CF8185F48AB9A04741E4BC3A7B3A0B591C3D88E6DF4C10568129C32C"

"Smart.Cloud.dll"

"0B4C106E5EB9B40EE4B7CA90F31ED01343C239FAE242CD00A5E5F338D394973F"

"Smart.Common.dll"

"405EE8E68ACF2E40E73304C5806150134E4DF3307F225984F1A5AE9E8507E638"

"Smart.OctoCloud.Contracts.dll"

"97A1D3A7F4E71C139161640B5F70BB46C27C0D09E9CCBB7FB439B98804115C85"

"Smart.OctoCloud.dll"

"7EFB919973F7CF08383C96A8AD2FD8234EAFD5E6D29C7048FA2001F0AD7AC549"

"Smart.Services.Wcf.dll"

"5C0205AB86910BAA8C68C7FD3509B90F090EC82B24F22CDDE7BBC71E2B581555"

"OctoCloud.Login.Website.dll"

"DBD2F44EB508D862F2732902B4E697D001616B1941A1607762D4DCBB1C91A546"

"SmartPlanFact.UI.dll"

"923811DC1B33B645C8D0E4E9808483A28DF1FCE7E986F6A783BBCE3E91677787"

Az értékelt konfiguráció elemei:

Platform

- Windows Server 2012 R2

Adatbázis

- MS SQL Server 2012

API

- .Net 4.6, C#
- ThinkTecture Identity Server 3 (OpenID certified, OAuth2/OpenID compatible): bearer token alapú jogosultság kezelés. Az oauth2 használatának szükségességét a rendszert használó, és ahhoz integrálódó végfelhasználók és szervezetek egységes hitelesítési és jogosultsági kezelése miatt szükséges.

II. A tanúsítás jellemzése

Jelen tanúsítás a rendszer biztonsági előirányzatában lefektetetett követelmények teljesülését vizsgálja.

II.1. Az alkalmazott értékelési módszer

A TRFlow rendszer értékelésére a MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) értékelési módszertant alkalmazták. A MIBÉTS értékelési módszertana a KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlásának (Az E-közigazgatási Keretrendszer követelménytár, 2009) részét képezi az alábbi címen: „Rendszerekre vonatkozó értékelési módszertan”.

Az értékelés garanciaszintje MIBÉTS fokozott (SAP-F).

II.2. A tanúsításhoz felhasznált értékelési jelentések azonosítása

Rendszer értékelési jelentés:

- Transzreklám - TRFlow rendszer ÉRTÉKELÉSI JELENTÉS v1.0

II.3. Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés, a fejlesztőkkel történt folyamatos konzultáció mellett, az alábbi fejlesztői bizonyítékok végleges verzióit használta fel:

Dokumentum / fájl neve	Beküldés időpontja
Transzreklam_SST_0.6.docx	2016.06.02.
SKMBT_C35160415092700.pdf	2016.04.11.
AVI_v1.1.odt	2016.05.05.
AVI_v1.1.pdf	2016.05.05.
FVI_v1.1.odt	2016.05.05.
FVI_v1.1.pdf	2016.05.05.
IBSZ_v1.1.odt	2016.05.05.
IBSZ_v1.1.pdf	2016.05.05.
Kockazatok_kiszamolasa.ods	2016.05.05.
LVI_v1.1.odt	2016.05.05.
LVI_v1.1.pdf	2016.05.05.
Transzreklam_IBSZ_anyagok_v1_1.zip	2016.05.05.
Transzreklam_velemeny_20160414_revEPM.odt	2016.05.05.
Transzreklam_SST_0.3 (3).docx	2016.05.18.
Transzreklam_SST_0.4.docx	2016.05.26.
Transzreklam_SST_velemenyezes_20160519_valasz.docx	2016.05.26.
1_1_rendszer_követelmények_és_telepítési_előfeltételek.docx	2016.06.01.
1_telepítési_útmutató_és_3_üzemeltetői_kézikönyv.docx	2016.06.01.
2_felhasználó_kézikönyv.docx	2016.06.01.
6_1_teszt_terv.xlsx	2016.06.01.
6_2_teszt_jegyzőkönyv_1.0.xlsx	2016.06.01.
7_1_rendszerterv.docx	2016.06.01.
7_minimális_rendszerkövetelmények.docx	2016.06.01.
8_műszaki_leírás.docx	2016.06.01.
9_alkalmazás_folyamat.docx	2016.06.01.

Kiszolgáló környezet leltár.docx	2016.06.01.
packages.docx	2016.06.01.
Transzreklam_SST_velemenyezes_20160530_valasz.docx	2016.06.01.
Transzreklam_ADVS_0.2.docx	2016.06.03.
Transzreklam_SST_0.6.docx	2016.06.03.
valaszok_20160601_mod.docx	2016.06.03.
AVI_v1.1.odt	2016.06.05.
AVI_v1.1.pdf	2016.06.05.
FVI_v1.1.odt	2016.06.05.
FVI_v1.1.pdf	2016.06.05.
IBSZ_v1.1.odt	2016.06.05.
IBSZ_v1.1.pdf	2016.06.05.
Kockazatok_kiszamolasa.ods	2016.06.05.
LVI_v1.1.odt	2016.06.05.
LVI_v1.1.pdf	2016.06.05.
Transzreklam_IBSZ_anyagok_v1_1.zip	2016.06.05.
Transzreklam_velemeny_20160414_revEPM.odt	2016.06.05.
Biztonsagi_teszt_jegyzokonyv_20160603.xlsx	2016.06.06.
AC-7-1.png	2016.06.06.
AC-7-2.png	2016.06.06.
AC-8.png	2016.06.06.
DB_Restore_1.PNG	2016.06.06.
DB_Restore_success.PNG	2016.06.06.
Full_Disaster_Recovery_success.PNG	2016.06.06.
F_MK_1-1.png	2016.06.06.
F_MK_1-2.png	2016.06.06.
F_MK_1-3.png	2016.06.06.
F_MK_2-1.png	2016.06.06.
F_MK_2-2.png	2016.06.06.
F_MK_6.png	2016.06.06.
F_MK_7-1.png	2016.06.06.
F_MK_7-2.png	2016.06.06.
F_MK_9.png	2016.06.06.
IA-5-1.png	2016.06.06.
IA-5-2.png	2016.06.06.
IA-6.png	2016.06.06.
logs.docx	2016.06.06.
S_MK_1.png	2016.06.06.
S_MK_2-1.png	2016.06.06.
S_MK_2-2.png	2016.06.06.
S_MK_2-3.png	2016.06.06.
S_MK_2-4.png	2016.06.06.
S_MK_3-1.png	2016.06.06.
S_MK_3-2.PNG	2016.06.06.
S_MK_4.PNG	2016.06.06.
AVI_v1.2.docx	2016.06.07.
BFIBH_v01.docx	2016.06.07.
FVI_v1.2.docx	2016.06.07.
IBSZ_v1.2.odt	2016.06.07.

KFIBH_v01.docx	2016.06.07.
LVI_v1.2.docx	2016.06.07.
cert1.png	2016.06.10.
cert2.png	2016.06.10.
cert3pvk.png	2016.06.10.
cert4_finish.png	2016.06.10.
cert4_finish_result.png	2016.06.10.
CreateCommonMachineKey.png	2016.06.10.
emailek.docx	2016.06.10.
icinga.png	2016.06.10.
logok.zip	2016.06.10.
services_leirasok_es_configok.zip	2016.06.10.
tesztek.docx	2016.06.10.
2016-06-15_AuditLog.txt	2016.06.15.
auditorral_vegzett_tesztek.docx	2016.06.15.
kulcsgeneralas_accessToken_restHIvas.docx	2016.06.15.
local_security_policy.docx	2016.06.15.
LogFileChecking_SystemWatching_Service.docx	2016.06.15.
Re Transzreklám - Sérülékenységvizsgálat eredménye észrevételezési jelentés (OR 1).msg	2016.06.15.
Transzreklam_ADVS_0.3.docx	2016.06.15.
trflow_kieg_20160615.zip	2016.06.15.
trflow_OR_2_valasz.doc	2016.06.15.
Web.config	2016.06.15.
ZyXel_tuzfal.docx	2016.06.15.
AVI_v1.3.docx	2016.06.17.
LVI_v1.3.docx	2016.06.17.
test.zip	2016.06.17.
TR_MISec_IBF_szerzodes_v1.pdf	2016.06.17.
Alapkonfiguráció v2.xslx	2016.06.17.
backend_hash.csv	2016.06.17.
login_hash.csv	2016.06.17.
ui_hash.csv	2016.06.17.

II.4. Az értékelési folyamat tanúsítási szempontú ellenőrzése

A tanúsítási jelentés készítői a teljes értékelési folyamatot figyelemmel kísérték, ellenőrizték:

- az értékelési folyamatok módszertani szempontú ellenőrzésével;
- különböző szakértői megbeszéléseken való részvétellel.

III. Az értékelés eredményei

III.1. A garanciális biztonsági követelményeknek való megfelelés

Az értékelés módszertana a MIBÉTS rendszerekre vonatkozó értékelési módszertanát (KIB 28. számú ajánlása) követte, az eredmények leírása is az ott meghatározott jelöléseket alkalmazza.

III.1.1. A rendszer biztonsági előirányzat értékelése

Értékelői feladatelem	határozat
ASST_INT.1: SST bevezetés	megfelelt
ASST_CCL.1: Megfelelőség nyilatkozat mértékadó dokumentumhoz	megfelelt
ASST_SPD.1 Biztonsági probléma meghatározás	megfelelt
ASST_OBJ.2: Biztonsági célok	megfelelt
ASST_REQ.2: Hazai katalógusból választott követelmények	megfelelt
ASST_SSS.1: STOE összefoglaló előírás	megfelelt
IV.1.7. Biztonsági tartományok	n/a[1]

III.1.2. A rendszer fejlesztés garanciaosztály értékelése

Értékelői feladatelem	határozat
ASDV_ARC.1 Biztonsági szerkezet leírás	megfelelt
ASDV_SIS.1: Informális interfész specifikáció	megfelelt
ASDV_OSC.1: Rendszer-működési biztonsági koncepció	megfelelt
ASDV_SDS.1: Alrendszer és komponens szintű biztonsági terv	megfelelt

III.1.3. A rendszer útmutató dokumentumok garanciaosztály értékelése

Értékelői feladatelem	határozat
ASGD_PRE.2: Az előkészítő útmutató igazolása	megfelelt
ASGD_OPE.2: Az üzemeltetési útmutató igazolása	megfelelt
ASGD_CON.2: A konfigurálási útmutató igazolása	megfelelt

III.1.4. A rendszer konfiguráció kezelés garanciaosztály értékelése

Értékelői feladatelem	határozat
ASCM_SBC.2: A rendszer alap konfiguráció igazolása	megfelelt
ASCM_ECC.2: A tanúsított komponensek ellenőrzése	megfelelt

[1] Biztonsági szempontból megkülönböztethető tartományokat nem definiáltak.

III.1.5. IV.5. A rendszer tesztelés garanciaosztály értékelése

Értékelői feladatelem	határozat
ASTE_FUN.1: Funkcionális tesztelés	megfelelt
ASTE_COV.1: A teszt lefedettség vizsgálata	megfelelt
ASTE_DPT.2: Tesztelés: alrendszerek	megfelelt
ASTE_IND.1: Független tesztelés mintán	megfelelt

III.1.6. A rendszer sebezhetőség felmérés garanciaosztály értékelése

A sérülékenység vizsgálat során olyan tesztesetek kerültek végrehajtásra, amelyek a TOE biztonsági funkcióinak megkerülését tesztelték.

Ellenőrzésre kerültek az STOE által használt harmadik feles alkalmazások a nyílt sérülékenység adatbázisok által.

A fenti vizsgálatok nem tártak fel kockázatokat, így az értékelés eredménye alapján a TOE üzemeltetési környezetében ellenáll egy megemelt-alap támadó képességgel rendelkező támadónak.

Értékelői feladatelem	határozat
ASVA_VAN.2: Független sebezhetőség vizsgálat	**megfelelt**

III.2. A Miniszterelnök Kabinetfőnöke 1/2016. (II.1.) rendeletében meghatározott funkcionális és biztonsági követelmények teljesítésének értékelése

Követelmény	határozat
F_MK_1 **MK 3. § a) az informatikai rendszer vékony klienses reszponzív - azaz hordozható és asztali eszközökön is használható - webes felületet biztosít a felhasználók számára**	*Döntés: megfelelt*
F_MK_2 **MK 3. § d) az informatikai rendszer lehetőséget biztosít a meglévő informatikai rendszerekkel való szabványos interfészen keresztül megvalósított interoperabilitásra**	*Döntés: megfelelt*
F_MK_3 **MK 3. § e) az informatikai rendszerre vonatkozóan felhasználói, fejlesztői és üzemeltetési dokumentáció áll rendelkezésre**	*Döntés: megfelelt*
F_MK_4 **MK 4. § a) naptári évenként legalább tízezer beszerzési eljárás adatainak tárolására és folyamatainak kezelésére alkalmas**	*Döntés: megfelelt*
F_MK_5 **MK 4. § b) az informatikai rendszeren keresztül továbbított (küldött és fogadott) adatok archiválására és tárolására a 2. §-ban meghatározott paraméterek szerint alkalmas**	*Döntés: megfelelt*
F_MK_6 **7. § A nyomon követendő rendszerparaméterek: a) a bejelentkezett felhasználók számának időbeli változása szerepkör és jogosultsági szint szerint**	*Döntés: megfelelt*
F_MK_7	*Döntés: megfelelt*

7. § A nyomon követendő rendszerparaméterek: b) a beszerzési eljárások állapota	
F_MK_8 **7. § A nyomon követendő rendszerparaméterek: c) az informatikai rendszer terheltsége**	*Döntés: megfelelt*
F_MK_9 **7. § A nyomon követendő rendszerparaméterek: d) átlagos válaszidők**	*Döntés: megfelelt*
F_MK_10 **8. § Az informatikai rendszernek alkalmasnak kell lennie** **a) a beszerzések teljesülésével kapcsolatos adatok valós idejű nyomon követése érdekében a tervek, megrendelések, vásárlási adatok, teljesítési igazolások és számlák feltöltésére**	*Döntés: megfelelt*
F_MK_11 **8. § Az informatikai rendszernek alkalmasnak kell lennie** **b) az informatikai rendszerből származtatható adatokból, információkból nyert kimutatások készítésére**	*Döntés: megfelelt*
F_MK_12 **8. § Az informatikai rendszernek alkalmasnak kell lennie** **c) dokumentált interfész kapcsolat biztosítására más állami közbeszerzési informatikai rendszerhez**	*Döntés: megfelelt*
S_MK_1 **MK 3. § b) az informatikai rendszer biztonságos kapcsolaton keresztül kommunikál**	*Döntés: megfelelt*
S_MK_2 **MK 3. § c) az informatikai rendszer jogosultságkezeléssel rendelkezik, amely biztosítja, hogy csak az illetékes felhasználók férhessenek hozzá az adatokhoz**	*Döntés: megfelelt*
S_MK_3 **MK 4. § c) az informatikai rendszerhez való hozzáférés teljes körű naplózása biztosított**	*Döntés: megfelelt*
S_MK_4 **MK 4. § d) az informatikai rendszerről rendszeres biztonsági mentés készül, amely alapján visszaállítható egy korábbi állapot**	*Döntés: megfelelt*
S_MK_5 **MK 4. § e) az informatikai rendszer 99,9%-os rendelkezésre állást nyújt munkanapokon a 6 és 20 óra közötti időszakban**	*Döntés: megfelelt*
S_MK_6 **MK 5. § Az informatikai rendszernek elkülönítetten kell kezelnie a Hivatal, az Érintett szervezet és a Szállító szerepköreit. Az egyes szerepkörökön belül elkülönítetten kell kezelni az adminisztrátori, az engedélyező és a felhasználói jogosultsági szinteket.**	*Döntés: megfelelt*
S_MK_7 **MK 6.§ A Hivatal rendelkezik felhasználói, engedélyező és adminisztrátor jogosultságokkal. Az érintett szervezet és a szállító felhasználói szerepkörrel rendelkezik.**	*Döntés: megfelelt*

III.3. IV.8. A 41/2015 BM rendelet (A:3, F:3, L:3,3,3) által meghatározott funkcionális és biztonsági követelmények teljesítésének értékelése

III.3.1. Általános védelmi intézkedések

Azonosító	Intézkedés, határozat
CA-3	**3.3.1.3 Az elektronikus információs rendszer kapcsolódásai** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
CA-9	**3.3.1.3.2 Belső rendszer kapcsolatok**

	Döntés: megfelelt *Vizsgálati módszerek: Dokumentáció*
CA-3 (5)	**3.3.1.3.3 Külső kapcsolódásokra vonatkozó korlátozások** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PS-1	**3.3.1.4 Személybiztonság** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.2. Tervezés

Azonosító	Intézkedés, határozat
PL-2	**3.3.2.2 Rendszerbiztonsági terv** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PL-7	**3.3.2.3 Cselekvési terv** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
PL-4	**3.3.2.4 Személyi biztonság** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.3. Rendszer és szolgáltatás beszerzés

Azonosító	Intézkedés, határozat
SA-3	**3.3.3.2 A rendszer fejlesztési életciklusa** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
SA-4 (9)	**3.3.3.3 Funkciók, portok, protokollok, szolgáltatások** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*

III.3.4. Biztonsági elemzés

Azonosító	Intézkedés, határozat
CA-1	**3.3.4.1 Biztonságelemzési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
CA-2	**3.3.4.2 Biztonsági értékelések** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PM-6	**3.3.4.4 A biztonsági teljesítmény mérése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.5. Tesztelés, képzés és felügyelet

Azonosító	Intézkedés, határozat
PM-14	**3.3.5.1.1 Tesztelési, képzési és felügyeleti eljárások** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PM-6	**3.3.5.2 A biztonsági teljesítmény mérése**

	Döntés: megfelelt *Vizsgálati módszerek: Dokumentáció*
RA-5	**3.3.5.3 Sérülékenység teszt** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Teszt*
RA-5 (1)	**3.3.5.3.2 Frissítési képesség** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
RA-5 (2)	**3.3.5.3.3 Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
RA-5 (5)	**3.3.5.3.4 Privilegizált hozzáférés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
RA-5 (4)	**3.3.5.3.5 Felfedhető információk** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.6. Konfigurációkezelés

Azonosító	Intézkedés, határozat
CM-1	**3.3.6.1 Konfigurációkezelési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
CM-2	**3.3.6.2 Alapkonfiguráció** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Audit*
CM-3	**3.3.6.3 A konfigurációváltozások felügyelete, változáskezelés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
CM-3 (2)	**3.3.6.3.2 Előzetes tesztelés és megerősítés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
CM-4	**3.3.6.4 Biztonsági hatásvizsgálat** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
CM-6	**3.3.6.6 Konfigurációs beállítások** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
CM-7	**3.3.6.7 Legszűkebb funkcionalitás** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*
CM-8	**3.3.6.8 Elektronikus információs rendszerelem leltár** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Audit*
CM-10	**3.3.6.10 A szoftverhasználat korlátozásai** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Audit*
CM-11	**3.3.6.11 A felhasználó által telepített szoftverek**

	Döntés: megfelelt *Vizsgálati módszerek: Dokumentáció*

III.3.7. Karbantartás

Azonosító	Intézkedés, határozat
MA-1	**3.3.7.1 Rendszer karbantartási eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
MA-2	**3.3.7.2 Rendszeres karbantartás** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.8. Adathordozók védelme

Azonosító	Intézkedés, határozat
MP-1	**3.3.8.1 Adathordozók védelmére vonatkozó eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
MP-2	**3.3.8.2 Hozzáférés az adathordozókhoz** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
MP-6	**3.3.8.6 Adathordozók törlése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
MP-7	**3.3.8.7 Adathordozók használata** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*

III.3.9. Azonosítás és hitelesítés

Azonosító	Intézkedés, határozat
IA-1	**3.3.9.1 Azonosítási és hitelesítési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
IA-2	**3.3.9.2 Azonosítás és hitelesítés (belső felhasználók)** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*
IA-2 (1)	**3.3.9.2.2 Hálózati hozzáférés privilegizált fiókokhoz** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*
IA-4	**3.3.9.4 Azonosító kezelés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Audit*
IA-5	**3.3.9.5 A hitelesítésre szolgáló eszközök kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*
IA-6	**3.3.9.6 A hitelesítésre szolgáló eszköz visszacsatolása** *Döntés: megfelelt* *Vizsgálati módszerek: Tesztelés*
IA-7	**3.3.9.7 Hitelesítés kriptográfiai modul esetén** *Döntés: megfelelt*

	Vizsgálati módszerek: Dokumentáció, Interjú
IA-8	**3.3.9.8 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*
IA-H	**3.3.9.8.2 Hitelesítésszolgáltatók tanúsítványának elfogadása** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.10. Hozzáférés ellenőrzés

Azonosító	Intézkedés, határozat
AC-1	**3.3.10.1 Hozzáférés ellenőrzési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AC-2	**3.3.10.2 Felhasználói fiókok kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
AC-3	**3.3.10.3 Hozzáférés ellenőrzés érvényesítése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AC-7	**3.3.10.7 Sikertelen bejelentkezési kísérletek** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*
AC-8	**3.3.10.8 A rendszerhasználat jelzése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*
AC-14	**3.3.10.12 Azonosítás/hitelesítés nélkül engedélyezett tevékenységek** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
AC-17	**3.3.10.13 Távoli hozzáférés** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AC-18	**3.3.10.14 Vezeték nélküli hozzáférés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AC-19	**3.3.10.15 Mobil eszközök hozzáférés ellenőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AC-20	**3.3.10.16 Külső elektronikus információs rendszerek használata** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AC-22	**3.3.10.18 Nyilvánosan elérhető tartalom** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*

III.3.11. Rendszer- és információsértetlenség

Azonosító	Intézkedés, határozat
SI-1	**3.3.11.2 Rendszer- és információsértetlenségre vonatkozó eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

SI-2	**3.3.11.3 Hibajavítás** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Audit*
SI-3	**3.3.11.4 Kártékony kódok elleni védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SI-4	**3.3.11.5 Az elektronikus információs rendszer felügyelete** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*
SI-5	**3.3.11.6 Biztonsági riasztások és tájékoztatások** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
SI-12	**3.3.11.12 A kimeneti információ kezelése és megőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.12. Naplózás és elszámoltathatóság

Azonosító	Intézkedés, határozat
AU-1	**3.3.12.1 Naplózási eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AU-2	**3.3.12.2 Naplózható események** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Audit*
AU-3	**3.3.12.3 Naplóbejegyzések tartalma** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-4	**3.3.12.4 Napló tárkapacitás** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
AU-5	**3.3.12.5 Naplózási hiba kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-6	**3.3.12.6 Naplóvizsgálat és jelentéskészítés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AU-8	**3.3.12.8 Időbélyegek** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Audit*
AU-9	**3.3.12.9 A naplóinformációk védelme** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Audit*
AU-11	**3.3.12.11 A naplóbejegyzések megőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
AU-12	**3.3.12.12 Naplógenerálás** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*

III.3.13. Rendszer- és kommunikációvédelem

Azonosító	Intézkedés, határozat
SC-1	**3.3.13.1 Rendszer- és kommunikációvédelmi eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
SC-5	**3.3.13.5 Túlterhelés –szolgáltatás megtagadás alapú támadás– elleni védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-7	**3.3.13.6 A határok védelme** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-12	**3.3.13.10 Kriptográfiai kulcs előállítása és kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-13	**3.3.13.11 Kriptográfiai védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Forráskód*
SC-15	**3.3.13.12 Együttműködésen alapuló számítástechnikai eszközök** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
SC-20	**3.3.13.16 Biztonságos név/cím feloldó szolgáltatások (hiteles forrás)** *Döntés: megfelelt* *Vizsgálati módszerek: -*
SC-21	**3.3.13.17 Biztonságos név/cím feloldó szolgáltatás (gyorsító táras)** *Döntés: megfelelt* *Vizsgálati módszerek: -*
SC-22	**3.3.13.18 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
SC-39	**3.3.13.22 A folyamatok elkülönítése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*

III.3.14. Szervezeti szintű alapfeladatok

Azonosító	Intézkedés, határozat
PM-1	**3.1.1.1 Informatikai biztonsági szabályzat** *Döntés: megfelel* *Vizsgálati módszerek: Dokumentáció*
PM-2	**3.1.1.2 Az elektronikus információs rendszerek biztonságáért felelős személy** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
CA-5	**3.1.1.3 Az intézkedési terv és mérföldkövei** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PM-5	**3.1.1.4 Informatikai rendszerek nyilvántartása** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PM-10	**3.1.1.5 Információbiztonsággal kapcsolatos engedélyezési eljárás** *Döntés: megfelelt*

	Vizsgálati módszerek: Dokumentáció

III.3.15. Kockázatelemzés

Azonosító	Intézkedés, határozat
RA-1	**3.1.2.1 Kockázatelemzési és kockázatkezelési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
RA-2	**3.1.2.2 Biztonsági osztályba sorolás** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
RA-3	**3.1.2.3 Kockázatelemzés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.16. Rendszer és szolgáltatás beszerzés

Azonosító	Intézkedés, határozat
SA-1	**3.1.3.1 Beszerzési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
SA-2	**3.1.3.2 Erőforrás igény felmérés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
SA-4	**3.1.3.3 Beszerzések** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
SA-5	**3.1.3.4 Az elektronikus információs rendszerre vonatkozó dokumentáció** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
SA-9	**3.1.3.6 Külső elektronikus információs rendszerek szolgáltatásai** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
CA-7	**3.1.3.8 Folyamatos ellenőrzés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.17. Üzletmenet (ügymenet) folytonosság tervezése

Azonosító	Intézkedés, határozat
CP-1	**3.1.4.1 Üzletmenet folytonosságra vonatkozó eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
CP-2	**3.1.4.2 Üzletmenet folytonossági terv informatikai erőforrás kiesésekre** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
CP-3	**3.1.4.3 A folyamatos működésre felkészítő képzés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
CP-9	**3.1.4.8 Az elektronikus információs rendszer mentései** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

CP-10	**3.1.4.9 Az elektronikus információs rendszer helyreállítása és újraindítása** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Tesztelés*

III.3.18. A biztonsági események kezelése

Azonosító	Intézkedés, határozat
IR-4	**3.1.5.1 A biztonsági események kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
IR-5	**3.1.5.4 A biztonsági események figyelése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
IR-6	**3.1.5.6 A biztonsági események jelentése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
IR-7	**3.1.5.7 Segítségnyújtás a biztonsági események kezeléséhez** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
IR-8	**3.1.5.8 Biztonsági eseménykezelési terv** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
IR-2	**3.1.5.9 Képzés a biztonsági események kezelésére** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.19. Emberi tényezőket figyelembe vevő – személy – biztonság

Azonosító	Intézkedés, határozat
PS-1	**3.1.6.1 Személybiztonsági eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PS-2	**3.1.6.2 Munkakörök, feladatok biztonsági szempontú besorolása** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PS-3	**3.1.6.3 A személyek ellenőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PS-4	**3.1.6.4 Eljárás a jogviszony megszűnésekor** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PS-5	**3.1.6.5 Az áthelyezések, átirányítások és kirendelések kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PS-7	**3.1.6.6 Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PS-8	**3.1.6.7 Fegyelmi intézkedések** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PL-2 (3)	**3.1.6.8 Belső egyeztetés**

	Döntés: megfelelt *Vizsgálati módszerek: Dokumentáció*
PL-4	**3.1.6.9 Viselkedési szabályok az interneten** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.20. Tudatosság és képzés

Azonosító	Intézkedés, határozat
PM-15	**3.1.7.1 Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AT-1	**3.1.7.2 Képzési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AT-2	**3.1.7.3 Biztonság tudatosság képzés** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AT-3	**3.1.7.5 Szerepkör, vagy feladat alapú biztonsági képzés** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
AT-4	**3.1.7.6 A biztonsági képzésre vonatkozó dokumentációk** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.3.21. Fizikai védelmi intézkedések értékelése

Azonosító	Intézkedés, határozat
PE-1	**3.2.1.2 Fizikai védelmi eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PE-2	**3.2.1.3 Fizikai belépési engedélyek** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció, Interjú*
PE-3	**3.2.1.4 Fizikai belépés ellenőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PE-6	**3.2.1.7 A fizikai hozzáférések felügyelete** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PE-8	**3.2.1.8 A látogatók ellenőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PE-12	**3.2.1.11 Vészvilágítás** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PE-13	**3.2.1.12 Tűzvédelem** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PE-14	**3.2.1.13 Hőmérséklet és páratartalom ellenőrzés** *Döntés: megfelelt*

	Vizsgálati módszerek: Dokumentáció
PE-15	**3.2.1.14 Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
PE-16	**3.2.1.15 Be- és kiszállítás** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*
MA-5	**3.2.1.19 Karbantartók** *Döntés: megfelelt* *Vizsgálati módszerek: Dokumentáció*

III.4. Javaslatok

Az alábbi javaslatok a rendszer jelenlegi vizsgálata, a tanúsítás fókusza szempontjából nem tartoznak az értékelés hatókörébe, de a biztonsági célok elérését segítheti megvalósításuk.

1. Javaslat

F_MK_6, F_MK_7, F_MK_8 követelményeket a rendszerben található naplófájlok feldolgozásával lehet teljesíteni, a rendszerparaméterek nyomon követése az IT üzemeltető részéről manuális munkát igényel. Javasoljuk, hogy a szükséges riportok előállítására dogozzanak ki automatizált folyamatokat.

2. Javaslat

A rendszer üzemeltetője végzett dokumentált helyreállítási teszteket. A magas rendelkezésre állási igény miatt javasoljuk, hogy a helyreállítási tesztek során a teljes helyreállítási folyamat legyen szimulálva, a helyreállítási idő kerüljön mérésre, legyen dokumentálva és legyen összehasonlítva az elvárt értékkel.

3. Javaslat

A rendszer üzemeltetője végzett dokumentált helyreállítási teszteket. A magas rendelkezésre állási igény miatt javasoljuk, hogy a helyreállítási tesztek során a teljes helyreállítási folyamat legyen szimulálva, a helyreállítási idő kerüljön mérésre, legyen dokumentálva és legyen összehasonlítva az elvárt értékkel.

4. Javaslat

Az alkalmazott vírusvédelmi megoldásokat véglegesítsék. Ha Társaság a rendszerben hosszútávon a NOD32 használata mellett döntött, akkor a szükséges tesztelés után telepítsék a szoftvert.

5. Javaslat

A rendszerben jelenleg használt felügyeleti megoldások a rendszer külső elérhetőségét nem tudják monitorozni. Javasolt a külső monitorozás megvalósítása, amely a szolgáltató rendelkezésre állásának ellenőrzését is szolgálhatja.

6. Javaslat

A magas rendelkezésre állási igény miatt az alkalmazott hideg tartalék helyett középtávon javasoljuk feladatátvételt (fail-over) támogató megoldás alkalmazását.

7. Javaslat

A mentések, naplóállományok, konfigurációs állományok jelenleg a hideg tartalékon tárolódnak. Javasoljuk ezeknek az adatoknak a tárolására középtávon biztonságos megoldás kialakítását (pl. külső adathordozóra történő mentés)

8. Javaslat

A jelentés sérülékenység vizsgálatról szóló mellékletében TRANSZREKLAM_BBT.docx leírt „Microsoft IIS "tilde" könyvtár felderítés” hiba segítségével a támadó olyan fájl és könyvtár neveket ismerhet meg, találhat meg, melyek érzékeny adatokat tartalmazhatnak. A sérülékenység az értékelés lezárásáig nem került javításra. Javasoljuk, hogy a hiba kerüljön javításra.

9. Javaslat

A kiszolgálón az alkalmazás által használt AngularJS keretrendszer verziószáma 1.2.13, amely 2014.02.14 –ei verzió. A jelenleg elérhető legfrissebb kiadás 1.5.6 több hibajavítást tartalmaz. Javasoljuk, hogy a megfelelő biztonsági hatásvizsgálat elvégzése után frissítsék az AngularJS verzióját.

10. Javaslat

A kiszolgálón publikusan elérhető a https://transzreklam.hu/loginserver/ids/ url-en az IdentityServer3 modul információs lapja, amely szoftververzióra vonatkozó információkat publikál. Javasoljuk, hogy korlátozzák az URL nyilvános elérhetőségét.

III.5. Következtetés

A rendszer értékelés fő következtetése az alábbi:

A Transzreklám – TRFlow rendszer 2016. június 17-én vizsgált verziója a rendszer biztonsági előirányzatban foglaltaknak megfelel a KIB 28-as Ajánlásában szereplő MIBÉTS módszertan szerinti fokozott SAP-F biztonsági szinten.

III.6. Feltételek

1. A jelen dokumentumban tanúsított kezdeti rendszerértékelés eredményeinek megerősítése, a tanúsítvány érvényességének megtartása és a maradvány kockázatok csökkentése céljából felülvizsgálati rendszerértékelést kell végrehajtani az alábbi esetekben:
    - a Tanúsítvány érvényességi időszakában évente egy alkalommal (tervezett felülvizsgálati rendszerértékelés),
    - a rendszer architektúrájában vagy funkcionalitásában bekövetkezett változtatásokra reagálva (rendkívüli felülvizsgálati rendszerértékelés).
2. A működtetett rendszer architektúrájában vagy funkcionalitásában bekövetkezett jelentős változásokat a Megrendelő köteles a Tanúsítónak a változás érvénybe léptetését követő 30 napon belül bejelenteni, a Tanúsítvány kiállítását megelőző vizsgálatoknak megfelelő mélységben a változások leírását tartalmazó dokumentációkat megküldeni.
3. A 2. esetben a tanúsítvány érvényességének fenntartásához a tanúsító értékeli a változásnak a hatásait és dönt a rendkívüli felülvizsgálati rendszerértékelés szükségességéről. A módosított

rendszer állapotra – megfelelőség esetén - Tanúsítvány Felülvizsgálati Jegyzőkönyvet állít ki. A tervezett vagy rendkívüli felülvizsgálati rendszerértékelés végrehajtásának feltételeit a Megrendelő időben köteles biztosítani.

III.7. Elvárások

A tanúsító elvárja, hogy a működtető tegyen meg mindent az újonnan bevezetett szabályzatok betartása érdekében. Az első tervezett felülvizsgálati rendszerértékelés koncentráljon a szabályzatokban megfogalmazott elvárások maradéktalan teljesülésének ellenőrzésére, a szükséges evidenciák begyűjtésére. A Tanúsítvány érvényességének fenntartása a bizonyítékok megfelelőségének függvénye.

IV. Hivatkozások, rövidítések

IV.1. A követelményeket tartalmazó dokumentum

MIBÉTS 2009 Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v4 2008.09.19) (a KIB 28-as számú Ajánlás része)

IV.2. Figyelembe vett jogszabályok, módszertani dokumentumok

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (IBTV)

1/2016. (II. 1.) Miniszterelnök Kabinetfőnöke rendelet a kormányzati kommunikációs beszerzések során alkalmazható informatikai rendszerrel szemben támasztott követelményekről

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

IV.3. Rövidítések

SETR	System Evaluation Technical Report	rendszer értékelési jelentés
STOE	System Target of Evaluation	a rendszer értékelés tárgya
AC	Access Control	Hozzáférés ellenőrzése
AU	Audit and Accountability	Naplózás és elszámoltathatóság
CM	Configuration Management	Konfigurációkezelés
CP	Contingency Plan	Üzletmenet (ügymenet) folytonosság
IA	Identification and Authentication	Azonosítás és hitelesítés
IR	Incident Response	Reagálás a biztonsági eseményekre
MA	System Maintenance	Karbantartás
MP	Media Protection	Adathordozók védelme
SC	System and Communications	Rendszer- és kommunikációvédelem
SI	System and Information Integrity	Rendszer- és információsértetlenség
PM	Program Management	Szervezeti szintű alapfeladatok
RA	Risk Assessment	Kockázatelemzés
PS	Personnel Security	Emberi tényezőket figyelembe vevő – személy – biztonság
AT	Awareness and Training	Tudatosság és képzés
PE	Physical and Environmental Protection	Fizikai és környezeti védelem