AASZC Galamb József Mezőgazdasági Technikum és Szakképző Iskola informatikai kockázatelemzési mátrixa és intézkedési terve

1. BEVEZETÉS

1.1. A kockázatelemzés alapja, tárgya, célja, készítője

A kockázatelemzés a minősített adat védelmének hatósági felügyeletét és a minősített adatok kezelésének hatósági engedélyezését ellátó Nemzeti Biztonsági Felügyelet által kiadott iránymutatás alapján készült, célja az AASzC Galamb József Mezőgazdasági Technikum és Szakképző Iskola intézménynél telepített, minősített adatot feldolgozó rendszerre vonatkozó kockázatok azonosítása és azok kezelésére vonatkozó intézkedések vizsgálata. Az elemzést a rendszerhez kijelölt rendszer-biztonsági felügyelettel megbízott rendszergazda készítette.

1.2. Rendszerszintű áttekintés

Az intézmény saját üzemeltetésű rendszert is alkalmaz, a szakmai rendszerek központilag biztosítottak, HTTPS protokoll alkalmazása mellet böngészőben elérhető alkalmazások, illetve a pénzügy részleg adatfeldolgozó alkalmazása RDP protokoll alkalmazása mellett távoli asztalon keresztül elérhető. A KIRA rendszer Java segédprogram segítségével érhető el ld. 1. tábla

Rendeltetésük: a szervezet feladatainak végrehajtásához kapcsolódó minősített adatok feldolgozásának biztosítása.

Adatkör és minősítés: nemzeti „Titkos!".

Elhelyezése: 6900 Makó Szép u.2-4.

Szolgáltatásai: oktatási adatok feldolgozása, iratfeldolgozás, pénzügyi, munkaügyi adatok feldolgozása.

Üzemeltetők: HC Delta Kft., Herman Ottó Intézet Nonprofit Kft., eKreta Informatikai Zrt., Magyar Államkincstár

Biztonsági üzemmód: a rendszerhez hozzáférő személyek mindegyike rendelkezik legalább alapfokú informatikai képesítéssel, de mindenki csak a saját munkához szükséges minősített adatokhoz férhet hozzá.

	Rendszer neve	üzemeltetés	elérés
1.	eKreta	központi	HTTPS
2.	Poszeidon iktatórendszer	központi	HTTPS
3.	EOS Ügyviteli Rendszer	központi	RDP
4.	helyi adatok, dokumentumok	helyi	SMB
5.	intézményi honlap	helyi	HTTP
6.	KIRA Központosított Illetmény számfejtési Rendszer	központi	Java
7.	ÉnPostám	központi	HTTPS
8.	Huntéka integrált könyvtári rendszer	központi	Java
9.	Kello	központi	HTTPS

2. A RENDSZER VÉDENDŐ ELEMEINEK MEGHATÁROZÁSA

2.1. A rendszer elemeinek azonosítása

2.1.1. A kezelt adatok és azok értékelése

A rendszeren a szervezetnél készített minősített dokumentumok készülnek, illetve más szervezetektől kapott adathordozók feldolgozását biztosítja legfeljebb „Titkos!" minősítési szintig. Az adatok kiemelt jelentőséggel bírnak a szervezet alapfeladatainak ellátása során, ezért védelmük különösen fontos.

2.1.2. Eszközök azonosítása és értékelése

A rendszert az asztali számítógépek, a kapcsolódó perifériák, nyomtató, alkotja, a telepített operációs rendszerekkel és a felhasználói programokkal, továbbá központi szolgáltatásként nyújtott alkalmazásokkal, valamint a kiadott adathordozókkal. A konfiguráció helyi szervert, valamint rejtjelző eszközöket nem tartalmaz.

A minősített adatállományokkal történő munkavégzés (kidolgozás, módosítás, új fájl létrehozása) a megfelelő külső adathordozókon engedélyezett. A minősített adathordozók kísérőlapjainak kitöltéséért a felhasználó a felelős, a titkos ügykezelő irányítása, és ellenőrzése mellett.

Ezen kívül külső adathordozó csak indokolt esetben csatlakoztatható a rendszerhez (biztonsági mentés végrehajtása, vírusdefiníciós adatbázis frissítésének a kivételével).

A minősített adathordozó eszközök nyilvántartásba vétele előtt a Rendszergazda meggyőződik annak vírusmentességéről.

A munkaállomás merevlemezes háttértárolója kivehető.

2.1.3. Külső kapcsolatot biztosító elemek, átviteli utak

A rendszer külső kapcsolatai rejtjelző eszköz alkalmazásával biztosítottak. A hálózati kábelek a rejtjelző eszközig ellenőrzött területen futnak, végig nyomon követhetőek

Érintett személyek

Az üzemeltetésben és biztonsági felügyeletben résztvevő személyeket a szervezet vezetője hivatalosan kijelölte a feladat ellátásra, ezzel kapcsolatos tevékenységüket a **munkaköri leírások** tartalmazzák.

A rendszer felhasználóiról a szervezet vezetője dönt. A felhasználók a telepített szoftverek futtatására, minősített adat feldolgozására (olvasás) és dokumentumok készítésére, valamint adatmentésre, és biztonsági másolatok készítésére illetve a nyomtató használatára jogosultak. Ha a rendszerrel kapcsolatos bármilyen működési rendellenességet tapasztalnak, akkor kötelesek a rendszerbiztonsági felügyelőt/rendszergazdát értesíteni. A hibaelhárítás elvégzésére a rendszergazda jogosult.

A munkaállomás felhasználói saját felhasználói névvel és jelszóval tudnak bejelentkezni, amelyet az első bejelentkezés alkalmával a Rendszergazda szóban közöl. Az első bejelentkezést követően a felhasználó köteles a jelszavát megváltoztatni, amelyre a rendszer külön fel is hívja a figyelmét, A jelszót bármilyen más adathordozón rögzíteni tilos. A jelszavát minden felhasználó köteles megjegyezni és gondoskodni arról, hogy más személy részére ne váljon hozzáférhetővé.

A rendszer működésében az alábbi személyek rendelkeznek a jelölt jogosultságokkal:
[a táblázat változtatható, törölni kell, ami nem szükséges, pl. rejtjelfelügyelő]

	Beosztás	Jogosultság
1	Biztonsági vezető (Intézményvezető)	ellenőrzési
2	Biztonsági vezető helyettes (Intézményvezető helyettes)	ellenőrzési
3	Rendszerbiztonsági felelős (Rendszergazda)	ellenőrzési, felhasználói, adminisztrátori
4	Felhasználók	felhasználói
5	Titkárság	felhasználói

2.2. A rendszer elemeinek értékelése

A 2.1 pontban felsorolt elemek táblázatos felsorolása és értékelése annak alapján, hogy milyen kockázatot jelent a minősített adatok feldolgozására. (1-10-es skálán, a legkockázatosabb 10-es). [kiegészíthető és a nem szükséges rész törölhető]

	Elsődleges vagyontárgy		Értékelés
1	**Információ**		8
2	**Másodlagos vagyontárgy**		
3	**Hardver**	munkaállomás	3
4		hálózati eszközök	1
5		adathordozók	6
6	**Szoftver**	operációs rendszer	4
7		felhasználói programok	4
8		adatbázisok	5
9	**Személyzet**	Biztonsági vezető	4
10		Rendszergazda	4
11		felhasználók	6
12		Titkos ügykezelők	4

3. A FENYEGETETTSÉG

3.1. A fenyegetettség felmérése:

A fenyegetettség megállapítása a fenyegetések felmérésén (fenyegetés lista, és az ezen kívüli fenyegetések azonosítása) és az előfordulási valószínűségek meghatározásán keresztül történt. A fenyegetés értékelésre kerül egy 10-es skálán, a fenyegetés veszélyességét tekintve az adott rendszer esetében (10-es a legveszélyesebb). Ezt követően a fenyegetés előfordulásának valószínűsége kerül értékelésre szintén 10-es skálán (10-es a legvalószínűbb). A kockázat értéke, a megkapott két számérték szorzataként értelmezhető.

A rendszernél értelmezhető fenyegetések kiválasztása az ISO/IEC 27000-es szabványcsalád alapján, azon belül is az „Információs technológia. Biztonságtechnika. **Információbiztonsági** kockázat kezelés." ISO/IEC 27005-ös szabvány általános fenyegetés listá**jából, valamint** helyi speciális fenyegetések megállapításával történik.

A fenyegetések valószínűségének megállapítási szempontjai:

- a fenyegetés gyakorisága (a tapasztalatok, statisztikák stb. alapján)
- a motiváció (a lehetséges támadók erőforrásai, az informatikai rendszer vagyontárgyainak a lehetséges támadók által érzékelhető vonzereje és sebezhetősége)
- az értékelendő földrajzi tényezők (pl. vegyi- és üzemanyag gyárak közelsége, szélsőséges időjárási viszonyok valószínűsége, és olyan tényezők, amelyek befolyással lehetnek az emberi tévedésekre és a berendezések hibás működésére, a véletlenszerű fenyegetési források tekintetében)
- az emberi tényező, mint az egyik legnagyobb probléma kiváltó ok a fenyegetések bekövetkezésének valószínűségében

3.2. Fenyegetéslista: (a lista a helyi viszonyoknak megfelelően változtatható)

Típus	Fenyegetések	Fenyegetettség szintje	Előfordulás valószínűsége	Kockázati érték
Fizikai kár	Tűzkár (terület elhagyásának akadályozottsága)	4	4	16
Fizikai kár	Vízkár (beázás, csőtörés)	3	2	6
Fizikai kár	Szennyeződés	3	3	9
Fizikai kár	Főbb balesetek	4	3	12
Fizikai kár	Berendezés vagy adathordozó megsemmisülés	4	4	16
Fizikai kár	Por, korrózió, fagyás	5	3	15
Fizikai kár	Épület statikai állapota	2	2	4
Természeti csapás	Szélsőséges klíma	3	3	9
Természeti csapás	Földrengés	1	1	1
Természeti csapás	Szélsőséges időjárás (vihar, villámlás)	6	4	24
Természeti csapás	Árvíz	1	1	1
Kritikus szolgáltatások kimaradása	Vízellátás	2	1	2

Típus	Fenyegetések	Fenyegetettség szintje	Előfordulás valószínűsége	Kockázati érték
Kritikus szolgáltatások kimaradása	Légkondicionálás	5	6	30
Kritikus szolgáltatások kimaradása	Áramkimaradás	5	5	25
Kritikus szolgáltatások kimaradása	Telekommunikációs kimaradás	5	5	25
Sugárzás okozta károk	Hősugárzás	2	2	4
Sugárzás okozta károk	EMP (elektromágneses sugárzás)	2	2	4
Kompromittálódás	Kompromittáló elektromágneses kisugárzás (tápszűrő hiánya, radiátor földeletlensége)	3	2	6
Kompromittálódás	Kémprogram és vírus	5	4	20
Kompromittálódás	Lehallgatás	3	2	6
Kompromittálódás	Külső kémkedés	4	2	8
Kompromittálódás	Adathordozó vagy dokumentum lopása	3	3	9
Kompromittálódás	Berendezés lopása	3	3	9
Kompromittálódás	Törölt vagy megsemmisített információ visszaállítása	4	3	12
Kompromittálódás	Az előírásoknak megfelelő iratmegsemmisítő hiánya	3	2	6
Kompromittálódás	Illetéktelen megismerés	3	3	9
Kompromittálódás	Nem megbízható forrásból származó adat (dezinformáció)	3	2	6
Kompromittálódás	Hardware illetéktelen módosítása	3	3	9
Kompromittálódás	Software illetéktelen módosítása	3	3	9
Kompromittálódás	A távközlési médiumok és üzenettovábbító eszközök (kép és hang rögzítésére alkalmas) helyes használatára vonatkozó szabályok ismeretének hiánya	4	5	20
Kompromittálódás	A fenyegetettség! helyzet lebecsülése	5	6	30
Kompromittálódás	Nem kielégítő képzés	5	6	30

Típus	Fenyegetések	Fenyegetettség szintje	Előfordulás valószínűsége	Kockázati érték
Kompromittálódás	Hiányos felelősségtudat	5	6	30
Kompromittálódás	Megszokási veszélyhelyzetek, napi rutin, kényelmesség	5	7	35
Kompromittálódás	Szervezeten kívüli személyek (látogatók, szerelők, szállítók, takarítók, karbantartók, stb.)	5	3	15
Kompromittálódás	Szervezeten belüli személyek szükségtelen bent tartózkodás	4	3	12
Kompromittálódás	Adathordozók (HDD, CD, floppy, pendrive, stb.) jogosulatlan használata	5	3	15
Kompromittálódás	A szervezet tulajdonát képező adathordozók és berendezések magáncélú használata	5	3	15
Kompromittálódás	A magántulajdonú adathordozók és berendezések szervezeti célú használata	7	8	56
Kompromittálódás	Pozíció meghatározása	3	3	9
Technikai meghibásodás	Berendezés meghibásodása	5	8	40
Technikai meghibásodás	Berendezés hibás működése	4	8	32
"Technikai meghibásodás	Software hibás működése	5	7	35
Technikai meghibásodás	Információs rendszer túlterhelése	5	6	30
Technikai meghibásodás	Rendszer karbantartási szabályainak megsértése	5	5	25
Technikai meghibásodások	Karbantartás hiánya	5	6	30
Technikai, meghibásodások	Tartozékok és pótalkatrészek utánpótlásának hiánya	5	7	35
Engedély nélküli műveletek	Berendezés illetéktelen használata	5	4	20
Engedély nélküli műveletek	Nem jogtiszta, másolt szoftver alkalmazása	6	3	18
Engedély nélküli műveletek	Állandó rendszerfelügyelet hiánya (munkaidő utáni riasztás)	5	4	20

Típus	Fenyegetések	Fenyegetettség szintje	Előfordulás valószínűsége	Kockázati érték
Engedély nélküli műveletek	Biztonságtudatosság hiánya (felhasználói hibák veszélye)	7	6	42
Engedély nélküli műveletek	Kilépés elmulasztása a felhasználói fiókból	5	6	30
Engedély nélküli műveletek	Adatok illetéktelen módosítása	6	3	18
Engedély nélküli műveletek	Illegális adatfeldolgozás	6	3	18
Funkciók veszélyeztetése	Felhasználás során bekövetkezet hiba	6	4	24
Funkciók veszélyeztetése	Iratok azonnali és pontos dokumentálása, vezetése (nyomonkövethetőség)	3	7	21
Funkciók veszélyeztetése	Jogosultsággal való visszaélés	5	4	20
Funkciók veszélyeztetése	Jogosultság illetéktelen megszerzése (nem megfelelő bonyolultságú, valamint nem megfelelően kezelt jelszavak)	5	3	15
Funkciók veszélyeztetése	Jogosulatlan hozzáférés, felhasználás kivizsgálásának hiánya	5	5	25
Funkciók veszélyeztetése	Indokolatlanul magas jogosultsági szint	6	5	30
Funkciók veszélyeztetése	Adathordozók ellenőrizetlen használata (pendrive, mp3 lejátszó, okostelefon, külső meghajtó stb.)	5	10	50
Funkciók veszélyeztetése	Műveletek megtagadása	5	3	15
Funkciók veszélyeztetése	Hiányzó vagy hiányos ellenőrzés, visszaellenőrzés	5	4	20
Funkciók veszélyeztetése	Személyek rendelkezésre állásának hiánya	6	4	24
Funkciók veszélyeztetése	Biztonsági incidensek esetén alkalmazandó fegyelmező intézkedések hiánya	4	5	20

3.3. Minimum biztonsági követelmények (jelölés: szürke) és elfogadható kockázat azonosítása

A fenti táblázat kockázati érték szerinti rendezése, elől a legmagasabb értékű elemek.

Típus	Fenyegetések	Fenyegetettség szintje	Előfordulás valószínűsége	Kockázati érték	Elfogadható minimum	Intézkedési terv	Megvalósítás kompetenciája
Funkciók veszélyeztetése	Adathordozók ellenőrizetlen használata	5	10	50	35	Az adathordozók használatának visszaszorítása	helyi
Funkciók veszélyeztetése	Indokolatlanul magas jogosultsági szint	6	5	30	35		
Kompromittálódás	A magántulajdonú adathordozók és berendezések szervezeti célú használata	7	8	56	35	Az adathordozók használatának visszaszorítása	helyi
Kompromittálódás	Megszokási veszélyhelyzetek, napi rutin, kényelmesség	5	7	35	35	Jelszavak mentésének, mellőzése.	helyi
Technikai meghibásodás	Berendezés meghibásodása	5	8	40	35	Folyamatos hardver monitorozás.	helyi
Technikai meghibásodás	Software hibás működése	5	7	35	35	Szoftverfrissítések	helyi
Kritikus szolgáltatások kimaradása	Légkondicionálás	5	6	30	30	Légkondicionáló beszerelése	helyi
Természeti csapás	Szélsőséges időjárás (vihar, villámlás)	6	4	24	20	Túlfeszültségvédők beszerzése	helyi

4. MEGLÉVŐ ÉS TERVEZETT ELLENINTÉZKEDÉSEK

A sorba rendezett fenyegetéslistában minimum biztonsági követelményként azonosított beszürkített fenyegetésekre vannak már meglévő ellentevékenységek, melyek vagy megszűntetik, vagy elfogadható szintre csökkentik a fennálló kockázatokat.

Hálózati elemek kockázatának csökkentése.

Tekintettel a hálózatban elterjedten használt vezeték nélküli adatátvitel igényére, ennek védelme fokozott biztonsági intézkedéseket igényel. Meg kell szüntetni az AP-k széttagolt használatát, és konfigurációikat egységesíteni kell biztonsági szempontból is. Erős kódolást kell alkalmazni, amely minimum WPA2 kódolást használjon, a dekódoló kulcsot rendszeresen cserélni kell. Ezen követelmények megvalósításához központilag menedzselhető eszközállomány beszerzése és a teljes hálózati struktúra újra tervezésére van szükség.

Fizikai kockázatok csökkentése

A **hardware elemek** és az adatok illetéktelen módosításának, valamint a jogosultsággal való visszaélés kockázatát teljes mértékben megszüntetni nem lehet, azonban az intézmény biztonsági területeire történő belépési előírásoknak történő megfelelés (mágneskártyás ellenőrzött, regisztrált belépés, személyi biztonsági feltételeknek történő megfelelés)

elfogadható szintre csökkenti azt. Megelőzően be kell azonosítani azokat a területeket, melyeket külső látogatók nem, szerelői, karbantartói tevékenységet külsősként végzők, pedig csak kísérettel látogathatnak.

A tűzkár kockázatát elfogadható szintre csökkenti a helységben elhelyezett tűzjelző berendezés, amely nagymértékben lerövidíti a tűz észlelése és oltása között eltelt időt.

A tartozékok és pótalkatrészek utánpótlási hiányának kockázatát elfogadható mértékűre csökkenti tartalékok képzése a működő eszközállomány 10%-os mértékének arányában.

Működési és szoftver elemek kompromitálhatóságának csökkentése

A **kémprogramok és vírusok** jelentette kockázatot csökkenti, hogy a minősített munkaállomás Informatikai Biztonsági Szabályzatában foglaltak szerint, a rendszer esetében csak a szervezet által biztosított, ügyvitel által nyilvántartásba vett és szükség szerint minősített külső adathordozók használhatók, más forrásból származó és magántulajdonú adathordozó eszközök használata tilos. A külső adathordozó csak indokolt esetben csatlakoztatható a rendszerhez (biztonsági mentés végrehajtása, vírusdefiníciós adatbázis frissítésének a kivételével). A minősített adathordozó eszközök nyilvántartásba vétele előtt a Titkos ügykezelő meggyőződik annak vírusmentességéről a Rendszergazda segítségével az alkalmazott vírusirtó program használatával. A rendszer a vírus és kémprogram valamint a hacker támadásoknak különösen kitett, két alapvető okból. Ezek

- a magán tulajdonban lévő eszközök, laptopok kiterjedt használata a hálózaton
- határvédelem nélküli lakossági végpont üzemben tartása
- kliensgépeken rendszergazdai jogok használata

Ezeket a sérülékenységeket eszközbeszerzéssel, a hálózat átstrukturálásával és szoftveres biztonsági intézkedésekkel meg kell szüntetni.

További sérülékenység a jelszavak használatának teljes mellőzése vagy gyenge jelszavak használata az **authentikáció** során. Ezt a gyakorlatot biztonsági intézkedésekkel, oktatással, figyelemfelhívással, intézményi informatikai működés bevezetésével (domain kialakítás, group policy, felhasználómenedzsment) lehet megszüntetni.

Az intézmény elektronikus levelezéssel tartja a kapcsolatot az alkalmazottal, társintézményekkel, központi irányítással és külső szereplőkkel. Ehhez a Google kisvállalati szolgáltatását veszi igénybe, ingyenesen. Ez a megoldás azt a biztonsági kockázatot rejti, hogy a Szolgáltató egyoldalúan módosíthat olyan Szerződési feltételeket, amelyek az intézmény számára kedvezőtlenek. Célszerű lenne intézményi saját, vagy központilag bérelt szerveren levelezési rendszert üzemeltetni, mely az intézmény kezelésében van.

Az intézményen belül keletkezett adatok mentése archiválása nem megoldott ezért az **adatbiztonság** súlyosan sérül. Jelenleg a keletkező dokumentumok csak a kliens gépek háttértárain vannak elhelyezve. Ennek megszüntetésére a fent említett intézményi struktúra kialakítása, osztott, központi mappák használata és adatmentésre alkalmas eszközök beszerzése lehet a megoldás.

5. SEBEZHETŐSÉG

Sebezhetőségként kerültek azonosításra a rendszer és rendszerelemek azon tulajdonságai, amelyek kihasználásával a fenyegetés a hatását ki tudja fejteni. Annak érdekében, hogy megszűnjön a kapcsolat a fenyegetés és a sebezhetőség között, meg kell vizsgálni a sebezhetőségeket az azonosított vagyontárgyak szempontjából. Az elektronikus információkezelő rendszerek általános támadhatósági lehetőségeit áttekintve a minősített munkaállomás esetében a következő sebezhetőségek határolhatók körül:

- A hardware, software elemek valamint a kezelt adatok illetéktelen módosításának lehetősége a rendszergazdai jogosultsággal rendelkező összes személy részéről.
- A rendszergazdai jogosultsággal történő visszaélés
- Fennáll a lehetősége a szoftver- és a hardverelemekben biztonsági rések szándékos létrehozásának.
- Hibás működés adódhat a szoftver- és a hardverelemek meghibásodásából, tervezési hibából vagy szándékos beavatkozás következtében.
- Sebezhetőségi pont az információ kompromittálhatósága az eszközök véletlen kisugárzásának felhasználásával.
- A kereskedelmi forgalomból szabadon vásárolható berendezések nem kerülnek a biztonsági kritériumok szerinti vizsgálat alá. Alacsony biztonsági szintű hálózati elemek, olcsó SOHO wifi routerek tömeges alkalmazása.
- A rendkívül csekély számú tartozék és pótalkatrész, szintén nagymértékben növeli a rendszer sebezhetőségét, amely végső esetben a rendszer kieséséhez is vezethet.
- a meglevő eszközállomány elavultsága
- már nem támogatott operációs rendszerek használata Windows XP! Windows 7 jelenléte a rendszerben
- azonosítás és autentikáció teljes hiánya, jelszóhasználat mellőzése vagy gyenge jelszavak használata
- magántulajdonú eszközök, laptopok, mobil eszközök, mobil adathordozók használata
- alapszintű víruskereső használata, központilag menedzselt helyett (frissítések ellenőrizhetetlensége, incidensek beazonosíthatatlansága)

6. A KOCKÁZATOK FELMÉRÉSE

6.1. Kockázatok

A kockázat a rendszerek gyenge pontjainak kihasználási valószínűsége a fenyegetések által, ami a rendszer kompromittálódásához vezet. A komoly kockázatok általában a rendszer legsebezhetőbb komponensei ellen irányuló legnagyobb és a legvalószínűbb fenyegetésekből fakadnak.

Annak érdekében, hogy a rendszerre irányuló fenyegetésekkel szemben fellépjünk, az alábbi biztonsági funkciók (ellenintézkedések) állnak rendelkezésünkre: [BF: Biztonsági funkció, a lista módosítható]

a. / BF 1 - Hozzáférések felügyelete

A rendszerbiztonsági (telepítési) környezeteibe való belépés, rendszerelemekhez (szoftver és hardver) és adathoz való hozzáférés szabályozásának lehetősége.

b. / BF 2 - Azonosítás és hitelesítés

A hozzáférésre jogosult személyek megbízható azonosítását biztosító eljárások (felhasználói azonosítóval és jelszóval történő azonosítás).

c. / BF 3 - Elszámoltathatóság

A végzett tevékenységgel való egyértelmű elszámoltathatóság (adatkezelés, telepítés, módosítás, törlés, rendszerparaméterek átállítása, jogosultság változtatása).

d. BF 4 - Minősítés jelölése

A rendszerben tárolt, feldolgozott és továbbított információk minősítési szintjüknek megfelelő kezelése.

e./ BF 5 - Sértetlenség ellenőrzés

A rendszerben és a feldolgozott adatokban történő illetéktelen módosítás lehetőségeinek következetes ellenőrzése.

f./ BF 6 - Rendelkezésre állás ellenőrzése

A jogos hozzáférések, szolgáltatások meglétének, a rendszer teljes területén folyamatos üzemeltetés biztosításának ellenőrzése.

g. / BF 7 - Kommunikáció ellenőrzése

Olyan biztonságos átviteli utak, szoftverek, eszközök és beállítások használata, amelyek biztosítják az adatok bizalmasságának és sértetlenségének megőrzését az átvitel során,

h. / BF 8 - Biztonsági (audit) ellenőrzések

A fizikai környezettel, a felhasználókkal, a dokumentálással, a szoftverrel, a felhasználói kezeléssel és a berendezésekkel, kapcsolatos biztonsági szempontból lényeges események, tevékenységek, és eljárások folyamatos monitorozása és ellenőrzése.

i. / Általános fenyegetések

Az általános fenyegetések a 3. pontban ismertetésre kerültek.

6.2. Rendszer-specifikus fenyegetések

A rendszer-specifikus fenyegetések, sebezhetőség és kockázatok szintjei, az információk és a munkaállomás szolgáltatásainak specifikus fenyegetései a következők [F: Fenyegetés, a lista módosítható]:

a. a./ F1 - Lehallgatás és kémkedés

A minősítési szintet elérő információk tárolására, feldolgozására vagy továbbítására alkalmas számítógéphez történő behatolási kísérlet valószínűsége hírszerző szervezetek, személyek által, ami a bizalmasság, sértetlenség és rendelkezésre állás sérülését eredményezheti.

b. F2 - Megszemélyesítés

A megszemélyesítés során jogosultság nélküli személy jogosultsággal rendelkező személynek adja ki magát azzal a céllal, hogy hozzáférhessen a munkaállomás azon adataihoz, amelyek megkönnyítik számára a hozzáférést.

c. F3 - Rejtett hozzáférés és szoros követés

A jogosulatlan személy a számítógép elemeihez/információihoz fizikai és/vagy elektronikus módszereket használva próbál hozzáférni.

d. F4 - Rosszindulatú szoftver

Fenyegetettséget jelent az engedély nélküli szoftver telepítése, a számítógépbe történő bejuttatása.

e. F5 - Jogosultsággal történő visszaélés

A rendszeren minden egyes felhasználó rendszergazdai jogosultságokkal rendelkezik, a speciális felhasználói segédprogram futtatási követelményei miatt, amely a hardware és software elemek, valamint a kezelt adatok kompromittálódásához vezethet.

F6 - A rendszer rendelkezésre állása

A csekély számú tartozék és pótalkatrész maga után vonja a rendszer meghibásodása utáni, alkalmazhatóságból történő kiesését.

Az azonosított fenyegetések és az ellenük alkalmazandó ellenintézkedések közötti kapcsolat a következő táblázatban foglalható össze:

	Biztonsági funkciók							
Fenyegetés	BF1	BF2	BF3	BF4	BF5	BF6	BF7	BF8
F1	X	X	X	X			X	X
F2	X	X	X				X	X
F3	X					X	X	X
F4	X	X			X	X	X	X
F5	X	X	X	X	X	X	X	X
F6						X	X	X

A fenyegetések hatásait csökkentő biztonsági ellenintézkedések végrehajtására a biztonsági felügyeletek által megvizsgált és engedélyezett, lehetőleg automatizált biztonsági funkciókat kell alkalmazni.

A biztonság kezdeti szintjét a „Titkos!" minősítési szintű adatok védelmére előírt biztonsági követelmények szerint kialakított és akkreditált rendszer biztonsági funkciói adják, amelyek a biztonsági felügyeletek által végzett ellenőrzések tapasztalatai szerint - szükségszerűen - kerülnek felülvizsgálatra, módosításra, alkalmazásra.

A szükségessé váló kiegészítő biztonsági funkciók alkalmazásáig mindenképpen számolni kell egy elfogadható érték alatti maradvány kockázattal,

A rendszer specifikus fenyegetések, sebezhetőség és kockázatok szintjeit az információk és a támogató rendszerszolgáltatások bizalmasságára, sértetlenségére és rendelkezésre állására az alábbi táblázat tartalmazza:

Fenyegetés	**A fenyegetés szintje**	**Sebezhetőség szintje**	**A kockázat szintje**
F1	alacsony	alacsony	alacsony
F2	alacsony	alacsony	alacsony
F3	alacsony	alacsony	alacsony
F4	alacsony	alacsony	közepes
F5	közepes	közepes	közepes
F6	magas	magas	magas

7. KONKLÚZIÓ

7.1. Az elemzés összegzése

Összességében megállapítható hogy a kockázatfelmérés, majd a kockázatelemzés a kezelt adatok bizalmassága, sértetlensége illetve rendelkezésre állásának vizsgálatára épült, kompromittáló tényezőt súlyos fenyegetéseket tárt fel.

Makó, 2022.06.14.

.....
Horváth Zoltán
igazgató

.....
Gregor Csaba
készítő
rendszergazda