e-Közigazgatási
Keretrendszer
Kialakítása

ÚMFT infovonal:
06 40 638 638
nfu@nfu.gov.hu • www.nfu.hu

Új Magyarország
FEJLESZTÉSI TERV

IT BIZTONSÁGI MŰSZAKI KÖVETELMÉNYEK A KÜLÖNBÖZŐ BIZTONSÁGI SZINTEKRE

KÖVETELMÉNY ELŐÍRÁS

A dokumentum az Új Magyarország Fejlesztési Terv keretében, az Államreform Operatív Program támogatásával, az „Elektronikus közigazgatási keretrendszer” tárgyú kiemelt projekt megvalósításának részeként készült. A dokumentum elkészítésében részt vett:

1.

Meta adat-táblázat

Megnevezés	Leírás
Cím (dc:Title)	IT biztonsági műszaki követelmények
Kulcsszó (dc:Subject)	IT biztonság; IT biztonsági szint; ajánlás; IT biztonsági követelmény
Leírás (dc:Description)	Az e-közigazgatási projektek tervezése és megvalósítása során elengedhetetlen, hogy az adott projekt megfelelő IT biztonsági műszaki követelmények alapján végezze a munkát. Annak elkerülésére, hogy a projektek önkényesen határozzák meg, vagy akár teljesen figyelmen kívül hagyják ezeket a tényezőket, elkészült egy háromszintű besorolás, és mindhárom kategóriához meghatározásra került egy olyan minimális vagy tipikus IT biztonsági műszaki követelményeket tartalmazó követelményrendszer, amely az adott projektre nézve kötelezően előírandó, betartandó és ellenőrizendő. Jelen Követelmény előírás tartalmazza a kategóriákhoz tartozó biztonsági műszaki követelményeket.
Típus (dc:Type)	szöveg
Forrás (dc:Source)	
Kapcsolat (dc:Relation)	
Terület (dc:Coverage)	
Létrehozó (dc:Creator)	e-Közigazgatási Keretrendszer Kialakítása projekt
Kiadó (dc:Publisher)	MEH
Résztvevő (dc:Contributor)	HunGuard Kft.
Jogok (dc:Rights)	
Dátum (dc:Date)	2008.08.22.
Formátum (dc:Format)	MS Word doc
Azonosító (dc:Identifier)	
Nyelv (dc:Language)	magyar
Verzió (dc:Version)	1.01
Státusz (State)	átadott verzió
Fájlnév (FileName)	EKK_ekozig_ITbiztonsagikovetelmenyrendszer_080822_V101.doc
Méret (Size)	1251 KB
Ár (Price)	
Felhasználási jogok (UserRights)	

2. Verziókövetési táblázat (a szabvány második oldala)

A dokumentum neve	IT biztonsági műszaki követelmények
A dokumentum készítőjének neve	HunGuard Kft.
A dokumentum jóváhagyójának neve	
A dokumentum készítésének dátuma	2008.08.22.
Verziószám	1.01
Összes oldalszám	113
A projekt azonosítója	EKK_ekozig

2.1. Változáskezelés

Verzió	**Dátum**	**A változás leírása**
V0.8	2008.07.07	Előminősítésre átadott verzió
V0.9	2008.07.24	Ellenőrzött, javított verzió
V1.0	2008.07.25	Átadott verzió
V1.01	2008.08.22	Hivatkozások táblázatos megadása

3. Szövegsablon

Megnevezés	Leírás
1. Előszó (Foreword)	.
2. Bevezetés (Preamble)	.
3. Alkalmazási terület (Scope)	IT biztonsági követelmények
4. Rendelkező hivatkozások (References)	.
5. Fogalom-meghatározások (Definitions)	.
6. A szabvány egyedi tartalma (UniqueContent)	.
7. Bibliográfia	.
8. Rövidítésgyűjtemény	.
9. Fogalomtár	.
10. Ábrák	.
11. Képek	.
12. Fogalmak	.
13. Verzió	.
14. Mellékletek (Appendix)	.

Tartalomjegyzék

4. Előszó

A közigazgatásban alkalmazott rendszerekkel szemben támasztott követelmény, hogy informatikai biztonsági szempontból megfelelőek legyenek.

Az IT biztonsági műszaki követelmények, olyan óvintézkedések (ellenintézkedések), melyek elsősorban az informatikai rendszer valósít meg, illetve hajt végre, a rendszer hardver, szoftver vagy förmver összetevőiben megvalósuló mechanizmusok segítségével.
Jelen dokumentum katalogizálja, és meghatározza az egyes biztonsági szintekhez tartozó biztonsági műszaki követelményeket.

Jelen dokumentum szorosan kapcsolódik az alábbi dokumentumokhoz:
„Útmutató az IT biztonsági szintek meghatározásához” c. Útmutató dokumentum [03]
„Minta biztonsági kategorizálás” c. Segédlet [04]
*„Rendszerekre vonatkozó értékelési módszertan „*c. Útmutató dokumentum [05]

5. Bevezetés

Az e-közigazgatási projektek tervezése és megvalósítása során elengedhetetlen, hogy az adott projekt megfelelő IT biztonsági műszaki követelmények alapján végezze a munkát. Annak elkerülésére, hogy a projektek önkényesen határozzák meg, vagy akár teljesen figyelmen kívül hagyják ezeket a tényezőket, készült el jelen dokumentum, mely minimális illetve tipikus IT biztonsági műszaki követelményeket tartalmazó követelményrendszer. *(„IT biztonsági műszaki követelmények a különböző biztonsági szintekre”* c. Követelmény előírás)

Ahhoz, hogy a biztonsági műszaki követelmények általában elérjék céljukat és az adott szolgáltatás tényleges biztonságát szolgálják, kielégítsék a velük szemben támasztott reális követelményeket, elég erősek és hatékonyak, ugyanakkor megvalósíthatóak legyenek, a szolgáltatás (IT termék, vagy rendszer) alapfeladataiból, a működési környezetből és feltételekből kiindulva kell meghatározni őket. A meghatározás módja többféle lehet, a nemzetközi és hazai szakirodalom, valamint a szabványok és legjobb gyakorlatok különböző eljárásokat kínálnak, de minden esetben egy fáradtságos és hosszú folyamat eredményeként adhatók meg. A megoldások általában a fenyegetettségek feltárásával, részletes kockázatbecslés után, kockázatkezelési eljárás keretében (MSZ ISO/IEC 17799 [01], ISO/IEC 27001 [02]) születnek meg, vagy magas szintű és jelentős mértékű előzetes szakmai munkát követően (pl. Common Criteria [07] Védelmi Profiljai) azok felhasználásával vezethetnek eredményre.

A projekt keretében kidolgozásra került követelmény előírás háromszintű besoroláson alapul, melynek fontossága abban rejlik, hogy egy szolgáltatás, vagy IT rendszer esetében könnyen meghatározható a megkívánt IT biztonsági szint, és mindhárom szinthez konkrét IT biztonsági technikai követelmények tartoznak. Az amerikai kormányzati és közigazgatási rendszerekben is használt, javasolt eljárás használatával (NIST SP 800-53 [06], FIPS PUB 199 [10], FIPS PUB 200 [11]) általános esetekben jóval gyorsabban lehet az adott projekt IT biztonsági műszaki követelményeit meghatározni. Speciális esetekben a biztonság egy-egy

igényelt területen tovább növelhető, az igények részletesebb feltárásával. Ennek a testre szabási, ún. tailorizálási tevékenységnek a fokozatos növelésével egyre pontosabb és pontosabb közelítése érhető el az eredeti kockázatkezelési módszeren alapuló procedúrának.

Az *„Útmutató az IT biztonsági szintek meghatározásához”* c. útmutató dokumentum [03] és az azt kiegészítő *„Minta biztonsági kategorizálás”* c. segédlet [04] eljárást adnak az egyes rendszerek, projektek IT biztonsági osztályba sorolására.

Jelen Követelmény dokumentum a konkrét projektek IT biztonsági osztályba sorolása után határozza meg az IT biztonsági technikai követelményeket az alábbi szerkezetben:

A 6. fejezet áttekinti a műszaki biztonsági intézkedéseket. A 6.1 fejezet áttekintést ad az útmutató alapját képező szabványok és ajánlásokról, illetve azokat egymásnak megfelelteti. A 6.2 fejezet a műszaki biztonsági intézkedések hat családjának részletes kifejtését tartalmazza. Megadva a konkrét intézkedést, azoknak esetleges bővítéseit, és a magyarázatul szolgáló kiegészítéseit. A 6.3 fejezet a műszaki biztonsági intézkedéseket kategorizálja be alacsony, fokozott és kiemelt kihatású biztonsági osztályokba, megadva az egyre részletesebb és erősségében bővülő műszaki biztonsági intézkedések. A 6.4 fejezet az alacsony, fokozott és kiemelt kihatású biztonsági osztályokba sorolt intézkedések garanciális követelményeit adja meg.

A 7-es fejezetben három melléklet segíti az olvasót az intézkedések használatában. A 7.1 fejezet a biztonsági tervként szolgáló rendszer biztonsági előirányzat struktúráját ismerteti. A 7.2-es fejezet a biztonsági napló menedzsmentről ad áttekintést kiegészítve a Naplózás és elszámoltathatóság (NA) intézkedés család elemeit. A 7.3-as fejezet az Azonosítás és hitelesítés (AH) intézkedéseinek alkalmazásához nyújt kiegészítő információkat, különös tekintettel a hitelesítésre használandó tokenekre.

A bibliográfia, a rövidítésgyűjtemény valamint a fogalomtár a jobb érthetőséget hivatott biztosítani.

6. Alkalmazási terület

Ez a dokumentum az informatikai rendszerek és informatikai biztonság szakértőinek készült beleértve:

- informatikai rendszerek és informatikai biztonság irányításával és felügyeletével foglalkozó vezetők (pl. informatikai igazgatók, magas beosztású informatikai tisztviselők és IT biztonságért felelős vezetők);
- az informatikai rendszer fejlesztéséért felelős személyek (program és projekt menedzserek, feladat/alkalmazás tulajdonosok, rendszertervezők, rendszer és alkalmazás programozók);
- az informatikai rendszer megvalósításáért és üzemeltetéséért felelős személyek (pl. az informatikai rendszer tulajdonosai, az információ tulajdonosai, az informatikai rendszer rendszergazdái, az informatikai rendszer biztonsági tisztviselői);
- az informatikai rendszer és informatikai biztonság felmérésével és megfigyelésével foglalkozó személyek (pl. auditorok, általános ellenőrök, értékelők és tanúsítók).

Az informatikai termékeket és rendszereket vagy informatikai biztonsággal kapcsolatos rendszereket készítő, vagy informatikai biztonsággal kapcsolatos szolgáltatásokat nyújtó kereskedelmi vállalatok szintén hasznosíthatják az itt leírt információkat.

7. Rendelkező hivatkozások

[01] MSZ ISO/IEC 17799:2006 Az információbiztonság irányítási gyakorlatának kézikönyve

[02] MSZ ISO/IEC 27001:2006 Az információbiztonság irányítási rendszerei. Követelmények

[03] Útmutató az IT biztonsági szintek meghatározásához BME IK 2008.

[04] Minta biztonsági kategorizálás BME IK 2008.

[05] Rendszerekre vonatkozó értékelési módszertan BME IK 2008.

[06] National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, December 2007

[07] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 2

[08] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 2

[09] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 2

[10] National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

[11] National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

[12] National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 2001

[13] National Institute of Standards and Technology Special Publication 800-28, Guidelines on Active Content and Mobile Code, October 2001.

[14] National Institute of Standards and Technology Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001.

[15] National Institute of Standards and Technology Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002.

[16] National Institute of Standards and Technology Special Publication 800-63, Version 1.0.2, Electronic Authentication Guideline April 2006.

[17] National Institute of Standards and Technology Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005.

[18] National Institute of Standards and Technology Special Publication 800-56A (Revised), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007.

[19] National Institute of Standards and Technology Special Publication 800-57 (Revised), Recommendation on Key Management, Part 1: General, March 2007.

[20] National Institute of Standards and Technology Special Publication 800-58, Security Considerations for Voice Over IP Systems, January 2005.

[21] National Institute of Standards and Technology Special Publication 800-77, Guide to IPsec VPNs, December 2005.

[22] National Institute of Standards and Technology Special Publication 800-81, Secure Domain Name System (DNS) Deployment Guide, May 2006.

[23] National Institute of Standards and Technology Special Publication 800-92, Guide to Computer Security Log Management, September 2006.

[24] National Institute of Standards and Technology Special Publication 800-95, Guide to Secure Web Services, August 2007.

[25] National Institute of Standards and Technology Special Publication 800-97, Establishing Robust Security Networks: A Guide to IEEE 802. 11i February 2007.

[26] RFC 3195 Reliable Delivery for syslog

Az alábbiakban megadjuk a rendelkező hivatkozások elérhetőségeit.

Cím	Külföldi elérhetőség	Magyar elérhetőség
MSZ ISO/IEC 17799:2006 Az információbiztonság irányítási gyakorlatának kézikönyve		MSZ ISO/IEC 17799:2006
MSZ ISO/IEC 27001:2006 Az információbiztonság irányítási rendszerei. Követelmények		MSZ ISO/IEC 27001:2006
Útmutató az IT biztonsági szintek meghatározásához		---

Cím	Külföldi elérhetőség	Magyar elérhetőség
Minta biztonsági kategorizálás		---
Rendszerekre vonatkozó értékelési módszertan		---
National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, December 2007	NIST SP 800-53	
Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 2	CC 3.1 Part 1	
Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 2	CC 3.1 Part 2	
Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 2	CC 3.1 Part 3	
National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.	FIPS 199	
National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.	FIPS 200	
National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 2001	FIPS 140-2	
National Institute of Standards and Technology Special Publication 800-28, Guidelines on Active Content and Mobile Code, October 2001.	NIST SP 800-28	
National Institute of Standards and Technology Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001.	NIST SP 800-32	

Cím	Külföldi elérhetőség	Magyar elérhetőség
National Institute of Standards and Technology Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002.	NIST SP 800-48	
National Institute of Standards and Technology Special Publication 800-63, Version 1.0.2, Electronic Authentication Guideline April 2006.	NIST SP 800-63	
National Institute of Standards and Technology Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005.	NIST SP 800-52	
National Institute of Standards and Technology Special Publication 800-56A (Revised), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007.	NIST SP 800-56A	
National Institute of Standards and Technology Special Publication 800-57 (Revised), Recommendation on Key Management, Part 1: General, March 2007.	NIST SP 800-57 Part 1	
National Institute of Standards and Technology Special Publication 800-58, Security Considerations for Voice Over IP Systems, January 2005.	NIST SP 800-58	
National Institute of Standards and Technology Special Publication 800-77, Guide to IPsec VPNs, December 2005.	NIST SP 800-77	
National Institute of Standards and Technology Special Publication 800-81, Secure Domain Name System (DNS) Deployment Guide, May 2006.	NIST SP 800-81	
National Institute of Standards and Technology Special Publication 800-92, Guide to Computer Security Log Management, September 2006.	NIST SP 800-92	
National Institute of Standards and Technology Special Publication 800-95, Guide to Secure Web Services, August 2007.	NIST SP 800-95	

Cím	Külföldi elérhetőség	Magyar elérhetőség
National Institute of Standards and Technology Special Publication 800-97, Establishing Robust Security Networks: A Guide to IEEE 802. 11i February 2007.	NIST SP 800-97	
RFC 3195 Reliable Delivery for syslog	RFC 3195	

8. Fogalom-meghatározások

Jelen dokumentum nem tartalmaz fogalom-meghatározásokat.

9. A műszaki biztonsági intézkedések

9.1. Áttekintés

9.1.1. Az ISO/IEC 17799 intézkedés kategóriái

Az MSZ ISO/IEC 17799:2006 útmutató szabvány [01], és az annak megfelelő a MSZ ISO/IEC 27001:2006 [02] követelmény szabvány a biztonságirányítás irányelveket és általános alapelveket állapít meg az információbiztonság irányításának kezdeményezésére, bevezetésére, fenntartására és fejlesztésére egy szervezeten belül. A szabvány 11 területen belül fogalmaz meg intézkedéseket.

Biztonsági szabályzat
Egy szervezet vezetésének egyértelmű irányt mutató dokumentumot kell kiadni, ami a működési célokkal összhangban van, és támogatást, valamint elkötelezettséget mutat az információbiztonság iránt.

Az információbiztonság szervezete
Egy szervezeten belül létre kell hozni irányítási keretrendszert, ami kialakítja és szabályozza az információbiztonság bevezetésének és alkalmazásának feltételrendszerét.

Vagyontárgyak kezelése
Egy szervezetnek minden vagyontárgyát nevesítve tulajdonoshoz kell kötnie, illetőleg be kell sorolnia információbiztonság szerinti.

Az emberi erőforrások biztonsága
Egy szervezetnek biztosítania kell, hogy az alkalmazottak, a szerződő felek a feladat végzése előtt megértsék felelősségüket és alkalmasak legyenek az elvégzendő feladatokra, végrehajtás közben tudatában legyenek az információbiztonsági fenyegetéseknek. Az esetleges szerződésbontások rendezett módon történjenek.

Fizikai védelem és a környezet védelme
Egy szervezetnek meg kell akadályozni a jogosulatlan fizikai hozzáférést, károsodást, a szervezet helyiségeinek és információinak zavarását, a berendezések elveszését, károsodását, ellopását, a vagyontárgyak veszélyeztetését és a szervezeti tevékenység folyamatosságának megszakítását.

A kommunikáció és az üzemeltetés irányítása
Egy szervezetnek biztosítania kell az eszközök helyes és biztonságos működését, az információk és szolgáltatások megfelelő szintű rendelkezésre állását, a meghibásodások kockázatának minimalizálását, a rendszerkomponensek és információk integritásának megőrzését, a hálózati infrastruktúra védelmét, a bizalmasság megtartását és a jogosulatlan információfeldolgozási tevékenységek felfedését.

Hozzáférés-ellenőrzés
Egy szervezetnek biztosítania kell, hogy az általa kezelt információkhoz kizárólag az erre feljogosított felhasználók férhessenek hozzá, meg kell, hogy akadályozza a jogosulatlan információelérést, akár a rendszeren akár a hálózaton vagy mobil eszközökön.

Információ rendszerek beszerzése, fejlesztése és fenntartása
Egy szervezetnek el kell érnie, hogy a biztonság az informatikai rendszer szerves részeként kezelődjön, ez által megelőzhető legyen az alkalmazásokban a hibák, a veszteségek, a jogosulatlan információmódosítások lehetősége, az információ bizalmassága, hitelessége vagy sértetlensége akár kriptográfiai eszközökkel megvédhető legyen, illetőleg csökkentse a közzétett műszaki sebezhetőségek hasznosításából származó releváns veszélyeket.

Információbiztonsági incidensek kezelése
Egy szervezetnek oly módon kell biztosítania az informatikai rendszerekhez kapcsolódó információbiztonsági események és gyenge pontok jelzését, hogy a helyesbítő tevékenységek időben megtehetőek legyenek.

Működés folytonosságának irányítása
Egy szervezetnek el kell hárítani a működés folyamatosságának megszakítását és meg kell védeni a kritikus működési folyamatokat az informatikai rendszerek nagy hibáinak vagy az üzemzavaroknak a hatásától.

Követelményeknek való megfelelés
Egy szervezetnek biztosítani a rendszerek megfelelését a szervezeti biztonsági szabályzatoknak, és el kell kerülni bármely jogi, törvényes, szabályozási vagy szerződési kötelezettségnek és bármilyen biztonsági követelménynek a megszegését.

9.1.2. A NIST SP 800-53 intézkedés családjai

Az IT biztonság követelményeit a részletesebb felosztást használó NIST 800-53 [06] szerinti 17 intézkedés család szempontjából is vizsgálhatjuk. A tizenhét terület széles bázisú, kiegyensúlyozott informatika biztonsági koncepciót képvisel, az információk és informatikai rendszerek védelmének menedzsment, üzemeltetési és műszaki szempontjaival egyaránt foglalkozik:

a) A menedzsment biztonsági intézkedések olyan óvintézkedések vagy ellenintézkedések, melyek a kockázatok és az informatikai rendszerek biztonságának menedzselésére koncentrálnak.
b) Az üzemeltetési biztonsági intézkedések olyan óvintézkedések vagy ellenintézkedések, melyeket elsősorban emberek valósítanak meg, hajtanak végre.
c) A műszaki biztonsági intézkedések olyan óvintézkedések vagy ellenintézkedések, melyeket elsősorban az informatikai rendszer valósít meg, hajt végre, a rendszer hardver, szoftver vagy förmver összetevőiben megvalósuló mechanizmusok segítségével.

Bár jelen dokumentum kizárólag a műszaki biztonsági intézkedések területére koncentrál, az alábbiakban rövid áttekintés következik a három kategóriába sorolt intézkedéscsaládokról.

9.1.2.1. Menedzsment biztonsági intézkedések

Kockázatfelmérés
Egy szervezetnél rendszeres időnként fel kell mérni a szervezeti működés során felmerülő kockázatokat (ideértve a szervezet küldetését, funkcióit, arculatát vagy jó hírnevét), a szervezeti értékeket és egyéneket, amely kockázatok a szervezeti informatikai rendszer működéséből és kapcsolódó információ feldolgozó, tároló vagy átviteli műveletekből származnak.

Tervezés
Egy szervezetnek az informatikai rendszeréhez biztonsági tervet kell készítenie, dokumentálnia, megvalósítania, és időszakonként felülvizsgálnia, mely leírja az életben lévő vagy tervezett biztonsági intézkedéseket, valamint a rendszerhez hozzáférő felhasználóktól elvárt magatartási szabályokat.

Rendszer és szolgáltatás beszerzés
Egy szervezetnek:

a) kellő erőforrást kell biztosítania informatikai rendszere megfelelő védelmére;
b) az informatikai rendszerre fejlesztési életciklus folyamatokat kell alkalmaznia, amely figyelembe veszi az informatikai biztonság szempontjait;
c) szoftverhasználatra és telepítésre vonatkozó megszorításokat kell érvényre juttatnia;
d) biztosítania kell, hogy külső szolgáltatói is kielégítő biztonsági intézkedéseket valósítanak meg a kihelyezett információk, alkalmazások és/vagy szolgáltatások védelme érdekében.

Biztonsági értékelés és akkreditálás
Egy szervezetnek:

e) rendszeres időközönként értékelnie kell a szervezet informatikai rendszerének biztonsági intézkedéseit, annak megállapításához, hogy az intézkedéseket hatékonyan alkalmazzák-e;
f) intézkedési tervet kell készítenie és végrehajtani a hiányosságok korrigálására, a rendszerekben meglévő sebezhetőségek csökkentésére vagy kiküszöbölésére;
g) engedélyeztetnie (akkreditáltatnia) kell az informatikai rendszerek működését és bármilyen rendszerkapcsolatot, kapcsolódást; és
h) folyamatosan felügyelnie, ellenőriznie kell a biztonsági intézkedéseket a hatékonyság folytonosságának biztosítása érdekében.

9.1.2.2. Üzemeltetési biztonsági intézkedések

Fizikai és környezeti védelem
Egy szervezetnek:

a) a jogosult felhasználókra kell korlátoznia az informatikai rendszerhez, berendezésekhez és a kapcsolódó üzemeltetési környezetekhez való fizikai hozzáférést;
b) védenie kell a fizikai létesítményt, és biztosítania kell az informatikai rendszerhez szükséges infrastruktúrát;
c) biztosítania kell az informatikai rendszerhez szükséges háttér és kiegészítő szolgáltatásokat;

d) védenie kell az informatikai rendszert a környezeti veszélyektől; és
e) megfelelő környezeti intézkedésekről kell gondoskodnia az informatikai rendszernek helyt adó létesítményekben.

Személyzettel kapcsolatos biztonság
Egy szervezetnek:
a) biztosítania kell, hogy a szervezeten belül (ideértve a külső szolgáltatókat is) felelősségi körrel, feladattal rendelkező személyek megbízhatóak és megfelelnek az adott pozícióra vonatkozó biztonsági kritériumoknak;
b) biztosítania kell, hogy a szervezeti információk és informatikai rendszerek védve legyenek a személyzeti mozgások esetére, így például egy felhasználó munkaköréből való eltávolítása vagy áthelyezése esetén; és
c) formális szankciókat kell alkalmaznia azon felhasználókra, akik nem tartják be a szervezeti biztonsági szabályokat és nem követik az életben lévő eljárásokat.

Tudatosság és képzés
Egy szervezetnek:
a) biztosítania kell, hogy az informatikai rendszer irányítói és felhasználói tudatában legyenek a tevékenységeikkel kapcsolatos biztonsági kockázatokkal, valamint az informatikai rendszerre vonatkozó törvényekkel, jogszabályi előírásokkal, szabványokkal, szabályzatokkal és eljárásokkal, továbbá
b) biztosítania kell, hogy a szervezet személyi állománya megfelelő képzésben részesüljön a számukra kijelölt, biztonsággal kapcsolatos feladatok és felelősségek teljesítése érdekében.

Üzletmenet folytonosság tervezése
Egy szervezetnek terveket kell készítenie, karbantartania és hatékonyan megvalósítania 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.

Karbantartás
Egy szervezetnek:
a) rendszeres és időszakos karbantartást kell végrehajtania az informatikai rendszerben; valamint
b) hatékony intézkedéseket kell foganatosítania az informatikai rendszer karbantartásához használt eszközökkel, technikákkal, mechanizmusokkal és személyzettel kapcsolatban.

Adathordozók védelme
Egy szervezetnek:
a) védenie kell a szervezetnél fellelhető papír alapú vagy digitális adathordozón lévő információit;
b) jogosult felhasználókra kell korlátoznia a hozzáférést a nyomtatott vagy digitális információkhoz és
c) a digitális adathordozóról biztonságosan törölnie kell a rajtuk lévő információt azok eltávolítása vagy újra használata előtt.

Reagálás a biztonsági eseményekre
Egy szervezetnek:

a) biztonsági események kezelésére alkalmas képességet kell kialakítania az informatikai rendszerére, amely magába foglalja a megfelelő előkészítést, észlelést, elemzést, behatárolást, helyreállítást és a felhasználói válaszok kezelése tevékenységeket; valamint
b) nyomon kell követnie, dokumentálnia és jelentenie kell az eseményeket a szervezetben erre kijelölt illetékes személynek és/vagy szervezetnek, hatóságnak.

Konfiguráció kezelés
Egy szervezetnek:

a) ki kell alakítania és karban kell tartania az informatikai rendszer alapkonfigurációját és leltárát (beleértve a hardvert, szoftvert, förmvert és a dokumentációt) az informatikai rendszer teljes életciklusában, továbbá
b) biztonságos konfigurációs beállításokat kell kialakítania és érvényre juttatnia az informatikai rendszerben alkalmazott informatikai termékekre.

Rendszer és információ sértetlenség
Egy szervezetnek:

c) azonosítania, jelentenie és ütemezett módon javítania kell az információ és informatikai rendszer hibákat;
d) védekeznie kell a kártékony kódok ellen a rendszer megfelelő helyein; és
e) ellenőriznie kell az informatikai rendszer biztonsági riasztásait és figyelmeztetéseit, továbbá meg kell tennie a megfelelő válaszlépéseket.

Megjegyzés: Ez utóbbi két (Konfiguráció kezelés, Rendszer és információ sértetlenség) intézkedés családba tartozó intézkedések értelmezhetőek műszaki biztonsági intézkedésekként is.

9.1.2.3. Műszaki biztonsági intézkedések

Azonosítás és hitelesítés
Egy szervezetnek azonosítania kell az informatikai rendszer felhasználóit, a felhasználók nevében működő folyamatokat vagy eszközöket, és hitelesítenie (vagy ellenőriznie) kell ezen felhasználók, folyamatok vagy eszközök azonosságát, mielőtt ezek hozzáférést kapnának az informatikai rendszerhez.

Hozzáférés ellenőrzés
Egy szervezetnek a jogosult felhasználókra, valamint a jogosult felhasználók nevében működő folyamatokra és eszközökre (ideértve a más informatikai rendszereket is) kell korlátoznia az informatikai rendszerhez való hozzáférést.

Naplózás és elszámoltathatóság
Egy szervezetnek:

a) az informatikai rendszerben naplórekordokat kell létrehoznia, ezeket pedig olyan szinten kell megvédenie és megőriznie, amely lehetővé teszi a jogosulatlan, törvénytelen vagy nem megfelelő rendszertevékenységek monitorozását, elemzését és jelentések készítését a naplók alapján, és
b) biztosítania kell, hogy az informatikai rendszer felhasználói tevékenységei nyomon követhetők legyenek, egészen az egyes tevékenységekért felelősséggel tartozó felhasználóig.

Rendszer és kommunikáció védelem
Egy szervezetnek:

a) monitoroznia, ellenőriznie és védenie kell a szervezet külső határain átmenő és a kulcsfontosságú belső határok közötti kommunikációkat (az informatikai rendszerek által továbbított vagy fogadott információkat); és
b) magas szintű terveket, szoftverfejlesztési technológiákat és rendszerfejlesztési elveket kell alkalmaznia, melyek hozzájárulnak a hatékony informatika biztonsághoz.

9.1.3. Common Criteria v3.1 követelményei

A Common Criteria [07] a funkcionális és garanciális követelmények szerinti megkülönböztetést alkalmazza az IT biztonság két különböző megközelítésének leírására.

A "funkcionális" minősítés arra vonatkozik, hogy a követelmény által meghatározott biztonsági funkcionalitásra szükség van-e egy termék, rendszer esetén.

A Common Criteria funkcionális követelményei [08] szabványos formában fogalmaznak meg IT biztonsági funkcionális követelményeket. Az értékelés tárgyára (TOE – Target of Evaluation) vonatkozóan a különböző TOE-kre az igényeknek megfelelő funkcionális követelmény csoport választható. A funkcionális követelmények kategóriákba soroltak: osztály, család és összetevő lebontás ad meg egy követelményt. Az összetevőn belül elemként megadott követelmények együtt érvényesek, így az összetevő a legalsóbb szintű választható egyed.

A garanciális követelmények [09] minősítés arra vonatkoznak, hogy a termék, rendszer a vállalat funkcionális követelményeket milyen garanciák mellett, milyen erősségi szinten tudja biztosítani.

Ugyanazon funkcionális követelmény halmazt különböző garanciális szinteken lehet teljesíteni. A garancia-összetevőket hét csoportba sorolja a CC, melyek: EAL1-EAL7, ahol a nagyobb számok egyre szigorúbb követelményeket jelentenek.

Az alábbiakban áttekintjük a Common Criteria legfrissebb, v3.1 verziója szerint ezeket a követelményeket. Az áttekintés során a CC-ben elfogadott (a követelményrendszerrel kapcsolatban még nem járatos olvasó számára részletesnek és bonyolultnak tűnő) terminológiát és rövidítéseket használjuk.

9.1.3.1. Funkcionális követelmények

Biztonsági naplózás FAU
A biztonsági naplózás velejárója a biztonsági tevékenységekhez kapcsolódó információk észlelése, rögzítése, tárolása és vizsgálata. Az ilyen tevékenységek napló rekordokat állítanak elő, amelyeket át lehet vizsgálni biztonsági szempontból. Az osztály olyan családokból áll, amelyek egyebek között követelményeket definiálnak a naplózható események kiválasztására, a napló rekordok vizsgálatára, azok védelmére és tárolására.

Kommunikáció FCO
A kommunikáció osztálya az adatcserében résztvevő csoportok azonosítójának biztonságával, a továbbított információ eredete (származásbizonyítás) azonosítójának és a továbbított információt fogadó azonosítójának (átvétel bizonyítás) megerősítésével és annak biztosításával, hogy sem a származtató nem tagadhatja le az üzenet elküldését, sem a fogadó annak átvételét.

Kriptográfiai támogatás FCS
Ezt az osztályt akkor alkalmazandó, ha az értékelés tárgya kriptográfiai funkciókat is megvalósít. Ezek a funkciók felhasználhatók például kommunikáció támogatására, azonosításra és hitelesítésre, adatok elkülönítésére. Az osztály két családja a kriptográfiai kulcsok működtetés közbeni használatát, illetve menedzselését fedi le.

Felhasználói adatok védelme FDP
Ez az osztály olyan családokat tartalmaz, amelyek a felhasználói adatok védelmével kapcsolatos követelményeket határoznak meg. A családok az értékelés tárgyán belüli adatokkal foglalkoznak azok importálása, exportálás és tárolása során, valamint a felhasználói adatokhoz tartozó biztonsági jellemzőkkel kapcsolatosak

Azonosítás és hitelesítés FIA
Az azonosításra és hitelesítésre vonatkozó követelmények a jogosult felhasználók egyértelmű azonosítását és a biztonsági jellemzőknek a felhasználókkal és alanyokkal való pontos összekapcsolását biztosítják. Ezen osztályban a családok a felhasználói azonosítók meghatározásával és ellenőrzésével, az értékelés tárgyával való kölcsönhatás jogosultságának meghatározásával, valamint a biztonsági jellemzőknek a jogosult felhasználókkal való pontos összekapcsolásával foglalkoznak.

Biztonságkezelés FMT
Ez az osztály arra szolgál, hogy meghatározza az értékelés tárgya biztonsági funkcióira vonatkozó biztonsági jellemzők, adatok és funkciók menedzsmentjét. Különböző menedzsment szerepkörök és ezek kölcsönhatása definiálható, mint pl. a képességek szétválasztása. Ez az osztály szolgál a többi funkcionális osztály menedzselési szempontjainak lefedésére is.

Titoktartás FPR
A magántitokkal kapcsolatos követelmények védelmet nyújtanak egy felhasználónak a felfedéssel szemben, illetve azzal szemben, hogy azonosítójukkal egy másik felhasználó visszaéljen. Ebben az osztályban a családok a névtelenséggel, az álnéven szerepléssel, összekapcsolhatatlansággal és megfigyelhetetlenséggel foglalkoznak.

Az értékelés tárgya biztonsági funkcióinak védelme FPT
Ez az osztály az értékelés tárgya biztonsági funkciói adatainak a védelmére koncentrál elsősorban, s nem a felhasználói adatokéra. Az osztály az értékelés tárgya biztonsági funkcióira vonatkozó mechanizmusok és adatok sértetlenségére és menedzselésére vonatkozik.

Erőforrás felhasználás FRU
Az erőforrás felhasználás három családot tartalmaz, melyek az igényelt erőforrások rendelkezésre állását biztosítják, (pl. feldolgozó kapacitás, tároló kapacitás). A családok a hibatűrésre, a szolgáltatások prioritására, illetve az erőforrások lefoglalására nézve részletezik a követelményeket.

Az értékelés tárgyához való hozzáférés FTA
Ez az osztály az azonosításra és hitelesítésre megadottakon kívül további funkcionális követelményeket határoz meg egy felhasználói aktív munkaszakasz létrehozásának szabályozására. Az értékelés tárgyához való hozzáférési követelmények olyanokat szabályoznak, mint a felhasználói aktív szakaszok számának és hatókörének korlátozása, a korábbi hozzáférések megjelenítése, a hozzáférési paraméterek módosítása.

Bizalmi elérési út/csatornák FTP
Ez az osztály megbízható kommunikációs útvonalakkal foglalkozik a felhasználók és a biztonsági funkciók között, illetve különböző értékelés tárgya biztonsági funkciói között. A megbízható útvonalak eszközt biztosítanak a felhasználónak ahhoz, hogy a biztonsági funkciókat közvetlenül aktivizálják. A felhasználó vagy a biztonsági funkció kezdeményezheti az adatcserét, s ez a csere garantáltan védett a nem megbízható alkalmazások módosításaival szemben

9.1.3.2. Garanciális követelmények

A Védelmi Profil értékelése APE
A PP értékelésének célja, hogy szemléltesse, a PP teljes, ellentmondásmentes és szakmailag helytálló. Az értékelt PP alkalmas arra, hogy ST-k fejlesztésének alapja legyen. Az ilyen PP alkalmas arra, hogy a nyilvántartásba felvegyék.

A Biztonsági Előirányzat értékelése ASE
Az ST értékelésének célja, hogy szemléltesse, az ST teljes, ellentmondásmentes, szakmailag helytálló, és ilyen módon alkalmas arra, hogy a neki megfelelő TOE értékelés alapja lehessen.

Fejlesztés ADV
Az ADV garanciacsalád olyan követelményeket definiál, amelyek információkat szolgáltatnak a TOE tervéről, annak szerkezetéről és interfészeiről. Ezek az információk képezik az alapját a TOE-ra végrehajtott tesztelésnek és sebezhetőségi elemzésnek.

Útmutató dokumentumok AGD
Az AGD garanciacsalád a fejlesztő által a felhasználó számára készítendő, előkészítő feladatokkal és működtetéssel kapcsolatos dokumentációk érthetőségével, lefedettségével és teljességével foglalkozik. A felhasználón a TOE-val kapcsolatos, SFR-nek megfelelő

műveleteket jogosultan végrehajtó személyt értjük. A minden felhasználói szerepkör számára szóló dokumentáció a TOE biztonságos előkészítésének és működtetésének fontos eleme.

Az életciklus meghatározása ALC
Az életciklus támogatás osztály követelményeket fogalmaz meg arra a garanciára, melyet egy jól definiált életciklus modell alkalmazásán keresztül a TOE fejlesztés (ideértve a hibajavítást is) minden lépésében, az eszközök és technikák, valamint a fejlesztői környezet védelméhez használt biztonsági intézkedésekben követni kell.

Tesztelés ATE
Az ATE osztály által előírt tevékenységek célja annak meghatározása, hogy a TOE az ST-ben leírtaknak megfelelően és az AVD osztályban leírt értékelési bizonyítékokban specifikáltak szerint működik-e. E döntés meghozatalát a fejlesztő által elvégzett TSF funkcionális tesztelés és az értékelő által elvégzett független TSF tesztelés elvégzése segíti.

Sebezhetőség felmérése AVA
Ez az osztály foglalkozik a TOE fejlesztése vagy működtetése során bevezetett kihasználható sebezhetőségek lehetőségével. Olyan elemzést jelent, melynek célja annak megállapítása, hogy a TOE fejlesztése és elvárt működése értékelése során vagy egyéb módszerekkel azonosított lehetséges sebezhetőségek vezethetnek-e oda, hogy egy támadó megsérti a funkcionális biztonsági követelményeket.

Összetett garancia csomag ACO
Az összetett garancia csomag(ok) (CAPs) olyan emelkedő szintű skálát jelent(enek), amelynek elemei az összetett TOE-kre vonatkozó garanciaszint elérésének és az ehhez szükséges költségeknek az egyensúlyát biztosítva jöttek létre. A CAP-ket összetett TOE-kre kell alkalmazni, amelyek komponens TOE értékelésen átesett (vagy az alatt álló) összetevőkből állnak. Az egyes összetevőket egy EAL vagy az ST-ben specifikált más garanciacsomag szerint tanúsítják. Elvárás, hogy egy összetett TOE-ra vonatkozó alapszintű garancia fennálljon az EAL1 alkalmazása révén, ami általában elérhető az összetevőkkel kapcsolatos nyilvánosan hozzáférhető információk alapján. (Az EAL1 a specifikáltak szerint alkalmazható mind az komponens, mind pedig az összetett TOE-ra). A CAP-k alternatív megközelítést ajánlanak egy összetett TOE garanciáinak megszerzéséhez az EAL1-nél magasabb szintű EAL-ok alkalmazása helyett.

9.1.4. A technikai biztonsági követelmények megfeleltetése

Az alábbi táblázat a három mértékadó szabvány technikai biztonsági intézkedései közötti megfeleltetést tartalmazza.
A megfeleltetés támpont jellegű, egyes esetekben egy-egy leképezés lehetséges, míg más esetekben CC osztályok, családok és összetevők kombinációjával formalizálható az adott biztonsági intézkedés.

	Biztonsági intézkedés neve	**ISO/IEC 17799/ 27001**	**Common Criteria v3.1**
Azonosítás és hitelesítés			
AH-1	Azonosítási és hitelesítési szabályzat és eljárásrend	15.1.1	FIA FIA_ATD
AH-2	Felhasználó azonosítása és hitelesítése	11.2.3 11.4.2 11.5.2	FIA_UID FIA_UAU
AH-3	Eszközök azonosítása és hitelesítése	11.4.2 11.4.3 11.7.1	FIA_UID FIA_UAU
AH-4	Azonosító kezelés	11.2.3 11.5.2	FIA_SOS
AH-5	A hitelesítésre szolgáló eszközök kezelése	11.5.2 11.5.3	FMT
AH-6	A hitelesítésre szolgáló eszköz visszacsatolása	11.5.1	FIA_UAU.7
AH-7	Hitelesítés kriptográfiai modul esetén	—	FCS_CKM FCS_COP
Hozzáférés ellenőrzése			
HE-1	Hozzáférés ellenőrzési szabályzat és eljárásrend	11.1.1 11.4.1 15.1.1	FDP_ACC FDP_ACF
HE-2	Felhasználói fiókok kezelése	6.2.2 6.2.3 8.3.3 11.2.1 11.2.2 11.2.4 11.7.2	FMT FIA FDP
HE-3	Hozzáférés ellenőrzés érvényre juttatása	11.2.4 11.4.5	FDP_ACF FDP_ACC

	Biztonsági intézkedés neve	**ISO/IEC 17799/ 27001**	**Common Criteria v3.1**
HE-4	Információ áramlás ellenőrzés érvényre juttatása	10.6.2 11.4.5 11.4.6 11.4.7	FDP_IFC FDP_IFF
HE-5	A felelősségek szétválasztása	10.1.3 10.6.1 10.10.1	FMT_SMR
HE-6	Legkisebb jogosultság	11.2.2	FDP_ACC FDP_ACF
HE-7	Sikertelen bejelentkezési kísérletek	11.5.1	FIA_AFL
HE-8	A rendszerhasználat jelzése	11.5.1 15.1.5	FTA_TAB
HE-9	Értesítés előző bejelentkezésről	11.5.1	FTA_TAH
HE-10	Egyidejű munkaszakasz kezelés	—	FTA_MCS
HE-11	A munkaszakasz zárolása	11.3.2	FTA_SSL
HE-12	A munkaszakasz lezárása	11.3.2 11.5.5	FTA_SSL
HE-13	Felügyelet és felülvizsgálat — hozzáférés ellenőrzés	10.10.2 11.2.4	FAU_SAR
HE-14	Azonosítás és hitelesítés nélkül engedélyezett tevékenységek	—	FIA_UAU.1 FIA_UID.1
HE-15	Automatikus jelölés	7.2.2	FDP_ICC, FDP_IFF
HE-16	Automatikus címkézés	7.2.2	FDP_ICC, FDP_IFF
HE-17	Távoli hozzáférés ellenőrzése	11.4.2 11.4.3 11.4.4	FDP_ACC, FDP_ACF, FDP_IFC, FDP_IFF
HE-18	A vezeték nélküli hozzáférésre vonatkozó korlátozások	11.4.2 11.7.1 11.7.2	FDP_ACC, FDP_ACF, FDP_IFC, FDP_IFF
HE-19	A hordozható és mobil eszközök hozzáférés ellenőrzése	11.7.1	FDP_ACC, FDP_ACF, FDP_IFC, FDP_IFF
HE-20	Külső informatikai rendszerek használata	6.1.4 9.2.5 11.7.1	

	Biztonsági intézkedés neve	ISO/IEC 17799/ 27001	Common Criteria v3.1
Naplózás és elszámoltathatóság			
NA-1	Naplózási és elszámoltathatósági szabályzat és eljárásrend	10.10 15.1.1	
NA-2	Naplózandó események	10.10.1	FAU_GEN.1
NA-3	A naplóbejegyzések tartalma	10.10.1 10.10.4	FAU_GEN.1
NA-4	Napló tárkapacitás	10.10.3	FAU_STG
NA-5	Naplózási hiba kezelése	10.10.3	FAU_STG.4
NA-6	Napló figyelése, vizsgálata és jelentések készítése	10.10.2 10.10.4 13.2.1	FAU_SAA FAU_SAR
NA-7	Naplócsökkentés, naplóriport készítés	10.10.3	FAU_SEL
NA-8	Időbélyegek	10.10.6	FPT_STM
NA-9	A napló információk védelme	10.10.3 15.1.3 15.3.2	FAU_STG.2
NA-10	Letagadhatatlanság	10.8.2 10.9.1 12.3.1	FAU_GEN.2
NA-11	A naplóbejegyzések megőrzése	10.10.1 15.1.3	FAU_STG.2
Rendszer és kommunikáció védelem			
RV-1	Rendszer és kommunikáció védelmi szabályzat és eljárásrend	10.8.1 15.1.1	
RV-2	Alkalmazás szétválasztás	11.4.5	FMT_SMF
RV-3	Biztonsági funkciók elkülönítése	11.4.5	FPT_ITT ADV_ARC
RV-4	Információ maradványok	10.8.1	FDP_RIP
RV-5	Szolgáltatás megtagadás elleni védelem	10.8.4 13.2.1	FPT_ITA FRU_RSA
RV-6	Erőforrás prioritás	—	FRU_PRS
RV-7	A határok védelme	11.4.6	
RV-8	Az adatátvitel sértetlensége	10.6.1 10.8.1 10.9.1	FPT_ITI FDP_UIT
RV-9	Az adatátvitel bizalmassága	10.6.1 10.8.1 10.9.1	FPT_ITC FDP_UCT

	Biztonsági intézkedés neve	**ISO/IEC 17799/ 27001**	**Common Criteria v3.1**
RV-10	A hálózati kapcsolat megszakítása	11.5.6	FTA_SSL.3
RV-11	Megbízható útvonal	10.9.2	FTP_ITC FTP_TRP
RV-12	Kriptográfiai kulcs előállítása és kezelése	12.3.1 12.3.2	FCS_CKM
RV-13	Jóváhagyott kriptográfia alkalmazása	—	FCS_COP
RV-14	Sértetlenség védelem nyilvános hozzáférés esetén	10.7.4 10.9.3	FDP_UIT FDP_SDI
RV-15	Telekommunikációs szolgáltatások korlátozása	—	
RV-16	Biztonsági paraméterek továbbítása	7.2.2 10.8.2 10.9.2	FDP_ITC.2 FDP_ETC.2
RV-17	Nyilvános kulcsú infrastruktúra tanúsítványok	12.3.2	
RV-18	Mobil kód korlátozása	10.4.1 10.4.2	
RV-19	Interneten Keresztüli Hangátvitel (VoIP)	—	
RV-20	Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)	—	
RV-21	Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)	—	
RV-22	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	—	
RV-23	Munkaszakasz hitelessége	—	FTA_TSE
Konfiguráció kezelés			
KK-1	Konfiguráció kezelési szabályzat és eljárásrend	12.4.1 12.5.1 15.1.1	ALC_CMC
KK-2	Alap konfiguráció	7.1.1 15.1.2	ALC_CMC
KK-3	Konfigurációváltozások	10.1.2 10.2.3 12.4.1 12.5.1 12.5.2 12.5.3	ALC_CMC
KK-4	A konfigurációváltozások felügyelete	10.1.2	ALC_CMC

	Biztonsági intézkedés neve	**ISO/IEC 17799/ 27001**	**Common Criteria v3.1**
KK-5	A változtatásokra vonatkozó hozzáférés korlátozások	11.6.1	ALC_CMC
KK-6	Konfigurációs beállítások		FMT
KK-7	Legszűkebb funkcionalitás		FMT
KK-8	Informatikai rendszer komponens leltár	7.1.1 15.1.2	ALC_CMS
Rendszer és információ sértetlenség			
RS-1	Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend	15.1.1	
RS-2	Hibajavítás	10.10.5 12.4.1 12.5.1 12.5.2 12.6.1	ALC_FLR
RS-3	Rosszindulatú kódok elleni védelem	10.4.1	
RS-4	Behatolás észlelési eszközök és technikák	10.6.2 10.10.1 10.10.2 10.10.4	FAU_SAA.3 FAU_SAA.4
RS-5	Biztonsági riasztások és tájékoztatások	6.1.7 10.4.1	FAU_ARP
RS-6	A biztonsági funkcionalitás ellenőrzése	—	FPT_TST ATE
RS-7	Szoftver és információ sértetlenség	12.2.1 12.2.2 12.2.4	FDP_UIT FDP_SDI
RS-8	Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem	—	
RS-9	A bemeneti információra vonatkozó korlátozások	12.2.1 12.2.2	FDP_ITC
RS-10	A bemeneti információ pontossága, teljessége és érvényessége	10.7.3 12.2.1 12.2.2	FDP_ITC
RS-11	Hibakezelés	12.2.1 12.2.2 12.2.3 12.2.4	ADV
RS-12	A kimeneti információ kezelése és megőrzése	10.7.3 12.2.4	FDP_ETC

9.2. A műszaki biztonsági intézkedések katalógusa

A műszaki biztonsági követelmények hat intézkedési családra tagozódnak. A családok tartalmazzák a biztonsági funkcionalitásához kapcsolódó biztonsági intézkedéseket. Minden intézkedési családot egy két karakteres azonosító jelöl.

A biztonsági intézkedések szerkezete három fő részből áll az intézkedés szekció, az intézkedés bővítése szekció és az intézkedés kiegészítése szekció.

Az intézkedés szekció egy tömör állítást fogalmaz meg egy konkrét biztonsági elemről, ami szükséges az informatikai rendszer valamilyen részének védelméhez. Az intézkedés leírja azokat a biztonsági tevékenységeket vagy lépéseket, amelyeket a szervezetnek vagy az informatikai rendszernek el kell végeznie. Néhány intézkedés az intézkedések katalógusából rendelkezik bizonyos rugalmassággal, és bizonyos az intézkedéssel kapcsolatos bemeneti értékeket a szervezet határozhat meg. Ezt a rugalmasságot az intézkedés szövegében található értékadás és választás operátorok segítségével lehet megvalósítani. Ez a két operátor biztosítja a lehetőséget a szervezet számára, hogy a biztonsági intézkedéseket saját feladati, üzleti vagy működési igényeihez igazítsa. Például egy szervezet meghatározhatja, hogy pontosan milyen eseményeket kell naplózni. Ezek rögzítése után a szervezet által meghatározott értékek az intézkedés részévé válnak, és a szervezetnek az így elkészült intézkedéseknek kell megfelelniük. Néhány értékadási művelet minimális vagy maximális értékeket határozhat meg, amelyek korlátozhatják a szervezet által megadott értéket. A választás művelet szintén korlátozhatja a bemeneti értékek lehetséges értékeit egy olyan előre megadott elemekből álló listával, amelyből a szervezetnek választania kell.

Az intézkedés bővítése szekció olyan biztonsági elemeket ír le, amelyek vagy további, de az alapintézkedéshez kapcsolódó funkcionalitást adnak, és/vagy növelik az alap intézkedés erejét. Mindkét esetben az intézkedés bővítést olyan informatikai rendszerekben alkalmazzák, ahol nagyobb védelemre van szükség az adatvesztés komolyabb lehetséges következményei miatt, vagy ha a szervezet a kockázatfelmérés hatására kiegészítéseket keres az alap intézkedés funkcionalitásához. Az intézkedés bővítéseit minden intézkedésen belüli sorban betűvel jelölik, hogy a bővítés könnyen azonosítható legyen, ha ki lett választva az eredeti intézkedés kiegészítésére. Az intézkedés javításának megjelölése csak arra szolgál, hogy a javítást azonosítani lehessen az intézkedés szerkezetében. A jelölés nem jelzi a javítás erejét a többihez képest, és nem feltételez hierarchikus kapcsolatot a javítások közt.

Az intézkedés kiegészítése szekció kiegészítő információkat tartalmaz egy biztonsági intézkedésről. A szervezetnek a megfelelő mértékben alkalmaznia kell az intézkedés kiegészítésében leírtakat, amikor definiálja, fejleszti vagy megvalósítja a biztonsági intézkedéseket. Bizonyos esetekben, az intézkedés kiegészítése több részletet tartalmaz az intézkedés követelményeiről vagy fontos tényezőkről (és a szükséges rugalmasságról) a biztonsági intézkedés megvalósításához a szervezet működési környezetének, konkrét feladatokkal kapcsolatos követelmények vagy a kockázat felmérésének összefüggésében. Ezen kívül szerepelhetnek még az intézkedés kiegészítésében hivatkozások is, ha érdekesek lehetnek a biztonsági intézkedés szempontjából.

9.2.1. Konfiguráció kezelés (KK)

9.2.1.1. KK-1 Konfiguráció kezelési szabályzat és eljárásrend

Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált konfiguráció kezelési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a konfiguráció kezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

Intézkedés kiegészítése: A konfiguráció kezelési szabályzat és az eljárásrendek konzisztensek a vonatkozó jogszabályokkal, a vezetői utasításokkal, a direktívákkal, a szabályzatokkal, az előírásokkal, a szabványokkal és az útmutatókkal. A konfiguráció kezelési szabályzat része lehet a szervezet általános informatika biztonsági szabályzatának. A konfiguráció kezelési eljárásrendeket ki lehet dolgozni általánosan a biztonsági program részeként, vagy szükség esetén az egyes informatikai rendszerekre.

9.2.1.2. KK-2 Alap konfiguráció

Intézkedés: A szervezet informatikai célrendszeréhez egy alap konfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges komponenseit.

Intézkedés bővítése:
a) A szervezet az alap konfiguráció frissítését az informatikai rendszer komponensek telepítésének a szerves részeként végzi.
b) A szervezet automatikus mechanizmusokat alkalmaz az informatikai rendszer naprakész, teljes, pontos, és állandóan rendelkezésre álló alap konfigurációjának a karbantartására.

Intézkedés kiegészítése: Ez az intézkedés egy alap konfigurációt határoz meg az informatikai rendszerekhez. Az alap konfiguráció információt biztosít az egyes komponensek összeállításához (pl. munkaállomások és notebook számítógépek esetében a telepített sztenderd szoftverek, ideértve a frissített javítócsomag információkat is) és a komponens logikai elhelyezését is megadja az informatikai rendszer architektúrájában. Az alap konfiguráció egyben egy jól definiált és dokumentált specifikáció is a szervezet számára, melyre az informatikai rendszer épül, és amelyben az esetleg szükséges eltérések is dokumentálásra kerülnek szükségessé tévő ok vagy cél feltüntetésével együtt. Kapcsolódó biztonsági intézkedések: KK-6, KK-8.

9.2.1.3. KK-3 A konfigurációváltozások felügyelete

Intézkedés: A szervezet dokumentálja és ellenőrzi az informatikai rendszerben történt változásokat. Megfelelő szervezeti tisztviselők hagyják jóvá az informatikai rendszer változásait, összhangban a szervezeti szabályzatokkal és eljárásrendekkel.

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat alkalmaz:
   aa) az informatikai rendszerben javasolt változások dokumentálására;
   ab) a megfelelő jóváhagyó tisztségviselők értesítésére;
   ac) a nem időben megkapott jóváhagyások kiemelésére;
   ad) a még nem jóváhagyott változások végrehajtásának a megakadályozására; és
   ae) az informatikai rendszerben végrehajtott változások teljes dokumentálására.

Intézkedés kiegészítése: A szervezet az informatikai rendszer konfigurációjában bekövetkezett változást a szervezet által jóváhagyott eljárásrend alapján kezeli. A konfigurációváltozás felügyelete magában foglalja az változások szisztematikus kezdeményezését, indoklását, megvalósítását, tesztelését/értékelését, felülvizsgálatát, és a változások elrendelését az informatikai rendszerben, ideértve a frissítéseket és a módosításokat is. A konfigurációváltozás felügyelete kiterjed az informatika technológiai termékek (pl. operációs rendszerek, tűzfalak, router-ek) konfigurációs beállításaira is. A szervezet sürgősségi változásokat is megfogalmaz a konfigurációváltozás felügyeleti eljárásrendjében, ideértve a hibák kiküszöböléséből származó változásokat. Az informatika rendszerben történő változtatás engedélyezéséhez szükséges, hogy a változtatás biztonsági elemzése megtörténjen, és pozitív eredménnyel záruljon. A szervezet naplózza az informatikai rendszer konfigurációjában történt változásokat. Kapcsolódó biztonsági intézkedések: KK-4, KK-6, RS-2.

9.2.1.4. KK-4 A konfigurációváltozások felügyelete

Intézkedés: A szervezet figyeli az informatikai rendszerben történt változásokat, és biztonsági hatásvizsgálatot végez a változások hatásainak meghatározására.

Intézkedés kiegészítése: A változások végrehajtása előtt, a változás jóváhagyási folyamatának részeként elemzi az informatikai rendszer változásának potenciális biztonsági hatásait. Az informatikai rendszer megváltozása után (ideérve a frissítést és módosítást), a szervezet ellenőrzi a biztonsági szolgáltatásokat, hogy a szolgáltatások továbbra is megfelelően működnek. A szervezet naplózza az informatikai rendszer konfigurációjának változásával összefüggő tevékenységeket. A konfiguráció változás monitorozása és a biztonsági hatás elemzés végrehajtása fontos elemek az informatikai rendszer biztonsági intézkedéseinek folyamatos értékelésének a szempontjából.

9.2.1.5. KK-5 A változtatásokra vonatkozó hozzáférés korlátozások

Intézkedés: A szervezet hozzáférési korlátozásokat juttat érvényre az informatikai rendszer (konfigurációs) változtatásaival kapcsolatban.

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat alkalmaz a hozzáférési korlátozások érvényre juttatására, és érvényre juttatási tevékenység auditálásának a támogatására.

Intézkedés kiegészítése: A hardver, szoftver és/vagy förmver komponensek tervezett vagy nem tervezett változtatásai jelentős hatással lehetnek a rendszer átfogó biztonságára. Ennek

megfelelően csak képzett és erre feljogosított személyek rendelkezhetnek olyan hozzáféréssel az informatikai rendszer komponenseihez, hogy változtatásokat kezdeményezhessenek, beleértve a frissítéseket és a módosításokat is.

9.2.1.6. KK-6 Konfigurációs beállítások

Intézkedés: A szervezet
- kötelező konfigurációs beállítást határoz meg az informatikai rendszerben használt információ technológiai termékekre;
- az információ technológiai termékek lehető legkorlátozóbb biztonsági beállításait konfigurálja, amely még megfelel a működési követelményeknek;
- dokumentálja a konfigurációs beállításokat; és
- érvényre juttatja a konfigurációs beállításokat az informatikai rendszer valamennyi komponensében.

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat alkalmaz a konfigurációs beállítások központi kezelésére, alkalmazására és ellenőrzésére.

Intézkedés kiegészítése: A konfigurációs beállítások az informatikai rendszerben található információ technológiai termékek konfigurálható paraméterei. A szervezet a konfigurációs beállítások változásait a szervezet szabályzatainak és eljárásrendjének megfelelően monitorozza és felügyeli. Kapcsolódó biztonsági intézkedések: KK-2, KK-3, RS-4.

9.2.1.7. KK-7 Legszűkebb funkcionalitás

Intézkedés: A szervezet az informatikai rendszert úgy konfigurálja, hogy az csak a szükséges lehetőségeket nyújtsa, illetve letiltja/korlátozza a következő funkciók, portok, protokollok és/vagy szolgáltatások használatát: [értékadás: a tiltott/korlátozott funkciók, portok, protokollok és/vagy szolgáltatások szervezet által definiált listája].

Intézkedés bővítése:

a) A szervezet átvizsgálja az informatikai rendszert [értékadás: a szervezet által meghatározott gyakorisággal], hogy meghatározza és kizárja a szükségtelen portokat, protokollokat és/vagy szolgáltatásokat.

Intézkedés kiegészítése: Az informatikai rendszerek széles körben képesek funkciók és szolgáltatások nyújtására. Lehetnek olyan alapértelmezetten engedélyezett funkciók és szolgáltatások, amelyek a szervezet alapvető működéséhez nem szükségesek. Továbbá sokszor kényelmesebb az informatikai rendszer egy komponensével több szolgáltatást nyújtani, de ez növeli a kockázatot ahhoz képest, mintha a szolgáltatást külön komponensek biztosítanák. Ahol megvalósítható, a szervezet korlátozza a komponens funkcionalitását eszközönként egy funkcióra (pl. levelező szerver vagy web szerver, de nem mindkettő egyszerre). Az informatikai rendszer vagy az egyes komponensek által nyújtott funkciók és szolgáltatások kerüljenek alapos átvizsgálásra, és határozzák meg, mely funkciók és szolgáltatások zárhatóak ki. (pl. Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, fájl megosztás)

9.2.1.8. KK-8 Informatikai rendszer komponens leltár

Intézkedés: A szervezet aktuális leltárt készít, dokumentálja és karbantartja az informatikai rendszer komponenseit és a vonatkozó tulajdonosi információkat.

Intézkedés bővítése:

a) A szervezet az informatikai rendszer komponensek leltárjának a frissítését a komponensek telepítésének a szerves részeként végzi.
b) A szervezet automatikus mechanizmusokat alkalmaz az informatikai rendszer komponensek leltárjának naprakész, teljes, pontos, és állandóan rendelkezésre álló karbantartására.

Intézkedés kiegészítése: A szervezet meghatározza, hogy az informatikai rendszer komponensei milyen részletességgel kerüljenek be a leltárba, úgy hogy ez megfeleljen menedzsment kívánalmainak (pl. nyomon követés, jelentés). Az informatikai rendszer komponensek leltárja tartalmazza mindazon információkat, amely szükséges lehet a szervezet számára a hatékony személyes anyagi felelősségre vonhatósághoz (pl. gyártó, modell szám, sorozat szám, szoftver licenc információ, rendszer/komponens tulajdonos). A komponens leltár kiterjed az informatikai rendszer teljességére. Kapcsolódó biztonsági intézkedések**:**
KK-2, KK-6.

9.2.2. Rendszer és információ sértetlenség (RS)

9.2.2.1. RS-1 Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend

Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált, a rendszer és információ sértetlenségére vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és információ sértetlenségére vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

Intézkedés kiegészítése: A rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrendek konzisztensek a vonatkozó jogszabályokkal, a vezetői utasításokkal, a direktívákkal, a szabályzatokkal, az előírásokkal, szabványokkal és az útmutatásokkal. A rendszer és információ sértetlenségre vonatkozó szabályzat része lehet az szervezet általános informatika biztonsági szabályzatának. A rendszer és információ sértetlenségre vonatkozó eljárásrendeket ki lehet dolgozni általánosan a biztonsági program részeként, vagy szükség esetén az egyes informatikai rendszerekre.

9.2.2.2. RS-2 Hibajavítás

Intézkedés: A szervezet az informatikai rendszerben talált hibákat jelenti, és kijavítja.

Intézkedés bővítése:

a) A szervezet központilag kezeli a hibajavítás folyamatát, és a javításokat automatikusan telepíti.
b) A szervezet rendszeres időszakonként vagy szükség esetén automatikus mechanizmusokat alkalmaz az informatikai rendszer hibajavítási állapotának meghatározására.

Intézkedés kiegészítése: A szervezet beazonosítja az informatikai rendszert alkotó szoftverek aktuálisan bejelentett hibáit (és a hibákból származó potenciális sebezhetőségeket). A szervezet (vagy a fejlesztett szoftver esetében szoftver fejlesztő/szállító és a karbantartást végző kereskedő/szerződő fél) azonnal teszteli a javítások, javító csomagok és gyors javítások hatékonyságát, és elemzi a szervezet informatikai rendszerére kifejtett esetleges mellékhatását, majd telepíti az újonnan kiadott biztonságot érintő javításokat, javító csomagokat, gyorsjavításokat. A biztonsági értékelés során fellelt hibák, a folyamatos monitorozás, incidens kezelési tevékenységek, vagy az informatikai rendszer hibáinak a kezelése is kiemelten kezelendő feladat. A hibajavítás beépül a konfiguráció kezelésbe, mint sürgős változtatás. Kapcsolódó biztonsági intézkedések: KK-3, RS-11.

9.2.2.3. RS-3 Rosszindulatú kódok elleni védelem

Intézkedés: Az informatikai rendszer rosszindulatú kódok elleni védelmet valósít meg, s ez automatikus frissítési lehetőséget is magában foglal.

Intézkedés bővítése:

a) A szervezet központilag kezeli a vírusvédelmi mechanizmusokat.
b) Az informatikai rendszer automatikusan frissíti a rosszindulatú kódok elleni védelmi mechanizmust.

Intézkedés kiegészítése: A szervezet rosszindulatú kódok elleni védelmi mechanizmust alkalmaz a kritikus informatikai rendszer belépő és kilépő pontjain (pl. tűzfalak, levelező szerverek, web szerverek, proxy szerverek, távoli elérést biztosító szerverek) valamint a munkaállomásokon, szervereken, vagy a hálózaton megtalálható mobil számítástechnikai eszközökön. A szervezet a rosszindulatú kódok elleni védelmi mechanizmussal felderíti és eltávolítja a rosszindulatú kódokat (pl. vírusok, férgek, trójaiak, kémprogramok), amelyek bekerülhetnek elektronikus levél, elektronikus levél csatolmánya, internet elérés, hordozható média (pl. USB eszköz, lemez, CD lemez), vagy más szokásos eszköz által, vagy az informatikai rendszer sebezhetőségének a kihasználásával. A szervezet frissíti a rosszindulatú kódok elleni védelmi mechanizmust (beleértve a legújabb vírus definíciókat), amikor az új kiadás rendelkezésre áll, megfelelve a konfiguráció kezelési szabályzatnak és eljárásrendnek. A szervezet mérlegeli, hogy több gyártótól származó rosszindulatú kódok elleni védelmi szoftvert használjon-e (pl. egy terméket használjon a határvédelmi eszközöknél és a szervereknél és egy másikat a munkaállomásokon). A szervezet mérlegeli továbbá, a rosszindulatú kódok felderítése és eltávolítása során kapott téves riasztások, és ezeknek az informatikai rendszer rendelkezésre állására gyakorolt esetleges hatását.

9.2.2.4. RS-4 Behatolás észlelési eszközök és technikák

Intézkedés: A szervezet eszközöket és technikákat alkalmaz az informatikai rendszerben történő események figyelésére, detektálja a támadásokat, és biztosítja a rendszer jogosulatlan használatának beazonosítását.

Intézkedés bővítése:

a) A szervezet összekapcsolja és összehangolja az egyedi behatolás észlelő rendszereket egy rendszerszintű behatolás észlelő rendszerré, közös protokollok felhasználásával.
b) A szervezet automatikus eszközöket használ az események közel valós idejű elemzésére.
c) A szervezet automatikus eszközöket használ a behatolás észlelő eszközök hozzáférés szabályzási és folyamat irányítási mechanizmusába történő integrálására, ezzel biztosítva a gyors reagálást a támadásra, azáltal, hogy lehetőséget biztosít e mechanizmusok átkonfigurálására, így támogatva a támadás elszigetelését és megszüntetését.
d) Az informatikai rendszer monitorozza a kimenő és bejövő kommunikációt, keresve a szokatlan és nem engedélyezett tevékenységeket és feltételeket. Magyarázat: Szokatlan/nem engedélyezett tevékenységek vagy feltételek közé tartozhat például a rosszindulatú kód jelenléte, az információ nem engedélyezett exportálása, vagy külső informatikai rendszer felé történő jelzés küldése.
e) Az informatikai rendszer valós idejű riasztást ad ki, amikor a következő veszély, vagy potenciális veszély áll fent: [értékadás: a szervezet által meghatározott veszélyek jeleinek a listája].

Intézkedés kiegészítése: Az informatikai rendszer monitorozása számos eszköz és technika alkalmazásával érhető el (pl. behatolás észlelő rendszerek, behatolás megelőző eszközök, rosszindulatú kódok elleni védelmi szoftver, napló bejegyzés monitorozó szoftver, hálózati forgalom monitorozó szoftver). A monitorozó eszközök az informatikai rendszerben stratégailag kiemelt helyeken kerülnek alkalmazásra (pl. bizonyos határvédelmi területeken, a kritikus alkalmazásokat kiszolgáló szerverfarmok közelében), hogy ott gyűjtsenek fontos információkat. A monitorozó eszközök a rendszerben ad hoc helyekre is telepítésre kerülhetnek bizonyos tranzakciók monitorozására. Ezen eszközök továbbá alkalmasak az informatikai rendszer biztonsági változtatásának a nyomon követésére is. Az összegyűjtött információ részletességét a szervezet határozza meg, a monitorozás céljának és az informatikai rendszer ezt támogató lehetőségei alapján. A szervezet megfelelő jogi tanácsadóval konzultál az informatikai rendszer valamennyi monitorozási tevékenységéről. A szervezet megemeli az informatikai rendszer monitorozási tevékenység szintjét, ha a szervezeti működés, a szervezeti vagyon fokozott kockázatnak van kitéve, vagy ha a rendészeti szervektől származó információk, titkosszolgálati információk, vagy más megbízható forrásból származó információk erre okot adnak. Kapcsolódó biztonsági intézkedések: HE-8.

9.2.2.5. RS-5 Biztonsági riasztások és tájékoztatások

Intézkedés: A szervezet folyamatosan fogadja az informatikai rendszerre vonatkozó biztonsági riasztásokat és figyelmeztetéseket, eljuttatja ezeket az illetékes személyekhez, illetve megfelelő válaszlépéseket foganatosít.

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat használ a biztonsági riasztások és figyelmeztetések szervezeten belüli szükséges terítésére.

Intézkedés kiegészítése: A szervezet dokumentálja a biztonsági riasztásokra, figyelmeztetésekre adandó válaszlépéseket. Kapcsolatot tart fent speciális IT biztonsággal kapcsolatos más szervezetekkel vagy csoportokkal (pl. informatikai biztonsági fórumok), melyek

- elérhetővé teszik a biztonsághoz kapcsolódó információkat (pl. fenyegetések, sebezhetőségek, legújabb biztonsági technológiák);
- hozzáférést biztosítanak biztonsági szakértőktől származó tanácsokhoz, és
- tökéletesítik a biztonsági bevált gyakorlatokat.

9.2.2.6. RS-6 A biztonsági funkcionalitás ellenőrzése

Intézkedés: Az informatikai rendszer ellenőrzi a biztonsági funkciók helyes működését [(egy vagy több) kiválasztás: a rendszer indításakor és újraindításakor; megfelelő privilégiummal rendelkező felhasználó parancsára; időszakosan, [értékadás: szervezet által meghatározott gyakorisággal]] és amennyiben hibákat fedeznek fel [(egy vagy több) kiválasztása: értesíti a rendszer adminisztrátort, leállítja a rendszert, újraindítja a rendszert].

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat alkalmaz a sikertelen automatikusan végrehajtott biztonsági tesztekről történő értesítésre.
b) A szervezet automatikus mechanizmusokat használ az elosztott biztonsági tesztek kezelésének segítésére.

Intézkedés kiegészítése: A biztonsági funkciók ellenőrzésének szükségessége valamennyi biztonsági funkcióra vonatkozik. Azon biztonsági funkciók, amelyekre nem lehet automatikus önellenőrzést végrehajtani, a szervezet vagy kiegészítő biztonsági intézkedést foganatosít, vagy kimondottan elfogadja a szükséges ellenőrzés elmaradásából adódó kockázatot.

9.2.2.7. RS-7 Szoftver és információ sértetlenség

Intézkedés: Az informatikai rendszer felismeri és védi a szoftverben és az információban bekövetkezett engedély nélküli változtatásokat.

Intézkedés bővítése:

a) A szervezet a szoftver és az információ sértetlenségét [értékadás: a szervezet által meghatározott gyakorisággal] újraértékeli, úgy hogy sértetlenség ellenőrzést végez a rendszeren.

b) A szervezet automatikus eszközöket alkalmaz a megfelelő személyek értesítésére, amennyiben a sértetlenség ellenőrzése során eltérést tapasztal.
c) A szervezet központilag kezelt sértetlenség ellenőrző eszközt üzemeltet.

Intézkedés kiegészítése: A szervezet sértetlenség ellenőrző alkalmazásokat használ, hogy bizonyítékokat keressen az informatikai rendszerben történő módosításokra, hibákra és mulasztásokra. A szervezet jól bevált szoftver mérnöki megoldásokat használ a kereskedelmi forgalomban kapható sértetlenség ellenőrző termékek esetében (pl. paritás ellenőrzés, ciklikus redundancia ellenőrzés (CRC), kriptográfiai hash értékek) és eszközöket használ az informatika rendszer és azon üzemelő alkalmazások sértetlenségének automatikus monitorozására.

9.2.2.8. RS-8 Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem

Intézkedés: Az informatikai rendszer kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelmet valósít meg.

Intézkedés bővítése:
a) A szervezet központilag kezeli a levélszemét elleni védelmi mechanizmust.
b) Az informatikai rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmust.

Intézkedés kiegészítése: A szervezet levélszemét elleni védelmet alkalmaz a kritikus informatika rendszer belépő pontjain (pl. tűzfalak, levelező szerverek, web szerverek, proxy szerverek, távoli elérését biztosító szerverek) valamint a munkaállomásokon, szervereken, vagy a hálózaton megtalálható mobil számítástechnikai eszközökön. A szervezet levélszemét elleni védelmi mechanizmusa észleli a kéretlen üzeneteket, és megfelelő ellenintézkedéseket foganatosít ellenük, amelyek érkezhetnek elektronikus levélben, elektronikus levél csatolmányaként, internet hozzáférés során, vagy más szokásos módon. Mérlegelendő különböző gyártótól származó levélszemét védelmi eszközök használata (pl. egy terméket használjon a határvédelmi eszközöknél és a szervereknél és egy másikat a munkaállomásokon).

9.2.2.9. RS-9 A bemeneti információra vonatkozó korlátozások

Intézkedés: A szervezet az informatikai rendszernek szóló információ bevitelt az erre jogosult személyekre korlátozza.

Intézkedés kiegészítése: A személyre vonatkozó információs rendszerbe történő információ beviteli jogosultság kiterjeszthető a tipikus rendszerszintű hozzáférés szabályzáson túl, hozzávéve az adott művelet/projekt felelősségeket is.

9.2.2.10. RS-10 A bemeneti információ pontossága, teljessége és érvényessége

Intézkedés: Az informatikai rendszer ellenőrzi az információ bemenetek pontosságát, teljességét, érvényességét és hitelességét.

Intézkedés kiegészítése: Az információ bemenetek pontosságának, teljességének, érvényességének és hitelességének az ellenőrzését az eredeti forráshoz lehető legközelebb kell elvégezni. Az informatikai rendszer bemeneteli értékeire vonatkozó ellenőrzési szabályok (pl. karakter készlet, számtartomány, elfogadható értékek) azért kerülnek meghatározásra, hogy a bemeneti érték megfelel-e a megadott definíciónak formátum és tartalom szempontjából. A parancsértelmezőknek átadott értékek előzetes vizsgálatra kerülnek, nehogy véletlenül parancsként kerüljenek értelmezésre. Az informatikai rendszer által ellenőrzött adatok pontosságának, teljességének, érvényességének és hitelességének a mértéke meghatározásában a szervezet szabályzata és a működési követelmények nyújtanak útmutatást.

9.2.2.11. RS-11 Hibakezelés

Intézkedés: Az informatikai rendszer eredményesen azonosítja és kezeli a hibákat, de nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak.

Intézkedés kiegészítése: A hibaüzenet formáját és tartalmát alaposan mérlegeli a szervezet. A hibaüzenetekhez csak az erre jogosult személyek férhetnek hozzá. Az informatikai rendszer által generált hibaüzenetek aktuális és hasznos információkat tartalmaznak, de nem fednek fel potenciálisan ártalmas információkat, amelyeket a támadók felhasználhatnak. Érzékeny információk (pl. számlaszámok, társadalombiztosítási számok és hitelkártya számok) nem kerülnek feltüntetésre a hiba naplókba, sem a hozzátartozó üzemeltetési üzenetekben. Az informatikai rendszer által felismert és kezelt hibák mértékének meghatározásában a szervezet szabályzata és működési követelmények nyújtanak útmutatást.

9.2.2.12. RS-12 A kimeneti információ kezelése és megőrzése

Intézkedés: A szervezet az informatikai rendszer kimenetét a szervezeti szabályzattal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

9.2.3. Azonosítás és hitelesítés (AH)

9.2.3.1. AH-1 Azonosítási és hitelesítési szabályzat és eljárásrend

Intézkedés: A szervezet kifejleszt, terjeszt, rendszeresen felülvizsgál és frissít:

- egy formális, dokumentált, az azonosításra és hitelesítésre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés, menedzsment kötelezettségei, koordináció a szervezet egységei közt; illetve

— egy formális, dokumentált eljárásrendet, amelynek célja az azonosításra és hitelesítésre vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

Intézkedés kiegészítése: Az azonosítási és hitelesítési szabályzat része lehet a szervezet általános informatikai szabályzatának. Az azonosítási és hitelesítési eljárásrendet ki lehet alakítani az általános biztonsági program részeként, vagy ha szükséges egy konkrét informatikai rendszerhez is.

9.2.3.2. AH-2 Felhasználó azonosítása és hitelesítése

Intézkedés: Az informatikai rendszer egyedileg azonosítja és hitelesíti a felhasználókat (vagy a felhasználók nevében eljáró eljárásokat)

Intézkedés bővítése

a) Az informatikai rendszer többtényezős hitelesítést használ a távoli hozzáférésre, ami kriptográfiai kulcsbirtoklás bizonyításán alapul. A kriptográfiai kulcsot tárolhatja [értékadás: Szoftver token, FIPS 140-2 [12] 1-es szinten tanúsított hardver; vagy FIPS 140-2 [12] 2-es vagy magasabb szinten tanúsított hardver.]
b) Az informatikai rendszer többtényezős hitelesítést használ a helyi hozzáférésre, ami kriptográfiai kulcsbirtoklás bizonyításán alapul. A kriptográfiai kulcsot tárolhatja [értékadás: Szoftver token, FIPS 140-2 [12] 1-es szinten tanúsított hardver; vagy FIPS 140-2 [12] 2-es vagy magasabb szinten tanúsított hardver.].
c) Az informatikai rendszer többtényezős hitelesítést használ a távoli hozzáférésre, ami kriptográfiai kulcsbirtoklás bizonyításán alapul. A kriptográfiai kulcsot FIPS 140-2 [12] 2-es vagy magasabb szinten tanúsított hardver tárolhatja.

Intézkedés kiegészítése: A felhasználókat minden hozzáférésnél egyedileg azonosítani és hitelesíteni kell kivéve, ha az adott hozzáférési kérelem külön dokumentálva van a szervezet által a HE-14-es biztonsági szabálynak megfelelően. A felhasználók hitelesítése történhet jelszavakon keresztül, tokenek segítségével, biometria segítségével vagy többtényezős hitelesítés esetén ezek kombinációjával.

Távoli hozzáférésnek minősül minden olyan hozzáférés a szervezet informatikai rendszeréhez (felhasználó vagy másik informatikai rendszer által), amelyben a kommunikáció egy külső, nem a szervezet által ellenőrzött hálózaton (pl. Internet) zajlik.

Helyi hozzáférésnek minősül minden olyan hozzáférés a szervezet informatikai rendszeréhez (felhasználó vagy másik informatikai rendszer által), amelyben a kommunikáció egy belső, a szervezet által ellenőrzött hálózaton (pl. intranet) zajlik, vagy közvetlenül az eszközhöz kapcsolódnak hálózat nélkül.

Az informatikai rendszer szintjén zajló felhasználó azonosítási és hitelesítési folyamaton kívül (belépés a rendszerbe), az alkalmazási szinten is lehetnek azonosítási és hitelesítési folyamatok ahol szükségesek, ezzel növelve a biztonságot a szervezeten belül.

A skálázhatóságot, a gyakorlatiasságot és biztonság kérdéseit egyszerre kell figyelembe venni, hogy egyensúly legyen az információk használatának egyszerűsége és az informatikai rendszerek adatainak (szervezeti műveletek, szervezeti vagyon) védelme közt. Kapcsolódó biztonsági intézkedések: HE-14, HE-17. További információk a 10.3 fejezetben illetve a NIST SP 800-63 [16] dokumentumban található.

9.2.3.3. AH-3 Eszközök azonosítása és hitelesítése

Intézkedés: Az informatikai rendszer bizonyos eszközöket azonosít és hitelesít, mielőtt kapcsolatot létesítene velük.

Intézkedés kiegészítése: Az informatikai rendszer a legtöbb esetben vagy ismert információkat (pl. Media Access Control (MAC) vagy Transmission Control Protocol/Internet Protocol (TCP/IP) címeket) vagy szervezeten belüli hitelesítési megoldásokat (pl. IEEE 802.1x és Extensible Authentication Protocol (EAP) vagy Radius szerver EAP-Transport Layer Security (TLS) hitelesítéssel) használ az eszközök azonosítására és hitelesítésére a belső és vagy külső hálózatain. Az eszköz hitelesítésének szükséges erősségét az informatikai rendszer biztonsági besorolása határozza meg (lásd „*Útmutató az IT biztonsági szintek meghatározásához*” [03]), a magasabb szint erősebb hitelesítést jelent.

9.2.3.4. AH-4 Azonosító kezelés

Intézkedés: A szervezet az alábbi módon kezeli a felhasználói azonosítókat:
- egyedileg azonosít minden felhasználót;
- ellenőrzi minden felhasználó azonosságát;
- egy új felhasználói azonosító kibocsátását adminisztrátori felhatalmazáshoz köti;
- garantálja, hogy a felhasználói azonosítót annak a félnek adták ki, akinek szánták;
- lezárja a felhasználói azonosítót egy, [értékadás: a szervezet által meghatározott időtartam]-ig tartó inaktivitás után, és
- archiválja a felhasználói azonosítókat.

Intézkedés kiegészítése: Az azonosító kezelés nem használható megosztott felhasználói fiókokra (pl. vendég és névtelen fiókokra)

9.2.3.5. AH-5 A hitelesítésre szolgáló eszközök kezelése

Intézkedés: A szervezet az alábbi módon kezeli a rendszer hitelesítésre szolgáló eszközeit:
- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
- adminisztratív eljárásokat vezet be a hitelesítésre szolgáló eszközök kezdeti szétosztására, az elvesztett/kompromittálódott vagy sérült eszközök esetére, illetve a hitelesítésre szolgáló eszközök visszavonására;
- az alapértelmezés szerinti hitelesítésre szolgáló eszközöket megváltoztatja az informatikai rendszer installálásának során; és
- időszakonként a hitelesítésre szolgáló eszközöket megváltoztatja/frissíti.

Intézkedés kiegészítése: Az informatikai rendszer hitelesítésre szolgáló eszközei lehetnek tokenek, PKI tanúsítványok, biometrikus adatok, jelszavak és kódkártyák. A felhasználóknak a hitelesítésre szolgáló eszközöket védeniük kell, az egyéni hitelesítő eszközeiket maguknál kell tartaniuk. Tilos ezeket megosztaniuk vagy kölcsönadniuk, illetve eszköz elveszetést vagy kompromittálódást azonnal jelenteniük kell.

Jelszó alapú hitelesítés esetén az informatikai rendszernek:
- meg kell óvnia a jelszavakat, hogy illetéktelen ne férjen hozzájuk, ne lehessen őket megváltoztatni tárolás vagy adatátvitel közben;
- meg kell, hogy akadályozza, hogy látszódjon a jelszó miközben begépelik;
- szabályoznia kell a jelszó minimális és maximális élettartamát; és
- meg kell tiltania a jelszavak újrafelhasználását meghatározott számú új jelszóig.

PKI alapú hitelesítés esetén az informatikai rendszer
- ellenőrzi a tanúsítványokat a hitelesítési útvonal követésével egy megbízható hitelesítőig;
- a felhasználónak ellenőrzést ad a privát kulcsa felett; és
- hozzárendeli a hitelesített azonosítót egy felhasználói fiókhoz.

9.2.3.6. AH-6 A hitelesítésre szolgáló eszköz visszacsatolása

Intézkedés: Az informatikai rendszer visszacsatolást biztosít a felhasználónak hitelesítési kísérlete során, és ez a visszacsatolás nem veszélyezteti a hitelesítési mechanizmust. Az informatikai rendszer elrejti a hitelesítési információk visszacsatolását a hitelesítési kísérlet során, így védve az információt az esetleges kihasználástól/illetéktelen használattól.

Intézkedés kiegészítése: Az informatikai rendszer visszacsatolása nem tartalmaz olyan információkat, aminek a segítségével egy illetéktelen felhasználó kijátszhatná a hitelesítési mechanizmust. Csillagok megjelenítése a jelszó gépelése közben egy példa lehet a hitelesítési információk visszacsatolásának elrejtésére.

9.2.3.7. AH-7 Hitelesítés kriptográfiai modul esetén

Intézkedés: Az informatikai rendszer olyan hitelesítési módszereket használ, amelyek megfelelnek a törvényeknek, vezetői döntéseknek, direktíváknak, szabályzatoknak, előírásoknak, szabványoknak, és a kriptográfiai modul hitelesítési útmutatójának.

Intézkedés kiegészítése: Jelenleg a kriptográfiai modulok általánosan elfogadott szabványa a FIPS 140-2 [12]. Ugyanakkor a NIST Kriptográfiai Modul Ellenőrzési Program által kiállított korábbi tanúsítványok is érvényesek maradtak, és a modulok alkalmasak további használatra vagy megvételre amíg a vonatkozó tanúsítványt vissza nem vonják. Alkalmazható más egyenértékű szabvány is.

9.2.4. Hozzáférés ellenőrzése (HE)

9.2.4.1. HE-1 Hozzáférés ellenőrzési szabályzat és eljárásrend

Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált hozzáférés ellenőrzési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettséget, és megfelelést; a koordináció a szervezeti entitások között;
- egy formális, dokumentált hozzáférés védelemre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés, menedzsment kötelezettségei, koordináció a szervezet egységei közt; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a hozzáférés ellenőrzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

Intézkedés kiegészítése: A hozzáférés védelmi szabályzat és eljárásrend összhangban kell lennie a törvényekkel, direktívákkal, szabályzatokkal, előírásokkal, szabványokkal és útmutatókkal. A hozzáférés védelmi szabályzata részét képezheti a vállalat általános informatikai biztonsági szabályzatának. A hozzáférés védelmi eljárásrendet az általános biztonsági programmal, vagy ha szükséges egy konkrét informatikai rendszerre vonatkozó biztonsági programmal együtt is ki lehet alakítani.

9.2.4.2. HE-2 Felhasználói fiókok kezelése

Intézkedés: A szervezet kezeli az informatikai rendszer felhasználói fiókjait, beleértve a felhasználói fiókok létrehozását, aktiválását, módosítását, felülvizsgálatát, letiltását és eltávolítását. A szervezet felülvizsgálja az informatikai rendszer felhasználói fiókjait [értékadás: a szervezet által meghatározott gyakoriság, de legalább évente].

Az intézkedés bővítése:

a) A szervezet automatizált mechanizmusokat alkalmaz a felhasználói fiókok kezelésének támogatására.
b) Az informatikai rendszer automatikusan leállítja az ideiglenes és a kényszerhelyzetben létrehozott felhasználói fiókokat [értékadás: az egyes felhasználói fiók típusokra a szervezet által definiált időtartam] letelte után.
c) Az informatikai rendszer automatikusan letiltja az inaktív felhasználói fiókokat [értékadás: a szervezet által meghatározott időtartam] letelte után.
d) A szervezet automatikus mechanizmusokat használ a felhasználói fiókok kialakítására, módosítására, zárolására, visszavonására és az egyes személyek értesítésére, ha szükséges.

Intézkedés kiegészítése: A felhasználói fiókok kezelése tartalmazza a különböző fióktípusok azonosítását (egyéni, csoport vagy rendszerfiók), a feltételek biztosítását a csoporttagságokhoz és a kapcsolódó engedélyek fiókokhoz rendelését. A szervezet azonosítja az informatikai rendszer hitelesített felhasználóit és meghatározza a hozzáférési jogokat.

A szervezet az informatikai rendszerhez a felhasználók hozzáférési jogait a következők alapján határozza meg:

— az érvényes „szükséges ismerni”/”szükséges megosztani” besorolások, amit a hivatalos feladatok határoznak meg és teljesíti az összes személyzeti biztonsági feltételt; illetve
— a kívánt rendszer használat.

A szervezet megfelelő azonosítást igényel új felhasználói fiókok létrehozásához, és minden ilyen igénylést jóvá kell hagyni. A szervezet külön ellenőrzi a vendég/névtelen felhasználói fiókokat valamint a szükségtelen felhasználói fiókokat eltávolítja, zárolja vagy más módon lezárja. A felhasználói fiókok kezelői értesítést kapnak, ha az informatikai rendszer felhasználói otthagyják a szervezetet, áthelyezik őket vagy a kapcsolódó felhasználói fiók megszűnik, zárolódik, vagy más módon lezáródik. A felhasználói fiókok kezelői akkor is értesítést kapnak, ha az informatikai rendszer használata vagy a „szükséges ismerni”/”szükséges megosztani” besorolás a felhasználó vonatkozásában megváltozik.

9.2.4.3. HE-3 Hozzáférés ellenőrzés érvényre juttatása

Intézkedés: Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszerhez való hozzáférés ellenőrzéséhez.

Az intézkedés bővítése:

a) Az informatikai rendszer biztosítja, hogy a biztonsági funkciókhoz (amelyek hardverben, szoftverben vagy förmverben valósulnak meg) és információkhoz való hozzáférés az erre feljogosított személyzetre (pl. biztonsági adminisztrátorok) korlátozódjon.
   Megjegyzés: A közvetlenül feljogosított személyzetbe tartoznak például a biztonsági adminisztrátorok, a rendszer és hálózati adminisztrátorok és más kiemelt jogú felhasználók. Kiemelt jogú felhasználók azok a személyek, akik a rendszert vezérlő, monitorozó vagy adminisztratív funkciókhoz hozzáférhetnek (pl. rendszeradminisztrátorok, informatikai rendszer biztonsági tisztviselői, üzemeltetők, rendszerprogramozók)

Intézkedés kiegészítése: A hozzáférés védelem szabályait (pl. azonosító alapú szabályok, szerep alapú szabályok, feltétel alapú szabályok) és a hozzájuk tartozó hozzáférés védelmet kikényszerítő mechanizmusokat (pl. hozzáférés ellenőrző listák (ACL), hozzáférés ellenőrző mátrixok, kriptográfia) a szervezetek arra használják, hogy szabályozzák a hozzáférést az informatikai rendszerben a felhasználók (vagy felhasználók nevében futó folyamatok) és a különböző objektumok (pl. eszközök, fájlok, rekordok, folyamatok, programok, tartományok) között. A hozzáférések informatikai rendszer szintjén való védelme mellett a hozzáférés védelmet kikényszerítő mechanizmusok az alkalmazások szintjén is kell, hogy működjenek, ha ez szükséges, ezzel magasabb szintű biztonságot nyújtva a szervezetben. Meg kell fontolni egy ellenőrzött, naplózott kézi vezérlésű rendszert az automatikus mechanizmusok felett, ami vészhelyzet vagy más komoly esemény alkalmával léphet életbe. Ha a hozzáférés védelmet kikényszerítő mechanizmus részeként a tárolt információ rejtjelezve van, a kriptográfiai eljárásnak meg kell felelnie a FIPS 140-2-nek [12] vagy más egyenértékű szabványnak. Kapcsolódó biztonsági intézkedés: RV-13.

9.2.4.4. HE-4 Információ áramlás ellenőrzés érvényre juttatása

Intézkedés: Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információ áramlás ellenőrzéséhez.

Intézkedés bővítése:

a) Az informatikai rendszer az információ áramlás szabályzásának kikényszerítését olyan címkék hozzárendelésével valósítja meg az információn vagy a forrás és cél objektumokon, amelyek az információ áramlás döntéseinek alapjai lesznek. Megjegyzés: Az információ áramlás szabályzásának kikényszerítésére címkék szolgálnak, például bizonyos típusú információk e címkék alapján továbbítódnak.
b) Az informatikai rendszer az információ áramlás szabályzásának kikényszerítését védett tartományok segítségével oldja meg (pl. tartomány típus szerinti szabályozás), ezek lesznek az információ áramlás döntéseinek alapjai.

Intézkedés kiegészítése: Az információáramlás határozza meg, hogyan és merre mozoghat az információ az informatikai rendszeren belül valamint az informatikai rendszerek közt (azt nem befolyásolja, hogy ki férhet hozzá az információhoz), tekintet nélkül a további hozzáférésekre az információhoz.

Néhány példa olyan korlátozásokra, amelyeket jobban meg lehet valósítani az információ áramlás szabályozásával, mint hozzáférés védelemmel:

- kiviteli korlát alá eső információk nyílt átvitele az Interneten,
- olyan külső forgalom blokkolása, ami a szervezetből származónak tünteti fel magát,
- webes kérések továbbításának megtagadása, ha nem a belső web proxy-n keresztül érkeznek.

Az információ áramlás szabályzatait és kényszerítő mechanizmusait gyakran használják az információáramlás ellenőrzésére a meghatározott források és célok közt (pl. hálózatok, személyek, eszközök) az informatikai rendszereken belül és az összekapcsolt rendszerek közt. Az információ áramlás szabályozása az információtól és az információ útjának karakterisztikájától függ. Konkrét példákat az információ áramlás szabályozását kikényszerítő mechanizmusokra a hálózat határait védő eszközökben lehet találni (pl. proxy-k, átjárók, rejtjelzett csatornák, tűzfalak és router-ek), amelyek olyan szabálykészleteket vagy konfigurációs beállításokat használnak, amelyek korlátozzák az informatikai rendszer szolgáltatásait vagy csomagszűrést alkalmaznak. Kapcsolódó biztonsági intézkedés: RV-7.

9.2.4.5. HE-5 A felelősségek szétválasztása

Intézkedés: Az informatikai rendszer érvényre juttatja a felelősségek szétválasztását az egyes munkakörökhöz kijelölt hozzáférési jogosultságokon keresztül.

Intézkedés kiegészítése: A szervezet megállapítja az egyes egységek felelősségét és elkülöníti a feladatokat, hogy megakadályozza az egyének feladataiból és kötelezettségeiből fakadó konfliktusokat. Van olyan hozzáférés védelmi szoftver az informatikai rendszerben, ami megakadályozza, hogy a felhasználók az összes olyan hozzáférési jogosultságot megszerezhessék, amelyek együttesen utána rosszindulatú célokra is felhasználhatóak.

A feladatok elkülönítésére példa lehet:

- a feladat funkciók és az informatikai rendszert támogató funkciók különböző személyek/szerepek közt vannak szétosztva;
- különböző személyek végzik az informatikai rendszert támogató funkciókat (pl. rendszerfelügyelet, rendszerprogramozás, minőségbiztosítás/tesztelés, konfiguráció-kezelés és hálózati biztonság);
- a biztonsággal foglalkozó személyek, akik a hozzáférés védelem funkcióit felügyelik, nem felügyelhetik a naplózás funkcióit is;

9.2.4.6. HE-6 Legkisebb jogosultság

Intézkedés: Az informatikai rendszer a felhasználók (illetve a felhasználók nevében fellépő eljárások) számára a megadott feladatok végrehajtásához szükséges leginkább korlátozó jogosultságok/privilégiumok, illetve hozzáférések összességét juttatják érvényre.

Intézkedés kiegészítése: A szervezet a legkisebb jogosultság elvét használja a konkrét feladatokhoz és az informatikai rendszerekhez (beleértve a portokat, hálózati protokollokat, szolgáltatásokat) a kockázat felméréseknek megfelelően, ezzel csökkentve a vállalat működését, a vállalati vagyont és az egyéneket fenyegető kockázatokat.

9.2.4.7. HE-7 Sikertelen bejelentkezési kísérletek

Intézkedés: Az informatikai rendszer egy [értékadás: a szervezet által definiált szám]-ként megadott korlátot juttat érvényre egy felhasználó egymást követő bejelentkezési kísérleteire, amelyek egy [értékadás: a szervezet által definiált időtartam]-on belül történtek. Amennyiben a sikertelen kísérletek a maximális számot túllépik, az információs rendszer automatikusan [választás: zárolja a felhasználói fiókot/csomópontot [értékadás: a szervezet által definiált időtartamig]; késlelteti a következő bejelentkezési kísérletet egy az [értékadás: szervezet által definiált késleltetési algoritmusnak megfelelően]].

Intézkedés bővítése:

a) Amikor sikertelen kísérletek száma eléri a maximális próbálkozások számát, az informatikai rendszer automatikusan zárolja a fiókot addig, amíg a rendszergazda azt vissza nem állítja.

Intézkedés kiegészítése: A szolgáltatás megtagadása (DoS) támadások lehetősége miatt bevezetett automatikus zárolások általában ideiglenesek és automatikusan megszűnnek egy előre meghatározott idő után.

9.2.4.8. HE-8 A rendszerhasználat jelzése

Intézkedés: Az informatikai rendszer egy jóváhagyott, a rendszerhasználatra vonatkozó jelzést ad a rendszerhez való hozzáférés engedélyezése előtt abból a célból, hogy a potenciális felhasználókat tájékoztatassa arról:

- hogy a felhasználó egy magyar közigazgatási informatikai rendszert használ;

- hogy lehetséges, hogy a rendszer használatot figyelhetik, rögzíthetik, illetve auditálhatják;
- hogy a rendszer jogosulatlan használata tilos, és büntetőjogi, valamint polgárjogi felelősségre vonással jár;
- hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti a figyelésbe és rögzítésbe. A rendszer által használt közlemény biztosítja a magántitokra és biztonságra vonatkozó értesítéseket, és mindaddig a képernyőn marad, amíg a felhasználó közvetlen műveletet nem végez az informatikai rendszerbe való bejelentkezéshez.

Intézkedés kiegészítése: Az adatvédelemi és a biztonsági szabályzat összhangban vannak a törvényekkel, vezetői döntésekkel, direktívákkal, szabályzatokkal, előírásokkal, szabványokkal és útmutatókkal. A rendszer használat értesítő üzeneteit egy vizuális figyelmeztető jelzéssel meg lehet oldani, ami akkor jelenik, meg, amikor valaki bejelentkezik a rendszerbe.

Nyilvánosan elérhető rendszerek esetén:

- A rendszer használat adatai elérhetőek, és ha szükséges bejelentkezés előtt megtekinthetőek.
- minden adatrögzítésre vagy naplózásra vonatkozó kapcsolat megfelel az adatvédelmi szabályoknak olyan rendszerek esetén, amelyek általában tiltják ezeket a tevékenységeket.
- a felhasználónak adott figyelmeztetés tartalmazza a rendszer engedélyezett felhasználásának leírását.

9.2.4.9. HE-9 Értesítés előző bejelentkezésről

Intézkedés: Az informatikai rendszer értesíti a felhasználót sikeres bejelentkezés esetén az utolsó bejelentkezés időpontjáról, és az azóta keletkezett sikertelen bejelentkezési próbálkozások számáról.

9.2.4.10. HE-10 Egyidejű munkaszakasz kezelés

Intézkedés: Az informatikai rendszer korlátozza az egyszerre történő bejelentkezések számát a következőre: [értékadás: a szervezet által meghatározott szám a párhuzamos munkaszakaszokra]

9.2.4.11. HE-11 A munkaszakasz zárolása

Intézkedés: Az informatikai rendszer [értékadás: a szervezet által definiált időtartam] inaktivitás után a munkaszakasz zárolásával megakadályozza a rendszerhez való további hozzáférést mindaddig, amíg a felhasználó nem azonosítja és hitelesíti magát újra a megfelelő eljárások alkalmazásával.

Intézkedés kiegészítése: A felhasználók közvetlenül kérhetik a munkaszakasz zárolását. A zárolás nem helyettesíti a kijelentkezést a rendszerből. A szervezet által definiált időtartam

összhangban kell, hogy legyen az általános szabályzattal, például távoli elérés és hordozható eszközök esetén az ajánlott időtartam nem lehet több mint 30 perc.

9.2.4.12. HE-12 A munkaszakasz lezárása

Intézkedés: Az informatikai rendszer automatikusan lezárja a munkaszakaszt egy, [értékadás: a szervezet által definiált időtartam] hosszúságú inaktivitás után.

Intézkedés bővítése:

a) Az automatikus munkaszakasz lezárás vonatkozik a helyi és távoli munkaszakaszokra is.

Intézkedés kiegészítése: Távoli munkaszakaszt lehet kezdeményezni, ha a felhasználó (vagy informatikai rendszer) egy külső, nem szervezet által ellenőrzött hálózaton (pl. Interneten) keresztül fér hozzá a rendszerhez.

9.2.4.13. HE-13 Felügyelet és felülvizsgálat — hozzáférés ellenőrzés

Intézkedés: A szervezet felügyeli és felülvizsgálja a felhasználók tevékenységét az informatikai rendszer hozzáférés ellenőrzése érvényre juttatása és használata tekintetében.

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat használ a felhasználói tevékenységek ellenőrzésére.

Intézkedés kiegészítése: A szervezet megvizsgálja a naplóbejegyzéseket (pl. felhasználói tevékenység napló), megkeresve a szervezeti eljárásrendnek nem megfelelő tevékenységeket. Megvizsgálja a informatikai rendszerrel kapcsolatos szokatlan tevékenységeket és időnként felülvizsgálja a hozzáférési jogok változásait. A vizsgálat gyakoribb azoknál a felhasználók a tevékenységére vonatkozóan, akik kiemelt szereppel vagy felelősséggel bírnak az informatikai rendszerben. A naplóbejegyzések vizsgálatának szintje az informatikai rendszer biztonsági szintjétől (lásd „*Útmutató az IT biztonsági szintek meghatározásához*” [03]) függ. Például egy alacsony kihatású biztonsági osztályba eső rendszer esetén nem kell minden munkaállomáson gyakran ellenőrizni a biztonsági naplót, elég inkább a központi helyeket ellenőrizni, mint például a web proxy vagy az email szerverek, kivéve, ha a körülmények a többi naplóbejegyzés megvizsgálását is szükségessé teszik.

9.2.4.14. HE-14 Azonosítás és hitelesítés nélkül engedélyezett tevékenységek

Intézkedés: A szervezet meghatározza azokat a speciális felhasználói tevékenységeket, amelyeket az informatikai rendszerben azonosítás és hitelesítés nélkül is végre lehet hajtani.

Intézkedés bővítése:

a) A szervezet csak olyan mértékben engedélyezi az azonosítás és hitelesítés nélkül végrehajtható tevékenységeket, amennyire az saját céljainak megfelel.

Intézkedés kiegészítése: A szervezet korlátozott tevékenységet engedélyez azoknak a felhasználóknak, akik azonosítás és hitelesítés nélkül használják a nyilvános web helyeket vagy más nyilvánosan elérhető rendszert. /Például nyilvános honlapján keresztül egy szervezet elérhetővé tehet bizonyos, de korlátozott információkat a felhasználók azonosítása és hitelesítése nélkül./ Kapcsolódó biztonsági intézkedés: AH-2.

9.2.4.15. HE-15 Automatikus jelölés

Intézkedés: Az informatikai rendszer megjelöli a kimenetet szabványos névkonvenciókkal, hogy egyértelművé tegye a különleges terjesztési, kezelési utasításokat.

Intézkedés kiegészítése: Az automatikus megjelölés a külső médiaelemeken használt jelölésekre vonatkozik (pl. az informatikai rendszerből származó papíralapú dokumentumok). A külső jelölésben használt jelöléseket meg kell különböztetni a HE-16-ban leírt belső adatstruktúrák jelölésétől.

9.2.4.16. HE-16 Automatikus címkézés

Intézkedés: Az informatikai rendszer megjelöli az információt az adattárakban, folyamatokban és adatátvitel közben.

Intézkedés kiegészítése: Az automatikus címkézés a belső adatstruktúrák megjelölésére vonatkozik (pl. rekordok, fájlok) az informatikai rendszeren belül. Az információ megjelölése az alábbiakkal összhangban történik:

- hozzáférés védelem követelményei;
- különleges kezelési és terjesztési instrukciók;
- az informatikai biztonsági szabályzat érvényre juttatásának követelményei.

9.2.4.17. HE-17 Távoli hozzáférés ellenőrzése

Intézkedés: A szervezet engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való távoli hozzáférés minden módszerét (pl. betárcsázás, Internet), beleértve a privilegizált funkciókhoz való távoli hozzáférést. Megfelelően feljogosított tisztviselők engedélyezik az informatikai rendszerhez való hozzáférés minden egyes hozzáférési módszerét, és minden egyes hozzáférési módszer használatához csak a szükséges felhasználókat jogosítják fel.

Intézkedés bővítése:

a) A szervezet automatizált mechanizmusokat alkalmaz a távoli hozzáférési módszerek figyelésére és ellenőrzésére.
b) A szervezet rejtjelzést alkalmaz a távoli hozzáférési munkaszakaszok bizalmasságának megvédésére.
c) A szervezet egy menedzselt hozzáférés ellenőrzési ponton keresztül minden távoli hozzáférést ellenőriz.

d) A szervezet magas jogosultsághoz kötött funkciókhoz csak komoly működéshez kapcsolódó igény esetén enged távoli hozzáférést, és ebben az esetben is dokumentálni kell ennek az indoklását az informatikai rendszer biztonsági tervében.

Intézkedés kiegészítése: Távoli hozzáférésnek minősül minden olyan hozzáférés a szervezet informatikai rendszeréhez (felhasználó vagy másik informatikai rendszer által), amelyben a kommunikáció egy külső, nem a szervezet által ellenőrzött hálózaton (pl. Internet) zajlik. A távoli hozzáférésre példa lehet a betárcsázós, szélessávú és vezeték nélküli kapcsolat. Távoli hozzáférés védelmet nem kell alkalmazni nyilvános web szerverek esetén vagy olyan rendszerek esetén, amelyeket direkt távoli elérésre terveztek. A szervezet korlátozza a hozzáférést betárcsázós kapcsolatokon keresztül (pl. a kérés forrása alapján), vagy kiszűri a nem engedélyezett kapcsolatokat illetve engedélyezett kapcsolatok bizonyos csoportjait (pl. VPN-t (Virtuális Magán Hálózatot) használó kapcsolatokat). Kapcsolódó biztonsági intézkedés: AH-2.

9.2.4.18. HE-18 A vezeték nélküli hozzáférésre vonatkozó korlátozások

Intézkedés: A szervezet:
- felhasználási korlátozásokat és megvalósítási útmutatót vezet be a vezeték nélküli technológiákra; és
- engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való vezeték nélküli hozzáféréseket.

Intézkedés bővítése:

a) A szervezet az informatikai rendszerhez való vezeték nélküli hozzáférés védelmére hitelesítést és rejtjelzést alkalmaz.
b) A szervezet megvizsgálja a nem engedélyezett vezeték nélküli hozzáférési pontokat a következő frekvencián: [értékadás: szervezet által meghatározott frekvencia] és megteszi a szükséges lépéseket, ha ilyen hozzáféréseket találnak. Magyarázat: A szervezet egy alapos vizsgálatot folytat nem engedélyezett vezeték nélküli hozzáférési pontokat keresve a kiemelten fontos informatikai rendszereket tartalmazó egységekben. A vizsgálat nem korlátozódik az egységen belül arra a területre, ahol a kiemelten fontos informatikai rendszer található.

Intézkedés kiegészítése: További információ a vezeték nélküli hálózatok biztonságáról a NIST SP 800-48 [15] és NIST SP 800-97 [25] dokumentumokban található

9.2.4.19. HE-19 A hordozható és mobil eszközök hozzáférés ellenőrzése

Intézkedés: A szervezet:
- felhasználási korlátozásokat és megvalósítási útmutatót vezet be a hordozható és mobil eszközökre; és
- engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való, hordozható és mobil eszközökön keresztüli hozzáféréseket.
- Megfelelően feljogosított tisztviselők engedélyezik a hordozható és mobil eszközök használatát.

Intézkedés bővítése:

a) A szervezet a hordozható és mobil eszközökön tárolt információk védelmére cserélhető merevlemezeket vagy kriptográfiát alkalmaz.

Intézkedés kiegészítése: Hordozható és mobil eszközök (pl. notebook-ok, pda-k, mobil telefonok és más kommunikációs eszközök, amelyek hálózati kapcsolatra képesek és különböző fizikai helyeken képesek működni) csak a szervezeti biztonsági szabályzattal és eljárásrenddel összhangban férhetnek hozzá az informatikai rendszerekhez. A biztonsági szabályzatok és eljárásrend érintheti az eszközök azonosítását és hitelesítését, a kötelező védelmi szoftverek használatát (pl. ártalmas programok detektálása, tűzfal), konfigurációkezelést, ártalmas kódokat kereső eszközök használatát, vírusvédelmi programok frissítését, kritikus szoftverfrissítések és javítások használatát, az operációs rendszer (és más rezidens szoftver) integritásvizsgálatát, szükségtelen hardverelemek semlegesítését (pl. vezeték nélküli eszközök, infravörös eszközök). A hordozható és mobil eszközökön található információ védelmét (pl. kriptográfia mechanizmusok használata a bizalmasság és az integritás védelmére adatok tároláshoz és az ellenőrzött területen kívüli adatátvitelhez) a fizikai közeg védelme intézkedés család tárgyalja.

9.2.4.20. HE-20 Külső informatikai rendszerek használata

Intézkedés: A szervezet meghatározza a feltételeket és szabályokat a feljogosított felhasználóknak a következőkre:

- hozzáférés az informatikai rendszerhez egy külső rendszerből;
- szervezet által ellenőrzött információk feldolgozása, tárolása és/vagy átvitele külső informatikai rendszerek segítségével.

Intézkedés bővítése:

a) A szervezet megtiltja a jogosult felhasználóknak külső informatikai rendszerek felhasználását a belső rendszeren található információk feldolgozására, tárolására vagy átvitelére, kivéve, ha a szervezet:
   af) ellenőrizni tudja a szükséges biztonsági intézkedések használatát a külső rendszeren, úgy ahogy az a biztonsági szabályzatban és biztonsági tervben le van írva;
   ag) jóváhagyott kapcsolat van az informatikai rendszerek közt, vagy megállapodás született azzal a szervezettel, amelyik a külső informatikai rendszert befogadja.

Intézkedés kiegészítése: A külső informatikai rendszerek olyan informatikai rendszerek vagy informatikai rendszereknek olyan összetevői, amelyek kívül esnek a szervezet által meghatározott hitelesítési határon, és amelyek esetében a szervezet nem ellenőrzi közvetlenül a biztonsági intézkedések használatát, vagy nem képes felmérni használatának eredményességét. Külső informatikai rendszerek lehetnek (de nem kizárólag) a szervezet által birtokolt informatikai rendszerek (pl. számítógépek, mobil telefonok vagy PDA-k); szervezet által birtokolt számítástechnikai vagy kommunikációs eszközök kereskedelmi vagy nyilvános elérhetőséggel (pl. szállodákban, kongresszusi központokban vagy repülőtereken); kormányzati szervek által birtokolt vagy ellenőrzött informatikai rendszerek; és olyan központi rendszerek, amelyeket nem a szervezet birtokol, üzemeltet, vagy nincsenek a szervezet közvetlen irányítása alatt.

Jogosult felhasználó lehet valaki a szervezet állományából, egy szerződött fél vagy bárki, aki jogosult a szervezeti informatikai rendszerhez való hozzáférésre. Ez az intézkedés nem vonatkozik a külső informatikai rendszerek szervezeti rendszerhez való hozzáférésre történő felhasználására és a nyilvános hozzáférésre szánt információkra (pl. információ elérésére a szervezeti informatikai rendszer nyilvános kapcsolódási pontjain keresztül). A szervezet meghatározza a feltételeket és szabályokat a külső informatikai rendszer használatához összhangban a szervezeti biztonsági szabályzattal és eljárásrenddel.

A feltételeknek és szabályoknak szabályoznia kell a következőket:
- a külső informatikai rendszereken keresztül elérhető alkalmazások a szervezet informatikai rendszerében
- a maximális biztonsági kategóriája a külső informatikai rendszeren feldolgozható, tárolható és átküldhető információknak.

9.2.5. Naplózás és elszámoltathatóság (NA)

9.2.5.1. NA-1 Naplózási és elszámoltathatósági szabályzat és eljárásrend

Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált naplózási szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a naplózási szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

Intézkedés kiegészítése: A naplózási és elszámoltathatósági szabályzat és eljárásrend összhangban van a hatályos törvényekkel, vezetői döntésekkel, direktívákkal, szabályzatokkal, előírásokkal, szabványokkal és útmutatókkal. A naplózási és elszámoltathatósági szabályzat és eljárásrend részét képezheti a szervezet általános informatikai szabályzatának. A naplózási és elszámoltathatósági szabályzat és eljárásrendet ki lehet alakítani általánosan és egy meghatározott informatikai rendszerhez is, ha ez szükséges. További információk a 10.2 fejezetben illetve a NIST SP 800-92 [23] dokumentumban található.

9.2.5.2. NA-2 Naplózandó események

Intézkedés: Az informatikai rendszer naplóbejegyzéseket állít elő a következő eseményekre: [értékadás: a szervezet által meghatározott naplózandó események].

Intézkedés bővítése:
a) Az informatikai rendszer biztosítja annak lehetőségét, hogy több különböző összetevőből származó naplóbejegyzésből össze lehessen állítani egy rendszerszintű (logikai vagy fizikai), időalapú naplót.
b) Az informatikai rendszer biztosítja annak a lehetőségét, hogy felügyelhető legyen, hogy események melyik csoportját a rendszer melyik különálló összetevője naplózza.

c) A szervezet időnként felülvizsgálja és frissíti a szervezet által naplózandó események listáját.

Intézkedés kiegészítése: Az intézkedésnek az a célja, hogy azonosítsa azokat a fontos eseményeket, amelyeket az informatikai rendszer kiemelten fontos és biztonságilag szempontból releváns eseményeiként naplózni kell. A szervezet meghatározza, hogy az informatikai rendszer mely összetevői végezzenek naplózási tevékenységet. Figyelembe kell venni, hogy a naplózási tevékenységek befolyásolhatják a rendszer teljesítményét. A kockázatfelmérések alapján a szervezet eldönti, melyek azok az események, amiket folyamatosan naplózni kell, és mely eseményeket kell csak bizonyos helyzetekben naplózni. A naplóbejegyzések az absztrakció különböző szintjein keletkezhetnek, beleértve a hálózaton keresztül közlekedő csomagok szintjét is. Az absztrakció szintjének megfelelő kiválasztása a naplózás kritikus kérdése, és különösen lényeges a problémák gyökerének megtalálásához. A biztonsági naplózás funkcióját össze kell hangolni a hálózati működés és állapotmonitorozási funkciókkal, javítva a kölcsönös együttműködést a kettő között, kiválasztva minden funkcióhoz a naplózandó információkat. A szervezet meghatározza azokat a naplózandó eseményeket, amelyek alkalmasak a biztonsági problémák utólagos kivizsgálására.

9.2.5.3. NA-3 A naplóbejegyzések tartalma

Intézkedés: Az informatikai rendszer a naplóbejegyzésekben elegendő információt gyűjt be ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

Intézkedés bővítése:

a) Az informatikai rendszer lehetőséget nyújt arra, hogy a fentieken túl, részletesebb információkat is be lehessen venni, a naplóbejegyzések típusa, elhelyezkedése vagy tárgya alapján.
b) Az informatikai rendszer biztosítja a lehetőséget, hogy központilag lehessen felügyelni a különálló összetevők által készített naplóbejegyzések tartalmát.

Intézkedés kiegészítése: A naplóbejegyzések tartalma a legtöbb bejegyzés esetén tartalmazza:

- az esemény dátumát és időpontját;
- a rendszer megfelelő összetevőjét (pl. szoftver összetevő, hardver összetevő) az esemény keletkezésének helyét;
- az esemény típusát;
- a felhasználó azonosítóját; és
- az esemény kimenetelét (siker vagy hiba).

9.2.5.4. NA-4 Napló tárkapacitás

Intézkedés: A szervezet a naplózásra elegendő méretű tárkapacitást jelöl ki, illetve úgy konfigurálja a naplózást, hogy megelőzze az adott tárkapacitás betelését.

Intézkedés kiegészítése: A szervezet megfelelő mennyiségű tárhelyet biztosít a naplóeseményeknek, számításba véve az elvégzendő naplózást és az azonnali naplózás követelményeit. Kapcsolódó biztonsági intézkedések: NA-2, NA-5, NA-6, NA-7, RS-2.

9.2.5.5. NA-5 Naplózási hiba kezelése

Intézkedés: Naplózási hiba esetén, vagy ha a naplózás tárkapacitás beteléshez közelít, az informatikai rendszer riasztást küld az adminisztrátornak, valamint a következő tevékenységeket is elvégzi: [értékadás: szervezet által meghatározott végrehajtandó tevékenységek (pl. az informatikai rendszer leállítása, a legrégebbi naplóbejegyzések felülírása, a naplózási folyamat leállítása)].

Intézkedés bővítése:

a) Az informatikai rendszer figyelmeztet, ha a lefoglalt naplózási tárhely eléri [értékadás: szervezet által meghatározott százalék a maximális naplózási tárhely arányában].
b) Az informatikai rendszer valósidejű riasztást küld, ha a következő hibaesemények bekövetkeznek: [értékadás: szervezet által definiált hibaesemények listája, amelyek valós idejű riasztást igényelnek].

Intézkedés kiegészítése: A naplófeldolgozás hibái lehetnek például szoftver/hardver hibák, hibák a naplórögzítési mechanizmusban, a naplózási tárhely kapacitásának túllépése. Kapcsolódó biztonsági intézkedések: NA-4.

9.2.5.6. NA-6 Napló figyelése, vizsgálata és jelentések készítése

Intézkedés: A szervezet rendszeresen áttekinti/átvizsgálja a naplóbejegyzéseket, nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, elemzi a gyanús tevékenységeket és a feltételezett megsértéseket, jelenti ezeket a megfelelő tisztviselőknek, illetve megteszi a szükséges intézkedéseket.

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének integrálására egy átfogó folyamattá, amely választ ad a gyanús tevékenységek ellen.
b) A szervezet automatikus mechanizmusokat használ a biztonsági személyzet riasztására a következő gyanús vagy szokatlan események esetén: [értékadás: a szervezet által meghatározott lista a gyanús vagy szokatlan eseményekről, amelyek esetén riasztás szükséges].

Intézkedés kiegészítése: A szervezet megnöveli a naplózás és naplóelemzés szintjét, ha olyan magasabb kockázat merül fel a szervezeti műveletekkel, a szervezeti vagyonnal vagy a szervezet tagjaival kapcsolatban, amiről a szervezet rendőrségi forrásból, hírszerzési forrásból, vagy más megbízható forrásból értesül.

9.2.5.7. NA-7 Naplócsökkentés, naplóriport készítés

Intézkedés: Az informatikai rendszer lehetőséget biztosít naplócsökkentésre és naplóriport készítésére.

Intézkedés bővítése:

a) Az informatikai rendszer biztosítja, hogy automatikusan fel lehessen dolgozni az érdekes naplóbejegyzéseket egy kiválasztható, feltétel alapú rendszer alapján.

Intézkedés kiegészítése: A naplószűrő, elemző és jelentő eszközök támogatják az eset megtörténte után az eset kivizsgálását az eredeti naplóbejegyzések megváltoztatása nélkül.

9.2.5.8. NA-8 Időbélyegek

Intézkedés: Az informatikai rendszer időbélyegeket biztosít a naplóbejegyzések előállításához.

Intézkedés bővítése:

a) A szervezet szinkronizálja a belső rendszer órákat a következő frekvencián [értékadás: szervezet által meghatározott frekvencia].

Intézkedés kiegészítése: A naplóbejegyzésekhez a belső rendszeróra alapján időbélyeg, azaz megbízható időjelzés készül (dátum és időpont).

9.2.5.9. NA-9 A napló információk védelme

Intézkedés: Az informatikai rendszer megvédi a napló információt és a naplózás eszközeit a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

Intézkedés bővítése:

a) Az informatikai rendszer a naplóbejegyzéseket hardver által védett, egyszer írható eszközre írja.

Intézkedés kiegészítése: A naplózási információk tartalmaznak mindent (pl. naplóbejegyzések, naplózási beállítások és naplózási jelentések), ami szükséges az informatikai rendszer tevékenységeinek sikeres naplózásához.

9.2.5.10. NA-10 Letagadhatatlanság

Intézkedés: Az informatikai rendszer lehetőséget biztosít annak meghatározására, hogy egy adott személy elvégzett-e egy meghatározott tevékenységet.

Intézkedés kiegészítése: Az adott személy által elvégzett tevékenység lehet információ létrehozása, üzenet küldése, információ jóváhagyása (pl. egyidejűség jelzése vagy szerződés aláírása) és üzenet fogadása. A letagadhatatlanság védelmet nyújt a későbbi állítások ellen, hogy az adott személy mégsem végezte el a meghatározott tevékenységet. A letagadhatatlanság védelmet nyújt a személynek a vádak ellen, hogy nem ő írt egy bizonyos dokumentumot, nem ő küldött el egy bizonyos üzenetet, nem ő fogadott egy üzenetet vagy nem ő írt alá egy dokumentumot. A letagadhatatlanság szolgáltatásainak segítségével megállapítható hogy az információ egy adott személytől származik-e, hogy egy személy elvégzett-e bizonyos tevékenységeket (pl. levél küldése, szerződés aláírása, beszerzés

jóváhagyása), vagy megkapott-e bizonyos információkat. A letagadhatatlanság szolgáltatásait számos technika és mechanizmus segítségével meg lehet valósítani (pl. digitális aláírás, digitális átvételi elismervény, időbélyeg).

9.2.5.11. NA-11 A naplóbejegyzések megőrzése

Intézkedés: A szervezet a naplóbejegyzéseket megőrzi [értékadás: a szervezet által meghatározott időtartam]-ig abból a célból, hogy támogatást nyújtson a rendkívüli események utólagos kivizsgálására, és hogy megfeleljen a jogszabályi és szervezeti információ megőrzési követelményeknek.

Intézkedés kiegészítése: A szervezet megőrzi a naplóbejegyzéseket addig, amíg azok szükségesek lehetnek adminisztratív, jogi, auditálási vagy más működési célra. A naplóbejegyzések csoportjait kell kialakítani a hozzájuk tartozó tevékenységek típusaival, és az ezekre a típusú tevékenységekre adott válasszal.

9.2.6. Rendszer és kommunikáció védelem (RV)

9.2.6.1. RV-1 Rendszer és kommunikáció védelmi szabályzat és eljárásrend

Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált, rendszer és kommunikáció védelmi szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és kommunikáció védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

Intézkedés kiegészítése: A rendszer és kommunikáció védelmi szabályzat és eljárásrend összhangban van a hatályos törvényekkel, vezetői döntésekkel, direktívákkal, szabályzatokkal, rendelkezésekkel, szabványokkal és útmutatókkal. A rendszer és kommunikáció védelmi szabályzat részét képezheti a szervezet általános informatikai biztonsági szabályzatának. A rendszer és kommunikáció védelmi eljárásrendet ki lehet fejleszteni általánosan, és egy bizonyos informatikai rendszerhez is, ha szükséges.

9.2.6.2. RV-2 Alkalmazás szétválasztás

Intézkedés: Az informatikai rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az informatikai rendszer menedzsment funkcionalitásától.

Intézkedés kiegészítése: A rendszer fizikailag és logikailag is elkülöníti a felhasználói felület szolgáltatásait (pl. nyilvános weblapok) az információt tároló és kezelő szolgáltatásoktól (pl. adatbázis kezelés) Az elválasztás megvalósítható különböző számítógépekkel, különböző CPU-val, operációs rendszerek különböző példányaival, különböző hálózati címekkel, ezek kombinációjával vagy akár egyéb módszerekkel is.

9.2.6.3. RV-3 Biztonsági funkciók elkülönítése

Intézkedés: A rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.

Intézkedés bővítése:

a) A rendszer a hardver szétválasztását használja a biztonsági funkciók elkülönítéséhez.
b) A rendszer elkülöníti a kritikus funkciókat (vagyis a hozzáférést kikényszerítő és információáramlást vezérlő funkciókat) mind a nem biztonsági funkcióktól, mind a többi biztonsági funkciótól.
c) A rendszer a lehető legkevesebb nem biztonsági funkciót hagyja a biztonsági funkciókat elkülönítő határon belül.
d) A rendszer biztonsági funkciói független modulokként vannak megvalósítva, elkerülve a felesleges együttműködést a modulok közt.
e) A rendszer biztonsági funkciói réteges struktúraként vannak megvalósítva, minimalizálva az együttműködést a rétegek közt, és elkerülve az alsóbb rétegek függőségét a felsőbb rétegek funkcionalitásától.

Intézkedés kiegészítése: A rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól partíciók, tartományok, stb. segítségével, beleértve a hozzáférés és integritás védelmét a biztonsági funkciókat végző hardver, szoftver és förmver elemeknek. A rendszer külön végrehajtási tartományt használ (pl. külön címtartomány) minden egyes végrehajtott folyamathoz.

9.2.6.4. RV-4 Információ maradványok

Intézkedés: Az informatikai rendszer meggátolja a megosztott rendszer erőforrások útján történő jogosulatlan és véletlen információáramlást.

Intézkedés kiegészítése: Az információ maradványokkal kapcsolatos intézkedések, amit adat újrahasznosításnak vagy adatmaradékoknak is hívnak, meggátolják, hogy az információhoz, beleértve annak rejtjelzett formáját is, egy régi felhasználó/szerep tevékenységének köszönhetően (vagy egy felhasználó/szerep nevében futó folyamat jóvoltából), bármilyen aktuális felhasználó/szerep (vagy folyamat) hozzáférhessen, még ha a megosztott erőforrásokhoz hozzáférést is szerez (pl. regiszterek, memória, másodlagos tár), miután az erőforrás visszakerül az informatikai rendszerbe.

9.2.6.5. RV-5 Szolgáltatás megtagadás elleni védelem

Intézkedés: Az informatikai rendszer védelmet nyújt a következő típusú szolgáltatás megtagadás jellegű támadásokkal szemben vagy korlátozza azok kihatásait: [értékadás: szolgáltatás megtagadás jellegű támadástípusok szervezet által meghatározott listája vagy egy elfogadott listára való hivatkozás].

Intézkedés bővítése:

a) A rendszer korlátozza a felhasználókat, hogy ne indíthassanak szolgáltatás megtagadása támadásokat más rendszerek vagy hálózatok ellen.

b) A rendszer kezeli a tartalék kapacitást, sávszélességet és más egyéb tartalék erőforrásokat is, hogy csökkentse az információ elárasztáson alapuló szolgáltatás megtagadása támadások hatását.

Intézkedés kiegészítése: Sokféle technológia létezik, amivel csökkenteni lehet, vagy bizonyos esetekben teljesen ki lehet védeni a szolgáltatás megtagadása típusú támadásokat. Például a határok védelmére szolgáló eszközök kiszűrhetik csomagok bizonyos típusait és megvédhetik a szervezet belső hálózatán található eszközöket a szolgáltatás megtagadása típusú támadás hatásaitól. A nyilvánosan elérhető rendszerek a kapacitás és a sávszélesség növelésével illetve a tartalék erőforrások kezelésével védhetőek.

9.2.6.6. RV-6 Erőforrás prioritás

Intézkedés: Az informatikai rendszer az erőforrások használatát prioritások szerint korlátozza.

Intézkedés kiegészítése: A prioritások védelme segít az alacsony prioritású folyamatoknak, hogy ne késleltessék vagy zavarják a magas prioritású folyamatok kiszolgáltatását.

9.2.6.7. RV-7 A határok védelme

Intézkedés: Az informatikai rendszer figyeli és ellenőrzi az informatikai rendszer külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációkat.

Intézkedés bővítése:

a) A szervezet a nyilvánosan hozzáférhető informatikai rendszer összetevőket (pl. nyilvános web szervereket) elkülönített alhálózatokban helyezi el, elkülönített fizikai hálózati interfészekkel.
   Megjegyzés: Nyilvánosan hozzáférhető informatikai rendszer összetevő lehet például a web szerver.
b) A szervezet meggátolja a nyilvános hozzáférést a szervezet belső hálózatához, kivéve azon eseteket, amikor a hozzáférés megfelelő védelmi intézkedések közbeiktatásával történik.
c) A szervezet korlátozza a hozzáférési pontok számát az informatikai rendszerhez, hogy jobban monitorozható legyen a kijövő és bejövő hálózati forgalom.
d) A szervezet kialakít egy felügyelt kapcsolódási pontot (határvédelmi eszközöket egy hatékony biztonsági architektúrában) a külső telekommunikációs szolgáltatóval, létrehozva azokat az intézkedéseket, amelyek szükségesek az átvitt információ bizalmasságának és integritásának védelméhez.
e) Az informatikai rendszer alapból tilt és kivételként engedélyez csak minden hálózati forgalmat (vagyis minden tiltva, engedélyezés kivételes esetben).
f) A szervezet megakadályozza az információ jogosulatlan átjuttatását a rendszer határain, vagy bármilyen jogosulatlan kommunikációt a határon keresztül, ha valami hiba történik a határvédelmi mechanizmusokban.

Intézkedés kiegészítése: Bármilyen kapcsolat az Internethez, más külső hálózathoz vagy informatikai rendszerhez, csak a felügyelt kapcsolódási pontokon keresztül történhet,

amelyeket megfelelő határvédelmi eszközök védenek (pl. proxy, átjáró, router, tűzfal, rejtjelzett csatorna) hatásos architektúrába szervezve (pl. routerek védik a tűzfalakat és az átjárók egy védett alhálózatban vannak, amit sokszor demilitarizált zónának vagy DMZ-nek is neveznek). Az informatikai rendszer határainak védelme egy kijelölt másodlagos telephelyen ugyanolyan szintű kell, hogy legyen, mint az elsődleges telephelyen.

A mélységi védekezés stratégiájának részeként a szervezet a különösen fontos informatikai rendszereit különböző fizikai tartományokra osztja (vagy környezetekre), és a fent leírt felügyelt kapcsolódási pont módszerével korlátozza vagy megtiltja a hálózati hozzáférést a szervezeti kockázatfelméréssel összhangban.

A szervezet gondosan figyelembe veszi a kereskedelmi telekommunikációs szolgáltatások tulajdonságait, például hogy ezeket a szolgáltatásokat csak másokkal megosztva lehet csak használni. A kereskedelmi telekommunikációs szolgáltatások általában olyan hálózati komponensekből és felügyeleti rendszerekből állnak, amit az összes csatlakozott felhasználó megosztva használ, és külső fél által felügyelt vonalakat és más egyéb szolgáltatási elemeket használhatnak. Ennek következtében, ezek az átviteli szolgáltatások magasabb kockázat forrásai lehetnek a szerződésben vállalt biztonsági intézkedések ellenére. Ezért ha ez a helyzet áll elő, a szervezetnek megfelelő kompenzációs biztonsági intézkedéseket kell hoznia, vagy el kell vállalnia a magasabb kockázatot.

9.2.6.8. RV-8 Az adatátvitel sértetlensége

Intézkedés: Az informatikai rendszer megvédi a továbbított információk sértetlenségét.

Intézkedés bővítése:

a) A szervezet kriptográfiai mechanizmusokat alkalmaz, hogy biztosítsa az információk adatátvitel közbeni megváltozásának felismerését, hacsak az átvitel nincsen más alternatív fizikai ellenintézkedésekkel védve. Megjegyzés: Az alternatív fizikai védelmi intézkedés lehet például egy védett elosztó rendszer.

Intézkedés kiegészítése: Ha a szervezet egy kereskedelmi szolgáltató átviteli szolgáltatásait termékként használja, nem egy teljesen rá szabott szolgáltatásként, nehéz lehet megszerezni a szükséges garanciát, hogy az adatátvitel integritásához szükséges intézkedések működnek. Ha nem kifizetődő vagy nem praktikus szerződésen keresztül biztosítani a szükséges biztonsági intézkedéseket és garanciát ezek hatékony működésére, a szervezetnek megfelelő kompenzációs biztonsági intézkedéseket kell hoznia, vagy el kell vállalnia a magasabb kockázatot.

9.2.6.9. RV-9 Az adatátvitel bizalmassága

Intézkedés: Az informatikai rendszer megvédi az átvitt információk bizalmasságát.

Intézkedés bővítése:

a) A szervezet kriptográfiai mechanizmusokat alkalmaz, hogy meggátolja az információk adatátvitel közbeni jogosulatlan felfedését, hacsak az átvitel nincsen

más alternatív fizikai ellenintézkedésekkel védve.
Megjegyzés: Az alternatív fizikai védelmi intézkedés lehet például egy védett elosztó rendszer.

Intézkedés kiegészítése: Ha a szervezet egy kereskedelmi szolgáltató átviteli szolgáltatásait termékként használja, nem egy teljesen rá szabott szolgáltatásként, nehéz lehet megszerezni a szükséges garanciát, hogy az átvitt információ bizalmassága nem sérül. Ha nem kifizetődő vagy nem praktikus szerződésen keresztül biztosítani a szükséges biztonsági intézkedéseket és garanciát ezek hatékony működésére, a szervezetnek megfelelő kompenzációs biztonsági intézkedéseket kell hoznia, vagy el kell vállalnia a magasabb kockázatot. Kapcsoló biztonsági intézkedés: HE-17. A virtuális magánhálózatokról és az IPSEC-ről a NIST SP 800-77 [21] dokumentumban a Transport Layer Security (TLS) használatáról a NIST SP 800-52 [17] dokumentumban további információ található.

9.2.6.10. RV-10 A hálózati kapcsolat megszakítása

Intézkedés: Az informatikai rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, vagy [értékadás: a szervezet által meghatározott időtartam] hosszú inaktivitás után.

Intézkedés kiegészítése: A szervezet ezt az intézkedést egy olyan kockázat kezelés keretében használja, amely a különleges feladatokat és működési követelményeket is figyelembe veszi.

9.2.6.11. RV-11 Megbízható útvonal

Intézkedés: Az informatikai rendszer egy megbízható kommunikációs útvonalat biztosít a felhasználó és a rendszer következő biztonsági funkciói között: [értékadás: szervezet által meghatározott minimálisan meghatározandó biztonsági funkciók, az informatikai rendszer hitelesítése és újrahitelesítése].

Intézkedés kiegészítése: A megbízható útvonalat a magas biztonsági szintű felhasználó és a rendszer biztonsági funkciói közti kapcsolatok esetében szokták használni (pl. bejelentkezés).

9.2.6.12. RV-12 Kriptográfiai kulcs előállítása és kezelése

Intézkedés: Az informatikai rendszer a kriptográfiai kulcsok előállítására és kezelésére automatikus támogató eljárásokkal ellátott mechanizmusokat, vagy manuális eljárásokat alkalmaz.

Intézkedés kiegészítése: A kriptográfiai kulcs kialakításról a NIST SP 800-56 [18], a kriptográfiai kulcs kezelésről a NIST SP 800-57 [19] dokumentumok adnak bővebb információt.

9.2.6.13. RV-13 Jóváhagyott kriptográfia alkalmazása

Intézkedés: Ha az informatikai rendszerben kriptográfiát alkalmaznak, a rendszer minden kriptográfiai műveletét (beleértve a kulcs előállítását is) azt szabványos algoritmussal kell megvalósítani.

Intézkedés kiegészítése: Az általánosan elfogadott szabvány a kriptográfia használatára az informatikai rendszerekben a FIPS 140-2 [12]. A NIST Kriptográfiai Modul hitelesítő Program által kiállított korábbi hitelesítő tanúsítványok érvényesek maradnak a használatra és megvételre addig, amíg a hitelesítési tanúsítványokat vissza nem vonják. Elfogatható továbbá hazai akkreditált vizsgálólaboratórium által végzett megfelelőség vizsgálat alapján kiállított tanúsító igazolás.

9.2.6.14. RV-14 Sértetlenség védelem nyilvános hozzáférés esetén

Intézkedés: A nyilvánosan elérhető rendszerek esetén az informatikai rendszer megvédi az információk és az alkalmazások sértetlenségét.

9.2.6.15. RV-15 Telekommunikációs szolgáltatások korlátozása

Intézkedés: Az informatikai rendszer meggátolja a telekommunikációs szolgáltatások együttműködő számítógép-használati mechanizmusainak (pl. video és audio konferenciák) távolról történő aktiválását, és közvetlen jelzéseket biztosít az ilyen mechanizmusok használatról a lokális felhasználók felé (pl. kamera vagy mikrofon használata).

Intézkedés bővítése:

a) Az informatikai rendszer lehetővé teszi a kamera és a mikrofon fizikai leválasztását a használat egyszerűsége érdekében.

Intézkedés kiegészítése: Az együttműködő számítógép-használati mechanizmusok lehetnek például hang és videó konferencia képességek. A közvetlen jelzések lehetnek például jelzések a helyi felhasználónak, ha a kamerát és/vagy a mikrofonokat aktiválták.

9.2.6.16. RV-16 Biztonsági paraméterek továbbítása

Intézkedés: Az informatikai rendszer megbízhatóan hozzárendeli a biztonsági paramétereket az informatikai rendszerek közt átvitt információkhoz.

Intézkedés kiegészítése: A biztonsági paraméterek lehetnek például biztonsági címkék vagy jelölések. A biztonsági paraméterek közvetlenül vagy közvetetten hozzá vannak rendelve az informatikai rendszerben található információkhoz.

9.2.6.17. RV-17 Nyilvános kulcsú infrastruktúra tanúsítványok

Intézkedés: Megfelelő hitelesítési rend szerint a szervezet vagy önmaga kiállít nyílt kulcsú tanúsítványt a vagy vásárol nyílt kulcsú tanúsítványt egy hitelesítés-szolgáltatótól.

Intézkedés kiegészítése: A szervezet minősített elektronikus aláírás tanúsítványok esetén, KGYHSZ által felültanúsított hitelesítés-szolgáltatótól vásárol tanúsítványt. A nyilvános kulcsú infrastruktúráról további információ található a NIST SP 800-32 [14] dokumentumban.

9.2.6.18. RV-18 Mobil kód korlátozása

Intézkedés: A szervezet
- korlátozza a mobil kód technika alkalmazhatóságát, erre vonatkozó útmutatót bocsát ki, a mobil kódok rosszindulatú használata által okozott potenciális károk miatt, valamint
- dokumentálja, figyeli és ellenőrzi a mobil kódok információs rendszeren belüli felhasználását. Megfelelő vezető engedélyezi a mobil kódok használatát.

Intézkedés kiegészítése: A mobil kód technikák lehetnek például JavaScript, ActiveX, PDF, Postscript, Shockwave filmek, Flash animációk, és VBScript. A használat korlátozása és a megvalósítási útmutató vonatkozik a szervereken telepített mobil kód és a letöltött és a munkaállomásokon futtatható mobil kódok kiválasztására és használatára. Az intézkedés eljárásrendje megakadályozza a nemkívánatos mobil kód fejlesztését, megszerzését és bevezetését az informatikai rendszeren belül. Az aktív tartalmakról és mobil kódokról további információ található a NIST SP 800-28 [13] dokumentumban.

9.2.6.19. RV-19 Interneten Keresztüli Hangátvitel (VoIP)

Intézkedés: A szervezet:
- használati korlátozásokat vezet be és megvalósítási útmutatót ad az Interneten Keresztüli Hangátvitel (VoIP) technológiákhoz, a rosszindulatú használat esetén okozható károkat felmérve; és
- engedélyezi, figyeli, és ellenőrzi a VoIP használatát az informatikai rendszeren belül.

Intézkedés kiegészítése: Az Interneten Keresztüli Hangátvitel (VoIP) biztonsági vonatkozásairól a NIST SP 800-58 [20] dokumentum ad bővebb információt.

9.2.6.20. RV-20 Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)

Intézkedés: Az informatikai rendszer, amely a név/cím feloldó szolgáltatást biztosítja, a hiteles adatokon kívül egyéb biztonsági adatokat is visszaad a feloldási kérésekre, mint például az információ eredete és integritási adatok.

Intézkedés bővítése:

a) Ha az informatikai rendszer egy elosztott, hierarchikus névtér részeként működik, akkor jeleznie kell a gyerektartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) tudnia kell hitelesíteni a bizalmi láncot a gyerek és szülő tartományok közt.

Intézkedés kiegészítése: Ez az intézkedés biztosítja a klienseknek, hogy az eredet hitelességéről és az integritás ellenőrzéséhez is kapjanak információt a szolgáltatáson keresztül a név/cím feloldó információk mellett. A DNS szerver egy példa olyan informatikai rendszerre, amelyik név/cím feloldó szolgáltatást nyújt, a digitális aláírások és kriptográfiai kulcsok lehetnek a biztonsági információk és a DNS erőforrás rekordok pedig példák a hiteles adatra. További információ található a NIST SP 800-81 [22] dokumentumban.

9.2.6.21. RV-21 Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)

Intézkedés: Az informatikai rendszer, amely a név/cím feloldó szolgáltatást biztosítja a helyi klienseknek eredet hitelesítést és adatintegritás ellenőrzést végez a hiteles forrásból származó válaszok esetén, ha a kliensek ezt igénylik.

Intézkedés bővítése:

a) Az informatikai rendszer az adatokon eredet hitelesítést és integritás vizsgálatot végez minden feloldott válasz esetén attól függetlenül, hogy a helyi kliens ezt kéri-e vagy sem.

Intézkedés kiegészítése: Egy feloldó vagy gyorsítótárat használó DNS szerver példa lehet egy helyi klienseket kiszolgáló név/cím feloldó szolgáltatásra és a felelős DNS szerverek pedig példák a hiteles forrásra.

9.2.6.22. RV-22 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

Intézkedés: Egy olyan informatikai rendszernek, amely az egész szervezet név/cím feloldását szolgálja ki, hibatűrőnek kell lennie, és működnie kell rajta a szerepkörök szétválasztásának.

Intézkedés kiegészítése: Egy DNS szerver példa lehet olyan informatikai rendszerre, ami név/cím feloldást szolgáltat. A hibák megakadályozására és a redundancia javítására általában két felelős DNS szervert szoktak üzemeltetni, egyiket elsődlegesnek konfigurálva a másikat pedig másodlagosnak. Ezen kívül a két szerver általában két külön alhálózatban található, és fizikailag is különböző helyeken vannak (vagyis nem ugyanabban a létesítményben találhatóak). Ha a szervezet informatikai erőforrásai szét vannak választva azokra az erőforrásokra, amelyek a belső hálózatban találhatóak, és azokra, amelyek a külső hálózatban, mindkét szerephez (külső és belső) kell rendelni felelős DNS kiszolgálót. A belső szerephez tartozó DNS kiszolgáló név/cím feloldást kell, hogy nyújtson mind a belső, mind a külső hálózathoz tartozó erőforrásokról, míg a külső szerephez tartozó DNS kiszolgálónak csak a külső hálózathoz tartozó erőforrásokhoz kell szolgáltatást nyújtani. Meg kell határozni azoknak a klienseknek a listáját, amelyek hozzáférhetnek valamelyik szerephez tartozó felelős DNS kiszolgálóhoz.

9.2.6.23. RV-23 Munkaszakasz hitelessége

Intézkedés: Az informatikai rendszer valamilyen mechanizmussal biztosítja a munkaszakaszok hitelességének védelmét.

Intézkedés kiegészítése: Ez az intézkedés a munkaszakasz kommunikációjának védelmére összpontosít, nem a csomagok szintjére. Az intézkedés célja az, hogy munkaszakasz szintű védelmet nyújtson, ha szükséges (pl. szolgáltatás orientált architektúrák esetén web alapú szolgáltatások nyújtása közben). A web szolgáltatások biztonságával, így a hitelességgel, kapcsolatban tartalmaz tovább információkat a NIST SP 800-95 [24]dokumentum.

9.3. Az alacsony, fokozott és kiemelt kihatású biztonsági osztályok minimálisan kielégítendő követelményei

Az alábbi táblázat a különböző biztonsági intézkedések egymásra épülő alkalmazását a három biztonsági osztályban.

	Biztonsági intézkedés neve	**Alacsony**	**Fokozott**	**Kiemelt**
		biztonsági osztály alapkonfigurációja		
Konfiguráció kezelés				
KK-1	Konfiguráció kezelési szabályzat és eljárásrend	KK-1	KK-1	KK-1
KK-2	Alap konfiguráció	KK-2	KK-2 (a)	KK-2 (a) (b)
KK-3	Konfigurációváltozások	--	KK-3	KK-3
KK-4	A konfigurációváltozások felügyelete	--	KK-4	KK-4
KK-5	A változtatásokra vonatkozó hozzáférés korlátozások	--	KK-5	KK-5 (a)
KK-6	Konfigurációs beállítások	KK-6	KK-6	KK-6 (a)
KK-7	Legszűkebb funkcionalitás	--	KK-7	KK-7 (a)
KK-8	Informatikai rendszer komponens leltár	KK-8	KK-8(a)	KK-8 (a) (b)
Rendszer és információ sértetlenség				
RS-1	Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend	RS-1	RS-1	RS-1
RS-2	Hibajavítás	RS-2	RS-2 (b)	RS-2(a) (b)
RS-3	Rosszindulatú kódok elleni védelem	RS-3	RS-3 (a) (b)	RS-3 (a) (b)
RS-4	Behatolás észlelési eszközök és technikák	--	RS-4 (d)	RS-4 (b) (d) (e)
RS-5	Biztonsági riasztások és tájékoztatások	RS-5	RS-5	RS-5 (a)
RS-6	A biztonsági funkcionalitás ellenőrzése	--	--	RS-6
RS-7	Szoftver és információ sértetlenség	--	--	RS-7 (a) (b)
RS-8	Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem	--	RS-8	RS-8 (a)
RS-9	A bemeneti információra vonatkozó korlátozások	--	RS-9	RS-9
RS-10	A bemeneti információ pontossága, teljessége és érvényessége	--	RS-10	RS-10
RS-11	Hibakezelés	--	RS-11	RS-11
RS-12	A kimeneti információ kezelése és megőrzése	--	RS-12	RS-12

	Biztonsági intézkedés neve	**Alacsony**	**Fokozott**	**Kiemelt**
		biztonsági osztály alapkonfigurációja		
Azonosítás és hitelesítés				
AH-1	Azonosítási és hitelesítési szabályzat és eljárásrend	AH-1	AH-1	AH-1
AH-2	Felhasználó azonosítása és hitelesítése	AH-2	AH-2 (a)	AH-2 (b) (c)
AH-3	Eszközök azonosítása és hitelesítése	--	AH-3	AH-3
AH-4	Azonosító kezelés	AH-4	AH-4	AH-4
AH-5	A hitelesítésre szolgáló eszközök kezelése	AH-5	AH-5	AH-5
AH-6	A hitelesítésre szolgáló eszköz visszacsatolása	AH-6	AH-6	AH-6
AH-7	Hitelesítés kriptográfiai modul esetén	AH-7	AH-7	AH-7
Hozzáférés ellenőrzése				
HE-1	Hozzáférés ellenőrzési szabályzat és eljárásrend	HE-1	HE-1	HE-1
HE-2	Felhasználói fiókok kezelése	HE-2	HE-2 (a) (b) (c) (d)	HE-2 (a) (b) (c) (d)
HE-3	Hozzáférés ellenőrzés érvényre juttatása	HE-3	HE-3(a)	HE-3 (a)
HE-4	Információ áramlás ellenőrzés érvényre juttatása	--	HE-4	HE-4
HE-5	A felelősségek szétválasztása	--	HE-5	HE-5
HE-6	Legkisebb jogosultság	--	HE-6	HE-6
HE-7	Sikertelen bejelentkezési kísérletek	HE-7	HE-7	HE-7
HE-8	A rendszerhasználat jelzése	HE-8	HE-8	HE-8
HE-9	Értesítés előző bejelentkezésről	--	--	--
HE-10	Egyidejű munkaszakasz kezelés	--	--	HE-10
HE-11	A munkaszakasz zárolása	--	HE-11	HE-11
HE-12	A munkaszakasz lezárása	--	HE-12	HE-12(a)
HE-13	Felügyelet és felülvizsgálat — hozzáférés ellenőrzés	HE-13	HE-13(a)	HE-13(a)
HE-14	Azonosítás és hitelesítés nélkül engedélyezett tevékenységek	HE-14	HE-14(a)	HE-14(a)
HE-15	Automatikus jelölés	--	--	HE-15
HE-16	Automatikus címkézés	--	--	--
HE-17	Távoli hozzáférés ellenőrzése	HE-17	HE-17(a)(b) (c) (d)	HE-17(a)(b) (c) (d)
HE-18	A vezeték nélküli hozzáférésre vonatkozó korlátozások	HE-18	HE-18(a)	HE-18(a)(b)

	Biztonsági intézkedés neve	Alacsony	Fokozott	Kiemelt
		biztonsági osztály alapkonfigurációja		
HE-19	A hordozható és mobil eszközök hozzáférés ellenőrzése	--	HE-19	HE-19
HE-20	Külső informatikai rendszerek használata	HE-20	HE-20 (a)	HE-20 (a)
Naplózás és elszámoltathatóság				
NA-1	Naplózási és elszámoltathatósági szabályzat és eljárásrend	NA-1	NA-1	NA-1
NA-2	Naplózandó események	NA-2	NA-2 (c)	NA-2 (a) (b) (c)
NA-3	A naplóbejegyzések tartalma	NA-3	NA-3 (a)	NA-3 (a) (b)
NA-4	Napló tárkapacitás	NA-4	NA-4	NA-4
NA-5	Naplózási hiba kezelése	NA-5	NA-5	NA-5 (a) (b)
NA-6	Napló figyelése, vizsgálata és jelentések készítése	--	NA-6 (b)	NA-6 (a) (b)
NA-7	Naplócsökkentés, naplóriport készítés	--	NA-7(a)	NA-7(a)
NA-8	Időbélyegek	NA-8	NA-8(a)	NA-8(a)
NA-9	A napló információk védelme	NA-9	NA-9	NA-9
NA-10	Letagadhatatlanság	--	--	--
NA-11	A naplóbejegyzések megőrzése	NA-11	NA-11	NA-11
Rendszer és kommunikáció védelem				
RV-1	Rendszer és kommunikáció védelmi szabályzat és eljárásrend	RV-1	RV-1	RV-1
RV-2	Alkalmazás szétválasztás	--	RV-2	RV-2
RV-3	Biztonsági funkciók elkülönítése	--	--	RV-3
RV-4	Információ maradványok	--	RV-4	RV-4
RV-5	Szolgáltatás megtagadás elleni	RV-5	RV-5	RV-5
RV-6	Erőforrás prioritás	--	--	--
RV-7	A határok védelme	RV-7	RV-7 (a) (b) (c) (d) (e)	RV-7 (a) (b) (c) (d) (e) (f)
RV-8	Az adatátvitel sértetlensége	--	RV-8	RV-8(a)
RV-9	Az adatátvitel bizalmassága	--	RV-9	RV-9(a)
RV-10	A hálózati kapcsolat megszakítása	--	RV-10	RV-10
RV-11	Megbízható útvonal	--	--	--
RV-12	Kriptográfiai kulcs előállítása és kezelése	--	RV-12	RV-12
RV-13	Jóváhagyott kriptográfia alkalmazása	RV-13	RV-13	RV-13
RV-14	Sértetlenség védelem nyilvános hozzáférés esetén	RV-14	RV-14	RV-14

	Biztonsági intézkedés neve	**Alacsony**	**Fokozott**	**Kiemelt**
		biztonsági osztály alapkonfigurációja		
RV-15	Telekommunikációs szolgáltatások korlátozása	--	RV-15	RV-15
RV-16	Biztonsági paraméterek továbbítása	--	--	--
RV-17	Nyilvános kulcsú infrastruktúra tanúsítványok	--	RV-17	RV-17
RV-18	Mobil kód korlátozása	--	RV-18	RV-18
RV-19	Interneten Keresztüli Hangátvitel (VoIP)	--	RV-19	RV-19
RV-20	Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)	--	RV-20	RV-20
RV-21	Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)	--	--	RV-21
RV-22	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	--	RV-22	RV-22
RV-23	Munkaszakasz hitelessége	--	RV-23	RV-23

9.3.1. Az alacsony kihatású biztonsági osztály követelményei

9.3.1.1. Konfiguráció kezelés (KK)

KK-1 Konfiguráció kezelési szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált konfiguráció kezelési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a konfiguráció kezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

KK-2 Alap konfiguráció
Intézkedés: A szervezet informatikai célrendszeréhez egy alap konfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges komponenseit.

KK-6 Konfigurációs beállítások
Intézkedés: A szervezet
- kötelező konfigurációs beállítást határoz meg az informatikai rendszerben használt információ technológiai termékekre;
- az információ technológiai termékek lehető legkorlátozóbb biztonsági beállításait konfigurálja, amely még megfelel a működési követelményeknek;
- dokumentálja a konfigurációs beállításokat; és
- érvényre juttatja a konfigurációs beállításokat az informatikai rendszer valamennyi komponensében.

KK-8 Informatikai rendszer komponens leltár
Intézkedés: A szervezet aktuális leltárt készít, dokumentálja és karbantartja az informatikai rendszer komponenseit és a vonatkozó tulajdonosi információkat.

9.3.1.2. Rendszer és információ sértetlenség (RS)

RS-1 Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált, a rendszer és információ sértetlenségére vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és információ sértetlenségére vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

RS-2 Hibajavítás
Intézkedés: A szervezet az informatikai rendszerben talált hibákat jelenti, és kijavítja.

RS-3 Rosszindulatú kódok elleni védelem
Intézkedés: Az informatikai rendszer rosszindulatú kódok elleni védelmet valósít meg, s ez automatikus frissítési lehetőséget is magában foglal.

RS-5 Biztonsági riasztások és tájékoztatások
Intézkedés: A szervezet folyamatosan fogadja az informatikai rendszerre vonatkozó biztonsági riasztásokat és figyelmeztetéseket, eljuttatja ezeket az illetékes személyekhez, illetve megfelelő válaszlépéseket foganatosít.

9.3.1.3. Azonosítás és hitelesítés (AH)

AH-1 Azonosítási és hitelesítési szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt, rendszeresen felülvizsgál és frissít:
- egy formális, dokumentált, az azonosításra és hitelesítésre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés, menedzsment kötelezettségei, koordináció a szervezet egységei közt; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja az azonosításra és hitelesítésre vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

AH-2 Felhasználó azonosítása és hitelesítése
Intézkedés: Az informatikai rendszer egyedileg azonosítja és hitelesíti a felhasználókat (vagy a felhasználók nevében eljáró eljárásokat)

AH-3 Eszközök azonosítása és hitelesítése
Intézkedés: Az informatikai rendszer bizonyos eszközöket azonosít és hitelesít, mielőtt kapcsolatot létesítene velük.

AH-4 Azonosító kezelés
Intézkedés: A szervezet az alábbi módon kezeli a felhasználói azonosítókat:
- egyedileg azonosít minden felhasználót;
- ellenőrzi minden felhasználó azonosságát;
- egy új felhasználói azonosító kibocsátását adminisztrátori felhatalmazáshoz köti;
- garantálja, hogy a felhasználói azonosítót annak a félnek adták ki, akinek szánták;
- lezárja a felhasználói azonosítót egy, [értékadás: a szervezet által meghatározott időtartam]-ig tartó inaktivitás után, és
- archiválja a felhasználói azonosítókat.

AH-5 A hitelesítésre szolgáló eszközök kezelése
Intézkedés: A szervezet az alábbi módon kezeli a rendszer hitelesítésre szolgáló eszközeit:
- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
- adminisztratív eljárásokat vezet be a hitelesítésre szolgáló eszközök kezdeti szétosztására, az elvesztett/kompromittálódott vagy sérült eszközök esetére, illetve a hitelesítésre szolgáló eszközök visszavonására;
- az alapértelmezés szerinti hitelesítésre szolgáló eszközöket megváltoztatja az informatikai rendszer installálásának során; és
- időszakonként a hitelesítésre szolgáló eszközöket megváltoztatja/frissíti.

AH-6 A hitelesítésre szolgáló eszköz visszacsatolása
Intézkedés: Az informatikai rendszer visszacsatolást biztosít a felhasználónak hitelesítési kísérlete során, és ez a visszacsatolás nem veszélyezteti a hitelesítési mechanizmust. Az informatikai rendszer elrejti a hitelesítési információk visszacsatolását a hitelesítési kísérlet során, így védve az információt az esetleges kihasználástól/illetéktelen használattól.

AH-7 Hitelesítés kriptográfiai modul esetén
Intézkedés: Az informatikai rendszer olyan hitelesítési módszereket használ, amelyek megfelelnek a törvényeknek, vezetői döntéseknek, direktíváknak, szabályzatoknak, előírásoknak, szabványoknak, és a kriptográfiai modul hitelesítési útmutatójának.

9.3.1.4. Hozzáférés ellenőrzése (HE)

HE-1 Hozzáférés ellenőrzési szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált hozzáférés ellenőrzési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettséget, és megfelelést; a koordináció a szervezeti entitások között;
- egy formális, dokumentált hozzáférés védelemre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés, menedzsment kötelezettségei, koordináció a szervezet egységei közt; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a hozzáférés ellenőrzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

HE-2 Felhasználói fiókok kezelése
Intézkedés: A szervezet kezeli az informatikai rendszer felhasználói fiókjait, beleértve a felhasználói fiókok létrehozását, aktiválását, módosítását, felülvizsgálatát, letiltását és eltávolítását. A szervezet felülvizsgálja az informatikai rendszer felhasználói fiókjait [értékadás: a szervezet által meghatározott gyakoriság, de legalább évente].

HE-3 Hozzáférés ellenőrzés érvényre juttatása
Intézkedés: Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszerhez való hozzáférés ellenőrzéséhez.

HE-7 Sikertelen bejelentkezési kísérletek
Intézkedés: Az informatikai rendszer egy [értékadás: a szervezet által definiált szám]-ként megadott korlátot juttat érvényre egy felhasználó egymást követő bejelentkezési kísérleteire, amelyek egy [értékadás: a szervezet által definiált időtartam]-on belül történtek. Amennyiben a sikertelen kísérletek a maximális számot túllépik, az információs rendszer automatikusan [választás: zárolja a felhasználói fiókot/csomópontot] [értékadás: a szervezet által definiált időtartamig]; késlelteti a következő bejelentkezési kísérletet egy az [értékadás: szervezet által definiált késleltetési algoritmusnak megfelelően].

HE-8 A rendszerhasználat jelzése
Intézkedés: Az informatikai rendszer egy jóváhagyott, a rendszerhasználatra vonatkozó jelzést ad a rendszerhez való hozzáférés engedélyezése előtt abból a célból, hogy a potenciális felhasználókat tájékoztatassa arról:

— hogy a felhasználó egy magyar közigazgatási informatikai rendszert használ;
— hogy lehetséges, hogy a rendszer használatot figyelhetik, rögzíthetik, illetve auditálhatják;
— hogy a rendszer jogosulatlan használata tilos, és büntetőjogi, valamint polgárjogi felelősségre vonással jár;
— hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti a figyelésbe és rögzítésbe. A rendszer által használt közlemény biztosítja a magántitokra és biztonságra vonatkozó értesítéseket, és mindaddig a képernyőn marad, amíg a felhasználó közvetlen műveletet nem végez az informatikai rendszerbe való bejelentkezéshez.

HE-13 Felügyelet és felülvizsgálat — hozzáférés ellenőrzés
Intézkedés: A szervezet felügyeli és felülvizsgálja a felhasználók tevékenységét az informatikai rendszer hozzáférés ellenőrzése érvényre juttatása és használata tekintetében.

HE-14 Azonosítás és hitelesítés nélkül engedélyezett tevékenységek
Intézkedés: A szervezet meghatározza azokat a speciális felhasználói tevékenységeket, amelyeket az informatikai rendszerben azonosítás és hitelesítés nélkül is végre lehet hajtani.

HE-17 Távoli hozzáférés ellenőrzése
Intézkedés: A szervezet engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való távoli hozzáférés minden módszerét (pl. betárcsázás, Internet), beleértve a privilegizált funkciókhoz való távoli hozzáférést. Megfelelően feljogosított tisztviselők engedélyezik az informatikai rendszerhez való hozzáférés minden egyes hozzáférési módszerét, és minden egyes hozzáférési módszer használatához csak a szükséges felhasználókat jogosítják fel.

HE-18 A vezeték nélküli hozzáférésre vonatkozó korlátozások
Intézkedés: A szervezet:
— felhasználási korlátozásokat és megvalósítási útmutatót vezet be a vezeték nélküli technológiákra; és
— engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való vezeték nélküli hozzáféréseket.

HE-20 Külső informatikai rendszerek használata
Intézkedés: A szervezet meghatározza a feltételeket és szabályokat a feljogosított felhasználóknak a következőkre:
— hozzáférés az informatikai rendszerhez egy külső rendszerből;
— szervezet által ellenőrzött információk feldolgozása, tárolása és/vagy átvitele külső informatikai rendszerek segítségével.

9.3.1.5. Naplózás és elszámoltathatóság (NA)

NA-1 Naplózási és elszámoltathatósági szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
— egy formális, dokumentált naplózási szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
— egy formális, dokumentált eljárásrendet, amelynek célja a naplózási szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

NA-2 Naplózandó események
Intézkedés: Az informatikai rendszer naplóbejegyzéseket állít elő a következő eseményekre: [értékadás: a szervezet által meghatározott naplózandó események].

NA-3 A naplóbejegyzések tartalma
Intézkedés: Az informatikai rendszer a naplóbejegyzésekben elegendő információt gyűjt be ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

NA-4 Napló tárkapacitás
Intézkedés: A szervezet a naplózásra elegendő méretű tárkapacitást jelöl ki, illetve úgy konfigurálja a naplózást, hogy megelőzze az adott tárkapacitás betelését.

NA-5 Naplózási hiba kezelése
Intézkedés: Naplózási hiba esetén, vagy ha a naplózás tárkapacitás beteléshez közelít, az informatikai rendszer riasztást küld az adminisztrátornak, valamint a következő tevékenységeket is elvégzi: [értékadás: szervezet által meghatározott végrehajtandó tevékenységek (pl. az informatikai rendszer leállítása, a legrégebbi naplóbejegyzések felülírása, a naplózási folyamat leállítása)].

NA-8 Időbélyegek
Intézkedés: Az informatikai rendszer időbélyegeket biztosít a naplóbejegyzések előállításához.

NA-9 A napló információk védelme
Intézkedés: Az informatikai rendszer megvédi a napló információt és a naplózás eszközeit a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

NA-11 A naplóbejegyzések megőrzése
Intézkedés: A szervezet a naplóbejegyzéseket megőrzi [értékadás: a szervezet által meghatározott időtartam]-ig abból a célból, hogy támogatást nyújtson a rendkívüli események utólagos kivizsgálására, és hogy megfeleljen a jogszabályi és szervezeti információ megőrzési követelményeknek.

9.3.1.6. Rendszer és kommunikáció védelem (RV)

RV-1 Rendszer és kommunikáció védelmi szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált, rendszer és kommunikáció védelmi szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és kommunikáció védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

RV-5 Szolgáltatás megtagadás elleni védelem
Intézkedés: Az informatikai rendszer védelmet nyújt a következő típusú szolgáltatás megtagadás jellegű támadásokkal szemben vagy korlátozza azok kihatásait: [értékadás: szolgáltatás megtagadás jellegű támadástípusok szervezet által meghatározott listája vagy egy elfogadott listára való hivatkozás].

RV-7 A határok védelme
Intézkedés: Az informatikai rendszer figyeli és ellenőrzi az informatikai rendszer külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációkat.

RV-13 Jóváhagyott kriptográfia alkalmazása
Intézkedés: Ha az informatikai rendszerben kriptográfiát alkalmaznak, a rendszer minden kriptográfiai műveletét (beleértve a kulcs előállítását is) azt szabványos algoritmussal kell megvalósítani.

RV-14 Sértetlenség védelem nyilvános hozzáférés esetén
Intézkedés: A nyilvánosan elérhető rendszerek esetén az informatikai rendszer megvédi az információk és az alkalmazások sértetlenségét.

9.3.2. A fokozott kihatású biztonsági osztály követelményei

9.3.2.1. Konfiguráció kezelés (KK)

KK-1 Konfiguráció kezelési szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált konfiguráció kezelési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a konfiguráció kezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

KK-2 Alap konfiguráció
Intézkedés: A szervezet informatikai célrendszeréhez egy alap konfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges komponenseit.

Intézkedés bővítése:
a) A szervezet az alap konfiguráció frissítését az informatikai rendszer komponensek telepítésének a szerves részeként végzi.

KK-3 A konfigurációváltozások felügyelete
Intézkedés: A szervezet dokumentálja és ellenőrzi az informatikai rendszerben történt változásokat. Megfelelő szervezeti tisztviselők hagyják jóvá az informatikai rendszer változásait, összhangban a szervezeti szabályzatokkal és eljárásrendekkel.

KK-4 A konfigurációváltozások felügyelete
Intézkedés: A szervezet figyeli az informatikai rendszerben történt változásokat, és biztonsági hatásvizsgálatot végez a változások hatásainak meghatározására.

KK-5 A változtatásokra vonatkozó hozzáférés korlátozások
Intézkedés: A szervezet hozzáférési korlátozásokat juttat érvényre az informatikai rendszer (konfigurációs) változtatásaival kapcsolatban.

KK-6 Konfigurációs beállítások
Intézkedés: A szervezet
- kötelező konfigurációs beállítást határoz meg az informatikai rendszerben használt információ technológiai termékekre;
- az információ technológiai termékek lehető legkorlátozóbb biztonsági beállításait konfigurálja, amely még megfelel a működési követelményeknek;
- dokumentálja a konfigurációs beállításokat; és
- érvényre juttatja a konfigurációs beállításokat az informatikai rendszer valamennyi komponensében.

KK-7 Legszűkebb funkcionalitás
Intézkedés: A szervezet az informatikai rendszert úgy konfigurálja, hogy az csak a szükséges lehetőségeket nyújtsa, illetve letiltja/korlátozza a következő funkciók, portok, protokollok

és/vagy szolgáltatások használatát: [értékadás: a tiltott/korlátozott funkciók, portok, protokollok és/vagy szolgáltatások szervezet által definiált listája].

KK-8 Informatikai rendszer komponens leltár
Intézkedés: A szervezet aktuális leltárt készít, dokumentálja és karbantartja az informatikai rendszer komponenseit és a vonatkozó tulajdonosi információkat.

Intézkedés bővítése:

a) A szervezet az informatikai rendszer komponensek leltárjának a frissítését a komponensek telepítésének a szerves részeként végzi.

9.3.2.2. Rendszer és információ sértetlenség (RS)

RS-1 Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált, a rendszer és információ sértetlenségére vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és információ sértetlenségére vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

RS-2 Hibajavítás
Intézkedés: A szervezet az informatikai rendszerben talált hibákat jelenti, és kijavítja.

Intézkedés bővítése:

a)
b) A szervezet rendszeres időszakonként vagy szükség esetén automatikus mechanizmusokat alkalmaz az informatikai rendszer hibajavítási állapotának meghatározására.

RS-3 Rosszindulatú kódok elleni védelem
Intézkedés: Az informatikai rendszer rosszindulatú kódok elleni védelmet valósít meg, s ez automatikus frissítési lehetőséget is magában foglal.

Intézkedés bővítése:

a) A szervezet központilag kezeli a vírusvédelmi mechanizmusokat.
b) Az informatikai rendszer automatikusan frissíti a rosszindulatú kódok elleni védelmi mechanizmust.

RS-4 Behatolás észlelési eszközök és technikák
Intézkedés: A szervezet eszközöket és technikákat alkalmaz az informatikai rendszerben történő események figyelésére, detektálja a támadásokat, és biztosítja a rendszer jogosulatlan használatának beazonosítását.

Intézkedés bővítése:

a)
b)

c)
d) Az informatikai rendszer monitorozza a kimenő és bejövő kommunikációt, keresve a szokatlan és nem engedélyezett tevékenységeket és feltételeket. Magyarázat: Szokatlan/nem engedélyezett tevékenységek vagy feltételek közé tartozhat például a rosszindulatú kód jelenléte, az információ nem engedélyezett exportálása, vagy külső informatikai rendszer felé történő jelzés küldése.
e)

RS-5 Biztonsági riasztások és tájékoztatások
Intézkedés: A szervezet folyamatosan fogadja az informatikai rendszerre vonatkozó biztonsági riasztásokat és figyelmeztetéseket, eljuttatja ezeket az illetékes személyekhez, illetve megfelelő válaszlépéseket foganatosít.

RS-8 Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem
Intézkedés: Az informatikai rendszer kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelmet valósít meg.

RS-9 A bemeneti információra vonatkozó korlátozások
Intézkedés: A szervezet az informatikai rendszernek szóló információ bevitelt az erre jogosult személyekre korlátozza.

RS-10 A bemeneti információ pontossága, teljessége és érvényessége
Intézkedés: Az informatikai rendszer ellenőrzi az információ bemenetek pontosságát, teljességét, érvényességét és hitelességét.

RS-11 Hibakezelés
Intézkedés: Az informatikai rendszer eredményesen azonosítja és kezeli a hibákat, de nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak.

RS-12 A kimeneti információ kezelése és megőrzése
Intézkedés: A szervezet az informatikai rendszer kimenetét a szervezeti szabályzattal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

9.3.2.3. Azonosítás és hitelesítés (AH)

AH-1 Azonosítási és hitelesítési szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt, rendszeresen felülvizsgál és frissít:
- egy formális, dokumentált, az azonosításra és hitelesítésre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés, menedzsment kötelezettségei, koordináció a szervezet egységei közt; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja az azonosításra és hitelesítésre vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

AH-2 Felhasználó azonosítása és hitelesítése
Intézkedés: Az informatikai rendszer egyedileg azonosítja és hitelesíti a felhasználókat (vagy a felhasználók nevében eljáró eljárásokat)

Intézkedés bővítése

a) Az informatikai rendszer többtényezős hitelesítést használ a távoli hozzáférésre, ami kriptográfiai kulcsbirtoklás bizonyításán alapul. A kriptográfiai kulcsot tárolhatja [értékadás: Szoftver token, FIPS 140-2 1-es szinten tanúsított hardver; vagy FIPS 140-2 2-es vagy magasabb szinten tanúsított hardver.]

AH-3 Eszközök azonosítása és hitelesítése

Intézkedés: Az informatikai rendszer bizonyos eszközöket azonosít és hitelesít, mielőtt kapcsolatot létesítene velük.

AH-4 Azonosító kezelés

Intézkedés: A szervezet az alábbi módon kezeli a felhasználói azonosítókat:

- egyedileg azonosít minden felhasználót;
- ellenőrzi minden felhasználó azonosságát;
- egy új felhasználói azonosító kibocsátását adminisztrátori felhatalmazáshoz köti;
- garantálja, hogy a felhasználói azonosítót annak a félnek adták ki, akinek szánták;
- lezárja a felhasználói azonosítót egy, [értékadás: a szervezet által meghatározott időtartam]-ig tartó inaktivitás után, és
- archiválja a felhasználói azonosítókat.

AH-5 A hitelesítésre szolgáló eszközök kezelése

Intézkedés: A szervezet az alábbi módon kezeli a rendszer hitelesítésre szolgáló eszközeit:

- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
- adminisztratív eljárásokat vezet be a hitelesítésre szolgáló eszközök kezdeti szétosztására, az elvesztett/kompromittálódott vagy sérült eszközök esetére, illetve a hitelesítésre szolgáló eszközök visszavonására;
- az alapértelmezés szerinti hitelesítésre szolgáló eszközöket megváltoztatja az informatikai rendszer installálásának során; és
- időszakonként a hitelesítésre szolgáló eszközöket megváltoztatja/frissíti.

AH-6 A hitelesítésre szolgáló eszköz visszacsatolása

Intézkedés: Az informatikai rendszer visszacsatolást biztosít a felhasználónak hitelesítési kísérlete során, és ez a visszacsatolás nem veszélyezteti a hitelesítési mechanizmust. Az informatikai rendszer elrejti a hitelesítési információk visszacsatolását a hitelesítési kísérlet során, így védve az információt az esetleges kihasználástól/illetéktelen használattól.

AH-7 Hitelesítés kriptográfiai modul esetén

Intézkedés: Az informatikai rendszer olyan hitelesítési módszereket használ, amelyek megfelelnek a törvényeknek, vezetői döntéseknek, direktíváknak, szabályzatoknak, előírásoknak, szabványoknak, és a kriptográfiai modul hitelesítési útmutatójának.

9.3.2.4. Hozzáférés ellenőrzése (HE)

HE-1 Hozzáférés ellenőrzési szabályzat és eljárásrend

Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált hozzáférés ellenőrzési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettséget, és megfelelést; a koordináció a szervezeti entitások között;
- egy formális, dokumentált hozzáférés védelemre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés, menedzsment kötelezettségei, koordináció a szervezet egységei közt; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a hozzáférés ellenőrzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

HE-2 Felhasználói fiókok kezelése
Intézkedés: A szervezet kezeli az informatikai rendszer felhasználói fiókjait, beleértve a felhasználói fiókok létrehozását, aktiválását, módosítását, felülvizsgálatát, letiltását és eltávolítását. A szervezet felülvizsgálja az informatikai rendszer felhasználói fiókjait [értékadás: a szervezet által meghatározott gyakoriság, de legalább évente].

Az intézkedés bővítése:

a) A szervezet automatizált mechanizmusokat alkalmaz a felhasználói fiókok kezelésének támogatására.
b) Az informatikai rendszer automatikusan leállítja az ideiglenes és a kényszerhelyzetben létrehozott felhasználói fiókokat [értékadás: az egyes felhasználói fiók típusokra a szervezet által definiált időtartam] letelte után.
c) Az informatikai rendszer automatikusan letiltja az inaktív felhasználói fiókokat [értékadás: a szervezet által meghatározott időtartam] letelte után..
d) A szervezet automatikus mechanizmusokat használ a felhasználói fiókok kialakítására, módosítására, zárolására, visszavonására és az egyes személyek értesítésére, ha szükséges.

HE-3 Hozzáférés ellenőrzés érvényre juttatása
Intézkedés: Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszerhez való hozzáférés ellenőrzéséhez.

Az intézkedés bővítése:

a) Az informatikai rendszer biztosítja, hogy a biztonsági funkciókhoz (amelyek hardverben, szoftverben vagy förmverben valósulnak meg) és információkhoz való hozzáférés az erre feljogosított személyzetre (pl. biztonsági adminisztrátorok) korlátozódjon.
   Megjegyzés: A közvetlenül feljogosított személyzetbe tartoznak például a biztonsági adminisztrátorok, a rendszer és hálózati adminisztrátorok és más kiemelt jogú felhasználók. Kiemelt jogú felhasználók azok a személyek, akik a rendszert vezérlő, monitorozó vagy adminisztratív funkciókhoz hozzáférhetnek (pl. rendszeradminisztrátorok, informatikai rendszer biztonsági tisztviselői, üzemeltetők, rendszerprogramozók)

HE-4 Információ áramlás ellenőrzés érvényre juttatása
Intézkedés: Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információ áramlás ellenőrzéséhez.

HE-5 A felelősségek szétválasztása
Intézkedés: Az informatikai rendszer érvényre juttatja a felelősségek szétválasztását az egyes munkakörökhöz kijelölt hozzáférési jogosultságokon keresztül.

HE-6 Legkisebb jogosultság
Intézkedés: Az informatikai rendszer a felhasználók (illetve a felhasználók nevében fellépő eljárások) számára a megadott feladatok végrehajtásához szükséges leginkább korlátozó jogosultságok/privilégiumok, illetve hozzáférések összességét juttatják érvényre.

HE-7 Sikertelen bejelentkezési kísérletek
Intézkedés: Az informatikai rendszer egy [értékadás: a szervezet által definiált szám]-ként megadott korlátot juttat érvényre egy felhasználó egymást követő bejelentkezési kísérleteire, amelyek egy [értékadás: a szervezet által definiált időtartam]-on belül történtek. Amennyiben a sikertelen kísérletek a maximális számot túllépik, az információs rendszer automatikusan [választás: zárolja a felhasználói fiókot/csomópontot] [értékadás: a szervezet által definiált időtartamig]; késlelteti a következő bejelentkezési kísérletet egy az [értékadás: szervezet által definiált késleltetési algoritmusnak megfelelően].

HE-8 A rendszerhasználat jelzése
Intézkedés: Az informatikai rendszer egy jóváhagyott, a rendszerhasználatra vonatkozó jelzést ad a rendszerhez való hozzáférés engedélyezése előtt abból a célból, hogy a potenciális felhasználókat tájékoztatassa arról:

- hogy a felhasználó egy magyar közigazgatási informatikai rendszert használ;
- hogy lehetséges, hogy a rendszer használatot figyelhetik, rögzíthetik, illetve auditálhatják;
- hogy a rendszer jogosulatlan használata tilos, és büntetőjogi, valamint polgárjogi felelősségre vonással jár;
- hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti a figyelésbe és rögzítésbe. A rendszer által használt közlemény biztosítja a magántitokra és biztonságra vonatkozó értesítéseket, és mindaddig a képernyőn marad, amíg a felhasználó közvetlen műveletet nem végez az informatikai rendszerbe való bejelentkezéshez.

HE-11 A munkaszakasz zárolása
Intézkedés: Az informatikai rendszer [értékadás: a szervezet által definiált időtartam] inaktivitás után a munkaszakasz zárolásával megakadályozza a rendszerhez való további hozzáférést mindaddig, amíg a felhasználó nem azonosítja és hitelesíti magát újra a megfelelő eljárások alkalmazásával.

HE-12 A munkaszakasz lezárása
Intézkedés: Az informatikai rendszer automatikusan lezárja a munkaszakaszt egy, [értékadás: a szervezet által definiált időtartam] hosszúságú inaktivitás után.

HE-13 Felügyelet és felülvizsgálat — hozzáférés ellenőrzés
Intézkedés: A szervezet felügyeli és felülvizsgálja a felhasználók tevékenységét az informatikai rendszer hozzáférés ellenőrzése érvényre juttatása és használata tekintetében.

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat használ a felhasználói tevékenységek ellenőrzésére.

HE-14 Azonosítás és hitelesítés nélkül engedélyezett tevékenységek

Intézkedés: A szervezet meghatározza azokat a speciális felhasználói tevékenységeket, amelyeket az informatikai rendszerben azonosítás és hitelesítés nélkül is végre lehet hajtani.

Intézkedés bővítése:

a) A szervezet csak olyan mértékben engedélyezi az azonosítás és hitelesítés nélkül végrehajtható tevékenységeket, amennyire az saját céljainak megfelel.

HE-17 Távoli hozzáférés ellenőrzése

Intézkedés: A szervezet engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való távoli hozzáférés minden módszerét (pl. betárcsázás, Internet), beleértve a privilegizált funkciókhoz való távoli hozzáférést. Megfelelően feljogosított tisztviselők engedélyezik az informatikai rendszerhez való hozzáférés minden egyes hozzáférési módszerét, és minden egyes hozzáférési módszer használatához csak a szükséges felhasználókat jogosítják fel.

Intézkedés bővítése:

a) A szervezet automatizált mechanizmusokat alkalmaz a távoli hozzáférési módszerek figyelésére és ellenőrzésére.
b) A szervezet rejtjelzést alkalmaz a távoli hozzáférési munkaszakaszok bizalmasságának megvédésére.
c) A szervezet egy menedzselt hozzáférés ellenőrzési ponton keresztül minden távoli hozzáférést ellenőriz.
d) A szervezet magas jogosultsághoz kötött funkciókhoz csak komoly működéshez kapcsolódó igény esetén enged távoli hozzáférést, és ebben az esetben is dokumentálni kell ennek az indoklását az informatikai rendszer biztonsági tervében.

HE-18 A vezeték nélküli hozzáférésre vonatkozó korlátozások

Intézkedés: A szervezet:

— felhasználási korlátozásokat és megvalósítási útmutatót vezet be a vezeték nélküli technológiákra; és
— engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való vezeték nélküli hozzáféréseket.

Intézkedés bővítése:

a) A szervezet az informatikai rendszerhez való vezeték nélküli hozzáférés védelmére hitelesítést és rejtjelzést alkalmaz.

HE-19 A hordozható és mobil eszközök hozzáférés ellenőrzése

Intézkedés: A szervezet:

— felhasználási korlátozásokat és megvalósítási útmutatót vezet be a hordozható és mobil eszközökre; és
— engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való, hordozható és mobil eszközökön keresztüli hozzáféréseket.

— Megfelelően feljogosított tisztviselők engedélyezik a hordozható és mobil eszközök használatát.

HE-20 Külső informatikai rendszerek használata
Intézkedés: A szervezet meghatározza a feltételeket és szabályokat a feljogosított felhasználóknak a következőkre:
— hozzáférés az informatikai rendszerhez egy külső rendszerből;
— szervezet által ellenőrzött információk feldolgozása, tárolása és/vagy átvitele külső informatikai rendszerek segítségével.

Intézkedés bővítése:
a) A szervezet megtiltja a jogosult felhasználóknak külső informatikai rendszerek felhasználását a belső rendszeren található információk feldolgozására, tárolására vagy átvitelére, kivéve, ha a szervezet:
ah) ellenőrizni tudja a szükséges biztonsági intézkedések használatát a külső rendszeren, úgy ahogy az a biztonsági szabályzatban és biztonsági tervben le van írva;
ai) jóváhagyott kapcsolat van az informatikai rendszerek közt, vagy megállapodás született azzal a szervezettel, amelyik a külső informatikai rendszert befogadja.

9.3.2.5. Naplózás és elszámoltathatóság (NA)

NA-1 Naplózási és elszámoltathatósági szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
— egy formális, dokumentált naplózási szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
— egy formális, dokumentált eljárásrendet, amelynek célja a naplózási szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

NA-2 Naplózandó események
Intézkedés: Az informatikai rendszer naplóbejegyzéseket állít elő a következő eseményekre: [értékadás: a szervezet által meghatározott naplózandó események].

Intézkedés bővítése:
a)
b)
c) A szervezet időnként felülvizsgálja és frissíti a szervezet által naplózandó események listáját.

NA-3 A naplóbejegyzések tartalma
Intézkedés: Az informatikai rendszer a naplóbejegyzésekben elegendő információt gyűjt be ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

Intézkedés bővítése:

a) Az informatikai rendszer lehetőséget nyújt arra, hogy a fentieken túl, részletesebb információkat is be lehessen venni, a naplóbejegyzések típusa, elhelyezkedése vagy tárgya alapján.

NA-4 Napló tárkapacitás

Intézkedés: A szervezet a naplózásra elegendő méretű tárkapacitást jelöl ki, illetve úgy konfigurálja a naplózást, hogy megelőzze az adott tárkapacitás betelését.

NA-5 Naplózási hiba kezelése

Intézkedés: Naplózási hiba esetén, vagy ha a naplózás tárkapacitás beteléshez közelít, az informatikai rendszer riasztást küld az adminisztrátornak, valamint a következő tevékenységeket is elvégzi: [értékadás: szervezet által meghatározott végrehajtandó tevékenységek (pl. az informatikai rendszer leállítása, a legrégebbi naplóbejegyzések felülírása, a naplózási folyamat leállítása)].

NA-6 Napló figyelése, vizsgálata és jelentések készítése

Intézkedés: A szervezet rendszeresen áttekinti/átvizsgálja a naplóbejegyzéseket, nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, elemzi a gyanús tevékenységeket és a feltételezett megsértéseket, jelenti ezeket a megfelelő tisztviselőknek, illetve megteszi a szükséges intézkedéseket.

Intézkedés bővítése:

a)

b) A szervezet automatikus mechanizmusokat használ a biztonsági személyzet riasztására a következő gyanús vagy szokatlan események esetén: [értékadás: a szervezet által meghatározott lista a gyanús vagy szokatlan eseményekről, amelyek esetén riasztás szükséges].

NA-7 Naplócsökkentés, naplóriport készítés

Intézkedés: Az informatikai rendszer lehetőséget biztosít naplócsökkentésre és naplóriport készítésére.

Intézkedés bővítése:

a) Az informatikai rendszer biztosítja, hogy automatikusan fel lehessen dolgozni az érdekes naplóbejegyzéseket egy kiválasztható, feltétel alapú rendszer alapján.

NA-8 Időbélyegek

Intézkedés: Az informatikai rendszer időbélyegeket biztosít a naplóbejegyzések előállításához.

Intézkedés bővítése:

a) A szervezet szinkronizálja a belső rendszer órákat a következő frekvencián [értékadás: szervezet által meghatározott frekvencia].

NA-9 A napló információk védelme

Intézkedés: Az informatikai rendszer megvédi a napló információt és a naplózás eszközeit a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

NA-11 A naplóbejegyzések megőrzése
Intézkedés: A szervezet a naplóbejegyzéseket megőrzi [értékadás: a szervezet által meghatározott időtartam]-ig abból a célból, hogy támogatást nyújtson a rendkívüli események utólagos kivizsgálására, és hogy megfeleljen a jogszabályi és szervezeti információ megőrzési követelményeknek.

9.3.2.6. Rendszer és kommunikáció védelem (RV)

RV-1 Rendszer és kommunikáció védelmi szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált, rendszer és kommunikáció védelmi szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és kommunikáció védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

RV-2 Alkalmazás szétválasztás
Intézkedés: Az informatikai rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az informatikai rendszer menedzsment funkcionalitásától.

RV-4 Információ maradványok
Intézkedés: Az informatikai rendszer meggátolja a megosztott rendszer erőforrások útján történő jogosulatlan és véletlen információáramlást.

RV-5 Szolgáltatás megtagadás elleni védelem
Intézkedés: Az informatikai rendszer védelmet nyújt a következő típusú szolgáltatás megtagadás jellegű támadásokkal szemben vagy korlátozza azok kihatásait: [értékadás: szolgáltatás megtagadás jellegű támadástípusok szervezet által meghatározott listája vagy egy elfogadott listára való hivatkozás].

RV-7 A határok védelme
Intézkedés: Az informatikai rendszer figyeli és ellenőrzi az informatikai rendszer külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációkat.

Intézkedés bővítése:
a) A szervezet a nyilvánosan hozzáférhető informatikai rendszer összetevőket (pl. nyilvános web szervereket) elkülönített alhálózatokban helyezi el, elkülönített fizikai hálózati interfészekkel.
   Megjegyzés: Nyilvánosan hozzáférhető informatikai rendszer összetevő lehet például a web szerver.
b) A szervezet meggátolja a nyilvános hozzáférést a szervezet belső hálózatához, kivéve azon eseteket, amikor a hozzáférés megfelelő védelmi intézkedések közbeiktatásával történik.
c) A szervezet korlátozza a hozzáférési pontok számát az informatikai rendszerhez, hogy jobban monitorozható legyen a kijövő és bejövő hálózati forgalom.

d) A szervezet kialakít egy felügyelt kapcsolódási pontot (határvédelmi eszközöket egy hatékony biztonsági architektúrában) a külső telekommunikációs szolgáltatóval, létrehozva azokat az intézkedéseket, amelyek szükségesek az átvitt információ bizalmasságának és integritásának védelméhez.
e) Az informatikai rendszer alapból tilt és kivételként engedélyez csak minden hálózati forgalmat (vagyis minden tiltva, engedélyezés kivételes esetben).

RV-8 Az adatátvitel sértetlensége
Intézkedés: Az informatikai rendszer megvédi a továbbított információk sértetlenségét.

RV-9 Az adatátvitel bizalmassága
Intézkedés: Az informatikai rendszer megvédi az átvitt információk bizalmasságát.

RV-10 A hálózati kapcsolat megszakítása
Intézkedés: Az informatikai rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, vagy [értékadás: a szervezet által meghatározott időtartam] hosszú inaktivitás után.

RV-12 Kriptográfiai kulcs előállítása és kezelése
Intézkedés: Az informatikai rendszer a kriptográfiai kulcsok előállítására és kezelésére automatikus támogató eljárásokkal ellátott mechanizmusokat, vagy manuális eljárásokat alkalmaz.

RV-13 Jóváhagyott kriptográfia alkalmazása
Intézkedés: Ha az informatikai rendszerben kriptográfiát alkalmaznak, a rendszer minden kriptográfiai műveletét (beleértve a kulcs előállítását is) azt szabványos algoritmussal kell megvalósítani.

RV-14 Sértetlenség védelem nyilvános hozzáférés esetén
Intézkedés: A nyilvánosan elérhető rendszerek esetén az informatikai rendszer megvédi az információk és az alkalmazások sértetlenségét.

RV-15 Telekommunikációs szolgáltatások korlátozása
Intézkedés: Az informatikai rendszer meggátolja a telekommunikációs szolgáltatások együttműködő számítógép-használati mechanizmusainak (pl. video és audio konferenciák) távolról történő aktiválását, és közvetlen jelzéseket biztosít az ilyen mechanizmusok használatról a lokális felhasználók felé (pl. kamera vagy mikrofon használata).

RV-17 Nyilvános kulcsú infrastruktúra tanúsítványok
Intézkedés: Megfelelő hitelesítési rend szerint a szervezet vagy önmaga kiállít nyílt kulcsú tanúsítványt a vagy vásárol nyílt kulcsú tanúsítványt egy hitelesítés-szolgáltatótól.

RV-18 Mobil kód korlátozása
Intézkedés: A szervezet
— korlátozza a mobil kód technika alkalmazhatóságát, erre vonatkozó útmutatót bocsát ki, a mobil kódok rosszindulatú használata által okozott potenciális károk miatt, valamint

— dokumentálja, figyeli és ellenőrzi a mobil kódok információs rendszeren belüli felhasználását. Megfelelő vezető engedélyezi a mobil kódok használatát.

RV-19 Interneten Keresztüli Hangátvitel (VoIP)
Intézkedés: A szervezet:
— használati korlátozásokat vezet be és megvalósítási útmutatót ad az Interneten Keresztüli Hangátvitel (VoIP) technológiákhoz, a rosszindulatú használat esetén okozható károkat felmérve; és
— engedélyezi, figyeli, és ellenőrzi a VoIP használatát az informatikai rendszeren belül.

RV-20 Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)
Intézkedés: Az informatikai rendszer, amely a név/cím feloldó szolgáltatást biztosítja a hiteles adatokon kívül egyéb biztonsági adatokat is visszaad a feloldási kérésekre, mint például az információ eredete és integritási adatok.

RV-22 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén
Intézkedés: Egy olyan informatikai rendszernek, amely az egész szervezet név/cím feloldását szolgálja ki hibatűrőnek kell lennie, és működnie kell rajta a szerep szétválasztásnak.

RV-23 Munkaszakasz hitelessége
Intézkedés: Az informatikai rendszer valamilyen mechanizmussal biztosítja a munkaszakaszok hitelességének védelmét.

9.3.3. A kiemelt kihatású biztonsági osztály követelményei

9.3.3.1. Konfiguráció kezelés (KK)

KK-1 Konfiguráció kezelési szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált konfiguráció kezelési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a konfiguráció kezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

KK-2 Alap konfiguráció
Intézkedés: A szervezet informatikai célrendszeréhez egy alap konfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges komponenseit.

Intézkedés bővítése:
a) A szervezet az alap konfiguráció frissítését az informatikai rendszer komponensek telepítésének a szerves részeként végzi.
b) A szervezet automatikus mechanizmusokat alkalmaz az informatikai rendszer naprakész, teljes, pontos, és állandóan rendelkezésre álló alap konfigurációjának a karbantartására.

KK-3 A konfigurációváltozások felügyelete
Intézkedés: A szervezet dokumentálja és ellenőrzi az informatikai rendszerben történt változásokat. Megfelelő szervezeti tisztviselők hagyják jóvá az informatikai rendszer változásait, összhangban a szervezeti szabályzatokkal és eljárásrendekkel.

KK-4 A konfigurációváltozások felügyelete
Intézkedés: A szervezet figyeli az informatikai rendszerben történt változásokat, és biztonsági hatásvizsgálatot végez a változások hatásainak meghatározására.

KK-5 A változtatásokra vonatkozó hozzáférés korlátozások
Intézkedés: A szervezet hozzáférési korlátozásokat juttat érvényre az informatikai rendszer (konfigurációs) változtatásaival kapcsolatban.

Intézkedés bővítése:
a) A szervezet automatikus mechanizmusokat alkalmaz a hozzáférési korlátozások érvényre juttatására, és érvényre juttatási tevékenység auditálásának a támogatására.

KK-6 Konfigurációs beállítások
Intézkedés: A szervezet
- kötelező konfigurációs beállítást határoz meg az informatikai rendszerben használt információ technológiai termékekre;
- az információ technológiai termékek lehető legkorlátozóbb biztonsági beállításait konfigurálja, amely még megfelel a működési követelményeknek;
- dokumentálja a konfigurációs beállításokat; és

— érvényre juttatja a konfigurációs beállításokat az informatikai rendszer valamennyi komponensében.

Intézkedés bővítése:

a) A szervezet automatikus mechanizmusokat alkalmaz a konfigurációs beállítások központi kezelésére, alkalmazására és ellenőrzésére.

KK-7 Legszűkebb funkcionalitás

Intézkedés: A szervezet az informatikai rendszert úgy konfigurálja, hogy az csak a szükséges lehetőségeket nyújtsa, illetve letiltja/korlátozza a következő funkciók, portok, protokollok és/vagy szolgáltatások használatát: [értékadás: a tiltott/korlátozott funkciók, portok, protokollok és/vagy szolgáltatások szervezet által definiált listája].

Intézkedés bővítése:

a) A szervezet átvizsgálja az informatikai rendszert [értékadás: a szervezet által meghatározott gyakorisággal], hogy meghatározza és kizárja a szükségtelen portokat, protokollokat és/vagy szolgáltatásokat.

KK-8 Informatikai rendszer komponens leltár

Intézkedés: A szervezet aktuális leltárt készít, dokumentálja és karbantartja az informatikai rendszer komponenseit és a vonatkozó tulajdonosi információkat.

Intézkedés bővítése:

a) A szervezet az informatikai rendszer komponensek leltárjának a frissítését a komponensek telepítésének a szerves részeként végzi.
b) A szervezet automatikus mechanizmusokat alkalmaz az informatikai rendszer komponensek leltárjának naprakész, teljes, pontos, és állandóan rendelkezésre álló karbantartására.

9.3.3.2. Rendszer és információ sértetlenség (RS)

RS-1 Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend

Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

— egy formális, dokumentált, a rendszer és információ sértetlenségére vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
— egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és információ sértetlenségére vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

RS-2 Hibajavítás

Intézkedés: A szervezet az informatikai rendszerben talált hibákat jelenti, és kijavítja.

Intézkedés bővítése:

a) A szervezet központilag kezeli a hibajavítás folyamatát, és a javításokat automatikusan telepíti.

b) A szervezet rendszeres időszakonként vagy szükség esetén automatikus mechanizmusokat alkalmaz az informatikai rendszer hibajavítási állapotának meghatározására.

RS-3 Rosszindulatú kódok elleni védelem
Intézkedés: Az informatikai rendszer rosszindulatú kódok elleni védelmet valósít meg, s ez automatikus frissítési lehetőséget is magában foglal.

Intézkedés bővítése:
a) A szervezet központilag kezeli a vírusvédelmi mechanizmusokat.
b) Az informatikai rendszer automatikusan frissíti a rosszindulatú kódok elleni védelmi mechanizmust.

RS-4 Behatolás észlelési eszközök és technikák
Intézkedés: A szervezet eszközöket és technikákat alkalmaz az informatikai rendszerben történő események figyelésére, detektálja a támadásokat, és biztosítja a rendszer jogosulatlan használatának beazonosítását.

Intézkedés bővítése:
a)
b) A szervezet automatikus eszközöket használ az események közel valós idejű elemzésére.
c)
d) Az informatikai rendszer monitorozza a kimenő és bejövő kommunikációt, keresve a szokatlan és nem engedélyezett tevékenységeket és feltételeket. Magyarázat: Szokatlan/nem engedélyezett tevékenységek vagy feltételek közé tartozhat például a rosszindulatú kód jelenléte, az információ nem engedélyezett exportálása, vagy külső informatikai rendszer felé történő jelzés küldése.
e) Az informatikai rendszer valós idejű riasztást ad ki, amikor a következő veszély, vagy potenciális veszély áll fent: [értékadás: a szervezet által meghatározott veszélyek jeleinek a listája].

RS-5 Biztonsági riasztások és tájékoztatások
Intézkedés: A szervezet folyamatosan fogadja az informatikai rendszerre vonatkozó biztonsági riasztásokat és figyelmeztetéseket, eljuttatja ezeket az illetékes személyekhez, illetve megfelelő válaszlépéseket foganatosít.

Intézkedés bővítése:
a) A szervezet automatikus mechanizmusokat használ a biztonsági riasztások és figyelmeztetések szervezeten belüli szükséges terítésére.

RS-6 A biztonsági funkcionalitás ellenőrzése
Intézkedés: Az informatikai rendszer ellenőrzi a biztonsági funkciók helyes működését [(egy vagy több) kiválasztás: a rendszer indításakor és újraindításakor; megfelelő privilégiummal rendelkező felhasználó parancsára; időszakosan, [értékadás: szervezet által meghatározott gyakorisággal]] és amennyiben hibákat fedeznek fel [(egy vagy több) kiválasztása: értesíti a rendszer adminisztrátort, leállítja a rendszert, újraindítja a rendszert].

RS-7 Szoftver és információ sértetlenség
Intézkedés: Az informatikai rendszer felismeri és védi a szoftverben és az információban bekövetkezett engedély nélküli változtatásokat.

Intézkedés bővítése:

a) A szervezet a szoftver és az információ sértetlenségét [értékadás: a szervezet által meghatározott gyakorisággal] újraértékeli, úgy hogy sértetlenség ellenőrzést végez a rendszeren.
b) A szervezet automatikus eszközöket alkalmaz a megfelelő személyek értesítésére, amennyiben a sértetlenség ellenőrzése során eltérést tapasztal.

RS-8 Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem
Intézkedés: Az informatikai rendszer kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelmet valósít meg.

Intézkedés bővítése:

a) A szervezet központilag kezeli a levélszemét elleni védelmi mechanizmust.

RS-9 A bemeneti információra vonatkozó korlátozások
Intézkedés: A szervezet az informatikai rendszernek szóló információ bevitelt az erre jogosult személyekre korlátozza.

RS-10 A bemeneti információ pontossága, teljessége és érvényessége
Intézkedés: Az informatikai rendszer ellenőrzi az információ bemenetek pontosságát, teljességét, érvényességét és hitelességét.

RS-11 Hibakezelés
Intézkedés: Az informatikai rendszer eredményesen azonosítja és kezeli a hibákat, de nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak.

RS-12 A kimeneti információ kezelése és megőrzése
Intézkedés: A szervezet az informatikai rendszer kimenetét a szervezeti szabályzattal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

9.3.3.3. Azonosítás és hitelesítés (AH)

AH-1 Azonosítási és hitelesítési szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt, rendszeresen felülvizsgál és frissít:

- egy formális, dokumentált, az azonosításra és hitelesítésre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés, menedzsment kötelezettségei, koordináció a szervezet egységei közt; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja az azonosításra és hitelesítésre vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

AH-2 Felhasználó azonosítása és hitelesítése
Intézkedés: Az informatikai rendszer egyedileg azonosítja és hitelesíti a felhasználókat (vagy a felhasználók nevében eljáró eljárásokat)

Intézkedés bővítése

a)
b) Az informatikai rendszer többtényezős hitelesítést használ a helyi hozzáférésre, ami kriptográfiai kulcsbirtoklás bizonyításán alapul. A kriptográfiai kulcsot tárolhatja [értékadás: Szoftver token, FIPS 140-2 1-es szinten tanúsított hardver; vagy FIPS 140-2 2-es vagy magasabb szinten tanúsított hardver.].
c) Az informatikai rendszer többtényezős hitelesítést használ a távoli hozzáférésre, ami kriptográfiai kulcsbirtoklás bizonyításán alapul. A kriptográfiai kulcsot FIPS 140-2 2-es vagy magasabb szinten tanúsított hardver tárolhatja.

AH-3 Eszközök azonosítása és hitelesítése
Intézkedés: Az informatikai rendszer bizonyos eszközöket azonosít és hitelesít, mielőtt kapcsolatot létesítene velük.

AH-4 Azonosító kezelés
Intézkedés: A szervezet az alábbi módon kezeli a felhasználói azonosítókat:
- egyedileg azonosít minden felhasználót;
- ellenőrzi minden felhasználó azonosságát;
- egy új felhasználói azonosító kibocsátását adminisztrátori felhatalmazáshoz köti;
- garantálja, hogy a felhasználói azonosítót annak a félnek adták ki, akinek szánták;
- lezárja a felhasználói azonosítót egy, [értékadás: a szervezet által meghatározott időtartam]-ig tartó inaktivitás után, és
- archiválja a felhasználói azonosítókat.

AH-5 A hitelesítésre szolgáló eszközök kezelése
Intézkedés: A szervezet az alábbi módon kezeli a rendszer hitelesítésre szolgáló eszközeit:
- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
- adminisztratív eljárásokat vezet be a hitelesítésre szolgáló eszközök kezdeti szétosztására, az elvesztett/kompromittálódott vagy sérült eszközök esetére, illetve a hitelesítésre szolgáló eszközök visszavonására;
- az alapértelmezés szerinti hitelesítésre szolgáló eszközöket megváltoztatja az informatikai rendszer installálásának során; és
- időszakonként a hitelesítésre szolgáló eszközöket megváltoztatja/frissíti.

AH-6 A hitelesítésre szolgáló eszköz visszacsatolása
Intézkedés: Az informatikai rendszer visszacsatolást biztosít a felhasználónak hitelesítési kísérlete során, és ez a visszacsatolás nem veszélyezteti a hitelesítési mechanizmust. Az informatikai rendszer elrejti a hitelesítési információk visszacsatolását a hitelesítési kísérlet során, így védve az információt az esetleges kihasználástól/illetéktelen használattól.

AH-7 Hitelesítés kriptográfiai modul esetén
Intézkedés: Az informatikai rendszer olyan hitelesítési módszereket használ, amelyek megfelelnek a törvényeknek, vezetői döntéseknek, direktíváknak, szabályzatoknak, előírásoknak, szabványoknak, és a kriptográfiai modul hitelesítési útmutatójának.

9.3.3.4. Hozzáférés ellenőrzése (HE)

HE-1 Hozzáférés ellenőrzési szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált hozzáférés ellenőrzési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettséget, és megfelelést; a koordináció a szervezeti entitások között;
- egy formális, dokumentált hozzáférés védelemre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés, menedzsment kötelezettségei, koordináció a szervezet egységei közt; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a hozzáférés ellenőrzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

HE-2 Felhasználói fiókok kezelése
Intézkedés: A szervezet kezeli az informatikai rendszer felhasználói fiókjait, beleértve a felhasználói fiókok létrehozását, aktiválását, módosítását, felülvizsgálatát, letiltását és eltávolítását. A szervezet felülvizsgálja az informatikai rendszer felhasználói fiókjait [értékadás: a szervezet által meghatározott gyakoriság, de legalább évente].

Az intézkedés bővítése:
a) A szervezet automatizált mechanizmusokat alkalmaz a felhasználói fiókok kezelésének támogatására.
b) Az informatikai rendszer automatikusan leállítja az ideiglenes és a kényszerhelyzetben létrehozott felhasználói fiókokat [értékadás: az egyes felhasználói fiók típusokra a szervezet által definiált időtartam] letelte után.
c) Az informatikai rendszer automatikusan letiltja az inaktív felhasználói fiókokat [értékadás: a szervezet által meghatározott időtartam] letelte után..
d) A szervezet automatikus mechanizmusokat használ a felhasználói fiókok kialakítására, módosítására, zárolására, visszavonására és az egyes személyek értesítésére, ha szükséges.

HE-3 Hozzáférés ellenőrzés érvényre juttatása
Intézkedés: Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszerhez való hozzáférés ellenőrzéséhez.

Az intézkedés bővítése:
a) Az informatikai rendszer biztosítja, hogy a biztonsági funkciókhoz (amelyek hardverben, szoftverben vagy förmverben valósulnak meg) és információkhoz való hozzáférés az erre feljogosított személyzetre (pl. biztonsági adminisztrátorok) korlátozódjon.
   Megjegyzés: A közvetlenül feljogosított személyzetbe tartoznak például a biztonsági adminisztrátorok, a rendszer és hálózati adminisztrátorok és más kiemelt jogú felhasználók. Kiemelt jogú felhasználók azok a személyek, akik a rendszert vezérlő, monitorozó vagy adminisztratív funkciókhoz hozzáférhetnek (pl. rendszeradminisztrátorok, informatikai rendszer biztonsági tisztviselői, üzemeltetők, rendszerprogramozók)

HE-4 Információ áramlás ellenőrzés érvényre juttatása
Intézkedés: Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információ áramlás ellenőrzéséhez.

HE-5 A felelősségek szétválasztása
Intézkedés: Az informatikai rendszer érvényre juttatja a felelősségek szétválasztását az egyes munkakörökhöz kijelölt hozzáférési jogosultságokon keresztül.

HE-6 Legkisebb jogosultság
Intézkedés: Az informatikai rendszer a felhasználók (illetve a felhasználók nevében fellépő eljárások) számára a megadott feladatok végrehajtásához szükséges leginkább korlátozó jogosultságok/privilégiumok, illetve hozzáférések összességét juttatják érvényre.

HE-7 Sikertelen bejelentkezési kísérletek
Intézkedés: Az informatikai rendszer egy [értékadás: a szervezet által definiált szám]-ként megadott korlátot juttat érvényre egy felhasználó egymást követő bejelentkezési kísérleteire, amelyek egy [értékadás: a szervezet által definiált időtartam]-on belül történtek. Amennyiben a sikertelen kísérletek a maximális számot túllépik, az információs rendszer automatikusan [választás: zárolja a felhasználói fiókot/csomópontot] [értékadás: a szervezet által definiált időtartamig]; késlelteti a következő bejelentkezési kísérletet egy az [értékadás: szervezet által definiált késleltetési algoritmusnak megfelelően].

HE-8 A rendszerhasználat jelzése
Intézkedés: Az informatikai rendszer egy jóváhagyott, a rendszerhasználatra vonatkozó jelzést ad a rendszerhez való hozzáférés engedélyezése előtt abból a célból, hogy a potenciális felhasználókat tájékoztatassa arról:

- hogy a felhasználó egy magyar közigazgatási informatikai rendszert használ;
- hogy lehetséges, hogy a rendszer használatot figyelhetik, rögzíthetik, illetve auditálhatják;
- hogy a rendszer jogosulatlan használata tilos, és büntetőjogi, valamint polgárjogi felelősségre vonással jár;
- hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti a figyelésbe és rögzítésbe. A rendszer által használt közlemény biztosítja a magántitokra és biztonságra vonatkozó értesítéseket, és mindaddig a képernyőn marad, amíg a felhasználó közvetlen műveletet nem végez az informatikai rendszerbe való bejelentkezéshez.

HE-10 Egyidejű munkaszakasz kezelés
Intézkedés: Az informatikai rendszer korlátozza az egyszerre történő bejelentkezések számát a következőre: [értékadás: a szervezet által meghatározott szám a párhuzamos munkaszakaszokra]

HE-11 A munkaszakasz zárolása
Intézkedés: Az informatikai rendszer [értékadás: a szervezet által definiált időtartam] inaktivitás után a munkaszakasz zárolásával megakadályozza a rendszerhez való további hozzáférést mindaddig, amíg a felhasználó nem azonosítja és hitelesíti magát újra a megfelelő eljárások alkalmazásával.

HE-12 A munkaszakasz lezárása
Intézkedés: Az informatikai rendszer automatikusan lezárja a munkaszakaszt egy, [értékadás: a szervezet által definiált időtartam] hosszúságú inaktivitás után.

Intézkedés bővítése:
a) Az automatikus munkaszakasz lezárás vonatkozik a helyi és távoli munkaszakaszokra is.

HE-13 Felügyelet és felülvizsgálat — hozzáférés ellenőrzés
Intézkedés: A szervezet felügyeli és felülvizsgálja a felhasználók tevékenységét az informatikai rendszer hozzáférés ellenőrzése érvényre juttatása és használata tekintetében.

Intézkedés bővítése:
a) A szervezet automatikus mechanizmusokat használ a felhasználói tevékenységek ellenőrzésére.

HE-14 Azonosítás és hitelesítés nélkül engedélyezett tevékenységek
Intézkedés: A szervezet meghatározza azokat a speciális felhasználói tevékenységeket, amelyeket az informatikai rendszerben azonosítás és hitelesítés nélkül is végre lehet hajtani.

Intézkedés bővítése:
a) A szervezet csak olyan mértékben engedélyezi az azonosítás és hitelesítés nélkül végrehajtható tevékenységeket, amennyire az saját céljainak megfelel.

HE-15 Automatikus jelölés
Intézkedés: Az informatikai rendszer megjelöli a kimenetet szabványos névkonvenciókkal, hogy egyértelművé tegye a különleges terjesztési, kezelési utasításokat.

HE-17 Távoli hozzáférés ellenőrzése
Intézkedés: A szervezet engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való távoli hozzáférés minden módszerét (pl. betárcsázás, Internet), beleértve a privilegizált funkciókhoz való távoli hozzáférést. Megfelelően feljogosított tisztviselők engedélyezik az informatikai rendszerhez való hozzáférés minden egyes hozzáférési módszerét, és minden egyes hozzáférési módszer használatához csak a szükséges felhasználókat jogosítják fel.

Intézkedés bővítése:
a) A szervezet automatizált mechanizmusokat alkalmaz a távoli hozzáférési módszerek figyelésére és ellenőrzésére.
b) A szervezet rejtjelzést alkalmaz a távoli hozzáférési munkaszakaszok bizalmasságának megvédésére.
c) A szervezet egy menedzselt hozzáférés ellenőrzési ponton keresztül minden távoli hozzáférést ellenőriz.
d) A szervezet magas jogosultsághoz kötött funkciókhoz csak komoly működéshez kapcsolódó igény esetén enged távoli hozzáférést, és ebben az esetben is dokumentálni kell ennek az indoklását az informatikai rendszer biztonsági tervében.

HE-18 A vezeték nélküli hozzáférésre vonatkozó korlátozások

Intézkedés: A szervezet:

- felhasználási korlátozásokat és megvalósítási útmutatót vezet be a vezeték nélküli technológiákra; és
- engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való vezeték nélküli hozzáféréseket.

Intézkedés bővítése:

a) A szervezet az informatikai rendszerhez való vezeték nélküli hozzáférés védelmére hitelesítést és rejtjelzést alkalmaz.

b) A szervezet megvizsgálja a nem engedélyezett vezeték nélküli hozzáférési pontokat a következő frekvencián: [értékadás: szervezet által meghatározott frekvencia] és megteszi a szükséges lépéseket, ha ilyen hozzáféréseket találnak. Magyarázat: A szervezet egy alapos vizsgálatot folytat nem engedélyezett vezeték nélküli hozzáférési pontokat keresve a kiemelten fontos informatikai rendszereket tartalmazó egységekben. A vizsgálat nem korlátozódik az egységen belül arra a területre, ahol a kiemelten fontos informatikai rendszer található.

HE-19 A hordozható és mobil eszközök hozzáférés ellenőrzése

Intézkedés: A szervezet:

- felhasználási korlátozásokat és megvalósítási útmutatót vezet be a hordozható és mobil eszközökre; és
- engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való, hordozható és mobil eszközökön keresztüli hozzáféréseket.
- Megfelelően feljogosított tisztviselők engedélyezik a hordozható és mobil eszközök használatát.

HE-20 Külső informatikai rendszerek használata

Intézkedés: A szervezet meghatározza a feltételeket és szabályokat a feljogosított felhasználóknak a következőkre:

- hozzáférés az informatikai rendszerhez egy külső rendszerből;
- szervezet által ellenőrzött információk feldolgozása, tárolása és/vagy átvitele külső informatikai rendszerek segítségével.

Intézkedés bővítése:

a) A szervezet megtiltja a jogosult felhasználóknak külső informatikai rendszerek felhasználását a belső rendszeren található információk feldolgozására, tárolására vagy átvitelére, kivéve, ha a szervezet:

aj) ellenőrizni tudja a szükséges biztonsági intézkedések használatát a külső rendszeren, úgy ahogy az a biztonsági szabályzatban és biztonsági tervben le van írva;

ak) jóváhagyott kapcsolat van az informatikai rendszerek közt, vagy megállapodás született azzal a szervezettel, amelyik a külső informatikai rendszert befogadja.

9.3.3.5. Naplózás és elszámoltathatóság (NA)

NA-1 Naplózási és elszámoltathatósági szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált naplózási szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a naplózási szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

NA-2 Naplózandó események
Intézkedés: Az informatikai rendszer naplóbejegyzéseket állít elő a következő eseményekre: [értékadás: a szervezet által meghatározott naplózandó események].

Intézkedés bővítése:
a) Az informatikai rendszer biztosítja annak lehetőségét, hogy több különböző összetevőből származó naplóbejegyzésből össze lehessen állítani egy rendszerszintű (logikai vagy fizikai), időalapú naplót.
b) Az informatikai rendszer biztosítja annak a lehetőségét, hogy felügyelhető legyen, hogy események melyik csoportját a rendszer melyik különálló összetevője naplózza.

NA-3 A naplóbejegyzések tartalma
Intézkedés: Az informatikai rendszer a naplóbejegyzésekben elegendő információt gyűjt be ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

Intézkedés bővítése:
a) Az informatikai rendszer lehetőséget nyújt arra, hogy a fentieken túl, részletesebb információkat is be lehessen venni, a naplóbejegyzések típusa, elhelyezkedése vagy tárgya alapján.
b) Az informatikai rendszer biztosítja a lehetőséget, hogy központilag lehessen felügyelni a különálló összetevők által készített naplóbejegyzések tartalmát.

NA-4 Napló tárkapacitás
Intézkedés: A szervezet a naplózásra elegendő méretű tárkapacitást jelöl ki, illetve úgy konfigurálja a naplózást, hogy megelőzze az adott tárkapacitás betelését.

NA-5 Naplózási hiba kezelése
Intézkedés: Naplózási hiba esetén, vagy ha a naplózás tárkapacitás beteléshez közelít, az informatikai rendszer riasztást küld az adminisztrátornak, valamint a következő tevékenységeket is elvégzi: [értékadás: szervezet által meghatározott végrehajtandó tevékenységek (pl. az informatikai rendszer leállítása, a legrégebbi naplóbejegyzések felülírása, a naplózási folyamat leállítása)].

Intézkedés bővítése:
a) Az informatikai rendszer figyelmeztet, ha a lefoglalt naplózási tárhely eléri [értékadás: szervezet által meghatározott százalék a maximális naplózási tárhely arányában].

b) Az informatikai rendszer valósidejű riasztást küld, ha a következő hibaesemények bekövetkeznek: [értékadás: szervezet által definiált hibaesemények listája, amelyek valós idejű riasztást igényelnek].

NA-6 Napló figyelése, vizsgálata és jelentések készítése
Intézkedés: A szervezet rendszeresen áttekinti/átvizsgálja a naplóbejegyzéseket, nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, elemzi a gyanús tevékenységeket és a feltételezett megsértéseket, jelenti ezeket a megfelelő tisztviselőknek, illetve megteszi a szükséges intézkedéseket.

Intézkedés bővítése:
a) A szervezet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének integrálására egy átfogó folyamattá, amely választ ad a gyanús tevékenységek ellen.
b) A szervezet automatikus mechanizmusokat használ a biztonsági személyzet riasztására a következő gyanús vagy szokatlan események esetén: [értékadás: a szervezet által meghatározott lista a gyanús vagy szokatlan eseményekről, amelyek esetén riasztás szükséges].

NA-7 Naplócsökkentés, naplóriport készítés
Intézkedés: Az informatikai rendszer lehetőséget biztosít naplócsökkentésre és naplóriport készítésére.

Intézkedés bővítése:
a) Az informatikai rendszer biztosítja, hogy automatikusan fel lehessen dolgozni az érdekes naplóbejegyzéseket egy kiválasztható, feltétel alapú rendszer alapján.

NA-8 Időbélyegek
Intézkedés: Az informatikai rendszer időbélyegeket biztosít a naplóbejegyzések előállításához.

Intézkedés bővítése:
a) A szervezet szinkronizálja a belső rendszer órákat a következő frekvencián [értékadás: szervezet által meghatározott frekvencia].

NA-9 A napló információk védelme
Intézkedés: Az informatikai rendszer megvédi a napló információt és a naplózás eszközeit a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

NA-11 A naplóbejegyzések megőrzése
Intézkedés: A szervezet a naplóbejegyzéseket megőrzi [értékadás: a szervezet által meghatározott időtartam]-ig abból a célból, hogy támogatást nyújtson a rendkívüli események utólagos kivizsgálására, és hogy megfeleljen a jogszabályi és szervezeti információ megőrzési követelményeknek.

9.3.3.6. Rendszer és kommunikáció védelem (RV)

RV-1 Rendszer és kommunikáció védelmi szabályzat és eljárásrend
Intézkedés: A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált, rendszer és kommunikáció védelmi szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, megfelelés; illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és kommunikáció védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

RV-2 Alkalmazás szétválasztás
Intézkedés: Az informatikai rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az informatikai rendszer menedzsment funkcionalitásától.

RV-3 Biztonsági funkciók elkülönítése
Intézkedés: A rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.

RV-4 Információ maradványok
Intézkedés: Az informatikai rendszer meggátolja a megosztott rendszer erőforrások útján történő jogosulatlan és véletlen információáramlást.

RV-5 Szolgáltatás megtagadás elleni védelem
Intézkedés: Az informatikai rendszer védelmet nyújt a következő típusú szolgáltatás megtagadás jellegű támadásokkal szemben vagy korlátozza azok kihatásait: [értékadás: szolgáltatás megtagadás jellegű támadástípusok szervezet által meghatározott listája vagy egy elfogadott listára való hivatkozás].

RV-7 A határok védelme
Intézkedés: Az informatikai rendszer figyeli és ellenőrzi az informatikai rendszer külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációkat.

Intézkedés bővítése:
a) A szervezet a nyilvánosan hozzáférhető informatikai rendszer összetevőket (pl. nyilvános web szervereket) elkülönített alhálózatokban helyezi el, elkülönített fizikai hálózati interfészekkel.
   Megjegyzés: Nyilvánosan hozzáférhető informatikai rendszer összetevő lehet például a web szerver.
b) A szervezet meggátolja a nyilvános hozzáférést a szervezet belső hálózatához, kivéve azon eseteket, amikor a hozzáférés megfelelő védelmi intézkedések közbeiktatásával történik.
c) A szervezet korlátozza a hozzáférési pontok számát az informatikai rendszerhez, hogy jobban monitorozható legyen a kijövő és bejövő hálózati forgalom.
d) A szervezet kialakít egy felügyelt kapcsolódási pontot (határvédelmi eszközöket egy hatékony biztonsági architektúrában) a külső telekommunikációs szolgáltatóval,

létrehozva azokat az intézkedéseket, amelyek szükségesek az átvitt információ bizalmasságának és integritásának védelméhez.

e) Az informatikai rendszer alapból tilt és kivételként engedélyez csak minden hálózati forgalmat (vagyis minden tiltva, engedélyezés kivételes esetben).
f) A szervezet megakadályozza az információ jogosulatlan átjuttatását a rendszer határain, vagy bármilyen jogosulatlan kommunikációt a határon keresztül, ha valami hiba történik a határvédelmi mechanizmusokban.

RV-8 Az adatátvitel sértetlensége

Intézkedés: Az informatikai rendszer megvédi a továbbított információk sértetlenségét.

Intézkedés bővítése:

a) A szervezet kriptográfiai mechanizmusokat alkalmaz, hogy biztosítsa az információk adatátvitel közbeni megváltozásának felismerését, hacsak az átvitel nincsen más alternatív fizikai ellenintézkedésekkel védve.
Megjegyzés: Az alternatív fizikai védelmi intézkedés lehet például egy védett elosztó rendszer.

RV-9 Az adatátvitel bizalmassága

Intézkedés: Az informatikai rendszer megvédi az átvitt információk bizalmasságát.

Intézkedés bővítése:

a) A szervezet kriptográfiai mechanizmusokat alkalmaz, hogy meggátolja az információk adatátvitel közbeni jogosulatlan felfedését, hacsak az átvitel nincsen más alternatív fizikai ellenintézkedésekkel védve.
Megjegyzés: Az alternatív fizikai védelmi intézkedés lehet például egy védett elosztó rendszer.

RV-10 A hálózati kapcsolat megszakítása

Intézkedés: Az informatikai rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, vagy [értékadás: a szervezet által meghatározott időtartam] hosszú inaktivitás után.

RV-12 Kriptográfiai kulcs előállítása és kezelése

Intézkedés: Az informatikai rendszer a kriptográfiai kulcsok előállítására és kezelésére automatikus támogató eljárásokkal ellátott mechanizmusokat, vagy manuális eljárásokat alkalmaz.

RV-13 Jóváhagyott kriptográfia alkalmazása

Intézkedés: Ha az informatikai rendszerben kriptográfiát alkalmaznak, a rendszer minden kriptográfiai műveletét (beleértve a kulcs előállítását is) azt szabványos algoritmussal kell megvalósítani.

RV-14 Sértetlenség védelem nyilvános hozzáférés esetén

Intézkedés: A nyilvánosan elérhető rendszerek esetén az informatikai rendszer megvédi az információk és az alkalmazások sértetlenségét.

RV-15 Telekommunikációs szolgáltatások korlátozása
Intézkedés: Az informatikai rendszer meggátolja a telekommunikációs szolgáltatások együttműködő számítógép-használati mechanizmusainak (pl. video és audio konferenciák) távolról történő aktiválását, és közvetlen jelzéseket biztosít az ilyen mechanizmusok használatról a lokális felhasználók felé (pl. kamera vagy mikrofon használata).

RV-17 Nyilvános kulcsú infrastruktúra tanúsítványok
Intézkedés: Megfelelő hitelesítési rend szerint a szervezet vagy önmaga kiállít nyílt kulcsú tanúsítványt a vagy vásárol nyílt kulcsú tanúsítványt egy hitelesítés-szolgáltatótól.

RV-18 Mobil kód korlátozása
Intézkedés: A szervezet
- korlátozza a mobil kód technika alkalmazhatóságát, erre vonatkozó útmutatót bocsát ki, a mobil kódok rosszindulatú használata által okozott potenciális károk miatt, valamint
- dokumentálja, figyeli és ellenőrzi a mobil kódok információs rendszeren belüli felhasználását. Megfelelő vezető engedélyezi a mobil kódok használatát.

RV-19 Interneten Keresztüli Hangátvitel (VoIP)
Intézkedés: A szervezet:
- használati korlátozásokat vezet be és megvalósítási útmutatót ad az Interneten Keresztüli Hangátvitel (VoIP) technológiákhoz, a rosszindulatú használat esetén okozható károkat felmérve; és
- engedélyezi, figyeli, és ellenőrzi a VoIP használatát az informatikai rendszeren belül.

RV-20 Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)
Intézkedés: Az informatikai rendszer, amely a név/cím feloldó szolgáltatást biztosítja a hiteles adatokon kívül egyéb biztonsági adatokat is visszaad a feloldási kérésekre, mint például az információ eredete és integritási adatok.

RV-21 Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)
Intézkedés: Az informatikai rendszer, amely a név/cím feloldó szolgáltatást biztosítja a helyi klienseknek eredet hitelesítést és adatintegritás ellenőrzést végez a hiteles forrásból származó válaszok esetén, ha a kliensek ezt igénylik.

RV-22 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén
Intézkedés: Egy olyan informatikai rendszernek, amely az egész szervezet név/cím feloldását szolgálja ki hibatűrőnek kell lennie, és működnie kell rajta a szerep szétválasztásnak.

RV-23 Munkaszakasz hitelessége
Intézkedés: Az informatikai rendszer valamilyen mechanizmussal biztosítja a munkaszakaszok hitelességének védelmét.

9.4. A biztonsági intézkedések garanciái

A garancia annak a bizalomnak az alapja, hogy egy információs rendszerben megvalósított biztonsági intézkedések hatékonyak az alkalmazásuk során. A garancia számos módon nyerhető, ideértve az alábbiakat:

- olyan tevékenységek, amelyeket a biztonsági intézkedések fejlesztő, kivitelezői végeztek el a tervezés, fejlesztés, továbbá megvalósítási technológiák és módszerek alkalmazása során;
- a biztonsági intézkedések értékelői által elvégzett tevékenységek a tesztelési és értékelési folyamatban, melyben annak megállapítása történik, hogy az intézkedéseket milyen fokon, mértékben valósították meg helyesen, a terveknek megfelelően működnek-e, és a rendszer biztonsági követelményeinek a kielégítése tekintetében a kívánt hatásokat érik-e el.

Az alábbiakban leírjuk az alacsony, fokozott és kiemelt szintű alapkészletben felsorolt biztonsági intézkedésekhez a minimális garanciális követelményeket.

Az alacsony szintű készletbe tartozó biztonsági intézkedések esetén a hangsúly azon van, hogy az alkalmazott intézkedés megfelel annak az elvárásnak, hogy nincsenek benne nyilvánvaló hibák, és amennyiben réseket fedeznek fel, azokat időben kezelik.

A fokozott készletbe eső intézkedéseknél a hangsúly az intézkedés helyességébe vetett emelt bizalmon van. Bár hibák valószínűleg ekkor is felszínre kerülnek (és eredményesen kezelik azokat), az intézkedés fejlesztője vagy az intézkedés megvalósítója az intézkedés részeként magába foglal speciális képességeket is azon bizalom növelése érdekében, hogy az intézkedés teljesíti feladatát vagy célját.

A kiemelt szintű készletbe tartozó intézkedések esetén a hangsúly arra esik, hogy megkövetelik, hogy az intézkedéseken belül azokat a képességeket, amelyek az intézkedések folyamatos, konzisztens működésének biztosításához szükségesek, és az intézkedés hatékonyságának folyamatos fenntartását segítik. Vannak egyéb garanciális követelmények, amelyek a biztonsági intézkedéseket fejlesztők és kivitelezők rendelkezésére állnak, és kiegészítik a fokozott és magas szintű alapkészlet minimális garanciális követelményeit annak érdekében, hogy védelmet nyújtsanak olyan fenyegetések ellen, amelyeket magasan képzett, erősen motivált és jól finanszírozott veszélyforrás egyedek jelentenek. A védelem ezen szintje olyan információs rendszerek esetén szükséges, melyeknél a szervezet nem hajlandó elfogadni az ilyen típusú veszélyforrások által jelentett kockázatokat.

A garanciális követelmények hierarchikus, egyre szigorodó követelményrendszert alkotnak.

9.4.1. Az alacsony kihatású biztonsági osztály garanciális követelményei

1. A biztonsági intézkedések fejtsék ki hatásukat, és teljesítsék a bennük közvetlenül megfogalmazott funkcionális követelményeket.

2. . A biztonsági intézkedéseket független, erre szakosodott értékelők értékeljék. Az értékelés módszertana feleljen meg a [05] dokumentum alap szintű értékelésének.

Kiegészítő útmutatás: Az alacsony kihatású biztonsági osztály biztonsági intézkedései esetén alapvető elvárás a biztonsági intézkedésekkel szemben, hogy azok nyilvánvaló hibákat ne tartalmazzanak, illetve a feltárt hibák kijavításával soron kívül foglalkozzanak.

9.4.2. A fokozott kihatású biztonsági osztály garanciális követelményei

1. A biztonsági intézkedések fejtsék ki hatásukat, és teljesítsék a bennük közvetlenül megfogalmazott funkcionális követelményeket. Az intézkedések fejlesztői/megvalósítói készítsék el az intézkedések funkcionális leírását olyan részletességgel, amely lehetővé teszi az intézkedések elemzését és tesztelését. Az intézkedések fejlesztői/megvalósítói az intézkedések szerves részeként szerepeltessék a kiosztott felelősségeket és speciális tevékenységeket annak érdekében, hogy amikor az intézkedéseket megvalósítják, azok teljesítsék megkívánt feladatukat vagy céljukat. Ilyen tevékenység például olyan szerkezetű és tartalmú naplórekordok készítése, melyből megállapítható a megkívánt feladat vagy cél teljesülése.

2. A biztonsági intézkedéseket független, erre szakosodott értékelők értékeljék. Az értékelés módszertana feleljen meg a [05] dokumentum fokozott szintű értékelésének.

Kiegészítő útmutatás: A fokozott kihatású biztonsági osztály biztonsági intézkedései esetén alapvető elvárás a biztonsági intézkedésekkel szemben a helyes megvalósítás és működés. A fejlesztőkkel/megvalósítókkal szemben elvárás, hogy különböző dokumentációkat készítsenek, melyek kimutatják, hogy az intézkedések teljesítik feladataikat és céljaikat. A dokumentációk az értékelők számára is szükségesek, hogy elemezhessék és tesztelhessék az intézkedéseket.

9.4.3. A kiemelt kihatású biztonsági osztály garanciális követelménye

1. A biztonsági intézkedések fejtsék ki hatásukat, és teljesítsék a bennük közvetlenül megfogalmazott funkcionális követelményeket. Az intézkedések fejlesztői/megvalósítói készítsék el az intézkedések funkcionális leírását és tervét/megvalósítását olyan részletességgel, amely lehetővé teszi az intézkedések elemzését és tesztelését (ideértve az intézkedést megvalósító összetevők közötti funkcionális interfészeket is). Az intézkedések fejlesztői/megvalósítói az intézkedések szerves részeként szerepeltessék a kiosztott felelősségeket és speciális tevékenységeket annak érdekében, hogy amikor az intézkedéseket megvalósítják, azok folyamatosan és következetesen (azaz az informatikai célrendszer egészében) teljesítsék megkívánt feladatukat vagy céljukat, továbbá segítsék az intézkedések hatékonyságának javítását. Ilyen tevékenység például olyan szerkezetű és tartalmú naplórekordok készítése, melyből megállapítható a megkívánt feladat vagy cél teljesülése.

2. A biztonsági intézkedéseket független, erre szakosodott értékelők mélyrehatóan értékeljék. Az értékelés módszertana feleljen meg a [05] dokumentum kiemelt szintű értékelésének.

3. Az intézkedéseket oly módon dolgozzák ki, hogy nagy biztonsággal támogatni tudják azt, hogy az intézkedések összessége teljes, konzisztens és helyes.

Magyarázat: A kiemelt kihatású biztonsági osztály biztonsági intézkedései esetén alapvető elvárás a biztonsági intézkedésekkel szemben a folyamatos, konzisztens működés és a hatékonyság folyamatos javítása. A fejlesztőkkel/megvalósítókkal szemben elvárás, hogy jelentős munkamennyiséget fektessenek az intézkedések tervezési, fejlesztési, megvalósítási és összetevő integrálási tesztelésébe, valamint ezek támogatásához elkészítsék a kapcsolódó tervezési és megvalósítási dokumentációkat. A kiemelt alapkonfiguráció biztonsági intézkedései esetén ezek a dokumentációk az értékelők számára is szükségesek, hogy mélyrehatóan elemezhessék és tesztelhessék az intézkedések belső összetevőit az intézkedések mélyreható értékelésének részeként. A kiegészítő (3.) garanciális követelmény arra irányul, hogy a magasan képzett, nagymértékben motivált és jól finanszírozott támadók ellen fogalmazzanak meg intézkedéseket. A védelem ezen szintjére olyan informatikai célrendszerekben van szükség, melyekben a szervezet nem fogadja el a fent említett támadókhoz kapcsolódó kockázatokat (sem).

10. Mellékletek

10.1. Rendszer biztonsági előirányzat

Az SST (rendszer biztonsági előirányzat, melyben az értékelés tárgyát a továbbiakban rendszer TOE vagy STOE jelöli) legfontosabb célja a szolgáltató rendszer megvalósított biztonsági képességeinek meghatározása. Ez a dokumentum tartalmazza azokat a lényeges rendszer információkat, amiknek való megfelelést bizonyítja az [05] dokumentumban részletesen leírt értékelési módszertan alapján elvégzett független értékelés. 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.

A szolgáltató rendszer műszaki és üzemeltetési biztonsági intézkedések integrált kombinációjából áll.

Az SST leírja a rendszer azon funkcionális viselkedését és követelményeit, melyek megvalósítják a biztonsági célokat, műszaki és üzemeltetési alapú mechanizmusok együttese által. Az SST tárgyalja továbbá azokat az intézkedéseket, amelyek garanciát jelentenek a szolgáltató rendszer képességeire nézve, hogy azok teljesítsék a funkcionális célokat, mialatt a rendszer a maradványkockázat elfogadható szintjén működik.

Az SST alkalmas kiindulópontot biztosít a szolgáltató rendszerek értékeléséhez. Az SST-nek ezért biztosítania kell a szolgáltató rendszer részletes és magyarázó leírását. A leírásának kellően részletesnek kell lennie, kimutatva, hogy a rendszerben minden kockázatot kielégítő módon kivédenek és minden szervezeti biztonsági szabályt megfelelően érvényre juttatnak műszaki és üzemeltetési intézkedések (illetve az ezeket megvalósító mechanizmusok) együttese által.

A rendszer biztonsági előirányzat elvárt felépítése a termék biztonsági előirányzat felépítésének általánosításával született. Az SST-nek tartalmaznia kell az alábbiakat:

a) a teljes STOE-ra alkalmazható közös elemek;
b) tartományra vonatkozó részek, az STOE-ban meghatározott minden biztonsági tartományra az egyes tartományok egyedi szempontjainak leírása.

A közös elemeknek tartalmaznia kell az alábbiakat:

a) SST bevezetés;
b) megfelelőségi nyilatkozatok;
c) biztonsági probléma meghatározás;
d) biztonsági célok;
e) kiterjesztett összetevő meghatározás;
f) biztonsági követelmények;
g) STOE összefoglaló előírás.

A tartományra vonatkozó részek keretében a rendszert alkotó minden egyes biztonsági tartományra az alábbiakat kell szerepeltetni:

a) biztonsági tartomány bevezetés;
b) biztonsági tartomány megfelelőségi nyilatkozatok;
c) biztonsági tartomány biztonsági probléma meghatározás;
d) biztonsági tartomány biztonsági célok;
e) biztonsági tartomány kiterjesztett összetevő meghatározás;
f) biztonsági tartomány biztonsági követelmények;
g) biztonsági tartomány összefoglaló előírás.

A tartományra vonatkozó rész üres lehet, amennyiben a rendszert nem osztják elkülönülő biztonsági tartományokra. A tartományra vonatkozó részek egyes szakaszai is opcionálisak. Csak akkor kell őket megadni, ha a biztonsági tartományoknak olyan egyedi biztonsági problémái, céljai vagy követelményei vannak, amelyek nem vonatkoznak az STOE egészére.

Egy STOE-re alap rendszer garanciacsomag (SAP-A) választása esetén az alábbi lényeges egyszerűsítések könnyítik meg az SST elkészítését:

a) A biztonsági követelményeket csak kinyilvánítani kell, nem pedig származtatni közvetlenül a biztonsági célokból, közvetve a biztonsági problémából. Ezzel összefüggésben:
   aa) nem kell megadni a biztonsági probléma meghatározást,
   ab) nem kell megadni a biztonsági célok indoklását (visszavezetve a biztonsági problémára),
   ac) nem kell megadni a biztonsági követelmények indoklását (visszavezetve azokat a biztonsági célokra).
b) A biztonsági követelményeket bármilyen mértékadó dokumentumból (szabványból, nyilvános műszaki követelményrendszerből, követelményeket megfogalmazó jogszabályból), és nem csak a félformális CC katalógusokból lehet kivenni.

Egy STOE-re fokozott rendszer garanciacsomag (SAP-F) választása esetén az alábbi lényeges egyszerűsítés könnyíti meg az SST elkészítését:

a) A biztonsági követelményeket csak kinyilvánítani kell, nem pedig származtatni közvetlenül a biztonsági célokból, közvetve a biztonsági problémából. Ezzel összefüggésben:
   aa) nem kell megadni a biztonsági probléma meghatározást,
   ab) nem kell megadni a biztonsági célok indoklását (visszavezetve a biztonsági problémára),
   ac) nem kell megadni a biztonsági követelmények indoklását (visszavezetve azokat a biztonsági célokra).

10.2. Biztonsági napló menedzsment

Egy szervezetnél a különböző rendszerek által kiváltott biztonsági eseményekről sokféle napló állományokban található bejegyzések nyújtanak információt. Ezen napló bejegyzések elsődleges forrásai a biztonsági szoftverek. Szerverek, munkaállomások vagy hálózati eszközök az információk széles skáláját naplózzák rendszer vagy biztonsági eseményként. A felhasználói programok, alkalmazások további jelentős esemény generátorként küldenek információt vagy az operációs rendszer napló állományába, vagy saját napló fájlba. Az IT rendszerek biztonsági naplóinak fajtája száma és mérete jelentősen megnövekedett, ez kiváltotta az igényt a biztonsági napló menedzsmentre, egybe foglalva a biztonsági napló esemény adatainak létrehozását, átvitelét, tárolását, kiértékelését és megsemmisítését. Egy megfelelő eljárásrenddel biztosítható a szükséges mennyiségű és minőségű biztonsági események adatainak elérhetősége a szervezet által szükségesnek tartott időtartam alatt. Az így rendelkezésre álló információk rendszeres kiértékelése a biztonsági incidensek (működési rendellenesség, rosszindulatú tevékenységek vagy a biztonsági szabályok megsértése) észlelése szempontjából kiemelkedő fontos.

A biztonsági napló menedzsment alapvető problémája összhangot teremteni a korlátozottan rendelkezésre álló erőforrások és napló adatok folyamatos beáramlása között. A naplók létrehozását és tárolást elsősorban a nagyszámú forrás, a különböző források adat struktúráinak ellentmondásai és a napló adatok mennyisége nehezíti. Gondoskodni szükséges a napló állományok bizalmasságának, sértetlenségének és rendelkezésre állásának fenntartásáról. Az adatok hatásos és eredményes elemzésére képes rendszer vagy hálózati rendszergazda megléte szintén problémás elem. A biztonsági napló menedzsment kihívásainak való megfelelés négy kulcselemből tevődik össze:

- megfelelő prioritásokkal kezelt a napló menedzsment az egész szervezetre kiterjesztve;
- a napló kezelés területére kidolgozott szabályok és eljárás rendek;
- bevezetett és szakszerűen működtetett naplókezelő infrastruktúra; és
- oktatás, képezés a napló menedzsmenttel kapcsolatos felelősségről.

A napló menedzsment infrastruktúra alatt azon hardver szoftver hálózati elem és tároló eszközök összességét értjük, ami a napló adatok kezelésében részt vesz. Jellemzően tartalmaz olyan funkciókat, ami a napló adatok vizsgálatát, azaz szűrését, csoportosítását, normalizálását és az összefüggések meghatározását segítik. Az infrastruktúra továbbá támogatást nyújt az adatok rendelkezésre állásának biztosításában, a napló adatok kezelésében, mint például, megtekintés elemzés, rotálás, archiválás valamint a napló állományok sértetlenség ellenőrzése.

A naplókezelő infrastruktúra két típusa a syslog alapú központosított naplózó rendszer, vagy egy biztonsági információ- és eseménykezelő célszoftver. Háromrétegű modell valósul meg mind a két esetben. Az első réteg a napló eseményt generáló végberendezést fedi le. A második réteg a központi napló szervert foglalja magába, ami tárolja és egységesíti a napló adatokat. A harmadik réteg a vezérlő, ami monitorozza, megjeleníti a napló adatokat, és kiegészítő funkcióként adminisztrálja a szervert illetve a végberendezéseket. A rétegek közötti kommunikáció általában a szervezet általános hálózati infrastruktúráján történik, de egyes

esetekben létrehozható külön kommunikációs csatorna is. Hálózathoz nem kapcsolódó, de napló menedzsment szempontjából fontos eszközök esetén a napló adatok off-line mozgatásáról külön eljárásrendben kell gondoskodni.

A syslog alapú központosított naplózó infrastruktúra esetén, minden végberendezés gyakorlatilag szabványos formátumú adathalmazt hoz létre és továbbít a szervernek. A syslog meglehetősen egyszerű szabványos protokoll a legtöbb operációs rendszer, hálózati eszköz biztonsági alkalmazás támogatja, használja. Az eredeti syslog szabvány nem nyújtott megfelelő részletezettséget a különböző típusú események kezeléséhez. Mivel nagyon kevés adat mezőt tartalmaz ezért sok forrásból származó napló események információ tartalmának kibontása bonyolult feladat. A syslog fejlesztése idején a biztonságnak még nem volt a maihoz fogható jelentősége, így nem tartalmaz megoldásokat a bizalmasság, sértetlenség, és rendelkezésre állás problémáira. A syslog alapú rendszerek biztonságának növelésére jött létre az RFC 3195 szabvány [26], ami megnövelt biztonsági képességeket fogalmaz meg. Különböző syslog megvalósításokhoz kiegészítő funkciókén hozzáadásra került, a megbízható adatküldés, rejtjeles adatátvitel, integritás védelem, hitelesítés automatikus esemény reagálás, napló fájl rejtjelzés és esemény szint korlátozás. Az alkalmazó szervezetnek tekintettel kell lenni a különböző syslog megvalósítások biztonsági képességei között felmerülő esetleges kompatibilitási problémákra.

A biztonsági információ és eseménykezelő célszoftver (security information and event management (SIEM)) a syslog szabványos struktúrájától eltérően speciális, gyártó függő szabadalmaztatott adat formátumot alkalmaz. A SIEM rendszerekben a szerver elsősorban az adatok elemzését végzi, míg a tárolás elkülönített adatbázis szerveren történik. A legtöbb SIEM termék esetében a végberendezésekre szükséges egy saját agent telepítése, aminek a funkciója a napló események szűrése, csoportosítása, és a megfelelő adat struktúra kialakítása. Az agent feladata továbbá a napló adatok eljuttatása a szerverhez valós időben vagy kis késleltetéssel.

A SIEM termékek a lehetséges napló források formátumainak többségét támogatják beleértve a korábban említett szabványos syslog-ot is. Mivel a különböző napló források adat formátumainak általában minden mezőjét képesek értelmezni, ezért a SIEM alapú napló menedzsment infrastruktúra magasabb fokon képes a sokféle végberendezés által generált napló adathalmazt formailag egységesíteni, vizsgálni és bennük összefüggéseket elemezni, mint a syslog alapú infrastruktúra. A SIEM termékek összetett környezetből származó adatok alapján képesek a jelentőséggel bíró eseményeket felderíteni és amennyiben szükséges automatikusan reakciót kiváltani. A SIEM rendszerek grafikus elemzés lehetőséget, tudásbázis kezelést, eseménykövetést, jelentéskészítést valamint a tárolt információk összefüggés elemzést tartalmazhat beépített funkcióként. Felkészültek továbbá a napló adatok bizalmasságának, sértetlenségének és rendelkezésre állásának terén.
Ugyan a SIEM rendszerek robosztusabb napló menedzsment képességekkel rendelkeznek a syslog alapú rendszereknél, de megvalósításuk bonyolultabb és drágább. Valamint a SIEM rendszerek agentjei erőforrás igényesebbek a végberendezéseken, mint a syslog kliens.

Egy jól működő napló menedzsment infrastruktúra kialakításának és bevezetésének előfeltétele a megfelelő tervezés és előkészítés. A szervezet igényeit kielégítő kiegyensúlyozott megbízható, hatékony naplókezelés csak így jöhet létre valós értéket teremtve az alkalmazó szervezeten belül.

A napló menedzsment tervezési folyamata részeként, a szervezetnek meg kell határoznia a naplókezelésben érintett egyének és csoportok szerepét és felelősségét. Így például a rendszer és hálózati rendszergazdák felelősek:

- a rendszer és hálózati eszközök naplózásának beállításáért;
- azok naplóeseményeinek rendszeres vizsgálatáért;
- ezen tevékenységgel kapcsolatos jelentések elkészítéséért; és
- a naplózó eszközök valamint a napló állományok karbantartásáért.

A biztonsági rendszergazdák felelősek:

- a log menedzsment infrastruktúra kezelésért működéséért;
- a biztonsági eszközök naplózásának beállításáért;
- ezen tevékenységgel kapcsolatos jelentések elkészítéséért; és
- a napló menedzsment egyéb szereplőinek támogatásáért.

A napló menedzsment bevezetése során felelősség ruházódik továbbá az alkalmazás fejlesztőre, a felülvizsgálóra, incidens kezelőre és a szervezet vezetőségére is.

A szerepek és felelősségek kiosztásakor figyelembe kell venni az elérhető előnyöket rendszer, és infrastruktúra szinten. A szervezetnek meg kell adni a szükséges támogatást a rendszer szintű adminisztrátoroknak úgy, mint, képzés, az információáramlási eljárásrend, technikai segítség és maguk a naplókezelő eszközök. A szervezetnek meg kell határoznia a naplókezelés és monitorozással szemben támasztott követelményeket és célokat. Ezen döntések alapján kell kibocsátani egy szabályzatot, ami a napló menedzsment minden aspektusában, - létrehozás, átvitel, tárolás, kiértékelés és megsemmisítés -, egyértelműen meghatározza a kötelező érvényű elvárásokat és javasolt ajánlásokat. Meg kell győződni arról, hogy a szervezet más a napló menedzsmenttel kapcsolatba hozható szabályzatai, eljárásrendjei szinkronban vannak-e a napló menedzsment elvárásaival, valamint a funkcionális és működési követelményekkel. A szervezet napló kezelési szabályzatában fontos kitérnie a naplózással kapcsolatos törvényi/jogi elvárásokra, mint például a bizonyítékként felhasználható napló állományok megőrzési kötelezettségének időtartama. A naplókezelési szabályzatot a szervezetnek időszakonként felülvizsgálni és igény szerint módosítania kell.

A naplózással kapcsolatos követelmények és ajánlások létrehozásával párhuzamosan elemezni kell a megvalósításhoz és működtetéshez szükséges technológiák és erőforrások lehetőségeit kitérve azok biztonsági vonatkozásaira, és a szervezetre vonatkozó törvényi jogi környezetre. Általánosságban egy szervezet csak a legfontosabb adatok naplózását és vizsgálatát írja elő követelményként, és egyéb adatok vonatkozásában csak ajánlásokat fogalmaz meg, amik betartása rendelkezésre álló idő és erőforrás függvényében történhet. Egyes esetekben a szervezet azt vállalja, hogy minden vagy közel minden lehetséges napló adatot létrehoz és tárol egy rövid időszakra előre nem meghatározva annak felhasználási célját a rendszer felhasználhatóságának és az erőforrás optimális kezelésének kárára.

A szabályok szerepkörök és felelősségek meghatározását követően, a szervezetnek meg kell tervezni úgy a napló menedzsment infrastruktúrát, hogy az a követelményeknek való megfelelést hatékonyan képes legyen támogatni. A tervezési időszakban az egész szervezetre vonatkozóan átgondolandó a rendszerbefoglalt valamint az egyedi napló adat forrásokkal

kapcsolatos jelenlegi és belátható jövőbeni igényeket. A tervezés során a következő tényezőkre kell tekintettel lenni:

- a feldolgozandó napló adatmennyiség;
- on-line és offline adat tárolás;
- az adatokkal kapcsolatos biztonsági igények; és
- a napló kiértékelés idő és emberi erőforrás igénye.

A rendszer és infrastruktúra szinten dolgozó adminisztrátorok a felelősségi körükbe tartózó rendszerek által rögzített naplókkal kell foglalkozniuk. Az elvégzendő feladatok körébe tartozik a napló forrás beállítása, napló elemzés elvégzése, az azonosított eseményekre történő kezdeti reagálás és a hosszútavú napló adat tárolás kezelése. A rendszer szintű adminisztrátor állítja be a naplóforrásokat, hogy azok a megfelelő információkat az elvárt formában és helyen szolgáltassák, illetve gondoskodik ezen információk megőrzéséről a szükséges ideig. A beállítások megtervezésekor nemcsak a végberendezéssel kapcsolatos, hanem a napló menedzsment infrastruktúrára más komponenseire történő hatásokat is figyelembe kell venni. Be kell állítani a megfelelő időszakokra vagy betelés esetre a napló rotációkat, illetve be kell állítani a rendszer viselkedését abban az esetben, ha az nem tud megfelelően reagálni a napló betelés esetére. A rendszer és infrastruktúra szinten dolgozó adminisztrátorok felelőssége továbbá a régi szükségtelen napló adatok megsemmisítése törlése, a napló adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megtartása. További kötelezettséget jelent a rendszer napló tevékenységének folyamatos fenntartása a folyamatok monitorozásával, teszteléssel, szoftver frissítések alkalmazásával, és új eszközök telepítésével.

Szükséges a szervezetnek arról döntenie hogyan osztja meg a kiértékelési feladatot a rendszer és infrastruktúra szinten dolgozó adminisztrátorok között. A felelősség szétosztásakor koncentrálni kell egyrészről a sokféle, de egyedi bejegyzések relatív fontosságára másrészről az összefüggésekre, ami rámutathat a naplóbejegyzések valódi értelmére. A kiértékelés végrehajtásának kulcseleme, hogy az vizsgáló ismeri, érti a rendszerekhez tartozó tipikus működést. E tudás megszerzésére a leghatásosabb mód a napló bejegyzések napi szintű rendszeres vizsgálata. Így kiszűrhető a fontos információt tartalmazó bejegyzések és azok, amik értelmezése nehézségbe ütközik. A rendszer szintű adminisztrátor azokat az eseményeket értékeli, amik a rendszer részletes ismerete nélkül értelmezhetetlenek. Amennyiben szignifikáns bejegyzést talál, az incidens reagálási szabályok alapján el kell döntenie és követnie a megfelelő eljárásrendet vagy a problémát visszaminősítve - például alacsony kihatású működési probléma - saját hatáskörben reagálnia. A rendszergazdának a reagálás részeként képesnek kell lennie a naplózási beállítások megváltoztatására a naplóesemények elburjánzásának megakadályozása vagy további információ gyűjtése céljából.

A szervezetnek rendszeresen tesztelnie és felül kell vizsgálnia a naplózási szabályzatát, folyamatait, és eljárásait annak érdekében, hogy azok valóban a szervezet által előírt módon zajlanak mind infrastrukturális mind rendszer szinten. Időszakonként át kell vizsgálni a naplókezelő infrastruktúra tervét és a szükséges változtatásokat meg kell tenni. A napló kezelés folyamatainak és eljárásainak rendszerét szintén rendszeresen felül kell vizsgálni a megváltozott környezet és az új veszélyeknek való hatékony ellenálló képesség fenntartása érdekében.

10.3. Elektronikus hitelesítés

Az elektronikus hitelesítés továbbiakban hitelesítés az IT rendszernek bemutatott felhasználó azonosság megbízható elfogadásának folyamata. A rendszerek a hitelesített személyekről el tudják dönteni, hogy az adott elektronikus tranzakció végrehajtására a személy feljogosított-e. A hitelesítés a legtöbb esetben hálózaton keresztül történik, ami lehet nyílt, mint például az Internet, vagy korlátozott hozzáférésű szervezeti belső hálózat.

A hitelesítés folyamatának első lépése a regisztráció. Egy *kérelmező* kinyilvánítja akaratát egy *regisztrálónak*, hogy *alanya* kíván lenni egy *hitelesítési szolgáltatást nyújtó* rendszernek (Credential Service Provider (CSP)), ami létrehoz, vagy regisztrál egy titkot (a továbbiakban *tokent*), valamint kibocsáthat egy *igazolást,* amiben a regisztrálónál ellenőrzött nevet és egyéb tulajdonságokat logikailag hozzákapcsolja tokenhez. A token vagy az igazolás használható fel a későbbi hitelesítési folyamatokba. A kérelmező neve lehet ellenőrzött név vagy álnév. Az ellenőrzött név hozzákapcsolódik egy valódi ember személyazonosságához, és ezt a kérelmezőnek bizonyítania kell mielőtt az ellenőrzött névhez kapcsolt igazolást megkapta, illetve a tokenjét regisztrálta, hogy az állított személyazonosság létező, és a kérelmezőhöz tartozik. A regisztráló és a CSP között mindig van kapcsolat. A legegyszerűbb és vélhetően a leggyakoribb eset, amikor mindkét folyamat egy entitás különböző funkciói által valósul meg.

A hitelesítés folyamatában a hitelesítést kérőt *igénylőnek*, az azonosságot megvizsgálót *ellenőrzőnek* hívjuk. Amikor az igénylő sikeresen bizonyította a token birtoklását az ellenőrzőnek egy hitelesítési protokoll szerint, az ellenőrző képes meghatározni, hogy az igénylő valóban azonos az állított személlyel. A hitelesítés során kizárólag az alany azonossága kerül megállapításra az nem, hogy az alany jogosultsága mire terjed ki. A feljogosítás egy külön eljárás ahol az alany azonossága és egyéb információk alapján eldöntésre kerül a kért tranzakció végrehajthatósága. A legtöbb esetben a hitelesítési szolgáltatást megosztva használják a különböző alkalmazások, de a feljogosítás folyamata már az alkalmazáson belül valósul meg.

10.3.1. Tokenek

A token olyan valami, amit az igénylő birtokol vagy felügyelete alatt tart és felhasználható az igénylő személyazonosságának hitelesítésére. Mivel a hitelesítés során a rendszer vagy alkalmazás az igénylőt hálózaton keresztül hitelesíti a hitelesítéshez használandó titkot a tokent védeni kell. A token lehet például egy kriptográfiai kulcs, ami rejtjelezve van egy emlékezeti jelszóból kialakított másik kulccsal. Így a támadónak a rejtjelzett kulcson kívül a jelszót is meg kell szereznie a token felhasználásához.

A hitelesítő rendszereket gyakran kategorizálják az szerint, hogy hány hitelesítési faktort vegyítenek. Általánosan elfogadottnak az alábbi három faktort tekinthető:

- Valamit tudni (emlékezeti jelszó)
- Valamit birtokolni (chip kártya)
- Valaminek lenni (ujjlenyomat)

A mindhárom faktort alkalmazó hitelesítő rendszer erősebbnek számít az egy vagy két faktort alkalmazóknál. Egy rendszer a több faktort közvetlenül is átadhatja az ellenőrzőnek, de egyenértékű az a megoldás is, amikor az ellenőrzőnek adandó titok számára az egyik faktor nyújt védelmet. Például egy hardver eszköz tartalmaz egy kriptográfiai kulcsot, de az ahhoz való hozzáférés vagy jelszó, vagy biológiai jellemző megadásával lehetséges. Így ez az eszköz annak ellenére valósít meg hatékony kétfaktoros hitelesítést, hogy az ellenőrzőnek csak a kriptográfiai kulcs vizsgálata a feladat.

A titok lehet aszimmetrikus kulcs pár vagy megosztott titok. Előbbi esetben a token az alany privát kulcsa, az ellenőrző a nyilvános kulcs ismeretében meggyőződhet, hogy az igénylő birtokolja a tokent, így azonos az alannyal.

A megosztott titok az lehet szimmetrikus kulcs vagy jelszó. A jelszó mivel általában megjegyezhető inkább a valamit tudni, míg a szimmetrikus kulcs inkább a valamit birtokolni faktorhoz tartozik. A jelszó mivel lényegesen kevesebb lehetséges értéket vehet fel, mint a kriptográfiai kulcs ezért sérülékenyebb a támadások ellen. Sőt a jelszó begépelése lehetőséget teremt a támadónak akár billentyűzet lefigyelés vagy egyszerű kilesés támadásra.

A tokenek négy fő kategóriáját lehet megkülönböztetni, amik egy vagy több hitelesítési faktort kezelnek.

Hard token: Olyan hardver eszköz, ami védetten tartalmaz kriptográfiai kulcsot. A hitelesítés az eszköz birtoklásán és a kulcs fölötti ellenőrzés bizonyításán alapul. Főbb tulajdonságai:

- jelszó vagy biometrikus adat megadásához köti a kriptográfiai kulcs aktiválását;
- meggátolja a kriptográfiai kulcs exportálását; és
- általános 2-es szintű, de fizikai biztonság területén 3-as szintű FIPS 140-2 tanúsítvánnyal rendelkezik.

Szoft token: Merevlemezen vagy más médián tárolt kriptográfiai kulcs. A hitelesítés a kulcs fölötti ellenőrzés bizonyításán alapul. Főbb tulajdonságai:

- A soft token kriptográfiai kulcsát rejtjelezni egy aktivizáló adatból származtatott kulccsal, ami tipikusan egy emlékezeti jelszó;
- a tartalmazott kriptográfiai modul lehet hardver eszköz vagy szoftver modul, és legalább 1-es szintű FIPS 140-2 tanúsítvánnyal, vagy hazai akkreditált vizsgálólaboratórium által végzett megfelelőség vizsgálatot tanúsító igazolással rendelkezik; és
- az aktivizáló adatot minden hitelesítési kezdeményezéshez külön elvárja és a hitelesítéshez használt kriptográfiai kulcs megoldott védtelen másolatát a használat után kötelezően eltörli.

Egyszer használatos jelszó token: Olyan személyre szabott eszköz, ami minden hitelesítés során különböző jelszót alkalmaz. Az eszköz tartalmazhat beviteli egységet karakteres vagy biometrikus adat megadására, illetve közvetlen számítástechnikai interfészt (általában USB). A jelszó generálását egy elfogadott szabványos blokk rejtjelző algoritmus vagy lenyomatoló függvény végzi, kiindulva a tokenben tárolt szimmetrikus kulcs és egy nonce keverékéből. A nonce lehet időinformáció, egy számláló aktuális értéke vagy az ellenőrző által megadott felhívó adat. Az egyszer használatos jelszó az eszközön kijelzésre kerül, és a felhasználó adja

meg a rendszernek. Ritkább esetben közvetlen kommunikáció is megvalósul. A jelszó élettartama limitált, általában egy percnél nem hosszabb.

Jelszó token: A titkot az igénylő memorizálja és felhasználja személyazonosságának hitelesítésére. A jelszó általában karakter sorozat, de létezik, képek piktogramok sorozatának megjegyzését igénylő rendszer is.

10.3.2. Tokenek biztonsági szintjei

A jelszavas hitelesítés könnyen megvalósítható és népszerű eljárás nagyon sok rendszer alkalmazza hitelesítési megoldásként. Ebben az esetben az azonosság megszemélyesítéséhez elegendő a jelszót ismerete. Mivel a felhasználók a hosszú és bonyolult jelszavak megjegyzésére gyakorlatilag ritkán vagy egyáltalán nem képesek, ezért a jelszó token támadások széles skálájával szemben sérülékeny úgy, mint kitalálás, szótártámadás, vagy a lehetséges értékkészletnek teljes kipróbálása. A tapasztalatok azt mutatják továbbá, hogy a felhasználók sérülékenyek “social engineering” támadás ellen, önként megadják a jelszavaikat megbízhatónak vélt, de ismeretlen támadónak.

Hard és szoft tokenek esetében két dolgot kell a megszemélyesítést igénylőnek birtokolnia, egyrészt magát a tokent és a jelszót, vagy azt a biometriai tulajdonságot, ami lehetővé teszi a kulcshoz való hozzáférést. Tehát mind a hard, mind a szoft token nagyobb garanciát biztosít, mint a jelszó token önmagában. Mivel a hard token fizikai eszköz, ezért annak ellopását könnyebb észrevenni, mint az esetleg másolható szoft tokenét, ezért használatával az elérhető biztonság nagyobb.

Az egyszer használatos jelszó token hasonló a hard tokenhez. Felhasználható jelszóval párosítva, esetleg biometriás aktiválással történő többfaktoros hitelesítéshez, azonban ezek az eszközök nem hoznak létre a hitelesítés folyamatában megosztott munkaszakasz kulcsot.

10.3.3. A hitelesítési tokenek megbízhatósági garancia szintjei.

A hitelesítés garancia szintje alatt azt értjük, hogy az elfogadó milyen szinten fogadhatja el a kérelmező személyazonosságát megegyezőnek a hitelesítési folyamat befejezése után az alanyéval. Az alap garancia szint megfelel az egyfaktoros hitelesítésnek. Az emelt szint megköveteli a kétfaktoros hitelesítést. A magas garanciaszint a kétfaktoros hitelesítést tanúsított hardver eszközzel történő alkalmazását követeli meg.

A garancia szinteken alkalmazható token típusok

Token típus	Alap	Emelt	Magas
	garancia szinten		
Jelszó token	✓	—	—
Szoft token	✓	✓	—
Egyszer használatos jelszó token	✓	✓	—
Hard token	✓	✓	✓

A garancia szinteken kivédett támadás típusok

Kivédett támadás típus	Alap	Emelt	Magas
	garancia szinten		
On-line kitalálás	✓	✓	✓
Visszajátszás	✓	✓	✓
Lehallgatás	✓	✓	✓
Ellenőrző megszemélyesítése	—	✓	✓
Man-in-the-middle	—	✓	✓
Munkaszakasz ellopás	—	—	✓

Alkalmazandó hitelesítés protokoll típus

Hitelesítési protokoll típusok	Alap	Emelt	Magas
	garancia szinten		
Aszimmetrikus kulcsbirtoklás bizonyítása	✓	✓	✓
Szimmetrikus kulcsbirtoklás bizonyítása	✓	✓	✓
Védett csatornán küldött jelszó	✓	—	—

A garancia szintek megfeleltetése a követelményrendszer biztonsági osztályainak

Hitelesítés típusa	Alacsony	Fokozott	Kiemelt
	biztonsági osztály minimális hitelesítési minimálisan elvárt garancia szintje		
Távoli	alap	emelt	magas
Helyi	alap	alap	emelt

11. Bibliográfia

National Institute of Standards and Technology Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995

Common Methodology for Information Technology Security Evaluation; Evaluation Methodology September 2007 Version 3.1 Revision 2

MSZ ISO/IEC 15408-1:2003 Informatika – Biztonságtechnika – Az informatikai biztonságértékelés közös szempontjai – 1. rész: Bevezetés és általános modell, 2. rész: A biztonság funkcionális követelményei, 3. rész: A biztonság garanciális követelményei

Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 1. számú segédlet: Modell és folyamatok

Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 2. számú segédlet: Útmutató a megbízók számára

Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 3. számú segédlet: Útmutató a fejlesztők számára

Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 4. számú segédlet: Útmutató az értékelők számára

Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 5. számú segédlet: MIBÉTS értékelési módszertan

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security /CCRA 2000 May/

BSI: Transition guide for ALC, ACM, ADO and AGD /Version 2.0, 22.01.2008/

BSI: Guidelines for Developer Documentation according to Common Criteria Version 3.1

12. Rövidítésgyűjtemény

CAP: Composed Assurance Packages (összetett garancia csomagok)
CC: Common Criteria (Közös szempontok)
CCRA: Common Criteria Recognition Arrangement (CC elfogadási egyezmény)
CEM: Common Evaluation Methodology (Közös értékelési módszertan)
CSP: Credential Service Provider (hitelesítési szolgáltatást nyújtó)
CRC: Cyclic Redundancy Check (ciklikus redundanciavizsgálat)
DMZ: DeMiltarizált Zóna
DNS: Domain Name System
DOS: Denial of Services (szolgáltatás megtagadás támadás)
EAL: Evaluation Assurance Level (értékelési garanciaszint)
EAP: Extensible Authentication Protocol
FIPS: Federal Information Processing Standards
IEC: International Electrotechnical Commission
IPSec: Internet Protokol Security
ISO: International Organization for Standardization
IT: Information technology (informatika)
MAC: Media Access Control
MIBÉTS: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
MSZ: Magyar Szabvány
NIST: National Institute of Standards and Technology
PDF: Portable Document Format
PP: Protection Profile (védelmi profil)
SF: Security Function (biztonsági funkció)
SFR: Security Functional Requirements (Funkcionális biztonsági követelmények)
SIEM: Security Information and Event Management (biztonsági információ és esemény kezelés)
SOF: Strength of Function (funkcióerősség)
SST: System Security Target (rendszer biztonsági előirányzat)
ST: Security Target (biztonsági előirányzat)
STOE: System Target of Evaluation (rendszer értékelés tárgya)
TCP/IP: Transmission Control Protocol/Internet Protocol
TLS: Transport Layer Security
TOE: Target of Evaluation (az értékelés tárgya)
TSF: TOE Security Functions (a TOE biztonsági funkciói)
TSFI: TOE Security Function Interface (a TOE biztonsági funkció interfész)
TSP: TOE Security Policy (a TOE biztonsági szabályzata)
VoIP: Voice over Internet Protokol (interneten keresztüli hangátvitel)
VPN: Virtual Private Network (Virtuális Magán Hálózatot)

13. Fogalomtár

Biometria: A biometria a felhasználó bizonyos testi tulajdonságainak használata például azonosítás és hitelesítés során.

Bizalmasság: A bizalmasság egy olyan biztonsági tulajdonság, amely lehetővé teszi, hogy az információ a jogosulatlan szubjektumok számára ne legyen elérhető, vagy ne kerüljön nyilvánosságra.

Hitelesség: A hitelesség az entitás egy olyan biztonsági tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz. A hitelesség (adatok esetében) az adat olyan biztonsági tulajdonsága, amely arra vonatkozik, hogy az adat (bizonyíthatóan) egy elvárt forrásból származik. Ehhez az szükséges, hogy az informatikai kapcsolatban lévő partnerek kölcsönösen (és egyértelműen) felismerjék egymást, és ez az állapot a kapcsolat teljes ideje alatt fennálljon.

IT: (informatika): Az informatika az információ ábrázolásának, elrendezésének, feldolgozásának, kezelésének a tudománya.

Informatikai biztonság: A informatikai biztonság az információs rendszer tulajdonsága, amely a rendszer biztonsági követelményeinek és céljainak teljesülését mutatja.

Informatikai rendszer: Informatikai rendszernek nevezzük azokat a számítógépeket, hálózatot, hardver elemeket, szoftver elemeket és telekommunikációt, amelyekre az alkalmazói rendszerek és az egyes informatikai szolgáltatások ráépülnek.

Életciklus: Egy rendszer tervezésétől a visszavonásáig vagy megsemmisítéséig tartó, egymás utáni állapotok által meghatározott folyamat, a következő fő szakaszokkal: kezdeti, fejlesztési vagy beszerzési, megvalósítási, üzemeltetési vagy karbantartási és visszavonási szakasz.

Letagadhatatlanság: Olyan biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az informatikai rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően.

Rendelkezésre állás: A rendelkezésre állás az információs rendszer olyan jellemzője, amely az adatok és információk meghatározott módon, helyen, mennyiségben, minőségben, időben stb. történő elérésére vonatkozik. Rendelkezésre álláson azt a valószínűséget értjük, amellyel egy meghatározott időintervallumon belül az informatikai rendszer a tervezésekor meghatározott funkcionalitásnak megfelelően, a feljogosított felhasználók által használható, azaz a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

Sértetlenség: A sértetlenség egy olyan biztonsági tulajdonság, amely azt jelenti, hogy az adatot, információt vagy programot csak az arra jogosultak változtathatják meg és azok észrevétlenül nem módosulhatnak. A sértetlenséget általában az információkra, adatokra, illetve a programokra értelmezik. Ez az alap-veszélyforrás a programokat is érinti, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani. A sértetlenség fogalma alatt gyakran értik a sérthetetlenségen túli teljességet, továbbá az

ellentmondás mentességet és a helyességet, együttesen: adat-integritást. Az integritás ebben az összefüggésben azt jelenti, hogy az információ valamennyi része rendelkezésre áll és elérhető.

Tanúsítvány: A tanúsítvány a CSP által kibocsátott olyan igazolás, amely az igénylő nyilvános kulcsát az igénylő személyéhez kapcsolja a CSP elektronikus aláírásával.

Token: A token (többnyire személyhez kötött) olyan kisméretű (biztonságos) eszköz, amelyből a hitelesítő adatok kinyerhetők.

Veszély: Az a lehetőség, hogy egy adott veszélyforrás (veszélyokozó egyed) sikeresen kihasznál egy sebezhetőséget.