Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Hozzáférés-felügyelet

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

2.1. Szabályzat és eljárásrendek 9
2.2. Fiókkezelés 12
2.3. Fiókkezelés – Automatizált fiókkezelés 16
2.4. Fiókkezelés – Automatizált ideiglenes és vészhelyzeti fiók kezelés 18
2.5. Fiókkezelés – Fiókok letiltása 20
2.6. Fiókkezelés – Automatikus naplózási műveletek 22
2.7. Fiókkezelés – Inaktivitásból fakadó kijelentkeztetés 24
2.8. Fiókkezelés – Dinamikus jogosultságkezelés 26
2.9. Fiókkezelés – Privilegizált fiókok 28
2.10. Fiókkezelés – Dinamikus fiókkezelés 30
2.11. Fiókkezelés – Megosztott és csoportfiókok használati korlátozása 32
2.12. Fiókkezelés – Használati feltételek 34
2.13. Fiókkezelés – Fiókok szokatlan használatának felügyelete 36
2.14. Fiókkezelés – Magas kockázatú személyek fiókjának letiltása 38
2.15. Hozzáférési szabályok érvényesítése 40
2.16. Hozzáférési szabályok érvényesítése – Kettős jóváhagyás 42
2.17. Hozzáférési szabályok érvényesítése – Kötelező hozzáférés-ellenőrzés 44
2.18. Hozzáférési szabályok érvényesítése – Mérlegelés alapú hozzáférés-felügyelet 47
2.19. Hozzáférési szabályok érvényesítése – Biztonsággal kapcsolatos információk 50
2.20. Hozzáférési szabályok érvényesítése – Szerepkör alapú hozzáférés-ellenőrzés 52
2.21. Hozzáférési szabályok érvényesítése – Hozzáférési engedélyek visszavonása 54
2.22. Hozzáférési szabályok érvényesítése – Szabályozott továbbítás 56

2.23. Hozzáférési szabályok érvényesítése – Hozzáférés-ellenőrző mechanizmusok ellenőrzött felülbírálata 58

2.24. Hozzáférési szabályok érvényesítése – Meghatározott információtípusokhoz való hozzáférés korlátozása 60

2.25. Hozzáférési szabályok érvényesítése – Alkalmazás-hozzáférés biztosítása és érvényesítése 62

2.26. Hozzáférési szabályok érvényesítése – Tulajdonság alapú hozzáférés-ellenőrzés 64

2.27. Hozzáférési szabályok érvényesítése – Kötelező és mérlegelés alapú hozzáférés-felügyelet 66

2.28. Információáramlási szabályok érvényesítése 69

2.29. Információáramlási szabályok érvényesítése – Az objektumok biztonsági tulajdonságai 72

2.30. Információáramlási szabályok érvényesítése – Feldolgozási tartományok 74

2.31. Információáramlási szabályok érvényesítése – Az információáramlás dinamikus irányítása 76

2.32. Információáramlási szabályok érvényesítése – Titkosított információk áramlásának irányítása 78

2.33. Információáramlási szabályok érvényesítése – Beágyazott adattípusok 80

2.34. Információáramlási szabályok érvényesítése – Metaadat 82

2.35. Információáramlási szabályok érvényesítése – Egyirányú információáramlási mechanizmusok 84

2.36. Információáramlási szabályok érvényesítése – Biztonsági szűrők 86

2.37. Információáramlási szabályok érvényesítése – Emberi beavatkozással történő felülvizsgálat 88

2.38. Információáramlási szabályok érvényesítése – Biztonsági szűrők engedélyezése és kikapcsolása 90

2.39. Információáramlási szabályok érvényesítése – Biztonsági szűrők konfigurálása 92

2.40. Információáramlási szabályok érvényesítése – Adattípus azonosítók 94

2.41. Információáramlási szabályok érvényesítése – Adatok alkotóelemeire való bontása..... 96

2.42. Információáramlási szabályok érvényesítése – Biztonsági szabályzat szűrési korlátozások 98

2.43. Információáramlási szabályok érvényesítése – Nem engedélyezett információk észlelése 100

2.44. Információáramlási szabályok érvényesítése – Tartományhitelesítés..... 102

2.45. Információáramlási szabályok érvényesítése – Metaadatok ellenőrzése 104

2.46. Információáramlási szabályok érvényesítése – Jóváhagyott megoldások 106

2.47. Információáramlási szabályok érvényesítése – Információáramlás fizikai vagy logikai szétválasztása 108

2.48. Információáramlási szabályok érvényesítése – Hozzáférés korlátozása..... 110

2.49. Információáramlási szabályok érvényesítése – Nem nyilvános információ módosítása 112

2.50. Információáramlási szabályok érvényesítése – Belső normalizált formátum..... 114

2.51. Információáramlási szabályok érvényesítése – Adattisztítás 116

2.52. Információáramlási szabályok érvényesítése – Szűrési műveletek ellenőrzése..... 118

2.53. Információáramlási szabályok érvényesítése – Redundáns szűrőmechanizmusok..... 120

2.54. Információáramlási szabályok érvényesítése – Lineáris szűrőcsatornák..... 122

2.55. Információáramlási szabályok érvényesítése – Összehangolt tartalomszűrés 124

2.56. Információáramlási szabályok érvényesítése – Több folyamatot használó szűrőmechanizmusok 126

2.57. Információáramlási szabályok érvényesítése – Hibás tartalom átvitelének megakadályozása..... 128

2.58. Információáramlási szabályok érvényesítése – Folyamatkövetelmények az információ átviteléhez..... 130

2.59. Felelősségek szétválasztása 132
2.60. Legkisebb jogosultság elve 135
2.61. Legkisebb jogosultság elve – Hozzáférés biztosítása a biztonsági funkciókhoz 137
2.62. Legkisebb jogosultság elve – Nem privilegizált hozzáférés biztosítása a nem biztonsági funkciókhoz 139
2.63. Legkisebb jogosultság elve – Hálózati hozzáférés a privilegizált parancsokhoz 141
2.64. Legkisebb jogosultság elve – Elkülönített feldolgozási tartományok 143
2.65. Legkisebb jogosultság elve – Privilegizált fiókok 145
2.66. Legkisebb jogosultság elve – Privilegizált hozzáférés szervezeten kívüli felhasználók számára 147
2.67. Legkisebb jogosultság elve – Felhasználói jogosultságok felülvizsgálata 149
2.68. Legkisebb jogosultság elve – Jogosultsági szintek kódvégrehajtáshoz 151
2.69. Legkisebb jogosultság elve – Privilegizált funkciók használatának naplózása 153
2.70. Legkisebb jogosultság elve – Nem-privilegizált felhasználók korlátozása 155
2.71. Sikertelen bejelentkezési kísérletek 157
2.72. Sikertelen bejelentkezési kísérletek – Mobil eszköz törlése vagy alaphelyzetbe állítása 160
2.73. Sikertelen bejelentkezési kísérletek – Biometrikus bejelentkezési kísérletek korlátozása 163
2.74. Sikertelen bejelentkezési kísérletek – Alternatív hitelesítési faktor használata 165
2.75. A rendszerhasználat jelzése 167
2.76. Legutóbbi bejelentkezési értesítés 169
2.77. Korábbi bejelentkezések jelzése – Sikertelen bejelentkezések 171
2.78. Korábbi bejelentkezések jelzése – Sikeres és sikertelen bejelentkezések 173
2.79. Korábbi bejelentkezések jelzése – Értesítés a fiókváltozásokról 175
2.80. Korábbi bejelentkezések jelzése – Kiegészítő bejelentkezési információk 177

2.81. Egyidejű munkaszakasz kezelés 179
2.82. Eszköz zárolása 181
2.83. Eszköz zárolása – Képernyőtakarás 183
2.84. A munkaszakasz lezárása 185
2.85. Munkaszakasz megszakítása – Felhasználó által kezdeményezett kijelentkezések 187
2.86. Munkaszakasz megszakítása – Megszakítási üzenet 189
2.87. Munkaszakasz megszakítása – Időkorlátozásra figyelmeztető üzenet 191
2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek 193
2.89. Biztonsági tulajdonságok 195
2.90. Biztonsági tulajdonságok – Dinamikus tulajdonságtársítás 199
2.91. Biztonsági tulajdonságok – Tulajdonságértékek jogosult személyek általi módosítása 201
2.92. Biztonsági tulajdonságok – Tulajdonságtársítások rendszerenkénti karbantartása 203
2.93. Biztonsági tulajdonságok – Tulajdonságok jogosult személyek által történő társítása. 205
2.94. Biztonsági tulajdonságok – Tulajdonságok megjelenítése a kimeneti objektumokon .. 207
2.95. Biztonsági tulajdonságok – Tulajdonságtársítás karbantartása 209
2.96. Biztonsági tulajdonságok – Következetes tulajdonságértelmezés 211
2.97. Biztonsági tulajdonságok – Tulajdonságtársítási technikák és technológiák 213
2.98. Biztonsági tulajdonságok – Tulajdonságok átcsoportosítása - Átminősítési mechanizmusok 215
2.99. Biztonsági tulajdonságok – A tulajdonságok konfigurálása felhatalmazott személyek által 217
2.100. Távoli hozzáférés 219
2.101. Távoli hozzáférés – Felügyelet és irányítás 222
2.102. Távoli hozzáférés – Bizalmasság és sértetlenség védelme titkosítás által 224
2.103. Távoli hozzáférés – Menedzselt hozzáférés-felügyeleti pontok 226

2.104. Távoli hozzáférés – Privilegizált parancsok és hozzáférés 228
2.105. Távoli hozzáférés – Hozzáférési mechanizmusra vonatkozó információk védelme .. 230
2.106. Távoli hozzáférés – Hozzáférés megszakítása vagy letiltása 232
2.107. Távoli hozzáférés – Távoli parancsok hitelesítése 234
2.108. Vezeték nélküli hozzáférés 236
2.109. Vezeték nélküli hozzáférés – Hitelesítés és titkosítás 238
2.110. Vezeték nélküli hozzáférés – Vezeték nélküli hálózat letiltása 240
2.111. Vezeték nélküli hozzáférés – Felhasználók általi konfiguráció korlátozása 242
2.112. Vezeték nélküli hozzáférés – Antennák és átviteli teljesítmény 244
2.113. Mobil eszközök hozzáférés-ellenőrzése 246
2.114. Mobil eszközök hozzáférés-ellenőrzése – Teljes eszköz vagy konténer-alapú titkosítás 248
2.115. Külső elektronikus információs rendszerek használata 250
2.116. Külső rendszerek használata – Engedélyezett használat korlátozásai 252
2.117. Külső rendszerek használata – Hordozható adattárolók használatának korlátozása ... 254
2.118. Külső rendszerek használata – A nem szervezeti tulajdonban lévő rendszerek használatának korlátozása 256
2.119. Külső rendszerek használata – Hálózati adattárolók használatának tiltása 258
2.120. Külső rendszerek használata – Hordozható adattárolók használatának tiltása 260
2.121. Információmegosztás 261
2.122. Információmegosztás – Automatizált döntéstámogatás 264
2.123. Információmegosztás – Információkeresés és visszakeresés 266
2.124. Nyilvánosan elérhető tartalom 268
2.125. Adatbányászat elleni védelem 270
2.126. Hozzáférés-ellenőrzésre vonatkozó döntések 273

2.127. Hozzáférés-ellenőrzési döntések – Hozzáférési engedélyek továbbítása..... 275

2.128. Felhasználó- vagy a folyamatazonosító ismerete nélküli hozzáférés-ellenőrzési döntések. 277

2.129. Referenciának való megfelelőség vizsgálata..... 279

2.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

2.1. A szervezet:

2.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint

2.1.1.1. - a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó hozzáférés-felügyeleti szabályzatot, amely

2.1.1.1.1. - meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá

2.1.1.1.2. - összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

2.1.1.2. - a hozzáférés-felügyeleti eljárásrendet, amely a hozzáférés-felügyeleti szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

2.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a hozzáférés-felügyeleti szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

2.1.3. Felülvizsgálja és frissíti az aktuális hozzáférés-felügyeleti szabályzatot, a hozzáférés-felügyeleti eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

A hozzáférés-felügyeleti szabályzatnak és a kapcsolódó eljárásrend(ek)nek illeszkednie kell az érintett szervezet kockázatkezelési stratégiájához. A megfelelő minőségben és megfelelő szempontok mentén elkészített szabályzatok és eljárásrendek nagy mértékben járulnak hozzá a szervezet biztonságának megőrzéséhez. Az elkészült szabályzatoknak és eljárásrendeknek összhangban kell lenniük egymással és a szervezet információbiztonsági környezetével. A szervezeti szintű biztonsági szabályzatok és eljárásrendek használata általában előnyösebb, hiszen szükségtelenné teheti a különböző szervezeti célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásrendeket. A szervezet azonban dönthet úgy (amennyiben a szervezet felépítése ezt indokolja), hogy a szabályzati szinten megjelenő követelményeket egy általános biztonsági szabályzatban [pl.: Információbiztonsági Szabályzat (IBSZ)], vagy

több szabályzatban implementálja, míg az eljárásrendek szintjén megjelenő követelményeket (melyek a szabályzatban foglalt követelményeket részletezik rendszer- és szerepköri szinten) beépítheti a rendszerbiztonsági tervébe, vagy több különböző dokumentumban jeleníti meg azokat. A szervezetnek kiemelt figyelmet kell fordítania mind a szabályzat, mind az eljárásrendek megfelelő frissítésére. A frissítéseket kiváltó események lehetnek értékelésből vagy (felül)vizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban. A szervezetnek szem előtt kell tartania, hogy az elvárt védelmi intézkedések egyszerű újraközlése nem minősülhet szervezeti szabályzatnak vagy eljárásrendnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell a hozzáférés-felügyeleti szabályzat és eljárásrendek kidolgozásával, dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatok ellátásáról.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a hozzáférés-felügyeleti szabályzatban foglaltak megfelelnek a szervezetre vonatkozó hatályos jogszabályoknak, irányelveknek, szabályozásoknak, szabványoknak és ajánlásoknak.
3. A szervezetnek - a megfelelő szereplők bevonásával, dokumentált módon - ki kell dolgoznia a vonatkozó szabályzatot és a kapcsolódó eljárásrendeket, és gondoskodnia kell a szabályzat és az eljárásrendek megfelelő kihirdetéséről, valamint az érintett felekkel történő megismertetéséről.
4. A szabályzat és a kapcsolódó eljárásrendek kidolgozásánál a szervezetnek figyelembe kell vennie a rá vonatkozó sajátosságokat. Az elvárt védelmi intézkedések szó szerinti átvétele nem minősül szervezeti szabályzatnak vagy eljárásrendnek.
5. A szervezetnek a gyakorlatban is alkalmaznia kell a hozzáférés-felügyeleti szabályzatban és az ahhoz kapcsolódó eljárásrendekben megfogalmazott elvárásokat, ezáltal biztosítva azok tényleges megvalósulását.
6. A szervezetnek felül kell vizsgálnia és szükség esetén frissítenie kell az aktuális hozzáférés-felügyeleti szabályzatot/szabályokat, illetve a kapcsolódó eljárásrendeket a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

Kapcsolódó intézkedések

8.1. Szabályzat és eljárásrendek

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

18.67. Információ kezelése és megőrzése

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.1. Hozzáférés ellenőrzési eljárásrend

ISO/IEC 27001:2023 referencia

5.2; 5.3; 7.5.1; 7.5.2; 7.5.3; A.5.1; A.5.2; A.5.4; A.5.15; A.5.31; A.5.36; A.5.37

NIST SP 800-53 rev.5 referencia

AC-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

2.2. FIÓKKEZELÉS

2.2. A szervezet:

2.2.1. Meghatározza és dokumentálja a rendszerben engedélyezett és kifejezetten tiltott fióktípusokat.

2.2.2. Kijelöli a fiókkezelőket.

2.2.3. Kialakítja a csoport- és szerepkör tagsági feltételeket és kritériumokat.

2.2.4. Meghatározza:

2.2.4.1. - a rendszerben engedélyezett felhasználókat.

2.2.4.2. - a csoport- és szerepkör tagságokat.

2.2.4.3. - a hozzáférési jogosultságokat és a felhasználói fiókokhoz tartozó szükséges jellemzőket minden egyes felhasználói fiókra.

2.2.5. A meghatározott szerepköröket betöltő személyek jóváhagyását kéri a felhasználói fiókok létrehozására vonatkozó kérelmek esetén.

2.2.6. Létrehozza, engedélyezi, módosítja, letiltja és törli a fiókokat a meghatározott irányelvek, eljárások, előfeltételek és kritériumok alapján.

2.2.7. Nyomon követi a fiókok használatát.

2.2.8. Értesíti a fiókkezelőket és a meghatározott személyeket vagy szerepköröket a következő esetekben:

2.2.8.1. - meghatározott időn belül, amikor a fiókok már nem szükségesek.

2.2.8.2. - meghatározott időn belül, amikor a felhasználók jogviszonya megszűnik.

2.2.8.3. - meghatározott időn belül, amikor a rendszerhasználat vagy az egyén számára szükséges ismeretek megváltoznak.

2.2.9. Engedélyezi a rendszerhez való hozzáférést a következők alapján:

2.2.9.1. - érvényes hozzáférési engedély;

2.2.9.2. - tervezett rendszerhasználat;

2.2.9.3. - egyéb, a szervezet által meghatározott jellemzők.

2.2.10. Ellenőrzi a felhasználói fiókokat a fiókkezelési követelmények betartása szempontjából, a meghatározott gyakorisággal.

2.2.11. Létrehoz és végrehajt egy folyamatot a megosztott vagy csoport felhasználói fiókok hitelesítési adatainak megváltoztatására az egyének csoportból történő eltávolításának esetére.

2.2.12. Összehangolja a fiókkezelési folyamatokat a felhasználók jogviszonyának megszűntetési folyamataival.

MAGYARÁZAT

Az EIR fióktípusok lehetnek például egyéni, megosztott, csoport, rendszer, vendég, névtelen, vészhelyzeti, fejlesztői, ideiglenes és szolgáltatási fiókok. Az érintett szervezet meghatározza, hogy milyen fióktípusok létesíthetők az EIR-en belül, és milyen fióktípusok használata tiltott. Bizonyos fióktípusok különleges jóváhagyási folyamat után állíthatók be az EIR-en, ilyen jóváhagyást hajthat végre például az EIR üzleti oldali felelőse, vagy az elektronikus információs rendszer biztonságáért felelős személy. A tiltott fióktípusokhoz tartozhatnak például kockázati alapon a megosztott, csoportos, vészhelyzeti, névtelen, ideiglenes és vendégfiókok.

Az ideiglenes és vészhelyzeti fiókok rövid távú használatra valók, speciális paraméterekkel ellátva. Az ilyen fiókok létrehozásakor a szervezet megfelelő körültekintéssel jár el, figyelembe véve a speciális fióktípusokkal együtt járó kockázatokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell az EIR-ben engedélyezett és kifejezetten tiltott fióktípusokat, mint például az egyéni, megosztott, csoport, rendszer, vendég, névtelen, vészhelyzeti, fejlesztői, ideiglenes és szolgáltatási fiókok.
2. A szervezetnek gondoskodnia kell a fiókkezeléssel kapcsolatos felelősi feladatok ellátásáról.
3. A szervezetnek ki kell alakítania a csoport- és szerepkör tagsági feltételeket és kritériumokat, figyelembe véve a biztonsági szempontokat.
4. A szervezetnek meg kell határoznia az EIR-ben engedélyezett felhasználókat, a csoport- és szerepkör tagságokat, a hozzáférési jogosultságokat és a felhasználói fiókokhoz tartozó szükséges jellemzőket minden egyes felhasználói fiókra.
5. A szervezetnek jóváhagyást kell kérnie a meghatározott szerepköröket betöltő személyektől a felhasználói fiókok létrehozására vonatkozó kérelmek esetén.
6. A szervezetnek a fiókokat a meghatározott irányelvek, eljárások, előfeltételek és kritériumok alapján kell kezelnie (létrehozás, engedélyezés, módosítás, letiltás és törlés).
7. A szervezetnek nyomon kell követnie a fiókok használatát, és naplóznia kell az azokkal végzett tevékenységeket.

8. A szervezetnek értesítenie kell a fiókkezelőket és a meghatározott személyeket vagy szerepköröket a következő esetekben: amikor a fiókok már nem szükségesek, amikor a felhasználók jogviszonya megszűnik, vagy amikor a rendszerhasználat vagy az egyén számára szükséges ismeretek megváltoznak.
9. A szervezetnek az EIR-hez való hozzáférést az érvényes hozzáférési engedély, a tervezett rendszerhasználat és egyéb, a szervezet által meghatározott jellemzők alapján kell engedélyeznie.
10. A szervezetnek ellenőriznie kell a felhasználói fiókokat a fiókkezelési követelmények betartása szempontjából, a meghatározott gyakorisággal.
11. A szervezetnek létre kell hoznia és végre kell hajtania egy folyamatot a megosztott vagy csoport felhasználói fiókok hitelesítési adatainak megváltoztatására az egyének csoportból történő eltávolításának esetére.
12. A szervezetnek össze kell hangolnia a fiókkezelési folyamatokat a felhasználók jogviszonyának megszüntetési folyamataival.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése
2.59. Felelősségek szétválasztása
2.60. Legkisebb jogosultság elve
2.100. Távoli hozzáférés
2.108. Vezeték nélküli hozzáférés
2.115. Külső elektronikus információs rendszerek használata
2.126. Hozzáférés-ellenőrzésre vonatkozó döntések
4.2. Naplózható események
4.40. Naplóbejegyzések létrehozása
6.18. A változtatásokra vonatkozó hozzáférés korlátozások

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.2. Felhasználói fiókok kezelése

ISO/IEC 27001:2023 referencia

A.5.16; A.5.18; A.8.2

NIST SP 800-53 REV.5 REFERENCIA

AC-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

2.3. FIÓKKEZELÉS – AUTOMATIZÁLT FIÓKKEZELÉS

2.3. A szervezet meghatározott automatizált mechanizmusok segítségével támogatja az EIR fiókjainak kezelését.

MAGYARÁZAT

Az automatizált fiókkezelés magában foglalja az automatizált mechanizmusok használatát az EIR fiókok létrehozásához, engedélyezéséhez, módosításához, letiltásához és eltávolításához. Az automatizált mechanizmus értesíti a fiókkezelőket, amikor egy fiókot létrehoznak, engedélyeznek, módosítanak, letiltanak, eltávolítanak vagy a megszokottól eltérően használnak. Emellett az automatizált mechanizmus monitorozza a fiókhasználatot.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek a 2.2-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek először létre kell hoznia automatizált mechanizmusokat, amelyek elvégzik az EIR fiókok létrehozását, engedélyezését, módosítását, letiltását és eltávolítását.
2. A szervezetnek az automatizált mechanizmusokat úgy kell kialakítania, hogy értesítést küldjenek az EIR fiókkezelőinek, amikor egy fiókot létrehoznak, engedélyeznek, módosítanak, letiltanak vagy eltávolítanak.
3. A szervezetnek biztosítania kell, hogy az automatizált mechanizmusok képesek a fiókhasználat monitorozására és a megszokottól eltérő használat észlelése esetén riasztást küldenek a fiókkezelőknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.2. Felhasználói fiókok kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.4. FIÓKKEZELÉS – AUTOMATIZÁLT IDEIGLENES ÉS VÉSZHELYZETI FIÓK KEZELÉS

2.4. Az EIR a meghatározott időtartam letelte után automatikusan eltávolítja vagy letiltja az ideiglenes és vészhelyzeti fiókokat.

MAGYARÁZAT

Az automatizált ideiglenes és vészhelyzeti fiókkezelés magában foglalja az ideiglenes és vészhelyzeti fiókok automatikus eltávolítását vagy letiltását egy előre meghatározott időszak után, ezzel kiküszöbölve azt, hogy az ilyen fiókok manuálisan, az EIR adminisztrátora által kerüljenek eltávolításra vagy letiltásra. Ez a funkció növeli az EIR biztonságát, mivel minimalizálja azoknak a fiókoknak a számát, amelyeket illetéktelen személyek esetlegesen felhasználhatnak. Az automatikus eltávolítás vagy letiltás azt is biztosítja, hogy az érintett szervezetnek ne kelljen manuálisan nyomon követnie és eltávolítania az ideiglenes fiókokat, ami időigényes és hibalehetőségeket rejt magában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek a 2.2-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. Aszervezetnek először meg kell határoznia az ideiglenes és vészhelyzeti fiókok élettartamát. Ez azt jelenti, hogy meg kell határozniuk, mennyi idő elteltével kerüljenek ezek a fiókok automatikusan eltávolításra vagy letiltásra az EIR-ben.
2. A szervezetnek implementálnia kell egy automatizált mechanizmust az EIR-ben, amely eltávolítja vagy letiltja az ideiglenes és vészhelyzeti fiókokat a meghatározott időtartam letelte után.
3. A szervezetnek ellenőriznie kell, hogy az automatizált folyamat megfelelően működik-e az EIR-ben. Ez azt jelenti, hogy rendszeresen ellenőrizni kell, hogy az ideiglenes és vészhelyzeti fiókok valóban eltávolításra vagy letiltásra kerülnek-e a meghatározott időtartam letelte után.
4. A szervezetnek gondoskodnia kell az ideiglenes és vészhelyzeti fiókok eltávolításának és letiltásának a naplózásáról az EIR-ben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.2. Felhasználói fiókok kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az időtartam (valamennyi fióktípus esetén) meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.5. FIÓKKEZELÉS – FIÓKOK LETILTÁSA

2.5. Az EIR a meghatározott időtartam letelte után letiltja a fiókokat, vagy amikor a fiókok:

2.5.1. - lejártak,

2.5.2. - már nem kapcsolódnak felhasználókhoz vagy egyénekhez,

2.5.3. - megsértik a szervezeti szabályokat, vagy

2.5.4. - meghatározott ideig inaktívak voltak.

MAGYARÁZAT

Az EIR letiltja azokat a fiókokat, amelyek lejártak, inaktívak vagy egyéb anomáliákat mutatnak, ezzel támogatva a legkisebb jogosultság és a legkisebb funkcionalitás elveit, amelyek csökkentik az EIR támadási felületét. Ez azt jelenti, hogy az EIR csak a szükséges hozzáférést és funkciókat biztosítja a felhasználóknak, ezzel minimalizálva a potenciális biztonsági kockázatokat. Ha egy fiók lejár, vagy már nem kapcsolódik egy felhasználóhoz vagy egyénhez, az EIR automatikusan letiltja azt, hogy megakadályozza a jogosulatlan hozzáférés lehetőségét. Az EIR szintén letiltja azokat a fiókokat, amelyek megsértik az érintett szervezet szabályait, biztonsági házirendjét. Ez tehát azt jelenti, hogy ha egy felhasználó olyan tevékenységet végez, ami ellentétes a szervezet irányelveivel, az EIR reagál és letiltja a fiókot, hogy megvédje a szervezet információit. Ha egy fiók meghatározott ideig inaktív, akkor az EIR által letiltásra kerül. Ez az intézkedés azért fontos, mert az inaktív fiókok gyakran jelentenek biztonsági kockázatot, mivel a támadók kihasználhatják őket a rendszerbe való behatolásra.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell állítania az EIR-ben a fiókok automatikus letiltását amennyiben azok lejártak, már nem kapcsolódnak a felhasználókhoz vagy egyénekhez, megsértik a szervezeti szabályokat vagy meghatározott ideig inaktívak voltak.
2. A szervezetnek naplóznia kell a fiókok letiltását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.2. Felhasználói fiókok kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.6. Fiókkezelés – Automatikus naplózási műveletek

2.6. Az EIR automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket.

Magyarázat

A fiókkezeléssel kapcsolatos naplózási műveletek a "Naplózható események" és a "Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel" kontrolloknál kerültek bővebben kifejtésre. Az EIR automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket. Az EIR naplózása kritikus szerepet játszik az érintett szervezet biztonsági szintjének megőrzésében. A naplózás segítségével a szervezet képes nyomon követni és ellenőrizni a felhasználói fiókokkal kapcsolatos tevékenységeket, beleértve a fiókok létrehozását, módosítását, engedélyezését, letiltását és eltávolítását. Ez lehetővé teszi a szervezet számára, hogy azonnal észlelje a gyanús vagy szabálytalan, a megszokottól eltérő tevékenységeket, és ezáltal megtegye a szükséges lépéseket a potenciális biztonsági események megelőzése érdekében.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell, hogy az EIR képes legyen automatikusan naplózni a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket.
2. A szervezetnek úgy kell konfigurálnia az EIR-t, hogy a megfelelő és általa elvárt naplótartalommal legyen képes a szükséges naplóállományokat előállítani.
3. A szervezetnek rendszeresen ellenőriznie kell az EIR naplóit, ezáltal megbizonyosodhat arról, hogy a fiókokkal kapcsolatos tevékenységek megfelelően naplózásra kerülnek.

Kapcsolódó intézkedések

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.2. Felhasználói fiókok kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.7. FIÓKKEZELÉS – INAKTIVITÁSBÓL FAKADÓ KIJELENTKEZTETÉS

2.7. A szervezet megköveteli a felhasználó kijelentkeztetését egy meghatározott inaktivitási időszak leteltét követően, vagy egy meghatározott időpontban.

MAGYARÁZAT

Az inaktivitásból fakadó kijelentkeztetés automatikus kikényszerítésével kapcsolatos elvárások az "Eszköz zárolása" kontrollnál kerültek bővebben kifejtésre. Az inaktivitásból fakadó kijelentkeztetés jellemzően a felhasználó tevékenységén, ill. annak hiányán alapszik. Amennyiben a felhasználó az érintett szervezet által meghatározott időtartamon belül nem végez tevékenységet az EIR-ben, az EIR automatikusan kijelentkezteti a felhasználót. Az inaktivitásból fakadó kijelentkeztetés tárgykörébe tartozik az is, amikor a szervezet az általa meghatározott időpontban jelentkezteti ki automatikusan a felhasználót. Ez a funkció segít megelőzni a jogosulatlan hozzáféréseket, különösen akkor, ha a felhasználó elfelejt kijelentkezni az EIR-ből.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az inaktivitási időtartamot, amelynek letelte után az EIR automatikusan kijelentkezteti a felhasználókat. Ez az időszak lehet egy meghatározott időpont, vagy egy meghatározott időtartam, amely alatt a felhasználó nem végez semmilyen tevékenységet.
2. A szervezetnek be kell állítania az EIR-ben az automatikus kijelentkezési funkciót, amely a meghatározott inaktivitási időtartam letelte után vagy a meghatározott időpontban automatikusan kijelentkezteti a felhasználókat.
3. A szervezetnek nyomon kell követnie a fiókok használatát, és naplóznia kell az azokkal végzett tevékenységeket. Ebből kifolyólag a szervezetnek naplóznia kell az automatikus kijelentkezéseket is.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.82. Eszköz zárolása

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.2. Felhasználói fiókok kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a felhasználók kijelentkeztetésére vonatkozó inaktivitási időtartam vagy időpont meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.8. Fiókkezelés – Dinamikus jogosultságkezelés

2.8. A szervezet meghatározott módon alkalmaz dinamikus jogosultságkezelési képességeket.

Magyarázat

A statikus fiókokat és előre meghatározott felhasználói jogosultságokat alkalmazó hozzáférés-felügyeleti megközelítésekkel ellentétben a dinamikus hozzáférés-felügyeleti megközelítések a dinamikus jogosultságkezeléssel, például a tulajdonságalapú hozzáférés-felügyelettel megkönnyített valós idejű hozzáférés-felügyeleti döntésekre támaszkodnak. Míg a felhasználói azonosítók időben viszonylag állandóak maradnak, a felhasználói jogosultságok jellemzően gyakrabban változnak a folyamatban lévő működési célok vagy üzleti követelmények és a szervezetek működési igényei alapján. A dinamikus jogosultságkezelés egyik példája a felhasználók jogosultságainak azonnali visszavonása, szemben azzal, amikor a felhasználóknak a jogosultságok változásainak tükrözése érdekében meg kell szakítaniuk és újra kell indítaniuk munkameneteiket. A dinamikus jogosultságkezelés olyan mechanizmusokat is tartalmazhat, amelyek dinamikus szabályok alapján változtatják meg a felhasználói jogosultságokat, szemben az egyes felhasználói profilok szerkesztésével. Ilyen például a felhasználói jogosultságok automatikus módosítása, ha a felhasználók a szokásos munkaidejükön kívül dolgoznak, ha megváltozik a munkakörük vagy a megbízásuk, vagy ha a rendszerek terhelés alatt vagy vészhelyzeti állapotban vannak. A dinamikus jogosultságkezelés magában foglalja a jogosultságok változásainak hatásait, például amikor a kommunikációhoz használt titkosító kulcsok megváltoznak.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a dinamikus jogosultságkezelési stratégiáját.
2. A szervezetnek be kell vezetnie a dinamikus jogosultságkezelési mechanizmusokat, amelyek lehetővé teszik a felhasználói jogosultságok változásait a szervezeti igényeknek megfelelően. Például ha a felhasználók a szokásos munkaidejükön kívül dolgoznak, illetve ha megváltozik a munkakörük vagy a megbízásuk.
3. A szervezetnek nyomon kell követnie a felhasználói fiókokkal kapcsolatos jogosultságok változását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.89. Biztonsági tulajdonságok

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a dinamikus jogosultságkezelési képességek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.9. FIÓKKEZELÉS – PRIVILEGIZÁLT FIÓKOK

2.9. A szervezet:

2.9.1. Létrehozza és kezeli a privilegizált fiókokat egy szerepköralapú vagy tulajdonságalapú hozzáférési rendszerrel összhangban.

2.9.2. Felügyeli a privilegizált szerepkörök vagy tulajdonságok hozzárendeléseit.

2.9.3. Felügyeli a szerepkörök vagy tulajdonságok változásait.

2.9.4. Visszavonja a hozzáférést, amikor a privilegizált szerepkörök vagy tulajdonságok hozzárendelése többé már nem releváns.

MAGYARÁZAT

A privilegizált szerepkörök olyan, a szervezet által meghatározott, jellemzően egyénekhez rendelt szerepkörök, amelyek lehetővé teszik a privilegizált jogosultságot birtoklók számára, hogy olyan, biztonsági szempontból fontos funkciókat hajtsanak végre, amelyek elvégzésére a normál felhasználók nem jogosultak. A privilegizált szerepkörök közé tartozik a kulcsok kezelése, a fiókkezelés, az adatbázisok adminisztrációja, a rendszerek és hálózatok adminisztrációja, valamint a webes adminisztráció. A szerepkör alapú hozzáférési szabályok az engedélyezett rendszer hozzáférést és a jogosultságokat szerepkörökbe szervezik. Ezzel szemben az tulajdonságalapú hozzáférési séma tulajdonságok alapján határozza meg az engedélyezett rendszer hozzáférést és jogosultságokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először létre kell hoznia és kezelnie a privilegizált fiókokat, amelyek összhangban vannak egy szerepköralapú vagy tulajdonságalapú hozzáférési rendszerrel. Ez azt jelenti, hogy a privilegizált hozzáféréseknek és jogosultságoknak a személyek szerepköreihez vagy tulajdonságaihoz kell igazodniuk az EIR-ben.
2. A szervezetnek nyomon kell követnie, hogy mely személyek rendelkeznek privilegizált hozzáféréssel, és milyen szerepkörök vagy tulajdonságok alapján kapták ezt a hozzáférést.
3. A szervezetnek nyomon kell követnie a szerepkörök vagy tulajdonságok változásait. Ha egy személy szerepköre vagy tulajdonságai megváltoznak, a szervezetnek ennek megfelelően módosítania kell a hozzáférési jogosultságokat az EIR-ben.

4. Ha a privilegizált szerepkörök vagy tulajdonságok hozzárendelése többé már nem releváns, az érintett szervezetnek vissza kell vonnia a hozzáférést.
5. A szervezetnek dokumentálnia, illetve naplóznia kell a fentebb leírtakat.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-2(7)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.10. FIÓKKEZELÉS – DINAMIKUS FIÓKKEZELÉS

2.10. A szervezet a meghatározott rendszerfiókok létrehozását, aktiválását, kezelését és letiltását dinamikusan végzi.

MAGYARÁZAT

Az érintett szervezet úgy tervezi meg a rendszerfiókok dinamikus kezelését, létrehozását, aktiválását és deaktiválását, hogy bizalmi kapcsolatokat, üzleti szabályokat és mechanizmusokat hoznak létre a megfelelő hitelesítésszolgáltatókkal a kapcsolódó jogosultságok és kiváltságok érvényesítésére. Az EIR fiókok dinamikus kezelése azt jelenti, hogy a szervezet képes azonosítani és reagálni a változó körülményekre és igényekre. Ez magában foglalja a fiókok automatikus létrehozását és aktiválását, amikor új felhasználók vagy alkalmazások jelennek meg, valamint a fiókok letiltását, amikor már nincs szükség rájuk.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek bizalmi kapcsolatokat, üzleti szabályokat és mechanizmusokat kell létrehoznia a megfelelő szolgáltatókkal, hogy ellenőrizhesse a kapcsolódó engedélyeket és jogosultságokat. Ez a lépés alapvető a dinamikus rendszerfiókok kezelésének, létrehozásának, aktiválásának és letiltásának tervezéséhez.
2. A szervezetnek meg kell valósítania, hogy automatikusan tudja kezelni a rendszerfiókokat, értve ezalatt azok dinamikus létrehozását, aktiválását, kezelését és letiltását.
3. A szervezetnek nyomon kell követnie a fiókok létrehozását, aktiválását, kezelését, letiltását és naplóznia kell az azokkal végzett tevékenységeket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.89. Biztonsági tulajdonságok

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerfiókok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.11. Fiókkezelés – Megosztott és csoportfiókok használati korlátozása

2.11. A szervezet csak meghatározott feltételeknek megfelelő megosztott és csoportfiókok használatát engedélyezi.

Magyarázat

A megosztott vagy csoporthoz rendelt fiókok használatának engedélyezése előtt az érintett szervezet mérlegeli az ilyen fiókokkal kapcsolatos elszámoltathatóság hiánya miatt megnövekedett kockázatot. A megosztott és csoportfiókok használatakor több felhasználó ugyanazt a fiókot használja, ami megnehezíti a tevékenységek egyértelmű nyomon követését. Ezért a szervezetnek gondosan mérlegelnie kell a megosztott és csoportfiókok használatának engedélyezését, és csak akkor szabad ezt megtennie, ha a fiókok használata megfelel a szervezet biztonsági követelményeinek.

A követelmény alkalmazásának lépései

1. A szervezetnek először értékelnie kell a megosztott és csoportfiókok használatának kockázatait. Tekintettel kell lenni arra, hogy ezek a fiókok csökkentik az elszámoltathatóságot, mivel nem egyértelmű, hogy ki használta a fiókot egy adott időpontban.
2. A szervezetnek meg kell határoznia a megosztott és csoportfiókok használatának feltételeit. Ezek a feltételek tartalmazhatják, hogy milyen esetekben engedélyezett a megosztott és csoportfiókok használata, milyen jogosultságokkal rendelkeznek ezek a fiókok, és milyen biztonsági intézkedések szükségesek a fiókok használatához.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a megosztott és csoportfiókokra vonatkozó feltételek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.12. FIÓKKEZELÉS – HASZNÁLATI FELTÉTELEK

2.12. A szervezet kikényszeríti a meghatározott körülmények és a használati feltételek betartását a meghatározott rendszerfiókok esetében.

MAGYARÁZAT

A használati feltételek meghatározása és betartatása segít a legkisebb jogosultság elvének érvényesítésében, a felhasználói elszámoltathatóság növelésében és a fiókok hatékony monitorozásának lehetővé tételében. A fiókok monitorozása magában foglalja a szervezeti keretszabályokat sértő fiókhasználat esetén generált figyelmeztetéseket. A szervezetek leírhatják azokat a konkrét feltételeket vagy körülményeket, amelyek mellett a rendszerfiókok használhatók, például a használatot a hét bizonyos napjaira, napszakokra vagy meghatározott időtartamra korlátozhatják.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a használati feltételeket és körülményeket a rendszerfiókok számára. Ezek a feltételek tartalmazhatják a fiókok használatának időpontjait, a használat időtartamát, és a használati jogosultságokat.
2. A szervezetnek implementálnia kell a megfelelő technikai megoldásokat, amelyek képesek kikényszeríteni a meghatározott használati feltételek és körülmények betartását. Ez magában foglalhatja a hozzáférés-felügyelettel kapcsolatos szabályok gyakorlatba történő átültetését, a fiókok használatának korlátozásait, és a fiókok használatának naplózását.
3. A szervezetnek rendszeresen ellenőriznie kell a rendszerfiókok használatát, így biztosítva a meghatározott körülmények és használati feltételek betartását. Ez magában foglalhatja a naplók ellenőrzését, a megszokottól eltérő fiókhasználati minták azonosítását, és az azokra történő reagálást.
4. Az érintett szervezetnek felül kell vizsgálnia és szükség esetén frissítenie kell a rendszerfiókokra meghatározott körülményeket és használati feltételeket a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a körülmények és használati feltételek illetve a rendszerfiókok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

2.13. FIÓKKEZELÉS – FIÓKOK SZOKATLAN HASZNÁLATÁNAK FELÜGYELETE

2.13. A szervezet:

2.13.1. Monitorozza az EIR fiókjainak a meghatározott, megszokottól eltérő használatát, és

2.13.2. jelentést készít az EIR fiókjainak megszokottól eltérő használatáról a meghatározott személyeknek vagy szerepköröknek.

MAGYARÁZAT

A fiókok szokatlan használatára utalhat, ha az EIR-hez köthető fiókba a megszokottól eltérő időpontban vagy eltérő helyről jelentkeznek be. A fiókokok szokatlan használatának felügyelete azt jelenti, hogy az érintett szervezet folyamatosan nyomon követi és elemzi a fiókok használatát, így azonosítva azokat a tevékenységeket, amelyek eltérnek a megszokottól. Ez magában foglalhatja a fiókokhoz való hozzáférés időpontjának, gyakoriságának, helyének vagy a fiókok által elvégzett műveletek típusának monitorozását. A fiókok megszokottól eltérő használata jelezhet a felhasználó részéről rosszindulatú tevékenységet vagy akár egy folyamatban lévő támadást is. Amennyiben a szervezet szokatlan használatot észlel, arról jelentést készít a meghatározott személyeknek vagy szerepköröknek. Ez elősegíti, hogy a szervezet gyorsan reagáljon a potenciális biztonsági eseményekre, illetve megtegye a szükséges lépéseket a kockázatok kezelésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mi számít "megszokott" vagy "megszokottól eltérő" használatnak az EIR fiókjai esetében. Ez magában foglalhatja a rendszerhez való hozzáférés időpontjait, helyét, gyakoriságát, a felhasznált funkciókat stb.
2. A szervezetnek implementálnia kell egy rendszert vagy folyamatot, amely képes nyomon követni és naplózni az EIR fiókjainak használatát. Ez lehet egy automatizált rendszer, amely folyamatosan monitorozza a fiókok tevékenységét, vagy manuális ellenőrzés, amelyet rendszeresen végeznek.
3. A szervezetnek be kell állítania értesítéseket vagy figyelmeztetéseket a megszokottól eltérő használat esetére. Ez lehet például egy e-mail alapú értesítés, ami a rendszergazdának jelez.

4. A szervezetnek jelentést kell készítenie a megszokottól eltérő használatról a meghatározott személyek vagy szerepkörök számára. Ez a jelentés tartalmazhatja a megszokottól eltérő tevékenységek részletes leírását, az esetleges kockázatokat és a javasolt intézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

5.14. Folyamatos felügyelet

9.34. Biztonsági eseménykezelési terv

18.13. Az EIR monitorozása

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.2. Felhasználói fiókok kezelése

ISO/IEC 27001:2023 REFERENCIA

A.8.16

NIST SP 800-53 REV.5 REFERENCIA

AC-2(12)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

2.14. Fiókkezelés – Magas kockázatú személyek fiókjának letiltása

2.14. A szervezet az általa meghatározott jelentős kockázat felfedezésétől számított meghatározott időtartamon belül letiltja az érintett felhasználók fiókjait.

Magyarázat

Az érintett szervezet által meghatározott jelentős kockázat azonosításától számított meghatározott időtartamon belül letiltja az érintett felhasználók fiókjait. A letiltott fiókokról készült dokumentációk/naplók segíthetnek az érintett szervezetnek megérteni a kockázat forrását, és segíthetnek a jövőbeni biztonsági események megelőzésében.

A követelmény alkalmazásának lépései

1. Az érintett szervezetnek meg kell határoznia azt a kockázati szintet, amelyet jelentős kockázatként azonosít.
2. A szervezetnek meg kell határoznia azt az időtartamot, amelyen belül letiltja azokat a felhasználói fiókokat, amelyek jelentős kockázatot jelentenek. Az időtartam meghatározásánál figyelembe kell venni a szervezet képességeit és ahhoz mérten egy olyan időkeretet kell megállapítani, ami alatt a lehető leggyorsabban le lehet tiltani az érintett felhasználók fiókjait.
3. A szervezetnek szorosan együtt kell működnie a rendszergazdákkal, a jogi területtel, a humánerőforrás-menedzserekkel és az elektronikus információs rendszer biztonságáért felelős személlyel, hogy meghatározzák a legmegfelelőbb intézkedéseket a magas kockázatot jelentő felhasználók fiókjainak letiltására, és további intézkedések foganatosítására.
4. Az érintett szervezetnek dokumentálnia/naplóznia kell a fiókok letiltását, beleértve a letiltás okát és időpontját.

Kapcsolódó intézkedések

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

18.13. Az EIR monitorozása

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.2. Felhasználói fiókok kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-2(13)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum, illetve a jelentős kockázatok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.15. HOZZÁFÉRÉSI SZABÁLYOK ÉRVÉNYESÍTÉSE

2.15. Az EIR a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott logikai hozzáférési jogosultságokat az információkhoz és a rendszer erőforrásaihoz.

MAGYARÁZAT

Az EIR-ben megvalósított logikai hozzáférés-felügyeleti szabályokkal szemben, a fizikai hozzáférés-felügyeleti szabályok a fizikai hozzáféréssel/belépéssel kapcsolatos kontrolloknál kerültek bővebben kifejtésre. Az hozzáférés-felügyeleti szabályzatok szabályozzák a hozzáférést az aktív entitások vagy alanyok és a passzív entitások vagy objektumok (azaz eszközök, fájlok, rekordok, domainek) között az érintett szervezet infrastruktúrájában. Az EIR biztosítja, hogy csak azok a felhasználók és folyamatok férjenek hozzá az információkhoz és az EIR erőforrásaihoz, akiknek erre jogosultságuk van. Ez a jogosultság a felhasználói szinttől, a felhasználói csoportokon át, egészen az alkalmazások és szolgáltatások szintjéig terjedhet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia a logikai hozzáférési jogosultságokat az EIR-hez. Ez magában foglalja a felhasználói jogosultságok, a rendszergazdai jogosultságok és a hozzáférési szintek meghatározását.
2. A szervezetnek létre kell hoznia egy szabályzatot, amely meghatározza, hogyan kell kezelni és érvényesíteni a logikai hozzáférési jogosultságokat az EIR-ben. Ez a szabályzat magában foglalja a jogosultságok létrehozásának, módosításának, törlésének és felülvizsgálatának folyamatát.
3. A szervezetnek implementálnia kell a logikai hozzáférési jogosultságokat az EIR-ben a szabályzatnak megfelelően. Ez magában foglalja a jogosultságok hozzárendelését a megfelelő felhasználókhoz, valamint a hozzáférési szintek beállítását.
4. A szervezetnek naplóznia kell a logikai hozzáférési jogosultságok használatát az EIR-ben. Ez magában foglalja a hozzáférési kísérletek, a sikeres és sikertelen hozzáférési események, valamint a jogosultságok módosításának naplózását.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.28. Információáramlási szabályok érvényesítése

2.59. Felelősségek szétválasztása

2.60. Legkisebb jogosultság elve

2.89. Biztonsági tulajdonságok

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

2.115. Külső elektronikus információs rendszerek használata

2.121. Információmegosztás

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.3. Hozzáférés ellenőrzés érvényesítése: Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

ISO/IEC 27001:2023 referencia

A.5.15; A.5.33; A.8.3; A.8.4; A.8.18; A.8.20; A.8.26

NIST SP 800-53 rev.5 referencia

AC-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

2.16. Hozzáférési szabályok érvényesítése – Kettős jóváhagyás

2.16. A szervezet kettős jóváhagyást követel meg a meghatározott privilegizált parancsok, vagy a szervezet által meghatározott egyéb műveletek végrehajtása esetében.

Magyarázat

A kettős jóváhagyás csökkenti a belső fenyegetésekkel kapcsolatos kockázatot. A kettős jóváhagyási mechanizmusok végrehajtásához két, felhatalmazással rendelkező személy jóváhagyása szükséges. Az összejátszás kockázatának csökkentése érdekében a szervezetek fontolóra veszik a kettős jóváhagyást igénylő feladatok rotációját. A szervezetek mérlegelik a kettős jóváhagyási mechanizmusok végrehajtásával kapcsolatos kockázatot, amikor azonnali válaszlépésekre van szükség. Például, ha egy EIR-ben sürgős beavatkozásra van szükség a köz- vagy környezeti biztonság érdekében, de a kettős jóváhagyás alkalmazása késleltetheti a választ.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia, mely privilegizált parancsok vagy egyéb műveletek igényelnek kettős jóváhagyást. Ez magában foglalhatja a rendszerkritikus műveleteket, a bizalmas adatokhoz történő hozzáférést, vagy a kritikus rendszerkonfigurációk módosítását.
2. A szervezetnek létre kell hoznia egy kettős jóváhagyási mechanizmust, amely megköveteli két, felhatalmazással rendelkező személy jóváhagyását a meghatározott műveletek végrehajtásához.
3. A szervezetnek gondoskodnia kell azon személyek felhatalmazásáról, akik képesek jóváhagyni a meghatározott műveleteket.
4. A szervezetnek naplóznia/dokumentálnia kell minden kettős jóváhagyási műveletet, ezáltal nyomon követhető ki és mikor hagyta jóvá a műveleteket.

Kapcsolódó intézkedések

7.35. Az elektronikus információs rendszer mentései

11.8. Adathordozók törlése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a privilegizált parancsok vagy egyéb műveletek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.17. HOZZÁFÉRÉSI SZABÁLYOK ÉRVÉNYESÍTÉSE – KÖTELEZŐ HOZZÁFÉRÉS-ELLENŐRZÉS

2.17. Az EIR az alábbi kötelező és a szervezet által meghatározott hozzáférés-felügyeleti szabályokat érvényesíti:

2.17.1. A szabályzat egységesen érvényes a rendszeren belüli minden alanyra és objektumra.

2.17.2. A hozzáféréssel rendelkező alanyt korlátozza az alábbi tevékenységek végrehajtásában:

2.17.2.1. - nem továbbíthatja az információt jogosulatlan alanyoknak vagy objektumoknak;

2.17.2.2. - nem adhatja át a jogosultságait más alanyoknak;

2.17.2.3. - nem módosíthatja az alanyokon, objektumokon, a rendszeren vagy rendszerelemeken meghatározott biztonsági tulajdonságokat;

2.17.2.4. - választhatja ki az újonnan létrehozott vagy módosított objektumokhoz rendelt biztonsági tulajdonságokat és tulajdonságértékeket, amelyeket a szabályzat határoz meg;

2.17.2.5. - nem módosíthatja a hozzáférés-felügyeleti szabályokat.

2.17.2.5.1. - A szabályzat részletesen meghatározza, hogy mely alanyok kaphatnak olyan privilegizált státuszt, amely nem vonatkozik sem a fent említett korlátozások egy részhalmazára, sem az egészre.

MAGYARÁZAT

A kötelező hozzáférés-felügyelet a nem mérlegelésen alapuló hozzáférés-felügyelet egyik típusa. A kötelező hozzáférés-felügyeleti szabályok korlátozzák, hogy az alanyok milyen műveleteket végezhetnek olyan objektumokból származó információkkal, amelyekhez már hozzáférést kaptak. Ez megakadályozza azt, hogy az alanyok az információt jogosulatlan alanyoknak és objektumoknak továbbítsák. A kötelező hozzáférés-felügyeleti szabályok korlátozzák az alanyok által a hozzáférés-felügyeleti jogosultságok továbbadásával kapcsolatban végrehajtható műveleteket; azaz egy jogosultsággal rendelkező alany nem adhatja tovább ezt a jogosultságot más alanyoknak. A házirend egységesen érvényesül minden olyan alanyra és objektumra, amely felett a rendszer rendelkezik, ellenkező esetben a hozzáférés-felügyelet megkerülhető. A szabályok a rendszer által korlátozottak.

A fent leírt megbízható alanyok a legkisebb jogosultság elvének megfelelő jogosultságokat kapnak (a "Legkisebb jogosultság elve" kontrolloknál kerül bővebben kifejtésre). A megbízható

alanyok csak a szervezeti célok vagy az üzleti igények teljesítéséhez szükséges minimális jogosultságokat kapják meg a fenti irányelveknek megfelelően. A védelmi intézkedés leginkább akkor alkalmazható, ha van olyan felhatalmazás, amely az ellenőrzött nem minősített információkhoz, vagy minősített információkhoz való hozzáférésre vonatkozó szabályokat határoz meg, és a rendszer egyes felhasználói nem jogosultak hozzáférni a rendszerben található összes ilyen információhoz. A kötelező hozzáférés-felügyelet a mérlegelés alapú hozzáférés-felügyelettel együtt is működhet, mely a "Hozzáférési szabályok érvényesítése – Mérlegelés alapú hozzáférés-felügyelet" kontroll esetében kerül bővebben kifejtésre. A kötelező hozzáférés-felügyeleti irányelvek által korlátozott alany továbbra is működhet a mérlegelésen alapuló hozzáférés-felügyelet kevésbé szigorú korlátozásai szerint, de a kötelező hozzáférés-felügyeleti irányelvek elsőbbséget élveznek a mérlegelésen alapuló hozzáférés-felügyelet kevésbé szigorú korlátozásaival szemben. Például, míg a kötelező hozzáférés-felügyeleti szabályok olyan korlátozásokat írnak elő, amelyek megakadályozzák, hogy az alany információt adjon át egy másik, más hatásköri vagy besorolási szinten működő alany számára, mérlegelésen alapuló hozzáférés-felügyelet lehetővé teszi az alany számára, hogy az információt bármely más, az alanyéval azonos hatásköri vagy besorolási szintű alany számára átadja.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a kötelező hozzáférés-felügyelet szabályait, melyek egységesen érvényesek az EIR minden alanyára és objektumára.
2. A szervezetnek biztosítania kell, hogy az EIR képes legyen a szabályok érvényesítésére. Ez magában foglalhatja az EIR hozzáférés-felügyeleti beállításainak konfigurálását, vagy további biztonsági intézkedések végrehajtását is megkövetelheti.
3. A szervezetnek biztosítania kell, hogy a szabályokat minden új alany és objektum esetében alkalmazzák, amikor azokat az EIR-be integrálják.
4. A szervezetnek ki kell alakítania egy folyamatot a szabályok végrehajtásának nyomon követésére és felülvizsgálatára is.
5. A szervezetnek naplóznia/dokumentálnia kell a mérlegelés alapú hozzáférés-felügyeleti szabályok alkalmazását, beleértve a hozzáférési jogosultságok hozzárendelését és azok változásait.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.17. A határok védelme

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kötelező hozzáférés-felügyeleti szabályok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.18. Hozzáférési szabályok érvényesítése – Mérlegelés alapú hozzáférés-felügyelet

2.18. Az EIR érvényesíti a meghatározott mérlegelés alapú hozzáférés-felügyeleti szabályokat a szervezet által meghatározott alanyok és objektumok halmazán, ahol a szabályzat meghatározza, hogy az információhoz való hozzáférést engedélyező alany az alábbiak közül egyet vagy többet megtehet:

2.18.1. Átadhatja az információt más alanyoknak vagy objektumoknak.

2.18.2. Átruházhatja a jogosultságait más alanyoknak.

2.18.3. Módosíthatja az alanyokon, objektumokon, a rendszeren vagy a rendszerelemeken található biztonsági tulajdonságokat.

2.18.4. Kiválaszthatja az újonnan létrehozott vagy módosított objektumokhoz rendelt biztonsági tulajdonságokat.

2.18.5. Módosíthatja a hozzáférés-felügyeleti szabályokat.

Magyarázat

A mérlegelésen alapuló hozzáférés-felügyeleti szabályok alkalmazása esetén az alanyok nincsenek korlátozva abban a tekintetben, hogy milyen műveleteket végezhetnek azokkal az információkkal, amelyekhez már hozzáférést kaptak. Így az információhoz való hozzáférést már megkapott alanyok nem akadályozhatók meg abban, hogy az információt más alanyoknak vagy objektumoknak átadják. A mérlegelésen alapuló hozzáférés-felügyelet a kötelező hozzáférés-felügyelettel együtt is működhet. Egy olyan alany, akinek a működését a kötelező hozzáférés-felügyeleti irányelvek korlátozzák, továbbra is működhet a mérlegelésen alapuló hozzáférés-felügyelet kevésbé szigorú korlátozásai mellett. Ezért, míg a kötelező hozzáférés-felügyelet olyan korlátozásokat ír elő, amelyek megakadályozzák, hogy egy alany információt adjon át egy másik, más hatásköri vagy besorolási szinten működő alany számára, addig a mérlegelésen alapuló hozzáférés-felügyelet lehetővé teszi az alany számára, hogy az információt bármely, azonos hatásköri vagy besorolási szinten lévő alany számára átadja. A szabályokat az EIR korlátozza. Ha az információ a rendszer ellenőrzési hatóköréből kikerül, további eszközökre lehet szükség annak biztosítására, hogy a korlátozások érvényben maradjanak. Míg a mérlegelésen alapuló hozzáférés-felügyelet hagyományos definíciói

személyazonosság-alapú hozzáférés-felügyeletet követelnek meg, a mérlegelésen alapuló hozzáférés-felügyelet e sajátos alkalmazása esetén ez a korlátozás nem szükséges.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a mérlegelés alapú hozzáférés-felügyeleti szabályokat a szervezet által meghatározott alanyok és objektumok halmazán.
2. A szervezetnek biztosítania kell, hogy az EIR képes legyen a szabályok érvényesítésére. Ez magában foglalhatja az EIR hozzáférés-felügyeleti beállításainak konfigurálását, vagy további biztonsági intézkedések végrehajtását is megkövetelheti.
3. A szervezetnek biztosítania kell, hogy a szabályokat minden új alany és objektum esetében alkalmazzák, amikor azokat az EIR-be integrálják.
4. A szervezetnek ki kell alakítania egy folyamatot a szabályok végrehajtásának nyomon követésére és felülvizsgálatára is.
5. A szervezetnek naplóznia/dokumentálnia kell a mérlegelés alapú hozzáférés-felügyeleti szabályok alkalmazását, beleértve a hozzáférési jogosultságok hozzárendelését és azok változásait.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a mérlegelés alapú hozzáférés-ellenőrzési szabály meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.19. Hozzáférési szabályok érvényesítése – Biztonsággal kapcsolatos információk

2.19. A szervezet megakadályozza a hozzáférést a meghatározott, biztonsági szempontból releváns információkhoz, kivéve, ha a rendszer biztonságos, de nem aktív rendszerállapotban van.

Magyarázat

A biztonsági szempontból releváns információ a rendszereken belüli olyan információ, amely potenciálisan befolyásolhatja a biztonsági funkciók működését vagy a biztonsági szolgáltatások nyújtását oly módon, hogy az a rendszer biztonsági szabályai érvényesítésének vagy a kódok és az adatok elkülönítésének hiányát eredményezheti. A biztonsági szempontból releváns információk közé tartoznak a hozzáférés-felügyeleti listák, az útválasztók (router) vagy tűzfalak szűrési szabályai, a biztonsági szolgáltatások konfigurációs paraméterei és a kriptográfiai kulcskezeléssel kapcsolatos információk. A biztonságos, nem aktív rendszerállapotok közé tartoznak azok az időszakok, amikor a rendszerek nem végeznek a szervezeti célokkal vagy üzleti tevékenységgel kapcsolatos feldolgozást. Például amikor a rendszer karbantartás, indítás, hibaelhárítás vagy leállítás miatt offline állapotban van.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania kell a biztonsági szempontból releváns információkat az EIR-ben.
2. A szervezetnek olyan szabályokat és eljárásokat kell létrehoznia, melyek alkalmazásával képes megakadályozni a hozzáférést a biztonsági szempontból releváns információkhoz (pl.: hozzáférés-felügyeleti listák, útválasztók (router) vagy tűzfalak szűrési szabályai), kivéve, ha az EIR biztonságos, de nem aktív állapotban van.

Kapcsolódó intézkedések

6.23. Konfigurációs beállítások

17.108. A folyamatok elkülönítése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonságkritikus információk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.20. Hozzáférési szabályok érvényesítése – Szerepkör alapú hozzáférés-ellenőrzés

2.20. A szervezet szerepkör alapú hozzáférési szabályokat alkalmaz a meghatározott alanyokra és objektumokra vonatkozóan. A hozzáféréseket a meghatározott szerepkörök és az ilyen szerepkörök betöltésére jogosult felhasználók alapján szabályozza.

Magyarázat

A szerepkör alapú hozzáférés-felügyelet olyan hozzáférés-felügyeleti szabályozás, amely az objektumokhoz és a rendszerfunkciókhoz való hozzáférést az alany meghatározott szerepe (pl. munkaköre) alapján érvényesíti. A szervezetek a munkakörökhöz és a szervezet által meghatározott szerepkörökhöz kapcsolódó, a rendszerekben végrehajtandó műveletekhez szükséges felhatalmazásokhoz (azaz jogosultságokhoz) kapcsolódó konkrét szerepköröket hozhatnak létre. Amikor a felhasználókat konkrét szerepkörökhöz rendelik, akkor az adott szerepkörökhöz meghatározott jogosultságokat vagy kiváltságokat kapnak. A szerepkör alapú hozzáférés-felügyelet leegyszerűsíti a szervezetek számára a jogosultságok kezelését, mivel a jogosultságokat nem közvetlenül minden felhasználóhoz rendelik hozzá (ami nagyszámú személyt jelenthet), hanem azt a szerepkörök hozzárendelésével kapják meg. A szerepkör alapú hozzáférés-felügyelet növelheti a biztonsági kockázatot, ha a szerepkörhöz rendelt egyének olyan információkhoz férnek hozzá, amelyek meghaladják a szervezet céljaihoz vagy üzleti funkciók támogatásához szükséges mértéket. A szerepkör alapú hozzáférés-felügyelet a kötelező vagy mérlegelésen alapuló hozzáférés-felügyelet formájában is megvalósítható. Azon szervezet esetében, mely kötelező hozzáférés-felügyeletként alkalmazza a szerepkör alapú hozzáférés-felügyeletet a "Kötelező hozzáférés-felügyelet" követelményei határozzák meg a szabályok által lefedett alanyok és objektumok körét.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a szerepköröket, amelyeket az EIR-en belül alkalmazni kíván. Ezek a szerepkörök általában a felhasználók által betöltött munkakörökön alapulnak.
2. Miután meghatározták a szerepköröket, a szervezetnek meg kell határoznia az egyes szerepkörökhöz tartozó hozzáférési jogosultságokat.

3. A szerepkörök és a hozzáférési jogosultságok meghatározása után a szervezetnek hozzá kell rendelnie a felhasználókat a megfelelő szerepkörökhöz.
4. A szervezetnek ki kell alakítania egy folyamatot a szabályok végrehajtásának nyomon követésére és felülvizsgálatára is.
5. A szervezetnek naplóznia/dokumentálnia kell a szerepkör alapú hozzáférés-felügyeleti szabályok alkalmazását, beleértve a felhasználók szerepkörökhöz történő hozzárendelését és a hozzáférési jogosultságok változásait.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szerepek és a szerepkörök betöltésére jogosult felhasználók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.21. HOZZÁFÉRÉSI SZABÁLYOK ÉRVÉNYESÍTÉSE – HOZZÁFÉRÉSI ENGEDÉLYEK VISSZAVONÁSA

2.21. A szervezet érvényesíti a hozzáférési jogosultságok visszavonását az alanyok és az objektumok biztonsági tulajdonságainak változása esetén, a szervezet által meghatározott, a hozzáférési jogosultságok visszavonásának időzítésére vonatkozó szabályok alapján.

MAGYARÁZAT

A hozzáférési jogosultságok visszavonására vonatkozó szabályok a visszavont jogosultságok típusai alapján eltérőek lehetnek. Például, ha egy alany eltávolításra kerül egy csoportból, a hozzáférés visszavonására csak az objektum következő megnyitásakor kerülhet sor, vagy amikor az alany legközelebb megpróbál hozzáférni az objektumhoz. A szervezetek alternatív megközelítéseket biztosítanak arra vonatkozóan, hogy hogyan lehet a visszavonást azonnal megtenni, ha a rendszerek nem képesek ilyen képességet biztosítani, és azonnali visszavonásra van szükség.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a hozzáférési jogosultságok visszavonásának időzítésére vonatkozó szabályokat. Ezek a szabályok változhatnak a visszavonandó hozzáférés típusától függően.
2. A szervezetnek rendszeresen ellenőriznie kell az EIR-ben található alanyok és objektumok biztonsági tulajdonságait. Ha változás történik, az érintett szervezetnek érvényesítenie kell a hozzáférési jogosultságok visszavonását.
3. A szervezetnek alternatív megoldásokat kell biztosítania a visszavonás azonnali érvényesítésére, ha az EIR nem képes erre, de azonnali visszavonásra van szükség.
4. A szervezetnek naplóznia kell a hozzáférési jogosultságok visszavonását, hogy nyomon követhető legyen, mikor és milyen változások történtek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hozzáférési jogosultságok visszavonásának időzítésére vonatkozó szabályok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.22. HOZZÁFÉRÉSI SZABÁLYOK ÉRVÉNYESÍTÉSE – SZABÁLYOZOTT TOVÁBBÍTÁS

2.22. A szervezet csak akkor továbbít információt az EIR-ből, ha:

2.22.1. a meghatározott fogadó rendszer vagy rendszerelem megfelel a szervezet által meghatározott követelményeknek, és

2.22.2. a szervezet által meghatározott követelményeket alkalmazzák a továbbítandó információ megfelelőségének ellenőrzésére.

MAGYARÁZAT

Legyen szó akár a szervezeten belüli továbbításról, akár a szervezeten kívüli továbbításról, az EIR-ből csak abban az esetben kezdeményezhető információ továbbítás, ha a fogadó rendszer vagy rendszerelem megfelel az érintett szervezet által elvárt követelményeknek. A szervezet csak akkor tudja közvetlenül védeni az információkat, ha azok a rendszeren belül vannak. További ellenőrzésekre lehet szükség annak biztosításához, hogy a szervezeti információk megfelelő védelemben részesüljenek, amint a rendszeren kívülre kerülnek. Azokban a helyzetekben, amikor a rendszer nem tudja meghatározni a külső rendszerek által nyújtott védelem megfelelőségét, kockázatcsökkentő intézkedésként a szervezet különféle eljárások alkalmazásával határozhatja meg, hogy a külső rendszerek megfelelő védelemmel rendelkeznek-e. A külső rendszerek megfelelő védelmének felmérési eszközei közé tartozik például az időszakos értékelések elvégzése, a fogadó rendszer tulajdonosának nyilatkoztatása a fogadó rendszer/rendszerelem biztonsági szintjéről. Példa erre az EIR összekapcsolása más rendszerekkel, de ide tartozik az is, mikor az EIR információt továbbít egy nyomtatónak, mely a szervezet által ellenőrzött területen található. Ebben az esetben különféle eljárásokkal biztosítható, hogy csak az arra jogosult személyek férjenek hozzá az adott nyomtatóhoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a követelményeket azokkal a rendszerekkel és rendszerelemekkel kapcsolatban, melyekbe az EIR-ből információt szeretne továbbítani.
2. A szervezetnek az információ továbbítása előtt meg kell győződnie arról, hogy a fogadó rendszer vagy rendszerelem megfelel az érintett szervezet által meghatározott

követelményeknek pl.: időszakos értékelések elvégzése, a fogadó rendszer tulajdonosának nyilatkoztatása a fogadó rendszer/rendszerelem biztonsági szintjéről.

3. A szervezetnek felügyelni kell minden információáramlást annak érdekében, hogy az információ a követelmények megkerülésével ne legyen továbbítható. Illetve amennyiben a továbbítás a követelmények megkerülésével mégis megtörtént, megtehesse a szükséges intézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.6. Információcsere

16.49. Külső elektronikus információs rendszerek szolgáltatásai

17.58. Biztonsági tulajdonságok átvitele

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.23. Hozzáférési szabályok érvényesítése – Hozzáférés-ellenőrző mechanizmusok ellenőrzött felülbírálata

2.23. A szervezet meghatározott feltételek esetén meghatározott szerepkörök számára biztosítja az automatizált hozzáférés-felügyeleti mechanizmusok ellenőrzött felülbírálatát.

Magyarázat

Bizonyos helyzetekben, például amikor emberi életet fenyegető veszély vagy olyan esemény következik be, amely veszélyezteti a szervezet kritikus fontosságú céljainak vagy üzleti funkcióinak végrehajtását, szükség lehet a hozzáférés-felügyeleti mechanizmusok felülbírálási képességére. A felülbírálási feltételeket a szervezetek határozzák meg, és csak ezekben az esetekben, korlátozott körülmények között használják. Az ilyen eseményeket a naplózási követelmények szerint ajánlott naplózni. Az ide vonatkozó naplózási követelmények a "Naplózható események" és a "Naplóbejegyzések létrehozása" kontrolloknál kerültek bővebben kifejtésre.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia azokat a feltételeket, amikor a hozzáférés-felügyeleti mechanizmusok felülbírálatára van szükség. Ilyen helyzetek lehetnek például, amikor emberéletet fenyegető veszély áll fenn, illetve amikor olyan esemény fenyegeti a szervezetet, mely szignifikáns hatást gyakorol a szervezeti célok elérésére és a működésfolytonosság biztosítására.
2. A szervezetnek meg kell határoznia azokat a szerepköröket, amelyek számára biztosítja az automatizált hozzáférés-felügyeleti mechanizmusok ellenőrzött felülbírálatát.
3. A szervezetnek naplóznia kell az automatizált hozzáférés-felügyeleti mechanizmusok felülbírálatát.

Kapcsolódó intézkedések

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.33. Letagadhatatlanság

4.40. Naplóbejegyzések létrehozása

4.48. Munkaszakasz-ellenőrzés

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a feltételek, illetve a szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.24. Hozzáférési szabályok érvényesítése – Meghatározott információtípusokhoz való hozzáférés korlátozása

2.24. A szervezet korlátozza a hozzáférést a meghatározott információtípusokat tartalmazó adattárakhoz.

Magyarázat

Az adott információhoz való hozzáférés korlátozásának célja, hogy rugalmasságot biztosítson az EIR-en belüli bizonyos információtípusokhoz való hozzáférés-felügyelet tekintetében. Például a szerepkör alapú hozzáférés-felügyelet alkalmazható arra, hogy az adatbázisban csak egy bizonyos típusú, személyazonosításra alkalmas információhoz lehessen hozzáférni, ahelyett, hogy az adatbázis egészéhez engedélyeznék a hozzáférést. Egyéb példa lehet a kriptográfiai kulcsokhoz, hitelesítési információkhoz és kiválasztott rendszerinformációkhoz való hozzáférés korlátozása. Az érintett szervezetnek biztosítania kell, hogy a hozzáférési jogosultságokat csak a szükséges mértékben adják meg. A felhasználóknak csak azokhoz az információkhoz kell hozzáférniük, amelyekre munkájuk elvégzéséhez szükségük van. Ez segít minimalizálni a kockázatot, hogy a felhasználók jogosulatlanul hozzáféréssel éljenek vagy módosítsanak érzékeny információkat.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia azokat az információtípusokat, amelyekhez korlátozni szeretné a hozzáférést az EIR-en belül.
2. A szervezetnek létre kell hoznia egy hozzáférés-felügyeleti szabályzatot, melyet a gyakorlatban is alkalmaznia kell. Ezáltal korlátozni tudja az egyes információtípusokhoz történő hozzáférést Például a szerepkör alapú hozzáférés-felügyelet biztosíthatja, hogy egy adatbázisban csak egy bizonyos típusú, személyazonosításra alkalmas információhoz lehessen hozzáférni, ahelyett, hogy az egész adatbázishoz engedélyeznék a hozzáférést.
3. A szervezetnek biztosítania kell, hogy a hozzáférési jogosultságokat csak a szükséges mértékben adják meg. Ez azt jelenti, hogy a felhasználók csak olyan információkhoz férnek hozzá, amelyekre a munkájuk elvégzéséhez szükségük van.

4. A szervezetnek naplóznia kell a hozzáférési kísérleteket. Ez azt jelenti, hogy minden hozzáférési kísérletet rögzíteni kell, beleértve a sikeres és sikertelen kísérleteket is. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon kövesse, ki, mikor és milyen információkhoz próbált hozzáférni.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.36. Rendszerelem leltár

6.52. Információ helyének azonosítása és dokumentálása

1.5. Elektronikus információs rendszerek nyilvántartása

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.4

NIST SP 800-53 REV.5 REFERENCIA

AC-3(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információ típusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.25. HOZZÁFÉRÉSI SZABÁLYOK ÉRVÉNYESÍTÉSE – ALKALMAZÁS-HOZZÁFÉRÉS BIZTOSÍTÁSA ÉS ÉRVÉNYESÍTÉSE

2.25. A szervezet:

2.25.1. biztosítja, hogy az alkalmazások a telepítési folyamat részeként hozzáférjenek a meghatározott rendszeralkalmazásokhoz és rendszerfunkciókhoz;

2.25.2. érvényesítési mechanizmust biztosít a jogosulatlan hozzáférés megakadályozására; és

2.25.3. jóváhagyja a hozzáférési jogosultságok változásait az alkalmazás első telepítése után.

MAGYARÁZAT

Az alkalmazás-hozzáférés biztosítása és érvényesítése olyan alkalmazásokra vonatkozik, amelyeknek hozzá kell férniük a meglévő rendszeralkalmazásokhoz és funkciókhoz, beleértve a felhasználói kapcsolatokat, globális helymeghatározó rendszereket, kamerákat, billentyűzeteket, mikrofonokat, hálózatokat, telefonokat vagy egyéb fájlokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy mely rendszeralkalmazásokhoz és rendszerfunkciókhoz szükséges hozzáférés az alkalmazások telepítése során.

2. A szervezetnek érvényesítési mechanizmust kell biztosítania a jogosulatlan hozzáférés megakadályozására a telepítési folyamat során. Ez magában foglalhatja a felhasználói hitelesítést, a hozzáférési jogosultságok ellenőrzését.

3. A szervezetnek jóvá kell hagynia a hozzáférési jogosultságok változásait az alkalmazás első telepítése után. A szervezetnek folyamatosan nyomon kell követnie és ellenőriznie kell a hozzáférési jogosultságokat, és jóvá kell hagynia minden változást.

4. A szervezetnek biztosítania kell, hogy a hozzáférési jogosultságok változásai naplózásra/dokumentálásra kerüljenek, és rendszeresen ellenőrizze a naplókat a jogosulatlan hozzáférési kísérletek vagy a jogosulatlan hozzáférési jogosultságok változásainak azonosítása érdekében.

Kapcsolódó intézkedések

6.26. Legszűkebb funkcionalitás

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-3(12)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.26. Hozzáférési szabályok érvényesítése – Tulajdonság alapú hozzáférés-ellenőrzés

2.26. A szervezet tulajdonság alapú hozzáférés-felügyeleti szabályokat alkalmaz a meghatározott alanyok és objektumok esetében. A hozzáférési jogosultságokat és engedélyeket a szervezet által meghatározott tulajdonságok alapján szabályozza.

Magyarázat

A tulajdonság, vagy más nevén attribútum alapú hozzáférés-felügyelet olyan hozzáférés-felügyeleti szabályozás, amely meghatározott szervezeti jellemzők (pl.: munkakör, személyazonosításra alkalmas tulajdonság(ujjlenyomat, íriszkép, arcarány)), tevékenységi jellemzők (pl. olvasási, írási, törlési jogosultság), környezeti jellemzők (pl. napszak, helyszín (lokáció)) és erőforrás jellemzők (pl. egy dokumentum osztályba sorolása) alapján korlátozza az EIR-hez történő hozzáférést az engedélyezett felhasználókra. A szervezet az egyes tulajdonságokon és engedélyeken (azaz jogosultságokon) alapuló szabályokat hozhat létre az EIR-ekben szükséges műveletek elvégzéséhez a szervezet által meghatározott tulajdonságok és szabályok alapján. Amikor a felhasználók a tulajdonság alapú hozzáférés-felügyeleti szabályokban vagy irányelvekben meghatározott jellemzőkkel rendelkeznek, akkor a megfelelő jogosultságok birtokában biztosítható számukra egy EIR-hez történő hozzáférés, vagy dinamikusan biztosítható számukra a hozzáférés egy védett erőforráshoz. A tulajdonság alapú hozzáférés-felügyelet a hozzáférés-felügyelet kötelező vagy mérlegelésen alapuló formájában is megvalósítható.

A követelmény alkalmazásának lépései

1. A szervezetnek a tulajdonság alapú hozzáférés-felügyelet megvalósításához meg kell határoznia azon tulajdonságokat melyek alapján hozzáférési jogosultságokat és engedélyeket oszt ki. Ilyen tulajdonságok lehetnek a következők: munkakör, személyazonosításra alkalmas tulajdonság (ujjlenyomat, íriszkép, arcarány), tevékenységi jellemzők (pl. olvasási, írási, törlési jogosultság), környezeti jellemzők (pl. napszak, helyszín (lokáció)), erőforrás jellemzők (pl. egy dokumentum osztályba sorolása).

2. A szervezetnek ki kell osztania a jogosultságokat és engedélyeket a meghatározott szabályok, tulajdonságok- és legkisebb jogosultság elve alapján.
3. A szervezetnek rendszeresen felül kell vizsgálnia a kiosztott jogosultságokat és a már nem szükséges jogosultságokat mielőbb vissza kell vonnia.
4. A szervezetnek naplóznia/dokumentálnia kell a tulajdonság alapú hozzáférés-felügyeleti szabályok alkalmazását, beleértve a felhasználók számára kiosztott jogosultságokat és a hozzáférési jogosultságok változásait.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-3(13)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hozzáférési jogosultságok és engedélyek szabályozására vonatkozó tulajdonságok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.27. Hozzáférési szabályok érvényesítése – Kötelező és mérlegelés alapú hozzáférés-felügyelet

2.27. A szervezet érvényesíti

2.27.1. a kötelező hozzáférés-felügyeleti szabályokat a meghatározott alanyok és objektumok halmazán; és

2.27.2. a mérlegelés alapú hozzáférés-felügyeleti szabályokat a meghatározott alanyok és objektumok halmazán.

Magyarázat

A kötelező hozzáférés-felügyeleti szabályok értelmében az érintett szervezet előre meghatározott szabályokat alkot, amelyek meghatározzák, hogy mely alanyok férhetnek hozzá mely objektumokhoz. Ez a szabályrendszer általában a biztonsági osztályokba sorolt objektumok és alanyok közötti interakciókat szabályozza.

A mérlegelés alapú hozzáférés-felügyeleti szabályok esetében a szervezet lehetővé teszi, hogy az alanyok saját belátásuk szerint döntsenek arról, hogy mely más alanyok férhetnek hozzá az általuk birtokolt vagy kezelt objektumokhoz. Ez a szabályrendszer általában a felhasználók közötti információmegosztást szabályozza. Ezzel szemben a kötelező hozzáférés-felügyeleti szabályok ezt nem teszik lehetővé.

A kötelező és a mérlegelésen alapuló hozzáférés-felügyeleti szabályok egyidejű alkalmazása további védelmet nyújthat a felhasználók vagy a felhasználók nevében eljáró folyamatok által végrehajtott kódok jogosulatlan futtatása ellen. Ez segít megelőzni, hogy egyetlen kompromittált felhasználó vagy folyamat veszélyeztesse az egész EIR-t.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia azokat az alanyokat és objektumokat, amelyekre a hozzáférés-felügyeleti szabályokat alkalmazni kell. Az alanyok lehetnek felhasználók, csoportok vagy folyamatok, míg az objektumok lehetnek fájlok, könyvtárak, adatbázisok stb. az EIR-en belül.

2. A szervezetnek érvényesítenie kell a kötelező hozzáférés-felügyeleti szabályokat a meghatározott alanyok és objektumok halmazán. Ez azt jelenti, hogy a hozzáférési jogosultságokat a felhasználók nem módosíthatják.
3. A szervezetnek érvényesítenie kell a mérlegelés alapú hozzáférés-felügyeleti szabályokat a meghatározott alanyok és objektumok halmazán. Ez azt jelenti, hogy a felhasználók képesek módosítani a hozzáférési jogosultságokat a saját objektumaikra, de csak a meghatározott keretek között.
4. A szervezetnek naplóznia kell a hozzáférési kísérleteket és a hozzáférési jogosultságok módosításait, hogy nyomon követhető legyen, ki, mikor és milyen jogosultságokkal fér hozzá az EIR objektumaihoz.
5. A szervezetnek rendszeresen felül kell vizsgálnia a hozzáférési jogosultságokat és a naplókat, hogy biztosítsa a hozzáférés-felügyeleti szabályok betartását és az esetleges biztonsági rések időben történő észlelését.
6. A szervezetnek képzést kell biztosítania a felhasználóknak a hozzáférés-felügyeleti szabályokról és a biztonsági előírásokról, hogy megértsék a szabályokat és tudják, hogyan kell betartani őket.

Kapcsolódó intézkedések

17.2. Rendszer és felhasználói funkciók szétválasztása
17.4. Biztonsági funkciók elkülönítése
2.28. Információáramlási szabályok érvényesítése

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-3(15)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.28. INFORMÁCIÓÁRAMLÁSI SZABÁLYOK ÉRVÉNYESÍTÉSE

2.28. A szervezet a meghatározott információáramlási szabályokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzése során.

MAGYARÁZAT

Az információáramlás-ellenőrzés szabályozza, hogy az információ hova utazhat az EIR-en belül és az EIR-ek között, és nincs tekintettel a későbbi hozzáférésekre. Az áramlásellenőrzési korlátozások közé tartozik olyan külső forgalom blokkolása, amely úgy tűnik, mintha az érintett szervezeten belülről származna, a belső web proxy szerveren kívüli webes kérések korlátozása, és az információáramlás korlátozása a szervezetek között az adatszerkezetek és a tartalom alapján. A szervezetek közötti információcsere szükség esetén történhet egy olyan egyezség segítségével, amelyben meghatározzák, hogy az információáramlási szabályok hogyan kerülnek érvényesítésre. Az ezzel kapcsolatos elvárások az "Információcsere" kontrollnál kerültek bővebben kifejtésre. A különböző biztonsági- és adatvédelmi tartományokban található EIR-ek közötti információcsere esetén fennállhat az a kockázat, hogy az információcsere megsérti egy vagy több tartomány biztonsági előírásait. Ilyen helyzetekben az egyes adatgazdák szolgálhatnak iránymutatással. Az információáramlási szabályok érvényesítésére lehet példa, mikor összekapcsolt EIR-ek között a szervezet megtiltja az információcserét (csak a hozzáférés engedélyezett, egyéb műveletek nem), továbbá az írási jogosultság ellenőrzése, mielőtt információ kerülne elfogadásra egy másik biztonsági tartományból vagy kapcsolat EIR-ből. A szervezet figyelembe veszi az információáramlás érvényesítése szempontjából kritikus fontosságú szűrési és/vagy ellenőrzési mechanizmusok (azaz hardver-, firmware- és szoftverkomponensek) megbízhatóságát is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az információáramlási szabályokat, amelyek szabályozzák, hogy az információ hova utazhat az EIR-en belül és az EIR-ek között.
2. A szervezetnek alkalmaznia kell a gyakorlatban a meghatározott információáramlási szabályokat pl.: olyan külső forgalom blokkolása, amely úgy tűnik, mintha a szervezeten belülről származna.

3. Szervezetek közötti információcsere esetén amennyiben szükséges, a szervezeteknek olyan egyezséget kell kötniük, melyben meghatározzák, hogy az információáramlási szabályok hogyan kerülnek érvényesítésre.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

2.60. Legkisebb jogosultság elve

2.89. Biztonsági tulajdonságok

2.100. Távoli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

2.121. Információmegosztás

4.33. Letagadhatatlanság

5.6. Információcsere

5.24. Belső rendszerkapcsolatok

6.26. Legszűkebb funkcionalitás

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.4. Információáramlás ellenőrzés érvényesítése: Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzéséhez az érintett szervezet által meghatározott információáramlás ellenőrzési szabályoknak megfelelően.

ISO/IEC 27001:2023 REFERENCIA

A.5.14; A.8.22; A.8.23

NIST SP 800-53 REV.5 REFERENCIA

AC-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információáramlási szabályok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.29. Információáramlási szabályok érvényesítése – az objektumok biztonsági tulajdonságai

2.29. A szervezet meghatározott biztonsági tulajdonságokat rendel a meghatározott információkhoz, forrás- és cél objektumokhoz kapcsolódóan, hogy a meghatározott információáramlási szabályokat kikényszerítse az információáramlást érintő döntések során.

Magyarázat

Az információáramlási szabályokat érvényesítő eljárások összehasonlítják az információkhoz, valamint a forrás- és célobjektumokhoz kapcsolódó biztonsági jellemzőket, és megfelelően reagálnak, amikor a szabályok által külön nem engedélyezett információáramlással találkoznak. Például egy bizalmasnak minősített információs objektumnak engedélyezik a bizalmasnak minősített célobjektumhoz való kapcsolódást, de egy titkosnak minősített információs objektumnak nem engedélyezik a bizalmasnak minősített célobjektumhoz való kapcsolódást. A biztonsági tulajdonságok közé tartozhatnak a forgalomszűrő tűzfalakban használt forrás- és célcímek is. Az információáramlás kikényszerítése egyértelmű biztonsági jellemzők pl. bizonyos típusú információk nyilvánosságra hozatalának ellenőrzésére használható.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia a biztonsági tulajdonságokat, amelyeket a meghatározott információkhoz, forrás- és cél objektumokhoz rendel. Ezek a tulajdonságok lehetnek például biztonsági címkék, mint a "Bizalmas" vagy "Nem nyilvános".
2. A szervezetnek ezután meg kell határoznia az információáramlási szabályokat, amelyeket ezek a biztonsági tulajdonságok kikényszerítenek. Például, egy "Nem nyilvános" címkével ellátott információ objektum nem áramolhat egy "Nyilvános" címkével ellátott cél objektumhoz.
3. A szervezetnek implementálnia kell az információáramlás ellenőrzési mechanizmusokat az EIR-ben. Ezek a mechanizmusok összehasonlítják az információhoz, forrás- és cél objektumokhoz rendelt biztonsági tulajdonságokat, és megfelelően reagálnak, amikor olyan információáramlásokkal találkoznak, amelyeket az információáramlási szabályok nem engedélyeznek kifejezetten.

4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az információáramlási szabályokat és ellenőrzési mechanizmusokat, hogy biztosítsa az EIR megfelelő biztonsági szintjének fenntartását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi tulajdonságok illetve az információ forrás- és célobjektum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.30. Információáramlási szabályok érvényesítése – Feldolgozási tartományok

2.30. A szervezet védett feldolgozási tartományokat használ a meghatározott információáramlási szabályok érvényesítésére, az információáramlással kapcsolatos döntések megalapozásához.

Magyarázat

A védett feldolgozási tartományok olyan feldolgozási terek, amelyek ellenőrzött kapcsolatban állnak más feldolgozási terekkel, lehetővé téve az e terek közötti és az információs objektumok közötti információáramlás ellenőrzését. A védett feldolgozási tartományt például a tartomány és típus szerinti szabályozás megvalósításával lehet biztosítani. A tartomány és típus szerinti ellenőrzés során a rendszerfolyamatokat tartományokhoz rendelik, az információkat típusokkal azonosítják, és az információáramlást a megengedett (azaz a tartomány és a típus által meghatározott) információhoz való hozzáférés, a tartományok közötti megengedett kommunikáció és a más tartományokba történő engedélyezett átviteli eljárások alapján ellenőrzik.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a védett feldolgozási tartományokat.
2. A védett feldolgozási tartományok létrehozása után, a szervezetnek implementálnia kell a tartomány és típus érvényesítést. A tartomány és típus érvényesítés során az EIR folyamatait tartományokhoz rendelik, az információt típusokkal azonosítják, és az információáramlást az engedélyezett információhoz való hozzáférések (azaz a tartomány és típus által meghatározott), a tartományok közötti engedélyezett jelzések, és az engedélyezett folyamat-átmenetek alapján ellenőrzik.
3. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a védett feldolgozási tartományokban történő információáramlást, hogy biztosítsa a meghatározott információáramlási szabályok betartását.

4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén változtatnia kell a védett feldolgozási tartományokon és az információáramlási szabályokon, hogy biztosítsa a megfelelő biztonsági szint fenntartását.

Kapcsolódó intézkedések

17.108. A folyamatok elkülönítése

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-4(2)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az információáramlási szabályok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.31. Információáramlási szabályok érvényesítése – Az információáramlás dinamikus irányítása

2.31. A szervezet kikényszeríti a meghatározott dinamikus információáramlási szabályokat.

Magyarázat

Az információáramlás dinamikus irányítására vonatkozó szervezeti szabályok közé tartozik az információáramlás engedélyezése vagy tiltása a változó körülmények, illetve a szervezeti célok vagy a működési megfontolások alapján. A változó körülmények közé tartoznak a kockázattűrő képesség változásai, amelyek a szervezeti célok vagy az üzleti igények fontosságának változásai, a fenyegetési környezet változásai, valamint a potenciálisan káros vagy kedvezőtlen események észlelése miatt következnek be.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a dinamikus információáramlási szabályokat
2. A szervezetnek figyelembe kell vennie a változó körülményeket, amelyek a szervezeti célok vagy az üzleti igények fontosságának változásai, a fenyegetési környezet változásai, valamint a potenciálisan káros vagy kedvezőtlen események észlelése miatt következnek be.
3. A szervezetnek biztosítania kell, hogy az EIR megfelelően alkalmazza a dinamikus információáramlási szabályokat.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a meghatározott dinamikus információáramlási szabályokat, hogy biztosítsa a megfelelő biztonsági szint fenntartását.

Kapcsolódó intézkedések

18.13. Az EIR monitorozása

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információáramlási szabályok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.32. Információáramlási szabályok érvényesítése – Titkosított információk áramlásának irányítása

2.32. A szervezet az információk dekódolásával, a titkosított információáramlás blokkolásával vagy a titkosított információk átvitelével próbálkozó kommunikációs folyamat megszakításával megakadályozza, hogy titkosított információkkal megkerüljék a meghatározott információáramlás-ellenőrzési mechanizmusokat.

Magyarázat

A szervezet az információk dekódolásával, a titkosított információáramlás blokkolásával vagy a titkosított információk átvitelével próbálkozó kommunikációs folyamat megszakításával csökkentheti annak a kockázatát, hogy a biztonsági ellenőrzési mechanizmusokat egy rendszer vagy szolgáltatás megkerülje. Gyakori példa erre a titkosított forgalom bontása DLP rendszerek használata esetén.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia és implementálnia kell az információáramlással kapcsolatos ellenőrzési mechanizmusokat. Ez magában foglalhatja a tartalom ellenőrzését, biztonsági szempontból beállított szűréseket és adattípus azonosítókat.
2. A szervezetnek biztosítania kell, hogy az EIR képes legyen dekódolni a titkosított információkat. Ez azt jelenti, hogy az EIR-nek vagy a szervezetnek rendelkeznie kell a megfelelő dekódoló eszközökkel és algoritmusokkal.
3. A szervezetnek blokkolnia kell a titkosított információáramlást az EIR-ben, amennyiben ezt a megoldást választja. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie azonosítani és blokkolni azokat a kommunikációs folyamatokat, amelyek titkosított információkat próbálnak átvinni.
4. A szervezetnek meg kell szakítania a kommunikációs folyamatokat, amelyek titkosított információkkal próbálják megkerülni az érintett szervezet által implementált információáramlással kapcsolatos ellenőrzési mechanizmusokat. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie azonosítani és megszakítani ezeket a folyamatokat.

5. A szervezetnek naplóznia kell az összes ilyen eseményt, hogy nyomon követhesse és elemezhesse a kiberbiztonsági eseményeket és biztonsági eseményeket. Ez azt jelenti, hogy az EIR-nek rendelkeznie kell a megfelelő naplózási és elemzési eszközökkel.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.13. Az EIR monitorozása

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információáramlási mechanizmusok illetve a folyamat vagy módszer meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

2.33. Információáramlási szabályok érvényesítése – Beágyazott adattípusok

2.33. A szervezet kikényszeríti az adattípusok más adattípusokba való beágyazására vonatkozó meghatározott korlátozásokat.

Magyarázat

Az adattípusok más adattípusokba való beágyazása csökkentheti az információáramlás hatékonyságát. Az adattípusok beágyazása magában foglalja a fájlok objektumként történő beillesztését más fájlokba, valamint a tömörített vagy archivált adattípusok használatát, amelyek több beágyazott adattípust is tartalmazhatnak. Az adattípusok beágyazására vonatkozó korlátozások figyelembe veszik a beágyazás szintjeit, és tiltják az adattípusok beágyazásának olyan szintjeit, amelyek meghaladják az ellenőrző eszközök képességeit.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az adattípusok beágyazásának korlátozásait. Ez magában foglalja a fájlok más fájlokba történő beágyazását, valamint a tömörített vagy archivált adattípusok használatát, amelyek több beágyazott adattípusból állhatnak.
2. A szervezetnek figyelembe kell vennie a beágyazás szintjeit, és meg kell tiltania azokat a beágyazási szinteket, amelyek meghaladják az ellenőrző eszközök képességeit.
3. A szervezetnek implementálnia kell a korlátozásokat az EIR-ben. Ez magában foglalja a beágyazott adattípusok ellenőrzését és szűrését, valamint a nem megfelelő beágyazások blokkolását.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a beágyazási korlátozásokat, hogy biztosítsa az EIR megfelelő biztonsági szintjét. Ez magában foglalja a beágyazási szintek és a korlátozások felülvizsgálatát, valamint az ellenőrző eszközök képességeinek értékelését, esetleges fejlesztését.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a limitációk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.34. INFORMÁCIÓÁRAMLÁSI SZABÁLYOK ÉRVÉNYESÍTÉSE – METAADAT

2.34. A szervezet meghatározott metaadatok alapján érvényesíti az információáramlási szabályokat.

MAGYARÁZAT

A metaadatok az adatok jellemzőit leíró információk. A metaadatok közé tartozhatnak az adatstruktúrákat leíró strukturális metaadatok vagy az adattartalmat leíró metaadatok. A metaadatokon alapuló engedélyezett információáramlás érvényesítése egyszerűbb és hatékonyabb információáramlás-ellenőrzést tesz lehetővé. A szervezet figyelembe veszi a metaadatok megbízhatóságát az adatok pontossága, az adatok sértetlensége (azaz a metaadatcímkék jogosulatlan megváltoztatása elleni védelem), valamint a metaadatoknak az adattartalomhoz való kötése (azaz a megfelelő bizonyossággal rendelkező, kellően erős kötési technikák alkalmazása) tekintetében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a metaadatokat, amelyek alapján az információáramlást szabályozni kívánja.
2. A szervezetnek meg kell határoznia az információáramlási szabályokat, amelyeket a metaadatok alapján kíván érvényesíteni.
3. A szervezetnek implementálnia kell a metaadatok alapján működő információáramlási szabályokat az EIR-ben. Ez magában foglalhatja a metaadatok címkézését, a címkék hozzárendelését az adatokhoz, és a címkék alapján történő információáramlás szabályozását.
4. A szervezetnek biztosítania kell a metaadatok megbízhatóságát az adatok pontosságával, az adatintegritással (azaz a metaadat címkék jogosulatlan változtatásai elleni védelem) és a metaadatok kötésével az adatokhoz (azaz elegendően erős kötési technikák alkalmazása megfelelő biztosítékkal).
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az információáramlási szabályokat és a metaadatok használatát, hogy biztosítsa az EIR megfelelő szintű biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.89. Biztonsági tulajdonságok

18.42. Szoftver- és információsértetlenség

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a metaadatok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.35. Információáramlási szabályok érvényesítése – Egyirányú információáramlási mechanizmusok

2.35. A szervezet hardver alapú áramlásszabályozó mechanizmusok segítségével kényszeríti ki az információk egyirányú áramlását.

Magyarázat

Az egyirányú áramlási mechanizmusokat egyirányú hálózatnak, egyirányú biztonsági átjárónak vagy adatdiódának is nevezhetjük. Az egyirányú áramlási mechanizmusok felhasználhatóak arra, hogy megakadályozzák az adatok exportálását egy magasabb biztonsági besorolás alá tartozó vagy minősített tartományból, illetve rendszerből, miközben lehetővé teszik az adatok importálását egy alacsonyabb biztonsági besorolás alá tartozó vagy nem minősített tartományból, illetve rendszerből.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia, hogy mely információkat szeretné egyirányúan áramoltatni. Ez általában magasabb biztonsági besorolású adatokat jelent, melyeket nem szabad exportálni, miközben alacsonyabb biztonsági besorolás alá tartozó vagy nem minősített adatokat lehetséges iimportálni.
2. Az érintett szervezetnek hardver alapú áramlásszabályozó mechanizmusokat kell bevezetnie. Ezeket a mechanizmusokat egyirányú hálózatnak, egyirányú biztonsági átjárónak vagy adatdiódának is nevezik.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.36. Információáramlási szabályok érvényesítése – Biztonsági szűrők

2.36. A szervezet:

2.36.1. Érvényesíti az információáramlás szabályozását a meghatározott biztonsági szűrők alkalmazásával, amelyek alapján döntéseket hoz az áramlásszabályozással kapcsolatban.

2.36.2. Blokkolja, megjelöli, módosítja vagy karanténba helyezi az adatokat, a meghatározott biztonsági szabályok szerint.

Magyarázat

A szervezet által meghatározott biztonsági szűrők az adatszerkezetekre és a tartalomra is vonatkozhatnak. Az adatszerkezetekre vonatkozó biztonsági szűrők például ellenőrizhetik a maximális fájlhosszúságot, a maximális mezőméretet és az adat-/fájltípusokat. Az adattartalomra vonatkozó biztonsági szűrők ellenőrizhetik az egyes szavakat, a felsorolásos értékeket vagy adatérték-tartományokat, valamint a rejtett tartalmat. A strukturált adatok lehetővé teszik az adattartalom alkalmazások általi értelmezését. A strukturálatlan adatok olyan digitális információkra utalnak, amelyeknek nincs adatszerkezete, vagy olyan adatszerkezettel rendelkeznek, amely nem könnyíti meg az adatok által közvetített információk hatásának vagy osztályozási szintjének kezelésére szolgáló szabálykészletek kialakítását, illetve az információáramlási döntéseket. A strukturálatlan adatok olyan képi objektumokból állnak, amelyek eredendően nem nyelvi alapúak (azaz kép-, video- vagy hangfájlok), valamint olyan szöveges objektumokból, amelyek írott vagy nyomtatott nyelveken alapulnak. A szervezetek egynél több biztonsági szűrőt is alkalmazhatnak az információáramlási szabályok céljainak teljesítése érdekében.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a biztonsági szűrőit, amelyek adatszerkezetekre és tartalmakra is vonatkozhatnak.

2. A szervezet által meghatározott, adatszerkezetekre vonatkozó biztonsági szűrők ellenőrizhetik a maximális fájlhosszúságot, a maximális mezőméretet és az adat-/fájltípusokat.

3. A szervezet által meghatározott, adattartalomra vonatkozó biztonsági szűrők ellenőrizhetik az egyes szavakat, felsorolásos értékeket vagy adatérték-tartományokat, valamint rejtett tartalmakat.

3. A szervezetnek meg kell határoznia a strukturált adatokat, amelyek lehetővé teszik az alkalmazások számára az adattartalom értelmezését. A strukturálatlan adatokra digitális információként kell tekinteni, amelyeknek nincs adatszerkezetük, vagy olyan adatszerkezetük van, amely nem segíti a szabálykészletek kialakítását az adatok által közvetített információ hatásának vagy besorolási szintjének kezelésére, vagy az áramlásszabályozási döntések meghatározásában.

4. A szervezet a fent meghatározott biztonsági szűrők alkalmazásával kell döntést hozzon az adatáramlással kapcsolatosan. Ez lehet blokkolás,megjelölés, módosítás vagy karanténba helyezés.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-4(8)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.37. Információáramlási szabályok érvényesítése – Emberi beavatkozással történő felülvizsgálat

2.37. A szervezet meghatározott feltételeket alkalmaz az információáramlás emberi beavatkozással történő felülvizsgálatára.

Magyarázat

A szervezet biztonsági szűrőket definiál minden olyan helyzetre, ahol automatizált információáramlás-szabályozási döntések meghozatalára kerülhet sor. Ha a teljesen automatizált áramlásszabályozási döntés nem lehetséges, akkor az automatizált biztonsági szűrés helyett vagy kiegészítéseként emberi beavatkozással történő felülvizsgálatot lehet alkalmazni. Az emberi beavatkozással történő felülvizsgálatokat akkor is alkalmazni lehet, ha a szervezet ezt szükségesnek ítéli.

A követelmény alkalmazásának lépései

1. A szervezet határozza meg az információáramlásra vonatkozó biztonsági szűrőket minden olyan eshetőségre, ahol automatizált, információáramlásra vonatkozó döntések lehetségesek.
2. A szervezet határozza meg, hogy mely esetekben nem lehetséges az automatizált biztonsági szűrés. Ezekben az esetekben a szűrés helyett vagy kiegészítésként emberi beavatkozással történő felülvizsgálatot kell alkalmazni.
3. A szervezet akkor is alkalmazhat emberi beavatkozással történő felülvizsgálatot, amennyiben azt szükségesnek ítéli.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információáramlások, illetve a feltételek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.38. Információáramlási szabályok érvényesítése – Biztonsági szűrők engedélyezése és kikapcsolása

2.38. A szervezet lehetővé teszi a jogosultsággal rendelkező adminisztrátorok számára, hogy meghatározott feltételek szerint engedélyezzék vagy kikapcsolják a meghatározott biztonsági szűrőket.

Magyarázat

A jogosultsággal rendelkező adminisztrátorok engedélyezhetik a biztonsági szűrőket a jóváhagyott adattípusok kezelésére. A jogosultsággal rendelkező adminisztrátoroknak lehetőségük van arra is, hogy az átvitt adatok típusa, a forrás- és cél biztonsági tartományok, valamint szükség szerint más biztonsági szempontból fontos jellemzők alapján kiválasszák az adott információáramláson alkalmazott szűrőket, illetve kikapcsolják azokat.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell, hogy az adminisztrátorok rendelkezzenek a szükséges hozzáféréssel ahhoz, hogy meghatározott feltételek szerint engedélyezzék vagy kikapcsolják a biztonsági szűrőket.
2. A szervezetnek biztosítania kell, hogy az adminisztrátorok megfelelő képzést és támogatást kapjanak biztonsági szűrők be- és kikapcsolásához.
3. A szervezetnek rendszeresen dokumentálnia/naplóznia kell az adminisztrátorok által elvégzett, biztonsági szűrőkkel kapcsolatos módosításokat.
4. A szervezetnek rendszeres időközönként felül kell vizsgálnia az adminisztrátorok biztonsági szűrőkkel kapcsolatos tevékenységét.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi szabályzati szűrők, illetve a feltételek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.39. Információáramlási szabályok érvényesítése – Biztonsági szűrők konfigurálása

2.39. A szervezet lehetővé teszi a kiemelt jogosultsággal rendelkező adminisztrátorok számára, hogy konfigurálják a meghatározott biztonsági szűrőket a különböző biztonsági szabályok támogatása érdekében.

Magyarázat

Az érintett szervezet lehetővé teszi a kiemelt jogosultsággal rendelkező adminisztrátorok számára, hogy konfigurálják a meghatározott biztonsági szűrőket a különböző biztonsági szabályok támogatása érdekében. Ez azt jelenti, hogy a kiemelt jogosultsággal rendelkező adminisztrátorok képesek beállítani és módosítani a biztonsági szűrőket. Például a kiemelt jogosultsággal rendelkező adminisztrátorok beállíthatják, hogy a szervezet által meghatározott szavakat tartalmazzák a biztonsági szűrők.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell, hogy a kiemelt jogosultsággal rendelkező adminisztrátorok rendelkezzenek a szükséges hozzáféréssel ahhoz, hogy konfigurálják a biztonsági szűrőket.
2. A szervezetnek biztosítania kell, hogy a kiemelt jogosultsággal rendelkező adminisztrátorok megfelelő képzést és támogatást kapjanak biztonsági szűrők konfigurálásához.
3. A szervezetnek rendszeresen dokumentálnia/naplóznia kell a kiemelt jogosultsággal rendelkező adminisztrátorok által elvégzett, biztonsági szűrőkkel kapcsolatos módosításokat.
4. A szervezetnek rendszeres időközönként felül kell vizsgálnia a kiemelt jogosultságokkal rendelkező adminisztrátorok biztonsági szűrőkkel kapcsolatos tevékenységét.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi szabályzati szűrők meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.40. Információáramlási szabályok érvényesítése – Adattípus azonosítók

2.40. A szervezet az információk különböző biztonsági tartományok közötti átvitelekor meghatározott adattípus azonosítókat használ az információáramlási döntésekhez szükséges adatok validálására.

Magyarázat

Az adattípus azonosítók közé tartoznak a fájlnevek, fájltípusok, fájlaláírások vagy tokenek, valamint a belső fájlaláírások vagy tokenek. Az EIR-ek csak olyan adatok átvitelét engedélyezik, amelyek megfelelnek az adattípus formátum leírásoknak. Az adattípusok azonosítása és hitelesítése az egyes megengedett adatformátumokhoz kapcsolódó, meghatározott leírásokon alapul. Az adattípus azonosítására nem használható csupán a fájlnév és a fájlszám. A tartalom szintaktikai és szemantikai hitelesítésen esik át, mely a leírással összevetve történik annak érdekében, hogy a tartalom az adott adattípusnak megfelelő legyen.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia azokat az adattípus azonosítókat, amelyeket az információk különböző biztonsági tartományok közötti átvitelekor használni fog. Ezek az alábbiak lehetnek: fájlnév, fájltípus, fájlaláírás vagy token, illetve belső fájlaláírás vagy token.
2. A szervezetnek biztosítania kell, hogy az EIR csak olyan adatok átvitelét engedélyezze, amelyek megfelelnek az adattípus formátum leírásoknak.
3. A szervezetnek nem szabad csak a fájlnév és szám alapján azonosítania az adattípusokat. Az adattartalmat szintaktikailag és szemantikailag is validálni kell a leírással összevetve, így biztosítva, hogy a tartalom az adott adattípusnak megfelelő legyen.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(12)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az adattípus azonosítók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.41. Információáramlási szabályok érvényesítése – Adatok alkotóelemeire való bontása

2.41. A szervezet az információk különböző biztonsági tartományok közötti átvitelekor az adatokat a szervezet által meghatározott elemeire bontja le annak érdekében, hogy az adatáramlási szabályokat kikényszerítő mechanizmusok működőképessége biztosított legyen.

Magyarázat

Az információknak azok átvitele előtt a szabályok szempontjából releváns elemeire való bontása megkönnyíti a forrással, a céllal, a tanúsítványokkal, a minősítéssel, a mellékletekkel és más, biztonsággal kapcsolatos elemek megkülönböztetésével kapcsolatos döntéseket. Az információáramlási szabályok kikényszerítésére szolgáló mechanizmusok szűrési, elemzési és/vagy tisztítási szabályokat alkalmaznak a szervezet által meghatározott adatok alkotóelemeire. Így megkönnyítik az információáramlási szabályok érvényesítését az ilyen típusú adatok - különböző biztonsági tartományokba történő - átvitele előtt.

A követelmény alkalmazásának lépései

1. A szervezet határozza meg, hogy az információk különböző biztonsági tartományok közötti átvitelekor milyen elemekre kell lebontani az adatokat.
2. A szervezetnek meg kell határoznia, hogy az információáramlási szabályok kikényszerítésére milyen mechanizmusokat alkalmaz.
3. A szervezetnek biztosítania kell, hogy az információk csak akkor kerüljenek átadásra a különböző biztonsági tartományok között, ha a szabály érvényesítésére szolgáló mechanizmusok sikeresen alkalmazták a szabályokat az információk releváns elemeire.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(13)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szabályzat szempontú alkotóelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.42. Információáramlási szabályok érvényesítése – Biztonsági szabályzat szűrési korlátozások

2.42. A szervezet az információk különböző biztonsági tartományok közötti átvitelekor érvényesíti a meghatározott biztonsági szabályzat alapján alkalmazott szűrőket, amelyek az adatszerkezetet és a tartalmat korlátozó, meghatározott formátumokat írnak elő.

Magyarázat

Az adatszerkezeti és tartalmi korlátozások csökkentik a lehetséges kártékony vagy nem engedélyezett tartalmak körét a tartományok közötti tranzakciókban. Az adatszerkezeteket korlátozó biztonsági szűrők közé tartozik a fájlméretek és a fájlmezők hosszának korlátozása. Az adattartalom biztonsági szűrői közé tartoznak a karakterkészletek kódolási formátumai, a karakteres adatmezők korlátozása, hogy csak alfanumerikus karaktereket tartalmazzanak, a speciális karakterek tiltása és a sémastruktúrák ellenőrzése.

A követelmény alkalmazásának lépései

1. A szervezetnek létre kell hoznia egy biztonsági szabályzatot, amely meghatározza a különböző biztonsági tartományok közötti információátvitel szabályait.
2. A szervezetnek a szabályzat alapján olyan szűrőket kell alkalmaznia, amelyek az adatszerkezetet és a tartalmat korlátozó, meghatározott formátumokat írnak elő.
3. A szervezet az adatszerkezeteket korlátozó biztonsági szűrők esetében korlátozhatja a fájlméreteket és a fájlmezők hosszát.
4. A szervezet az adattartalom biztonsági szűrői esetében meghatározhatja a karakterkészletek kódolási formátumait, korlátozhatja a karakteres adatmezőket, tilthatja a speciális karaktereket és ellenőrizheti a sémastruktúrákat.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(14)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi szabályzati szűrők meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.43. Információáramlási szabályok érvényesítése – Nem engedélyezett információk észlelése

2.43. A szervezet megvizsgálja az információt a különböző biztonsági tartományok közötti átvitel során annak érdekében, hogy a nem engedélyezett információ észlelése esetén - a biztonsági szabályok szerint - megtiltsa annak továbbítását.

Magyarázat

Ha az EIR észleli az engedély nélküli információt, akkor a biztonsági szabályok szerint meg kell tiltania annak továbbítását. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie az adatok áramlásának blokkolására vagy karanténba helyezésére, ha azok nem felelnek meg a biztonsági követelményeknek. A nem engedélyezett információk közé tartozik a rosszindulatú kód, a forráshálózatból nem továbbítható információ, illetve olyan futtatásra alkalmas kód, ami képes megzavarni, illetve károsítani a célhálózatban található szolgáltatásokat vagy EIR-eket .

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, hogy melyek azok az információk, melyek továbbítása nem engedélyezett a biztonsági tartományok közötti átvitel során.
2. A szervezetnek implementálnia kell egy olyan megoldást, amely képes megvizsgálni és észlelni a nem engedélyezett információkat a biztonsági tartományok közötti átvitel során.
3. Ha a szervezet észleli a nem engedélyezett információ átvitelét, a szervezetnek azonnal meg kell tiltania annak továbbítását. Ez magában foglalhatja a hálózati forgalom blokkolását, az EIR leállítását, illetve a hálózati kapcsolatok megszakítását.

Kapcsolódó intézkedések

18.8. Kártékony kódok elleni védelem

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(15)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a nem engedélyezett információk illetve a biztonsági és adatvédelmi szabályzat meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.44. Információáramlási szabályok érvényesítése – Tartományhitelesítés

2.44. A szervezet egyedileg azonosítja és hitelesíti a forrás- és célpontokat (szervezetenként, rendszerenként, alkalmazásonként, szolgáltatásonként, egyénekként) az információátvitel során.

Magyarázat

Az EIR-eken belül áramló információk forrás- és célpontjainak azonosítása lehetővé teszi az események rekonstruálását, és elősegíti a szabályzatok betartását azáltal, hogy a szabályzatok megsértését konkrét szervezeteknek vagy személyeknek tulajdonítja. A sikeres tartományhitelesítés megköveteli, hogy a rendszercímkék különbséget tegyenek az információk előkészítésében, küldésében, fogadásában vagy terjesztésében részt vevő rendszerek, szervezetek és személyek között.

A követelmény alkalmazásának lépései

1. A szervezetnek egyedileg kell azonosítania és hitelesítenie a forrás- és célpontokat (szervezet, rendszer, alkalmazás, szolgáltatás, egyén) az információátvitel során.
2. A szervezetnek biztosítania kell, hogy a rendszercímkék különbséget tegyenek az információk előkészítésében, küldésében, fogadásában vagy terjesztésében részt vevő rendszerek, szervezetek és személyek között.
3. A szervezetnek képesnek kell lennie arra, hogy az EIR-eken belül áramló információk forrás- és célpontjainak azonosítása által rekonstruálni tudja az eseményeket. Emellett elősegíti a szabályzatok betartását azáltal, hogy a szabályzatok megsértését konkrét szervezethez vagy személyhez tudja kötni.

Kapcsolódó intézkedések

8.2. Azonosítás és hitelesítés

8.10. Eszközök azonosítása és hitelesítése

8.41. Szolgáltatás azonosítása és hitelesítése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(17)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.45. Információáramlási szabályok érvényesítése – Metaadatok ellenőrzése

2.45. A szervezet az információk különböző biztonsági tartományok közötti átvitele során meghatározott biztonsági szűrőket alkalmaz a metaadatokra.

Magyarázat

Minden információ (beleértve a metadatokat is) szűrés és ellenőrzés tárgyát képezi. A metaadatok szűrése különösen fontos, mivel ezek az adatok gyakran tartalmazhatnak bizalmas információkat (pl.: készítő neve, készítéshez használt szoftver, geolokációs adat stb.). Az érintett szervezet a metaadatokra alkalmazott biztonsági szűrésekkel biztosítja az EIR biztonságát és védi a bizalmas információkat a különböző biztonsági tartományok közötti átvitel során.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia, hogy milyen metaadatokat használhat, illetve továbbíthat az EIR.
2. A szervezetnek létre kell hoznia biztonsági szűrőket, amelyek képesek azonosítani és szűrni a metaadatokat a biztonsági tartományok közötti átvitel során.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-4(19)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi szabályzati szűrők meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.46. INFORMÁCIÓÁRAMLÁSI SZABÁLYOK ÉRVÉNYESÍTÉSE – JÓVÁHAGYOTT MEGOLDÁSOK

2.46. A szervezet jóváhagyott konfigurációs megoldásokat alkalmaz az információáramlás ellenőrzésére a biztonsági tartományok között.

MAGYARÁZAT

Az érintett szervezetnek biztosítania kell, hogy az információáramlás ellenőrzésére megfelelően konfigurált, jóváhagyott megoldásokat alkalmazzon a biztonsági tartományok között. Ez magában foglalja a megfelelő hozzáférési szabályok, hálózati szűrők és tűzfalak beállítását, melyek megakadályozzák a nem kívánt információáramlást.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek jóváhagyott konfigurációs megoldásokat kell alkalmaznia a biztonsági tartományok közötti információáramlás ellenőrzésének lebonyolításához.
2. A szervezetnek a gyakorlatban is alkalmaznia kell a jóváhagyott konfigurációs megoldásokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(20)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a jóváhagyott konfigurációs megoldások, illetve az információ meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.47. Információáramlási szabályok érvényesítése – Információáramlás fizikai vagy logikai szétválasztása

2.47. A szervezet meghatározott mechanizmusokkal vagy technikákkal fizikailag vagy logikailag szétválasztja az információáramlásokat, hogy a meghatározott információtípusok szerinti elkülönítést megvalósítsa.

Magyarázat

A meghatározott adattípusokhoz kapcsolódó információáramlások elkülönítésének érvényesítése fokozhatja a védelmet azáltal, hogy biztosítja, az információk nem keverednek az adatátvitel során, és lehetővé teszi az adatáramlás ellenőrzését más módon nem megvalósítható átviteli útvonalakon keresztül. A szétválasztható információk típusai közé tartozik a bejövő és kimenő kommunikációs forgalom, a szolgáltatási kérelmek és válaszok, valamint a különböző biztonsági hatású vagy osztályozási szint alá eső információk.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, mely információtípusokat kívánja elkülöníteni. A szétválasztható információk típusai közé tartozik a bejövő és kimenő kommunikációs forgalom, a szolgáltatási kérelmek és válaszok, valamint a különböző biztonsági hatású vagy osztályozási szint alá eső információk.
2. A szervezetnek ki kell dolgoznia és be kell vezetnie olyan mechanizmusokat vagy technikákat, amelyek fizikailag vagy logikailag szétválasztják az információáramlásokat.

Kapcsolódó intézkedések

17.96. Rendszer felosztása

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(21)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a mechanizmusok vagy technikák illetve az információ típusai szerinti elválasztás meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.48. Információáramlási szabályok érvényesítése – Hozzáférés korlátozása

2.48. Amikor az EIR egyetlen készülékről több különböző biztonsági tartományban található informatikai platformhoz, alkalmazáshoz vagy adathoz biztosít hozzáférést, megakadályozza az információáramlást a különböző biztonsági tartományok között.

Magyarázat

Az EIR képes arra, hogy több különböző biztonsági tartományban található informatikai platformhoz, alkalmazáshoz vagy adathoz hozzáférést biztosítson a felhasználók számára anélkül, hogy a különböző biztonsági tartományok közötti adat- vagy információáramlást engedélyezze. Az EIR így biztosítja, hogy az érintett szervezetben az információk ne kerüljenek át egyik biztonsági tartományból a másikba. Például egy EIR különböző biztonsági osztályok alapján biztosít hozzáférést a felhasználók számára, miközben elkülöníti az információt.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell, hogy amennyiben az EIR több különböző biztonsági tartományban található informatikai platformhoz, alkalmazáshoz vagy adathoz biztosít hozzáférést a felhasználók számára, az EIR képes legyen megakadályozni az információáramlást a különböző biztonsági tartományok között.
2. A szervezet például bevezethet egy olyan hozzáférési megoldást, amely lehetővé teszi a felhasználók számára, hogy különböző biztonsági osztályok alapján férjenek hozzá az információkhoz, miközben az információk elkülönítésre kerülnek.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(22)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.49. INFORMÁCIÓÁRAMLÁSI SZABÁLYOK ÉRVÉNYESÍTÉSE – NEM NYILVÁNOS INFORMÁCIÓ MÓDOSÍTÁSA

2.49. A szervezet a meghatározott eljárásokat alkalmazva módosítja a nem nyilvános információkat a különböző biztonsági tartományok közötti átvitel során.

MAGYARÁZAT

A nem nyilvános információk - különböző biztonsági tartományok közötti átvitel során történő - módosítása segíthet megelőzni az adatszivárgást, vagy az esetleges támadást. Az érintett szervezet a nem nyilvános információkat módosíthatja a maszkolás, a permutáció (a bizalmas információ elemeinek vagy karaktereinek helyének megváltoztatása), a módosítás (változtatás - az eredeti adatok átalakítása, módosítása), az eltávolítás (bizonyos információrészek eltávolítása), vagy a kihúzás/feketítés (a bizalmas információ bizonyos részeinek kihúzása, feketítése, olvashatatlanná tétele) segítségével.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely információk minősülnek nem nyilvánosnak az EIR-ben.
2. A szervezetnek be kell vezetnie és alkalmaznia kell azokat az eljárásokat, amelyek lehetővé teszik a nem nyilvános információk módosítását. Ez magában foglalhatja az adatok maszkolását, permutációját (a bizalmas információ elemeinek vagy karaktereinek helyének megváltoztatása), módosítását (változtatás - az eredeti adatok átalakítása, módosítása), eltávolítását (bizonyos információrészek eltávolítása) vagy kihúzását/feketítését (a bizalmas információ bizonyos részeinek kihúzása, feketítése, olvashatatlanná tétele).
3. A szervezetnek biztosítania kell, hogy az EIR-ben lévő nem nyilvános információk módosítása a különböző biztonsági tartományok közötti átvitel során megtörténjen.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.11

NIST SP 800-53 REV.5 REFERENCIA

AC-4(23)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a módosítási tevékenység és/vagy módosítás meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.50. Információáramlási szabályok érvényesítése – Belső normalizált formátum

2.50. Az EIR a különböző biztonsági tartományok közötti információátvitel során a beérkező adatokat normalizált formátumba hozza, majd újra formázza, hogy azok összhangban legyenek az elvárt adatformátummal.

Magyarázat

Az adatok normalizált formába történő átalakítása az egyik leghatékonyabb mechanizmus a rosszindulatú támadások és a nagyszámú adatszivárgás kivédésére. Az EIR először a beérkező adatokat normalizált formátumba hozza. Ez azt jelenti, hogy az adatokat egy olyan formátumba alakítja, amely egységes és következetes, így könnyen összehasonlítható és elemezhető. Ez a lépés segít azonosítani és kiszűrni azokat az adatokat, amelyek nem felelnek meg a biztonsági előírásoknak vagy amelyek potenciálisan károsak lehetnek. Ezután az EIR újra formázza az adatokat, hogy azok összhangban legyenek az elvárt adatformátummal. Ez azt jelenti, hogy az adatokat olyan formátumba alakítja, amely megfelel az érintett szervezet által meghatározott és elfogadott adatformátumoknak. Ez a lépés biztosítja, hogy az adatok kompatibilisek legyenek az érintett szervezet rendszereivel és alkalmazásaival, illetve azokat könnyen fel lehessen használni.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell, hogy az EIR képes legyen az adatok normalizálására. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie az adatok átalakítására egy egységes és következetes formátumba, amelyet a kapcsolódó EIR-ek képesek feldolgozni.
2. A szervezetnek továbbá biztosítania kell, hogy az EIR képes legyen az adatok újraformázására is. Ez azt jelenti, hogy az EIR képes átalakítani az adatokat olyan formátumba, amely megfelel a szervezet által elvárt adatformátumnak.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(24)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.51. INFORMÁCIÓÁRAMLÁSI SZABÁLYOK ÉRVÉNYESÍTÉSE – ADATTISZTÍTÁS

2.51. Amikor az EIR információt továbbít különböző biztonsági tartományok között, az adatokat a meghatározott szabályoknak megfelelően megtisztítja, hogy minimalizálja a rosszindulatú tartalom átvitelét.

MAGYARÁZAT

Az EIR az információ különböző biztonsági tartományok közötti átvitelekor adattisztítást végez, azaz olyan folyamatokat alkalmaz, amelyek segítségével minimalizálhatók a kártékony tartalom továbbításából, a kártékony kódok terjedéséből, valamint a szteganográfiával kódolt adatokból adódó kockázatok. Az adattisztítás olyan folyamat, mely során visszavonhatatlanul eltávolításra vagy megsemmisítésre kerül az adathordozón (pl.: merevlemez, SSD, mobileszköz, CD, DVD) tárolt adat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a szabályokat, amelyek szerint az adatokat megtisztítja, mielőtt azokat továbbítja különböző biztonsági tartományok között.
2. A szervezetnek alkalmaznia kell a gyakorlatban egy adattisztítási folyamatot az EIR-ben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

11.8. Adathordozók törlése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.10

NIST SP 800-53 REV.5 REFERENCIA

AC-4(25)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szabályzat meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.52. Információáramlási szabályok érvényesítése – Szűrési műveletek ellenőrzése

2.52. A szervezet rögzíti és ellenőrzi a tartalomszűrési műveleteket és azok eredményeit a szűrt információra vonatkozóan, a biztonsági tartományok között történő információátvitel során.

Magyarázat

A tartalomszűrés az a folyamat, amelynek során az információkat egy tartományokon átívelő megoldáson keresztül átvizsgálják, és meghatározzák, hogy az információ megfelel-e egy előre meghatározott biztonsági szabályrendszernek. A tartalomszűrési műveleteket és a szűrési műveletek eredményeit az egyes üzenetekre vonatkozóan rögzítik, hogy meggyőződjenek arról, hogy a megfelelő szűrési műveleteket hajtották végre. A tartalomszűrési jelentések segítenek a hibaelhárítási műveletekben, például annak megállapításával, hogy az üzenet tartalma miért módosult és/vagy miért nem sikerült a szűrési folyamat. A szűrési műveletek ellenőrzésére vonatkozó, naplózást érintő információk a "Naplózható események" és a "Naplóbejegyzések létrehozása" kontrolloknál kerültek bővebben kifejtésre.

A követelmény alkalmazásának lépései

1. A szervezetnek rögzítenie és ellenőriznie kell a tartalomszűrési műveleteket, illetve azok eredményeit a szűrt információra vonatkozóan a biztonsági tartományok között történő információátvitel során.
2. Az érintett szervezetnek tartalomszűrési jelentéseket kell készítenie, amelyek segíthetnek a hibaelhárításban.

Kapcsolódó intézkedések

4.2. Naplózható események

4.3. Naplóbejegyzések tartalma

4.40. Naplóbejegyzések létrehozása

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(26)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.53. Információáramlási szabályok érvényesítése – Redundáns szűrőmechanizmusok

2.53. A szervezet olyan tartalomszűrési megoldásokat alkalmaz a különböző biztonsági tartományok között történő információk átvitele során, amelyek redundáns és független szűrőmechanizmusokat biztosítanak minden adattípusra.

Magyarázat

A tartalomszűrés az a folyamat, amelynek során az információkat egy tartományokon átívelő megoldáson keresztül átvizsgálják, és meghatározzák, hogy az információ megfelel-e egy előre meghatározott biztonsági szabályrendszernek. A redundáns és független szűrőmechanizmusok alkalmazásával biztosítható a szűrési mechanizmusok rendelkezésre állása, mivel nem csak egy szűrőrendszer működik.

A követelmény alkalmazásának lépései

1. A szervezetnek olyan szűrőrendszereket kell implementálnia, amelyek redundáns működésre képesek, ezáltal folyamatosan képesek ellenőrizni az információkat, amikor azok áthaladnak a biztonsági tartományokon.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-4(27)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.54. Információáramlási szabályok érvényesítése – Lineáris szűrőcsatornák

2.54. A szervezet olyan lineáris tartalomszűrési folyamatot hajt végre a különböző biztonsági tartományok között történő információk átvitele során, amelyeket szabadon választható és kötelező hozzáférési szabályokkal kényszerít ki.

Magyarázat

A tartalomszűrés az a folyamat, amelynek során az információkat egy tartományokon átívelő megoldáson keresztül átvizsgálják, és meghatározzák, hogy az információ megfelel-e egy előre meghatározott biztonsági szabályrendszernek. A lineáris tartalomszűrési folyamat használata biztosítja, hogy a szűrési mechanizmusok nem kerülhetők meg és folyamatosan végrehajtásra kerüljenek.

A követelmény alkalmazásának lépései

1. A szervezetnek létre kell hoznia egy lineáris tartalomszűrési folyamatot. Ez a folyamat magában foglalja a különböző biztonsági tartományok közötti átvitel során az információk vizsgálatát. Ennek során megállapításra kerül, hogy az információk megfelelnek-e egy előre meghatározott szabályrendszernek.
2. A szervezetnek biztosítania kell, hogy a tartalomszűrési folyamatok ne legyenek megkerülhetők és folyamatosan végrehajtásra kerüljenek. A szűrési folyamatoknak mindig aktívnak kell lenniük a különböző biztonsági tartományok közötti információátvitel során.
3. A szervezetnek a különböző biztonsági tartományok között történő információk átvitele során olyan lineáris tartalomszűrési folyamatot kell végrehajtania, melyeket szabadon választható és kötelező hozzáférés-felügyelettel kényszerít ki.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(28)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.55. Információáramlási szabályok érvényesítése – Összehangolt tartalomszűrés

2.55. A szervezet tartalomszűrő rendszert alkalmaz az információk különböző biztonsági tartományok közötti átvitelekor annak biztosítása érdekében, hogy:

2.55.1. a tartalomszűrő mechanizmusok hiba nélkül sikeresen végrehajthassák a feladatukat;

2.55.2. a tartalomszűrési műveletek megfelelő sorrendben történjenek, és megfeleljenek a meghatározott biztonsági szabályzati előírásainak.

Magyarázat

A tartalomszűrés az a folyamat, amelynek során az információkat egy tartományokon átívelő megoldáson keresztül átvizsgálják, és meghatározzák, hogy az információ megfelel-e egy előre meghatározott biztonsági szabályrendszernek. Az összehangolt tartalomszűrés koordinálja az egyes mechanizmusok végrehajtási sorrendjét (manuális és automata módon) a tartalomszűrési folyamat során. A tartalomszűréssel kapcsolatos jelentések gyakran használt mechanizmusok, mellyel a szervezet biztosítja, hogy az elvárt szűrési műveletek valóban sikeresen megtörténnek.

A követelmény alkalmazásának lépései

1. A szervezetnek implementálnia kell egy tartalomszűrő rendszert, amely képes a különböző biztonsági tartományok közötti átvitel során megjelenő információ ellenőrzésére és annak meghatározására, hogy az információ megfelel-e a meghatározott szabályoknak.
2. A szervezetnek összehangolt tartalomszűrést kell implementálnia, amely koordinálja az egyes mechanizmusok végrehajtási sorrendjét (manuális és automata módon) a tartalomszűrési folyamat során.
3. A szervezetnek rendszeresen ellenőriznie kell a tartalomszűrési mechanizmus hatékonyságát és megbízhatóságát. Ezt megteheti úgy is, hogy a tartalomszűréssel kapcsolatos jelentéseket folyamatosan nyomon követi.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-4(29)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.56. Információáramlási szabályok érvényesítése – Több folyamatot használó szűrőmechanizmusok

2.56. A szervezet a különböző biztonsági tartományok közötti információátvitel során több folyamatot használó tartalomszűrési mechanizmust valósít meg.

Magyarázat

A tartalomszűrési mechanizmusok megvalósításához több különböző folyamat használata javasolt az érintett szervezet esetében, mely jelentősen csökkenti annak az esélyét, hogy olyan hibajelenség lépjen fel, mely az egész tartalomszűrési folyamat működésképtelenségét okozhatja.

A követelmény alkalmazásának lépései

1. A szervezetnek ki kell dolgoznia és be kell vezetnie egy tartalomszűrési mechanizmust, amely több folyamatot használ. Ezáltal jelentősen csökkenthető annak az esélye, hogy olyan hibajelenség lépjen fel, mely az egész tartalomszűrési folyamat működésképtelenségét okozhatja.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-4(30)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.57. Információáramlási szabályok érvényesítése – Hibás tartalom átvitelének megakadályozása

2.57. A szervezet a különböző biztonsági tartományok közötti információátvitel során megakadályozza a hibásan átadott tartalom átvitelét a fogadó tartományba.

Magyarázat

A szűrési ellenőrzéseken fennakadó, hibásan átadandó tartalom károsíthatja a rendszert, ha az átvitelre kerül a fogadó tartományba, ezért az érintett szervezetnek szükséges meggátolnia az átadás folyamatát. Ez azt jelenti, hogy a szervezetnek hatékony szűrési és ellenőrzési mechanizmusokat kell bevezetnie, amelyek képesek azonosítani és megakadályozni a hibás tartalom átvitelét.

A követelmény alkalmazásának lépései

1. A szervezetnek olyan hatékony szűrőmechanizmust kell alkalmaznia, amely képes azonosítani és megakadályozni a hibása átadott tartalom átvitelét a fogadó tartományba.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-4(31)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.58. Információáramlási szabályok érvényesítése – Folyamatkövetelmények az információ átviteléhez

2.58. A különböző biztonsági tartományok közötti információátvitel során a szűrőcsatornák közötti információátviteli folyamat:

2.58.1. nem szűri az üzenetek tartalmát;

2.58.2. ellenőrzi és jóváhagyja a szűrési metaadatokat;

2.58.3. biztosítja, hogy a szűrési metaadatokhoz társított tartalom sikeresen átment a szűrésen; és

2.58.4. átadja a tartalmat a cél szűrőcsatornának.

Magyarázat

A különböző biztonsági tartományok közötti információátvitel során alkalmazott szűrőcsatornák közötti információátviteli folyamat minimális összetettséggel és funkcionalitással kell rendelkezzen, hogy biztosítani tudja az egyszerű és megfelelő működést.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell, hogy az információátviteli folyamatok a szűrőcsatornák között minimális összetettséggel és funkcionalitással rendelkezzenek. Ez biztosítja, hogy a folyamatok helyesen működjenek.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-4(32)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.59. FELELŐSSÉGEK SZÉTVÁLASZTÁSA

2.59. A szervezet:

2.59.1. azonosítja és dokumentálja azokat a meghatározott feladatokat, amelyeket az egyéneknek elkülönített módon kell ellátniuk; és

2.59.2. meghatározza az EIR hozzáférési jogosultságait annak érdekében, hogy támogassa a feladatok szétválasztását.

MAGYARÁZAT

A felelősségek szétválasztása kiküszöböli az engedélyezett jogosultságokkal való visszaélés lehetőségét, és segít csökkenteni a rosszindulatú, összejátszás nélküli tevékenység kockázatát. A felelősségek szétválasztása magában foglalja az üzleti funkciók és a támogató funkciók különböző személyek, szerepkörök, szervezeti egységek közötti megosztását, az IT üzemeltetési és IT üzemeltetés-ellenőrzési funkciók különböző személyek, szerepkörök, szervezeti egységek közötti megosztását, a rendszertámogatási funkciók különböző személyekkel történő elvégzését, valamint annak biztosítását, hogy a hozzáférés-felügyeleti funkciókat kezelő biztonsági személyzet ne kezelje az ellenőrzési funkciókat is. Mivel a felelősségek szétválasztásának megsértése kiterjedhet a rendszerekre és alkalmazási tartományokra, az érintett szervezet a feladatok szétválasztására vonatkozó irányelvek kidolgozásakor a rendszerek és rendszerelemek teljes egészét veszi figyelembe. A felelősségek szétválasztásának érvényesítése, illetve kikényszerítése a "Fiókkezelés", a "Hozzáférés-ellenőrzés érvényesítése", az "Azonosítás és hitelesítés", az "Azonosító kezelés" és a "Személyazonosság igazolása" kontrolloknál kerültek bővebben kifejtésre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell azokat a feladatokat, amelyeket az egyéneknek elkülönített módon kell ellátniuk. Ezzel összefüggésben a szervezetnek az EIR hozzáférési jogosultságait is úgy kell kialakítania, hogy az támogassa a felelősségek szétválasztását.

2. A szervezetnek meg kell határoznia, hogy milyen, egymással összeférhetetlen felelősségek vannak a szervezetnél. A szervezetnek ennek figyelembevételével kell kialakítania a

munkavállalók számára kiosztott jogosultságokat pl.: egy pénzügyi területen dolgozó munkavállaló ne legyen képes egyszerre kifizetést kezdeményezni és jóváhagyni.

3. A szervezet a felelősségek szétválasztását a megfelelő hozzáférési jogosultságok mellett kettős jóváhagyást és négy szem elvet alkalmazó biztonsági kontrollokkal is meg lehet oldani.

4. A szervezetnek meghatározott időközönként felül kell vizsgálnia a kiosztott jogosultságokat és szükség esetén meg kell szüntetnie a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat. Emellett a változó és jóváhagyott felelősségek alapján szükség esetén módosítania kell a kiosztott jogosultságokat.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.60. Legkisebb jogosultság elve

4.25. Naplóinformációk védelme

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.49. Felhasználó által telepített szoftver

7.35. Az elektronikus információs rendszer mentései

8.2. Azonosítás és hitelesítés

8.14. Azonosító kezelés

8.21. A hitelesítésre szolgáló eszközök kezelése

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.5. A felelősségek szétválasztása

ISO/IEC 27001:2023 referencia

A.5.3

NIST SP 800-53 rev.5 referencia

AC-5

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.60. LEGKISEBB JOGOSULTSÁG ELVE

2.60. A szervezet a legkisebb jogosultság elvét alkalmazza, és a felhasználók vagy a felhasználók nevében eljáró folyamatok számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

MAGYARÁZAT

Az érintett szervezet a legkisebb jogosultság elvét alkalmazza a meghatározott felelősségek és az EIR-ek esetében. A legkisebb jogosultság elvét a rendszerfolyamatokra is alkalmazza, biztosítva, hogy a folyamatok csak a számukra szükséges hozzáférési szinttel rendelkezzenek a szervezet céljainak vagy üzleti funkcióinak végrehajtásához. A szervezet fontolóra veszi további folyamatok, szerepkörök és fiókok létrehozását amennyiben azok szükségesek legkisebb jogosultság elvének érvényesítéséhez. A szervezet a legkisebb jogosultság elvét alkalmazza a szervezethez köthető EIR-ek fejlesztése, implementálása és működtetése során.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie és meg kell határoznia, hogy a szervezeten belüli egyes munkakörök feladatellátásához milyen jogosultságok szükségesek.
2. A szervezetnek a felhasználók vagy a felhasználók nevében eljáró folyamatokhoz csak a feladatok végrehajtásához minimálisan szükséges jogosultságokat szabad biztosítania.
3. A szervezetnek meghatározott időközönként felül kell vizsgálnia a kiosztott jogosultságokat és szükség esetén meg kell szüntetnie a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat. Emellett a változó és jóváhagyott felelősségek alapján szükség esetén módosítania kell a kiosztott jogosultságokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.59. Felelősségek szétválasztása

2.89. Biztonsági tulajdonságok

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.49. Felhasználó által telepített szoftver

13.2. Rendszerbiztonsági terv

1.13. Belső fenyegetés elleni program

16.16. Biztonságtervezési elvek

16.76.1. Fejlesztési folyamat, szabványok és eszközök

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.6. Legkisebb jogosultság elve

ISO/IEC 27001:2023 REFERENCIA

A.5.15; A.8.2; A.8.18

NIST SP 800-53 REV.5 REFERENCIA

AC-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.61. Legkisebb jogosultság elve – Hozzáférés biztosítása a biztonsági funkciókhoz

2.61. A szervezet:

2.61.1. Kizárólag az általa meghatározott személyeknek vagy szerepköröknek engedélyez hozzáférést a biztonsági funkciókhoz.

2.61.2. A szervezett kizárólag az általa meghatározott személyeknek vagy szerepköröknek engedélyez hozzáférést a biztonságkritikus információkhoz.

Magyarázat

A biztonsági funkciók közé tartozik a rendszerfiókok létrehozása, a hozzáférési jogosultságok konfigurálása, a monitorozni kívánt események beállításainak konfigurálása és a behatolás észlelés paramétereinek beállítása. A biztonságkritikus információk közé tartoznak az útválasztók (router) vagy tűzfalak szűrési szabályai, a biztonsági szolgáltatások konfigurációs paraméterei, a kriptográfiai kulcskezeléssel kapcsolatos információk és a hozzáférés-felügyeleti listák. A jogosultsággal rendelkező személyek közé tartoznak a biztonságért felelős személyek, a rendszergazdák, a programozók és más jogosultsággal rendelkező felhasználók.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia azokat a személyeket vagy szerepköröket, akik hozzáférhetnek az EIR biztonsági funkcióihoz és a biztonságkritikus információkhoz.

2. A szervezetnek a legkisebb jogosultság elvét szem előtt tartva kell kiosztania a jogosultságokat.

3. A szervezetnek meghatározott időközönként felül kell vizsgálnia a kiosztott jogosultságokat és szükség esetén meg kell szüntetnie a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat. Emellett a változó és jóváhagyott felelősségek alapján szükség esetén módosítania kell a kiosztott jogosultságokat.

Kapcsolódó intézkedések

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

4.25. Naplóinformációk védelme

12.2. A fizikai belépési engedélyek

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.6. Legkisebb jogosultság elve

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek és szerepek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.62. Legkisebb jogosultság elve – Nem privilegizált hozzáférés biztosítása a nem biztonsági funkciókhoz

2.62. A szervezet megköveteli, hogy a meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező fiókok felhasználói a nem biztonsági funkciók használatához ne privilegizált fiókot vagy szerepkört használjanak.

Magyarázat

Annak megkövetelése, hogy a meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező fiókok felhasználói a nem biztonsági funkciók használatához ne privilegizált fiókot vagy szerepkört használjanak csökkenti a szervezet biztonsági szempontú kitettségét. A szerepkörök bevezetése olyan helyzetekben nyújthat megoldást, amikor egy szervezet hozzáférés-felügyeleti szabályokat alkalmaz (pl.: szerepkör alapú hozzáférés-felügyelet), illetve ahol a szerepkör változása ugyanolyan mértékű biztosítékot nyújt a felhasználó és a felhasználó nevében működő folyamatok hozzáférési jogosultságainak változásában, mint amit egy privilegizált és nem privilegizált fiók közötti váltás nyújtana.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie, hogy a meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező fiókok felhasználói a nem biztonsági funkciók használatához ne privilegizált fiókot vagy szerepkört használjanak.
2. A szervezetnek a privilegizált felhasználói fiókot használó felhasználók számára létre kell hoznia nem privilegizált fiókokat is.

Kapcsolódó intézkedések

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

13.3.1. Viselkedési szabályok

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.6. Legkisebb jogosultság elve

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági funkciók vagy biztonságkritikus információk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.63. Legkisebb jogosultság elve – Hálózati hozzáférés a privilegizált parancsokhoz

2.63. A szervezet csak kényszerű üzemeltetési okokból engedélyezi a hálózati hozzáférést a meghatározott privilegizált parancsokhoz, és dokumentálja az ilyen hozzáférés indoklását a rendszerbiztonsági tervében.

Magyarázat

A hálózati hozzáférés a helyi hozzáféréssel szemben a hálózati kapcsolaton keresztül történő bármilyen hozzáférés. A hálózati hozzáférés engedélyezésekor az érintett szervezetnek gondosan mérlegelnie kell annak kockázatait, tekintettel arra, hogy a hálózati hozzáférés engedélyezése (különösen a privilegizált funkciókhoz) növelheti a biztonsági kockázatokat.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia azokat a privilegizált parancsokat, amelyekhez a hálózati hozzáférés engedélyezett lehet.
2. Az érintett szervezetnek meg kell határoznia azokat a kényszerű üzemeltetési okokat, amelyek alapján a hálózati hozzáférés engedélyezhető a meghatározott privilegizált parancsokhoz.
3. A szervezetnek dokumentálnia kell a tervezett, ilyen jellegű hozzáférés indoklását. Ez magában foglalja a kényszerű üzemeltetési okok részletes leírását, valamint a hozzáférés időtartamát és gyakoriságát.

Kapcsolódó intézkedések

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.6. Legkisebb jogosultság elve

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a privilegizált parancsok illetve a kényszerű üzemeltetési okok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

2.64. Legkisebb jogosultság elve – Elkülönített feldolgozási tartományok

2.64. A szervezet elkülönített feldolgozási tartományokat biztosít a felhasználói jogosultságok pontosabb kiosztásának lehetővé tétele érdekében.

Magyarázat

A felhasználói jogosultságok pontosabb kiosztására szolgáló elkülönített feldolgozási tartományok biztosítása magában foglalja a virtualizációs technikák használatát, amelyek lehetővé teszik a további felhasználói jogosultságok használatát egy virtuális gépen belül, miközben korlátozzák a jogosultságokat más virtuális gépekre, vagy az alapul szolgáló fizikai gépre, külön fizikai tartományok megvalósításával, valamint hardveres vagy szoftveres tartományelválasztó mechanizmusok alkalmazásával.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a felhasználói jogosultságokat, és meg kell határozni, hogy mely felhasználók milyen jogosultságokkal rendelkeznek.
2. A szervezetnek implementálnia kell hardveres vagy szoftveres tartományelválasztó mechanizmusokat, virtualizációs környezetet, vagy olyan megoldásokat, amelyek lehetővé teszik a felhasználói jogosultságok pontosabb kiosztását.
3. A szervezetnek elkülönített fizikai tartományokat is célszerű létrehoznia. Ez azt jelenti, hogy a rendszerek különböző részei különböző fizikai helyeken lehetnek, és csak bizonyos felhasználók férhetnek hozzájuk.
4. A szervezetnek meghatározott időközönként felül kell vizsgálnia a kiosztott jogosultságokat és szükség esetén meg kell szüntetnie a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat. Emellett a változó és jóváhagyott felelősségek alapján szükség esetén módosítania kell a kiosztott jogosultságokat.

Kapcsolódó intézkedések

2.28. Információáramlási szabályok érvényesítése

17.2. Rendszer és felhasználói funkciók szétválasztása

17.4. Biztonsági funkciók elkülönítése

17.87. Elfedés és megtévesztés

17.96. Rendszer felosztása

17.108. A folyamatok elkülönítése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.65. LEGKISEBB JOGOSULTSÁG ELVE – PRIVILEGIZÁLT FIÓKOK

2.65. A szervezet az EIR privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

MAGYARÁZAT

A privilegizált fiókokat, beleértve a szuperfelhasználói fiókokat, általában rendszer adminisztrátorként tüntetik fel különféle kereskedelmi forgalomban kapható operációs rendszerekben. A privilegizált fiókok használatának korlátozása meghatározott személyekre vagy szerepkörökre megakadályozza, hogy a privilegizált jogosultságokkal nem rendelkező felhasználók hozzáférjenek privilegizált információkhoz vagy privilegizált funkciókhoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezetnek meg kell határoznia, mely személyek vagy szerepkörök rendelkezhetnek privilegizált fiókokkal.
2. A szervezetnek meghatározott időközönként felül kell vizsgálnia a kiosztott jogosultságokat és szükség esetén meg kell szüntetnie a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat. Emellett a változó és jóváhagyott felelősségek alapján szükség esetén módosítania kell a kiosztott jogosultságokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

8.2. Azonosítás és hitelesítés

10.4. Karbantartási eszközök

10.11. Távoli karbantartás

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.6. Legkisebb jogosultság elve

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.66. Legkisebb jogosultság elve – Privilegizált hozzáférés szervezeten kívüli felhasználók számára

2.66. A szervezet megtiltja a szervezeten kívüli felhasználók számára az EIR-hez való privilegizált hozzáférést.

Magyarázat

A szervezeti felhasználó egy munkavállaló vagy egy olyan személy, akit a szervezet egy munkavállalóval egyenértékű státuszúnak tekint. A szervezeti felhasználók közé tartozhatnak ilyen alapon a szerződéses partnerek vagy a más szervezetektől kirendelt személyek is. A nem szervezeti felhasználó olyan felhasználó, aki nem minősül szervezeti felhasználónak. A munkavállalókkal egyenértékű státusz megadására vonatkozó szabályok és eljárások magukban foglalják a szükséges ismeretek elsajátítását és a szervezethez fűződő kapcsolat figyelembevételét. Az érintett szervezet megtiltja a szervezeten kívüli felhasználók számára az EIR-hez való privilegizált hozzáférést. Ez azt jelenti, hogy a szervezet felhasználói, vagy ilyen értelemben annak minősülő felhasználói rendelkezhetnek olyan jogosultságokkal, amelyek lehetővé teszik számukra az EIR-hez való privilegizált hozzáférését vagy módosítását. A szervezeten kívüli felhasználók számára kizárólag korlátozott hozzáférés biztosítható.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia és dokumentálnia kell, hogy kik minősülnek szervezeten belüli felhasználónak. Ez lehet minden olyan személy, aki az érintett szervezet alkalmazottja, vagy aki az érintett szervezet által alkalmazottnak tekintendő. Ide tartozhatnak a szerződéses partnerek vagy a más szervezetektől kirendelt személyek is.
2. A szervezetnek meg kell határoznia, hogy ki minősül szervezeten kívüli felhasználónak.
3. A szervezetnek meg kell tiltania a szervezeten kívüli felhasználók számára az EIR-hez való privilegizált hozzáférést. Számukra a szervezet kizárólag korlátozott hozzáférést biztosíthat.
4. A szervezet a szervezeten kívüli felhasználók esetében úgy is eljárhat, hogy csak meghatározott időre biztosít számukra korlátozott hozzáférést. Amennyiben lehetséges, a

megadott hozzáféréshez automatikus lejárat is köthető. Így a szervezet nem felejti el megszüntetni a kiosztott hozzáférést.

5. A szervezetnek meghatározott időközönként felül kell vizsgálnia a kiosztott jogosultságokat és szükség esetén meg kell szüntetnie a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat. Emellett a változó és jóváhagyott felelősségek alapján szükség esetén módosítania kell a kiosztott jogosultságokat.

Kapcsolódó intézkedések

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

8.2. Azonosítás és hitelesítés

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-6(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.67. LEGKISEBB JOGOSULTSÁG ELVE – FELHASZNÁLÓI JOGOSULTSÁGOK FELÜLVIZSGÁLATA

2.67. A szervezet:

2.67.1. Meghatározott időközönként felülvizsgálja a szerepkörök vagy felhasználói csoportok által hozzáférhető jogosultságokat annak érdekében, hogy ellenőrizze a jogosultságok szükségességét.

2.67.2. Amennyiben szükséges, elvégzi a jogosultságok újra osztását vagy megszüntetését, hogy azok megfelelően tükrözzék a szervezet céljait és az üzleti igényeket.

MAGYARÁZAT

Bizonyos kiosztott felhasználói jogosultságok szükségessége idővel változhat a szervezeti célok, üzleti funkciók, a működési környezet, a technológiák, vagy a fenyegetettségek fényében. Szükséges a kiosztott felhasználói jogosultságok időszakos felülvizsgálata annak megállapításához, hogy a jogosultságok továbbra is helytállóak-e. Amennyiben megállapításra kerül, hogy egy kiosztott jogosultság már nem szükséges, úgy az érintett szervezet meg kell tennie a megfelelő korrekciós intézkedéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet leltárat készít a kiosztott jogosultságokról. Ez magába foglalja az érintett felhasználókat, a jogosultságok fennállásának kezdetét és további, a szervezet által meghatározott információkat.

2. A szervezetnek meghatározott időközönként felül kell vizsgálnia a kiosztott jogosultságokat és szükség esetén meg kell szüntetnie a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat. Emellett a változó és jóváhagyott felelősségek alapján szükség esetén módosítania kell a kiosztott jogosultságokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.14. Folyamatos felügyelet

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.68. Legkisebb jogosultság elve – Jogosultsági szintek kódvégrehajtáshoz

2.68. A szervezet megakadályozza, hogy az általa meghatározott szoftverek magasabb jogosultsági szinteken fussanak, mint a szoftvert futtató felhasználók jogosultsági szintje.

Magyarázat

Bizonyos esetekben egyes szoftvereknek emelt jogosultságokkal kell futniuk a számukra szükséges funkciók végrehajtásához. Amennyiben a szoftver funkciójának végrehajtásához szükséges jogosultságok magasabb szintűek, mint az ilyen szoftvereket futtató szervezeti felhasználókhoz rendelt jogosultságok, akkor ezek a felhasználók - közvetve - a megadottnál nagyobb jogosultságokkal rendelkezhetnek.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia, mely szoftverek futnak magasabb jogosultsági szinten, mint a szoftvert futtató felhasználók jogosultsági szintje. Ez magában foglalja az összes szoftver áttekintését.
2. A szervezetnek meg kell határoznia, hogy mely szoftverek futtathatók magasabb jogosultsági szinten, és melyek nem.
3. A szervezetnek be kell vezetnie egy rendszert, amely képes megakadályozni, hogy a szoftverek magasabb jogosultsági szinten fussanak, mint a szoftvert futtató felhasználók jogosultsági szintje. Ez magában foglalhatja a szoftverek futtatásának korlátozását bizonyos jogosultsági szinteken. pl.: portable szoftverek futtatásának megakadályozása
4. Amennyiben szükség van a kontroll megkerülésére, mert az adott szoftver nem futtatható kisebb jogosultsági szinten, az érintett szervezetnek fel kell mérni az ezzel járó kockázatokat és tájékoztatni kell erről az érintett szervezet elektronikus információs rendszer biztonságáért felelős személyét.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szoftver meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.69. LEGKISEBB JOGOSULTSÁG ELVE – PRIVILEGIZÁLT FUNKCIÓK HASZNÁLATÁNAK NAPLÓZÁSA

2.69. Az EIR naplózza a privilegizált funkciók végrehajtását.

MAGYARÁZAT

A privilegizált funkciók visszaélésszerű használata, a jogosult felhasználók, vagy az EIR egy vagy több felhasználóját kompromittáló, jogosulatlan külső felhasználó által - akár szándékosan, akár véletlenül - komoly és folyamatos aggodalomra ad okot, és jelentős negatív hatással lehet az érintett szervezetre. A privilegizált funkciók használatának naplózása és elemzése az egyik módja az ilyen jellegű visszaélések észlelésének. Ez segíthet csökkenteni a belső- és a tartós fejlett fenyegetések kockázatát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek naplóznia kell a privilegizált funkciók végrehajtását.
2. A szervezet meghatározott gyakorisággal felülvizsgálja és elemzi az EIR által előállított naplókban a privilegizált funkciók végrehajtásával kapcsolatos naplóbejegyzéseket a nem megfelelő vagy szokatlan tevékenységre utaló jelek és az ilyen tevékenységek lehetséges hatásai szempontjából.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.3. Naplóbejegyzések tartalma

4.40. Naplóbejegyzések létrehozása

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.6. Legkisebb jogosultság elve

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.70. LEGKISEBB JOGOSULTSÁG ELVE – NEM-PRIVILEGIZÁLT FELHASZNÁLÓK KORLÁTOZÁSA

2.70. Az EIR megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre.

MAGYARÁZAT

A privilegizált funkciók közé tartoznak a megvalósított biztonsági és adatvédelmi megoldások letiltása, megkerülése vagy módosítása, a rendszerfiókok létrehozása, a rendszer sértetlenségének ellenőrzése és a kriptográfiai kulcskezelési tevékenységek menedzselése. A nem privilegizált felhasználók olyan személyek, akik nem rendelkeznek fentebb felsorolt privilegizált funkciókkal. A nem privilegizált felhasználókkal szemben védelmet igénylő privilegizált funkciók közé tartoznak a behatolásérzékelési és -megelőzési mechanizmusok vagy a rosszindulatú kódfuttatás elleni védelmi mechanizmusok. A nem privilegizált felhasználóknak a privilegizált funkciók végrehajtásában való megakadályozását a "Hozzáférés-ellenőrzés érvényesítése (Hozzáférés-felügyelet)" követelmény biztosítja.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mi számít privilegizált funkciónak.
2. A szervezetnek azonosítania kell a privilegizált felhasználókat, azaz azokat a személyeket, akik rendelkeznek privilegizált funkciók végrehajtására alkalmas jogosultságokkal.
3. A szervezetnek hozzá kell rendelnie a privilegizált felhasználókat a privilegizált funkciókhoz úgy, hogy a nem privilegizált fiókok ne férjenek hozzá olyan privilegizált funkciókhoz, melyekhez nem rendelkeznek megfelelő jogosultsággal.
4. A szervezetnek naplóznia kell a privilegizált funkciók végrehajtását.
5. A szervezet meghatározott gyakorisággal felülvizsgálja és elemzi az EIR által előállított naplókban a privilegizált funkciók végrehajtásával kapcsolatos naplóbejegyzéseket a nem megfelelő vagy szokatlan tevékenységre utaló jelek és az ilyen tevékenységek lehetséges hatásai szempontjából.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-6(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.71. SIKERTELEN BEJELENTKEZÉSI KÍSÉRLETEK

2.71. A szervezet:

2.71.1. Az általa meghatározott esetszám korlátot alkalmazza a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire.

2.71.2. EIR-je automatikusan zárolja a felhasználói fiókot vagy csomópontot a meghatározott időtartamra, vagy ameddig a rendszergazda fel nem oldja annak zárolását, vagy késlelteti a következő bejelentkezési lehetőséget a meghatározott algoritmus szerint. Továbbá értesíti a rendszergazdát, ha a sikertelen próbálkozások maximális számát túllépték.

MAGYARÁZAT

A sikertelen bejelentkezési kísérletek korlátozásának és a megengedett próbálkozások számának túllépése esetén követendő további lépéseknek szükségessége független attól, hogy a bejelentkezés helyi vagy hálózati kapcsolaton keresztül történt. A szolgáltatásmegtagadás lehetősége miatt kezdeményezett automatikus zárolások általában ideiglenesek, és automatikusan feloldódnak egy előre meghatározott, az érintett szervezet által meghatározott időszak után. Késleltetési algoritmus használata esetén az érintett szervezetek különböző algoritmusokat alkalmazhatnak a különböző rendszerelemekre, attól függően, hogy a rendszerelem milyen képességekkel rendelkezik. A sikertelen bejelentkezési kísérletekre adott válaszok az operációs rendszer és az alkalmazás szintjén is megvalósíthatók. Az érintett szervezet által meghatározott intézkedések, amelyek a megengedett egymást követő érvénytelen bejelentkezési kísérletek számának túllépése esetén lépnek életbe lehetnek például egy titkos kérdés megválaszolásának megkövetelése a felhasználónév és jelszó mellett, egy korlátozott felhasználói képességekkel rendelkező zárolási mód bevezetése, bejelentkezés korlátozása és egy meghatározott IP (Internet Protocol) címhez, mint forráscímhez kötése, CAPTCHA igényelése az automatizált támadások megakadályozása érdekében, vagy felhasználói profilok alkalmazása, melyek a bejelentkezést megfelelő napszakhoz, IP címhez, eszközhöz vagy MAC (Media Access Control) címhez köthetik.. Ha az automatikus zárolás, vagy a késleltetési algoritmus végrehajtása nem történik meg, a szervezet más intézkedések kombinációját is mérlegelheti a kimerítő próbálkozásos módszerre (brute-force) épülő támadások megakadályozása érdekében. A szervezet arra is kérheti a felhasználókat, hogy válaszoljanak egy titkos kérdésre, mielőtt a megengedett sikertelen bejelentkezési kísérletek

száma túllépné a meghatározott értéket. Egy fiók automatikus feloldása egy meghatározott időszak után általában nem engedélyezett, azonban lehetnek kivételek a szervezeti célok vagy igények figyelembevételével.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meghatározott esetszám korlátot kell alkalmaznia a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire.
2. A szervezetnek implementálnia kell egy olyan megoldást, amely képes nyomon követni és naplózni a sikertelen bejelentkezési kísérleteket.
3. A szervezetnek biztosítania kell, hogy a meghatározott esetszám túllépése esetén az EIR automatikusan zárolja a felhasználói fiókot egy meghatározott időtartamra vagy amíg a rendszergazda fel nem oldja a zárolást. Emellett késleltetheti a következő bejelentkezési lehetőséget egy meghatározott algoritmus szerint.
4. A szervezetnek biztosítania kell, hogy az EIR értesíti a rendszergazdát, amennyiben a sikertelen próbálkozások maximális számát túllépte egy felhasználó.
5. A szervezet például az alábbi intézkedéseket határozhatja meg a meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire: titkos kérdés megválaszolása a felhasználónév és jelszó mellett, korlátozott felhasználói képességekkel rendelkező zárolási mód bevezetése, bejelentkezés korlátozása és egy meghatározott Internet Protocol (IP) címhez, mint forráscímhez kötése, CAPTCHA használata az automatizált támadások megakadályozására, illetve felhasználói profilok alkalmazása, melyek a bejelentkezést megfelelő napszakhoz, IP címhez, eszközhöz vagy MAC címhez köthetik.
6. A szervezetnek meghatározott időközönként, rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a bejelentkezési kísérletekkel kapcsolatos intézkedéseket, így biztosítva azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés
2.76. Legutóbbi bejelentkezési értesítés
4.2. Naplózható események
4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
8.21. A hitelesítésre szolgáló eszközök kezelése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.7. Sikertelen bejelentkezési kísérletek

ISO/IEC 27001:2023 REFERENCIA

A.8.5

NIST SP 800-53 REV.5 REFERENCIA

AC-7

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

2.72. Sikertelen bejelentkezési kísérletek – Mobil eszköz törlése vagy alaphelyzetbe állítása

2.72. Előzetesen meghatározott számú egymást követő sikertelen bejelentkezési kísérletet követően a szervezet törli vagy alaphelyzetbe állítja a szervezet által meghatározott mobileszközökről származó információt, a meghatározott adattörlési és adattisztítási követelményeknek és technikáknak megfelelően.

Magyarázat

A mobil eszköz egy olyan számítástechnikai eszköz ami annyira kis méretű, hogy egy személy képes hordozni, emellett úgy tervezték meg, hogy fizikai kapcsolat nélkül is képes legyen működni, illetve helyi, nem eltávolítható vagy eltávolítható adattárolóval és saját áramforrással rendelkezik. A törlés vagy alaphelyzetbe állítás csak olyan mobil eszköznél lép életbe, ahol a szervezet által meghatározott számú egymást követő sikertelen bejelentkezési kísérlet megtörténik. Bejelentkezés alatt a mobil eszközre történő bejelentkezés értendő, nem a mobil eszközön található egyes felhasználói fiókokra történő bejelentkezés. A mobileszközön található felhasználói fiókba történő sikeres bejelentkezés nullára állítja a sikertelen bejelentkezések számát.

A törlés vagy alaphelyzetbe állítás lehet, hogy felesleges, ha az eszközön található információkat megfelelően erős titkosítási mechanizmusok védik, ezt az érintett szervezetnek kell mérlegelnie.

Az érintett szervezetnek előre meg kell határoznia, hogy hány sikertelen bejelentkezési kísérlet után törölje vagy állítsa alaphelyzetbe a mobileszközökről származó információt. Ez a szám lehet fix, vagy változhat a kockázati szinttől függően. Az érintett szervezetnek továbbá meg kell határoznia az adattörlési és adattisztítási követelményeket és technikákat is, amelyeknek megfelelően a törlés vagy alaphelyzetbe állítás történik. Ezek a követelmények és technikák biztosítják, hogy az adatokat nem lehet visszaállítani vagy visszaszerezni a törlés vagy alaphelyzetbe állítás után. Érdemes a piacon található megoldások használata ilyen esetekre. Az érintett szervezetnek naplóznia kell a sikertelen bejelentkezési kísérleteket és a törlési vagy alaphelyzetbe állítási műveleteket is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy hány sikertelen bejelentkezési kísérlet után törölje vagy állítsa alaphelyzetbe a mobil eszközökről származó információt. Ez a szám lehet fix vagy változhat a kockázat szinttől függően.
2. A szervezetnek meg kell határoznia, hogy mely mobil eszköz esetén szükséges az azon található információk törlése vagy alaphelyzetbe állítása, amennyiben az előzetesen meghatározott számú, egymást követő sikertelen bejelentkezési kísérlet megtörténik.
3. A szervezetnek implementálnia kell egy olyan megoldást, amely képes nyomon követni és naplózni a sikertelen bejelentkezési kísérleteket.
4. A szervezetnek egy olyan megoldást kell bevezetnie, ami képes arra, hogy az előzetesen meghatározott számú egymást követő sikertelen bejelentkezési kísérletet követően automatikusan törölje vagy alaphelyzetbe állítsa a mobil eszközön található információkat.
5. A szervezetnek meg kell határoznia az adattörlési és adattisztítási követelményeket és technikákat is, amelyeknek megfelelően a törlés vagy alaphelyzetbe állítás történik. Ezek a követelmények és technikák biztosítják, hogy az adatokat nem lehet visszaállítani a törlés vagy alaphelyzetbe állítás után.
6. Sikeres bejelentkezés esetén az EIR-nek automatikusan nullára kell állítania a sikertelen bejelentkezési kísérletek számát.
7. A szervezetnek mérlegelnie kell, hogy szükséges-e az adatok törlése vagy alaphelyzetbe állítása, ha az információkat megfelelően erős titkosítási mechanizmusok védik.
8. A szervezetnek meghatározott időközönként, rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a bejelentkezési kísérletekkel kapcsolatos intézkedéseket, így biztosítva azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.113. Mobil eszközök hozzáférés-ellenőrzése

11.6. Adathordozók szállítása

11.8. Adathordozók törlése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.10

NIST SP 800-53 REV.5 REFERENCIA

AC-7(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a mobileszközök, illetve az adattörlési és adattisztítási követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.73. Sikertelen bejelentkezési kísérletek – Biometrikus bejelentkezési kísérletek korlátozása

2.73. A szervezet korlátozza a sikertelen biometrikus bejelentkezési kísérletek számát.

Magyarázat

A biometriával történő sikeres hitelesítés képességét számos tényező befolyásolhatja, ahogyan a piacon kapható termékek funkcionális és felismerési képességei is eltérnek. A szervezet az általa meghatározott tényezők alapján választja ki a felhasználók számára a megfelelő számú próbálkozást, mely igazodik az alkalmazott technológiához és kockázatokkal arányos védelmet biztosít.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, hogy mely EIR-ek esetén lehetséges, illetve szükséges a biometrikus bejelentkezés.
2. A szervezetnek meg kell határoznia a biometrikus bejelentkezési kísérletek maximális számát.
3. A szervezetnek implementálnia kell egy olyan megoldást, amely képes nyomon követni és naplózni a sikertelen bejelentkezési kísérleteket.
4. A szervezetnek biztosítania kell, hogy a meghatározott biometrikus bejelentkezési kísérlet számának túllépése esetén az EIR automatikusan zárolja a felhasználói fiókot egy meghatározott időtartamra vagy amíg a rendszergazda fel nem oldja a zárolást. Emellett késleltetheti a következő bejelentkezési lehetőséget egy meghatározott algoritmus szerint.
5. A szervezetnek biztosítania kell, hogy az EIR értesíti a rendszergazdát, amennyiben a sikertelen próbálkozások maximális számát túllépte egy felhasználó.
6. A szervezetnek meghatározott időközönként, rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a bejelentkezési kísérletekkel kapcsolatos intézkedéseket, így biztosítva azok hatékonyságát és naprakészségét.

Kapcsolódó intézkedések

8.10. Eszközök azonosítása és hitelesítése

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-7(3)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a szám meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.74. Sikertelen bejelentkezési kísérletek – Alternatív hitelesítési faktor használata

2.74. A szervezet:

2.74.1. Meghatározott számú, egymást követő sikertelen bejelentkezési kísérletet követően engedélyezi az elsődleges hitelesítési faktortól eltérő, meghatározott hitelesítési faktor használatát;

2.74.2. EIR-je meghatározott ideig korlátozza az alternatív faktor használatával végrehajtott egymást követő érvénytelen bejelentkezési kísérletek számát.

Magyarázat

A további hitelesítési faktorok használata támogatja a rendelkezésre állási célt, és lehetővé teszi a véletlenül kizárt felhasználó számára, hogy más hitelesítési faktorokat használjon a zárolás feloldására. Ez azt jelenti, hogy ha egy felhasználó többször is sikertelenül próbál bejelentkezni, az EIR lehetővé teszi számára, hogy egy másik hitelesítési módszert használjon.

A követelmény alkalmazásának lépései

1. A szervezetnek egy olyan hitelesítési rendszert kell alkalmaznia, mely lehetővé teszi, hogy amennyiben egy felhasználó a meghatározott számú, egymást követő sikertelen bejelentkezési kísérletet követően kizárta magát, akkor egy, az elsődleges hitelesítési faktortól eltérő, alternatív hitelesítési faktort használhasson a zárolás feloldására.

2. A szervezetnek az alternatív hitelesítési faktor esetében is meg kell határoznia az egymást követő érvénytelen bejelentkezési kísérletek számát.

3. A szervezetnek implementálnia kell egy olyan megoldást, amely képes nyomon követni és naplózni a sikertelen bejelentkezési kísérleteket.

4. A szervezetnek biztosítania kell, hogy az EIR értesíti a rendszergazdát, amennyiben a sikertelen próbálkozások maximális számát túllépte egy felhasználó.

5. A szervezetnek meghatározott időközönként, rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a bejelentkezési kísérletekkel kapcsolatos intézkedéseket, így biztosítva azok hatékonyságát és naprakészségét.

Kapcsolódó intézkedések

8.10. Eszközök azonosítása és hitelesítése

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-7(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.75. A RENDSZERHASZNÁLAT JELZÉSE

2.75.1. Az EIR a rendszer használata előtt megjelenít a felhasználóknak egy meghatározott rendszerhasználati értesítést vagy üzenetet, amely biztonsági értesítést tartalmaz a szervezetre vonatkozó, hatályos jogszabályi előírásokban, irányelvekben, szabályozásokban, eljárásrendekben, szabványokban és útmutatókban meghatározottak szerint és tartalmazza, hogy:

2.75.1.1. - a felhasználók a szervezet EIR-ét használják.

2.75.1.2. - a rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.

2.75.1.3. - a rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár.

2.75.1.4. - a rendszer használata az előbbiekben részletezett feltételek elfogadását jelenti.

2.75.2. Az EIR mindaddig fenntartja a rendszerhasználati értesítést a képernyőn, amíg a felhasználók nem fogadják el a használati feltételeket és nem tesznek egyértelmű lépéseket a rendszerbe való bejelentkezésre vagy a rendszerhez való további hozzáférésre.

2.75.3. Nyilvánosan hozzáférhető rendszerek esetén az értesítés legalább az alábbiakat tartalmazza:

2.75.3.1. - a felhasználók a szervezet EIR-ét használják.

2.75.3.2. - a rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.

2.75.3.3. - a rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár.

MAGYARÁZAT

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

KAPCSOLÓDÓ INTÉZKEDÉSEK

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

ISO/IEC 27001:2023 REFERENCIA

NIST SP 800-53 REV.5 REFERENCIA

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

2.76. LEGUTÓBBI BEJELENTKEZÉSI ÉRTESÍTÉS

2.76. Az EIR a sikeres bejelentkezést követően értesíti a felhasználót a legutóbbi bejelentkezés időpontjáról.

MAGYARÁZAT

A korábbi bejelentkezési értesítés mind a felhasználói felületeken keresztül történő elérésre, mind a más típusú architektúrákban történő elérésre alkalmazható. Az utolsó sikeres bejelentkezésre vonatkozó információk lehetővé teszik a felhasználó számára, hogy felismerje, ha a megadott dátum és időpont nem egyezik a felhasználó utolsó hozzáférésével.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR képes legyen naplózni és tárolni a felhasználók bejelentkezési adatait. Ez magában foglalja a bejelentkezés időpontját és dátumát.
2. A szervezetnek úgy kell beállítania az EIR-t, hogy a sikeres bejelentkezés után értesítést küldjön a felhasználónak a legutóbbi bejelentkezés időpontjáról. Ez lehet egy egyszerű üzenet, amely megjelenik a felhasználói felületen, vagy egy e-mail, amelyet a felhasználó e-mail címére küldenek.
3. A szervezetnek biztosítania kell, hogy az EIR rendszeresen frissíti a bejelentkezéssel kapcsolatos adatokat, annak érdekében, hogy a felhasználók mindig a legfrissebb információkat kapják meg.
4. A szervezetnek tájékoztatnia kell a felhasználókat arról, hogy mi a teendő amennyiben egy felhasználó eltérést tapasztal az utolsó bejelentkezés idejével kapcsolatosan.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.71. Sikertelen bejelentkezési kísérletek

13.3.1. Viselkedési szabályok

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.5

NIST SP 800-53 REV.5 REFERENCIA

AC-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.77. KORÁBBI BEJELENTKEZÉSEK JELZÉSE – SIKERTELEN BEJELENTKEZÉSEK

2.77. Az EIR a sikeres bejelentkezést követően értesíti a felhasználót az utolsó sikeres bejelentkezés óta történt sikertelen bejelentkezési kísérletek számáról.

MAGYARÁZAT

Az utolsó sikeres bejelentkezés óta történt sikertelen bejelentkezési kísérletek számáról szóló információk lehetővé teszik a felhasználó számára, hogy felismerje, hogy a sikertelen bejelentkezési kísérletek száma összhangban van-e a felhasználó tényleges bejelentkezési kísérleteinek számával.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR képes legyen naplózni és tárolni a felhasználók bejelentkezési adatait. Ez magában foglalja a bejelentkezés időpontját és dátumát, a sikertelen bejelentkezések rögzítését.
2. A szervezetnek úgy kell beállítania az EIR-t, hogy a sikeres bejelentkezés után értesítést küldjön a felhasználónak a sikertelen bejelentkezési kísérletek számáról. Ez lehet egy egyszerű üzenet, amely megjelenik a felhasználói felületen, vagy egy e-mail, amelyet a felhasználó e-mail címére küldenek.
3. A szervezetnek biztosítania kell, hogy az EIR rendszeresen frissíti a bejelentkezéssel kapcsolatos adatokat, annak érdekében, hogy a felhasználók mindig a legfrissebb információkat kapják meg.
4. A szervezetnek tájékoztatnia kell a felhasználókat arról, hogy mi a teendő amennyiben egy felhasználó eltérést tapasztal a sikertelen bejelentkezési kísérletek vonatkozásában.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-9(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.78. KORÁBBI BEJELENTKEZÉSEK JELZÉSE – SIKERES ÉS SIKERTELEN BEJELENTKEZÉSEK

2.78. Az EIR a sikeres bejelentkezést követően tájékoztatja a felhasználót a sikeres bejelentkezések és a sikertelen bejelentkezési kísérletek számáról a meghatározott időszakra vonatkozóan.

MAGYARÁZAT

A megadott időszakon belüli sikeres és sikertelen bejelentkezési kísérletek számáról szóló információk lehetővé teszik a felhasználó számára annak felismerését, hogy a bejelentkezési kísérletek száma és jellege összhangban van-e a felhasználó tényleges bejelentkezési kísérleteivel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR képes legyen naplózni és tárolni a felhasználók bejelentkezési adatait. Ez magában foglalja a bejelentkezés időpontját és dátumát, a sikertelen- és sikeres bejelentkezések rögzítését.
2. A szervezetnek úgy kell beállítania az EIR-t, hogy a sikeres bejelentkezés után értesítést küldjön a felhasználónak egy meghatározott időszakon belüli sikertelen- és sikeres bejelentkezések számáról. Ez lehet egy egyszerű üzenet, amely megjelenik a felhasználói felületen, vagy egy e-mail, amelyet a felhasználó e-mail címére küldenek.
3. A szervezetnek biztosítania kell, hogy az EIR rendszeresen frissíti a bejelentkezéssel kapcsolatos adatokat, annak érdekében, hogy a felhasználók mindig a legfrissebb információkat kapják meg.
4. A szervezetnek tájékoztatnia kell a felhasználókat arról, hogy mi a teendő amennyiben egy felhasználó eltérést tapasztal a sikertelen bejelentkezési kísérletek vonatkozásában.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-9(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.79. KORÁBBI BEJELENTKEZÉSEK JELZÉSE – ÉRTESÍTÉS A FIÓKVÁLTOZÁSOKRÓL

2.79. A rendszer a sikeres bejelentkezést követően értesíti a felhasználót a meghatározott időszak alatt a felhasználói fiók biztonsággal kapcsolatos jellemzőinek vagy beállításainak változásairól.

MAGYARÁZAT

A biztonsággal kapcsolatos fiókjellemzők meghatározott időszakon belüli változásaira vonatkozó információk lehetővé teszik a felhasználók számára, hogy felismerjék, ha a módosítások a tudtuk nélkül történtek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie egy olyan funkciót az EIR-ben, amely képes nyomon követni és rögzíteni a felhasználói fiókok biztonsági jellemzőinek és beállításainak változásait.
2. A szervezetnek gondoskodni kell arról, hogy az EIR generáljon értesítéseket a felhasználók számára minden alkalommal, amikor változás történik a fiókjuk biztonsági jellemzőiben vagy beállításaiban. Ez magában foglalhatja a jelszó, a biztonsági kérdések, a hitelesítési módszerek vagy a fiókhoz hozzáférő eszközök változásait.
3. A szervezetnek be kell állítania egy meghatározott időszakot, amely alatt az EIR értesítést küld a felhasználónak a változásokról. Ez lehet például azonnali értesítés, napi, heti vagy havi összefoglaló, attól függően, hogy milyen gyakran várhatók változások és mennyire kritikusak ezek a biztonság szempontjából.
4. A szervezetnek biztosítania kell, hogy az EIR naplózza az összes változást és értesítést, hogy később vissza lehessen követni a változásokat és ellenőrizni lehessen a rendszer működését.
5. A szervezetnek tájékoztatnia kell a felhasználókat arról, hogy mi a teendő amennyiben olyan értesítést kapnak, mely szerint változás történt a fiókjukban anélkül, hogy ők maguk hajtották volna végre azt.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-9(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az a felhasználói fiók biztonságával kapcsolatos jellemzők vagy paraméterek illetve az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.80. KORÁBBI BEJELENTKEZÉSEK JELZÉSE – KIEGÉSZÍTŐ BEJELENTKEZÉSI INFORMÁCIÓK

2.80. Az EIR a sikeres bejelentkezést követően a szervezet által meghatározott további információkat közöl a felhasználónak.

MAGYARÁZAT

A szervezet meghatározhatja, hogy a felhasználóknak bejelentkezéskor milyen további információkat szolgáltat, ilyen lehet például az utolsó bejelentkezés lokációja. A felhasználó lokációját olyan információk alapján határozhatják meg, melyeket az EIR-ek is felismernek pl.: IP (Internet Protocol) cím, a bejelentkezésre használt eszköz jellemzői.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy milyen további információkat szeretne közölni a felhasználóval a sikeres bejelentkezést követően pl.: az utolsó bejelentkezés lokációja
2. Fenti esetben az EIR-nek képesnek kell lennie arra, hogy meghatározza a felhasználó lokációját, melyet például IP (Internet Protocol) cím alapján tud megtenni.
3. Az EIR-nek képesnek kell lennie arra, hogy ezeket az információkat naplózza, és a sikeres bejelentkezést követően közölje a felhasználóval.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-9(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kiegészítő információ meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.81. EGYIDEJŰ MUNKASZAKASZ KEZELÉS

2.81. A szervezet az EIR-ben meghatározott számra korlátozza az egyidejű munkaszakaszok számát minden egyes meghatározott fiókra vagy fióktípusra vonatkozóan.

MAGYARÁZAT

Az érintett szervezet meghatározhatja az egyidejű munkaszakaszok maximális számát az EIR fiókokra globálisan, fióktípusonként, fiókonként, vagy az előbb felsoroltak bármely kombinációjával. Például a szervezet korlátozhatja az egyidejű munkaszakaszok számát a rendszer adminisztrátorok vagy más, fokozottan bizalmas területeken vagy létfontosságú alkalmazásokban dolgozó személyek számára. Az egyidejű munkaszakasz-ellenőrzés az EIR fiókok egyidejű munkaszakaszait kezeli. Azonban nem foglalkozik az egyidejű munkaszakaszokkal, melyeket egyetlen felhasználó több EIR fiókon keresztül nyitott meg.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az EIR-ben a maximális egyidejű munkaszakaszok számát. Ezt meghatározhatja globálisan, fióktípusonként, fiókonként, vagy az előbb felsoroltak kombinációjával. Például a szervezet korlátozhatja az egyidejű munkaszakaszok számát a rendszer adminisztrátorok vagy más, fokozottan bizalmas területeken vagy létfontosságú alkalmazásokban dolgozó személyek számára.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.73. Munkaszakasz hitelessége

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.9. Egyidejű munkaszakasz kezelés: Az érintett szervezet az elektronikus információs rendszerben meghatározott számra korlátozza az egyidejű munkaszakaszok számát, a meghatározott fiókok vagy fiók típusok számára külön-külön.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a fiók vagy fióktípus illetve a szám meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

2.82. ESZKÖZ ZÁROLÁSA

2.82. A szervezet:

2.82.1. Meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén, az eszköz zárolásával megakadályozza az EIR-hez való további hozzáférést.

2.82.2. Fenntartja az eszköz zárolását mindaddig, amíg a felhasználó a megfelelő azonosítási és hitelesítési eljárásokat el nem végzi.

MAGYARÁZAT

Egy eszköz zárolása ideiglenes intézkedés, amely akkor kerül végrehajtásra, amikor egy felhasználó abbahagyja a munkát és eltávolodik az EIR közvetlen közeléből, de nem akar kijelentkezni, mert távolléte ideiglenes. Egy eszköz zárolását az operációs rendszer vagy az alkalmazás szintjén lehet végrehajtani. Közelség alapú zárolást is lehet alkalmazni a zárolás végrehajtására (pl.: Bluetooth-alapú eszköz használatával). A felhasználó által kezdeményezett eszköz zárolás fizikai interakciót követel meg az eszköz zárolásának érvényesítéséhez. Egy eszközt előre beállított szabály alapján is lehet zárolni pl.: meghatározott időtartamú felhasználói inaktivitás alapján. Egy eszköz zárolásával nem helyettesíthető az EIR-ből történő kijelentkezés.

A szervezet meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén, az eszköz zárolásával megakadályozza az EIR-hez való további hozzáférést. Az érintett szervezet fenntartja az eszköz zárolását mindaddig, amíg a felhasználó a megfelelő azonosítási és hitelesítési eljárásokat el nem végzi. Ez azt jelenti, hogy a felhasználónak újra be kell jelentkeznie a rendszerbe, mielőtt hozzáférhetne az EIR-hez. Ez a folyamat segít megakadályozni a jogosulatlan hozzáférést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie egy olyan megoldást, ami képes az eszközöket zárolni és egyúttal megakadályozni az EIR-hez történő további hozzáférést, ha a felhasználó meghatározott időtartamig inaktív, vagy ha a felhasználó maga kezdeményezi a zárolást. Az eszköz zárolásának az operációs rendszer vagy az alkalmazási szintjén kell történnie.

2. A szervezetnek fenn kell tartania az eszköz zárolását mindaddig, amíg a felhasználó a megfelelő azonosítási és hitelesítési eljárásokat el nem végzi.

3. A szervezet az eszköz zárolásával nem helyettesítheti a rendszerekből történő kijelentkezést.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.71. Sikertelen bejelentkezési kísérletek

8.43. Újrahitelesítés

13.3.1. Viselkedési szabályok

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.10. A munkaszakasz zárolása

ISO/IEC 27001:2023 referencia

A.7.7; A.8.1

NIST SP 800-53 rev.5 referencia

AC-11

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

2.83. Eszköz zárolása – Képernyőtakarás

2.83. A szervezet az eszköz zárolása során elrejti a kijelzőn lévő információkat.

Magyarázat

Az érintett szervezet az eszköz zárolása során elrejti a kijelzőn lévő információkat. A szervezet az eszköz kijelzőjén statikus vagy dinamikus képeket jelenít meg a zárolás időtartama alatt. Az eszköz zárolása során a szervezetnek gondoskodnia kell arról, hogy a kijelzőn lévő információk ne legyenek láthatóak. Ezáltal a szervezet megakadályozza a jogosulatlan személyek számára történő hozzáférést.

A követelmény alkalmazásának lépései

1. A szervezetnek az eszközök zárolását úgy kell megvalósítania, hogy a zárolás során elrejtse a kijelzőn lévő információkat. A szervezet az eszköz kijelzőjén statikus vagy dinamikus képeket jelenít meg a zárolás időtartama alatt pl.: képernyőkímélő, váltakozó fényképek és színek, üres képernyő stb.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.10. A munkaszakasz zárolása

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-11(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.84. A MUNKASZAKASZ LEZÁRÁSA

2.84. Az EIR automatikusan lezárja a munkaszakaszt a szervezet által meghatározott feltételek, vagy a munkaszakasz megszakítását igénylő események után.

MAGYARÁZAT

Egy logikai munkamenet akkor kezdődik, amikor egy felhasználó (vagy a felhasználó nevében cselekvő folyamat) hozzáfér az érintett szervezet EIR-jéhez. Az ilyen felhasználói munkameneteket le lehet zárni a hálózati munkaszakaszok megszüntetése nélkül. A munkaszakasz lezárása befejezi az összes, a felhasználó logikai munkaszakaszával összefüggő folyamatot, kivéve azokat a folyamatokat, amelyeket a felhasználó (azaz a munkaszakasz tulajdonosa) kifejezetten arra hoz létre, hogy a munkaszskasz megszüntetése után is folytatódjanak. Az automatikus munkamenet megszakítást igénylő feltételek vagy kiváltó események közé tartoznak a szervezet által meghatározott felhasználói inaktivitási időszakok, célzott válaszok bizonyos típusú biztonsági eseményekre, vagy egy adott napszakra, időtartamra korlátozott EIR használat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és be kell állítania azokat a feltételeket, amelyek alapján az EIR automatikusan lezárja a felhasználói munkaszakaszt. Ezek a feltételek tartalmazhatják a felhasználói inaktivitás meghatározott időszakait, célzott válaszokat bizonyos típusú biztonsági eseményekre, vagy a rendszerhasználat időbeli korlátozásait.
2. A szervezetnek biztosítania kell, hogy az EIR képes legyen lezárni a munkaszakaszt anélkül, hogy megszakítaná a hálózati kapcsolatokat.
3. A szervezetnek be kell állítania az EIR-t úgy, hogy a munkaszakasz lezárása után minden, a felhasználói munkaszakaszhoz kapcsolódó folyamatot leállít, kivéve azokat, amelyeket a felhasználó kifejezetten arra hozott létre, hogy a munkaszakasz lezárása után is folytatódjanak.

KAPCSOLÓDÓ INTÉZKEDÉSEK

10.11. Távoli karbantartás

17.46. A hálózati kapcsolat megszakítása

17.73. Munkaszakasz hitelessége

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.11. A munkaszakasz lezárása: Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-12

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a munkamenet-megszakítást előidéző feltételek vagy kiváltó események meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.85. MUNKASZAKASZ MEGSZAKÍTÁSA – FELHASZNÁLÓ ÁLTAL KEZDEMÉNYEZETT KIJELENTKEZÉSEK

2.85. Az EIR biztosítja a kijelentkezési lehetőséget a felhasználó által kezdeményezett kommunikációs munkaszakaszból, ha az ahhoz történő hozzáférés hitelesítést igényel.

MAGYARÁZAT

Azon információs erőforrások, amelyekhez a felhasználók hitelesítéssel férnek hozzá, magukban foglalják a helyi munkaállomásokat, az adatbázisokat és a jelszóval védett weboldalakat vagy webalapú szolgáltatásokat. Az EIR-nek minden olyan, a felhasználó által kezdeményezett munkaszakaszból biztosítania kell a kijelentkezés lehetőségét, ahol az ahhoz történő hozzáférés hitelesítésen keresztül valósul meg.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az olyan típusú EIR-eknél melyekhez történő hozzáférés hitelesítést igényel, kijelentkezési lehetőséget biztosít a felhasználók számára az általuk kezdeményezett kommunikációs munkaszakaszból.
2. A szervezetnek implementálnia kell egy kijelentkezési funkciót az EIR-ben. Ez a funkció lehetővé teszi a felhasználók számára, hogy biztonságosan kijelentkezzenek az EIR-ből, amikor be kívánják fejezni a munkaszakaszukat.
3. A szervezetnek biztosítania kell, hogy a kijelentkezési funkció jól látható és könnyen használható legyen a felhasználók számára.
4. A szervezetnek naplóznia kell a felhasználók ki- és bejelentkezési tevékenységeit az EIR-ben. Ez segít nyomon követni a felhasználói tevékenységeket, és lehetővé teszi az érintett szervezet számára, hogy azonosítsa a potenciális biztonsági problémákat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-12(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információforrások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.86. MUNKASZAKASZ MEGSZAKÍTÁSA – MEGSZAKÍTÁSI ÜZENET

2.86. Az EIR egyértelmű kijelentkezési üzenetet jelenít meg a felhasználók számára, amely jelzi a hitelesített kommunikációs munkaszakaszok befejezését.

MAGYARÁZAT

Webes hozzáférés esetén az EIR a kijelentkezési üzenetet azután jelenti meg, miután a hitelesített munkaszakasz megszakításra került. Az EIR által megjelenített kijelentkezési üzenet világosan jelezheti a felhasználóknak, hogy a munkamenetük befejeződött, és ezáltal csökkentheti a nem szándékos hozzáférési kísérletek számát. Bizonyos típusú munkamenetek, például a fájlátviteli protokoll (FTP) munkaszakasz esetén, az EIR a munkaszakasz befejezése előtt küld kijelentkezéssel kapcsolatos üzenetet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek az EIR-ben implementálnia kell egy funkciót, amely egyértelmű kijelentkezési üzenetet jelenít meg a felhasználók számára, amikor a hitelesített munkaszakaszok befejeződnek. Ennek az üzenetnek egyértelműen jeleznie kell a munkaszakasz befejezését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-12(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.87. MUNKASZAKASZ MEGSZAKÍTÁSA – IDŐKORLÁTOZÁSRA FIGYELMEZTETŐ ÜZENET

2.87. Az EIR egyértelmű üzenetet jelenít meg a felhasználók számára, amely jelzi, hogy a munkaszakasz a meghatározott idő leteltét követően véget ér.

MAGYARÁZAT

Az EIR a munkaszakasz lejáratának közeledtével figyelmezteti a felhasználókat, és lehetőséget biztosít számukra a munkaszakasz folytatására. A munkaszakasszal kapcsolatos időkorlátozás beállítása "A munkaszakasz lezárása" kontrollnál elvárt követelményeken alapul.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell állítania az EIR-ben egy olyan funkciót, amely figyelmezteti a felhasználókat a munkaszakasz lejáratának közelgő időpontjára és lehetőséget biztosít számukra a munkaszakasz folytatására.
2. A szervezetnek meg kell határoznia a munkaszakasz lejáratának időpontját.
3. A szervezetnek előre meg kell határoznia és be kell állítania a vonatkozó paramétereket az EIR-ben, hogy a rendszer időben értesítse a felhasználókat a munkamenetük lejáratáról.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-12(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az a munkamenet lejáratához szükséges idő meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.88. AZONOSÍTÁS VAGY HITELESÍTÉS NÉLKÜL ENGEDÉLYEZETT TEVÉKENYSÉGEK

2.88. A szervezet:

2.88.1. Azonosítja azon felhasználói tevékenységeket, amelyek - a szervezeti célokkal és üzleti funkciókkal összhangban - az EIR-ben azonosítás vagy hitelesítés nélkül is végrehajthatók.

2.88.2. A rendszerbiztonsági tervben dokumentálja és megindokolja azokat a felhasználói tevékenységeket, amelyek azonosítás vagy hitelesítés nélkül is végrehajthatók.

MAGYARÁZAT

Bizonyos felhasználói tevékenységek végrehajhatók azonosítás és hitelesítés nélkül is, amennyiben a szervezet úgy dönt. A szervezet például olyan esetekben engedélyezhet azonosítás és hitelesítés nélküli felhasználói tevékenységet, mikor a felhasználóknak egy publikusan elérhető weboldalhoz kell hozzáférniük vagy amikor mobiltelefonon fogadnak hívásokat. Olyan felhasználói tevékenység nem minősül azonosítás és hitelesítés nélkül engedélyezett tevékenységnek, melynek megtételéhez már egyszer szükség volt azonosításra és hitelesítésre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a felhasználói tevékenységeket, amelyeket az EIR-ben azonosítás vagy hitelesítés nélkül is végrehajthatnak.
2. A szervezetnek meg kell határoznia azokat a tevékenységeket, amelyek normál esetben azonosítást vagy hitelesítést igényelnek, de bizonyos körülmények között lehetővé teszik az azonosítási vagy hitelesítési mechanizmusok megkerülését.
3. A szervezetnek dokumentálnia és indokolnia kell az EIR-ben azonosítás vagy hitelesítés nélkül végrehajtható felhasználói tevékenységeket a rendszerbiztonsági tervben.
4. A szervezetnek rendszeresen felül kell vizsgálnia ezeket az azonosítást és hitelesítést nem igénylő felhasználói tevékenységeket, és amennyiben azok már nincsenek összhangban a szervezeti célokkal és az üzleti funkciókkal, meg kell szüntetnie azokat.

Kapcsolódó intézkedések

2.75.1. A rendszerhasználat jelzése

8.2. Azonosítás és hitelesítés

13.2. Rendszerbiztonsági terv

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-14

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

2.89. BIZTONSÁGI TULAJDONSÁGOK

2.89. A szervezet:

2.89.1. Lehetővé teszi biztonsági tulajdonságértékek hozzárendelését a tárolt, feldolgozott vagy továbbított információkhoz.

2.89.2. Gondoskodik arról, hogy a tulajdonságtársítások létrejöhessenek és fennmaradhassanak az információval együtt.

2.89.3. Meghatározza azokat a biztonsági tulajdonságokat, amelyek engedélyezettek a meghatározott EIR-ek számára.

2.89.4. Meghatározza a megengedett tulajdonságértékeket vagy tulajdonságérték tartományokat a meghatározott tulajdonságokhoz.

2.89.5. Naplózza a tulajdonságok változásait.

2.89.6. Meghatározott időközönként felülvizsgálja a meghatározott biztonsági tulajdonságokat.

MAGYARÁZAT

Az információk rendszeren belüli megjelenítésére az adatszerkezeteknek vagy adatstruktúráknak nevezett absztrakciók segítségével kerül sor. A belső adatstruktúrák különböző típusú entitásokat jelölhetnek, aktív és passzív entitásokat egyaránt. Az aktív entitások, más néven alanyok, jellemzően egyénekhez, eszközökhöz vagy egyének nevében eljáró folyamatokhoz kapcsolódnak. A passzív entitások, más néven objektumok jellemzően olyan adatszerkezetekhez kapcsolódnak, mint például rekordok, tárolók, táblázatok, fájlok, folyamatok közötti csatornák és kommunikációs portok. A biztonsági tulajdonság a metaadat egy fajtája. Olyan absztrakciók, amelyek az aktív és passzív entitások alapvető tulajdonságait vagy jellemzőit képviselik az információk védelme szempontjából. A biztonsági tulajdonságok explicit vagy implicit módon társíthatók a szervezeti EIR-ekben vagy rendszerelemekben található információkhoz. A tulajdonságok olyan aktív entitásokhoz társíthatók, amelyek képesek információt küldeni vagy fogadni, információt áramoltatni az objektumok között, vagy megváltoztatni a rendszer állapotát. Ezek a tulajdonságok passzív entitásokhoz (azaz objektumokhoz) is társíthatók, amelyek információt tartalmaznak vagy fogadnak. Az adatokhoz vagy információkhoz kötött tulajdonságok lehetővé teszik a hozzáférés-felügyelet és az információáramlás-szabályozás érvényesítését, beleértve az adatmegőrzési korlátokat is. Ez szervezeti folyamatokon, rendszerfunkciókon vagy mechanizmusokon keresztül történik. A

rendszerek által alkalmazott csatolási technikák befolyásolják a tulajdonságok információhoz való kötésének (ún. "information binding") erősségét. A csatolási technikák befolyásolják a szervezetek által megkövetelt további felülvizsgálatok számát és mértékét. A tulajdonságok tartalma vagy a hozzárendelt értékei közvetlenül befolyásolhatják az egyéneknek a szervezeti információkhoz való hozzáférési képességét.

A szervezetek meghatározhatják a célok vagy az üzleti funkciók támogatásához szükséges rendszerekben a kötelezően vezetett biztonsági tulajdonságok típusait. Egy biztonsági tulajdonsághoz számos érték rendelhető. Az engedélyezett tulajdonságtartományok és értékek meghatározásával a szervezetek biztosítják, hogy az tulajdonságértékek hasznosak és helytállóak legyenek. A címkézés a biztonsági tulajdonságok a rendszereken belüli adatstruktúrák által képviselt alanyokhoz és objektumokhoz való hozzárendelésére utal. Ez megkönnyíti az információbiztonsági szabályok rendszeralapú érvényesítését. A címkézés magában foglalja az információk jogi és megfelelőségi követelményeknek megfelelő minősítését (pl. titkos, bizalmas, nyilvános), az információ kompromittálódásának vagy megsemmisülésének hatását, a nagy értékű eszközinformációkat, a hozzáférési jogosultságokat, az adatok életciklus-védelmét (pl. a titkosítást és az adatok lejáratát. A biztonsági címkék értéke megegyezhet az adathordozók jelölésével (pl. szigorúan titkos, titkos, bizalmas).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek lehetővé kell tennie a biztonsági tulajdonságértékek hozzárendelését a tárolt, feldolgozott vagy továbbított információkhoz. Ez azt jelenti, hogy a szervezetnek olyan rendszert kell létrehoznia, amely képes az információkhoz biztonsági tulajdonságokat rendelni.
2. A szervezetnek gondoskodnia kell arról, hogy a tulajdonságtársítások létrejöhessenek és fennmaradhassanak az információval együtt. Ez azt jelenti, hogy a szervezetnek biztosítania kell, hogy a tulajdonságok hozzárendelése az információhoz konzisztens és állandó legyen.
3. A szervezetnek meg kell határoznia azokat a biztonsági tulajdonságokat, amelyek engedélyezettek a meghatározott EIR-ek számára. Ez azt jelenti, hogy a szervezetnek döntenie kell arról, mely biztonsági tulajdonságokat engedélyezi az EIR-ekben.
4. A szervezetnek meg kell határoznia a tulajdonságértékeket vagy tulajdonságérték tartományokat a meghatározott tulajdonságokhoz. Ez azt jelenti, hogy a szervezetnek döntenie

kell arról, milyen értékek vagy értéktartományok megengedettek a különböző biztonsági tulajdonságokhoz.

5. A szervezetnek naplóznia kell a tulajdonságok változásait. Ez azt jelenti, hogy a szervezetnek nyomon kell követnie és rögzítenie kell a biztonsági tulajdonságok változásait.

6. A szervezetnek meghatározott időközönként felül kell vizsgálnia a meghatározott biztonsági tulajdonságokat. Ez azt jelenti, hogy a szervezetnek rendszeresen ellenőriznie kell a biztonsági tulajdonságokat, hogy biztosítsa, hogy még mindig megfelelnek a szervezet biztonsági követelményeinek.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.60. Legkisebb jogosultság elve

2.121. Információmegosztás

2.129. Referenciának való megfelelőség vizsgálata

4.2. Naplózható események

4.33. Letagadhatatlanság

11.3. Adathordozók címkézése

12.48. Rendszerelemek jelölése

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-16

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.90. Biztonsági tulajdonságok – Dinamikus tulajdonságtársítás

2.90. A szervezet dinamikusan társítja a biztonsági tulajdonságokat a meghatározott alanyokhoz és objektumokhoz, a meghatározott információbiztonsági előírásoknak megfelelően, az információk létrehozásakor és összeállításakor.

Magyarázat

A biztonsági tulajdonságok dinamikus társítása akkor alkalmazható, amikor az információ biztonsági jellemzői idővel változnak. Az attribútumok változhatnak az információ aggregációja miatt, az egyéni hozzáférési jogosultságok (pl. beállított privilégiumok) változásai miatt, az információ biztonsági osztályának változása, vagy a szabályok változása miatt. A biztonsági tulajdonságok helyzetfüggően is változhatnak.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia azokat az alanyokat és objektumokat, amelyekhez a biztonsági tulajdonságokat társítani kell. Ez magában foglalhatja a felhasználókat, rendszereket, alkalmazásokat, adatokat stb.
2. A szervezetnek meg kell határoznia a biztonsági tulajdonságokat, amelyeket társítani kell az alanyokhoz és objektumokhoz. Ez magában foglalhatja a megőrzési beállításokat, hozzáférési jogosultságokat, biztonsági osztályt stb.
3. A szervezetnek meg kell határoznia az információbiztonsági előírásokat, amelyeknek meg kell felelnie. Ez magában foglalhatja a szervezet belső szabályzóit, jogszabályi követelményeket, iparági szabványokat stb.
4. A szervezetnek implementálnia kell egy megoldást, amely képes dinamikusan társítani a biztonsági tulajdonságokat az alanyokhoz és objektumokhoz. Ez magában foglalhatja a szoftverfejlesztést, konfigurációs beállításokat, rendszerintegrációt stb.
5. A szervezetnek dokumentálnia kell a biztonsági tulajdonságok dinamikus társításának tevékenységeit, hogy bizonyítékot szolgáltasson a megfelelőségről és segítse a jövőbeli vizsgálatokat.

6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági tulajdonságok dinamikus társításának folyamatát, hogy biztosítsa a megfelelőséget.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-16(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az alanyok és objektumok illetve a biztonsági szabályok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.91. BIZTONSÁGI TULAJDONSÁGOK – TULAJDONSÁGÉRTÉKEK JOGOSULT SZEMÉLYEK ÁLTALI MÓDOSÍTÁSA

2.91. A szervezet lehetőséget biztosít a jogosult személyeknek vagy a nevükben eljáró folyamatoknak, a kapcsolódó biztonsági tulajdonságértékek meghatározására vagy megváltoztatására.

MAGYARÁZAT

Az egyes tulajdonságok tartalma vagy a hozzájuk rendelt értékek közvetlenül befolyásolhatják az egyének azon képességét, hogy hozzáférjenek a szervezeti információkhoz. Ezért fontos, hogy a rendszerek képesek legyenek az engedélyezett személyekre korlátozni a biztonsági tulajdonságok létrehozásának vagy módosításának lehetőségét. Az érintett szervezetnek biztosítania kell a jogosult személyeknek vagy a nevükben eljáró folyamatoknak a lehetőséget, hogy meghatározzák vagy megváltoztassák a kapcsolódó biztonsági tulajdonságértékeket. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie arra, hogy korlátozza az attribútumok létrehozásának vagy módosításának képességét csak a jogosult személyekre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely személyek jogosultak a biztonsági tulajdonságértékek meghatározására vagy megváltoztatására az EIR-en belül.
2. A szervezetnek implementálnia kell egy olyan rendszert, amely lehetővé teszi a jogosult személyek számára, hogy meghatározzák vagy megváltoztassák a biztonsági tulajdonságértékeket.
3. A szervezetnek biztosítania kell, hogy a jogosult személyek képesek legyenek ellenőrizni és módosítani a biztonsági tulajdonságértékeket. Ez magában foglalhatja a rendszeres ellenőrzéseket és a naplók áttekintését, hogy biztosítsák a megfelelő hozzáférést és a biztonsági paraméterek betartását.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági tulajdonságértékeket, hogy biztosítsa az EIR védelmét és a jogosult személyek hozzáférését. Ez magában foglalhatja a naplók áttekintését és a biztonsági paraméterek frissítését.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-16(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.92. Biztonsági tulajdonságok – Tulajdonságtársítások rendszerenkénti karbantartása

2.92. A szervezet fenntartja a meghatározott biztonsági tulajdonságok sértetlenségét és hozzárendelését a meghatározott alanyokhoz és objektumokhoz.

Magyarázat

A biztonsági tulajdonságok alanyokhoz és objektumokhoz való társításának és sértetlenségének kellő megbízhatósággal történő fenntartása segít annak biztosításában, hogy a tulajdonságok társításait automatizált szabályok alapjául lehessen használni. Az egyes elemek, például a biztonsági konfigurációs fájlok sértetlenségének fenntartása olyan sértetlenség-ellenőrzési mechanizmus használatával történhet, amely észleli az anomáliákat és az ismert alapkövetelményektől eltérő változásokat. Az automatizált, házirendben foglalt intézkedések közé tartozik például a megőrzési idő lejárta, a hozzáférés-felügyeleti döntések, az információáramlás-ellenőrzési döntések és az információ nyilvánosságra hozatalára vonatkozó döntések.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell biztosítania kell, hogy a biztonsági tulajdonságok és tartalmuk sértetlen marad. Hozzá kell rendelnie a meghatározott alanyokhoz és objektumokhoz az EIR-en belül.
2. A szervezetnek implementálnia kell egy sértetlenség felügyeleti mechanizmust, amely képes észlelni az anomáliákat és a változásokat. Ez kiemelten fontos a biztonsági konfigurációs fájlok esetében.
3. A szervezetnek automatizált beavatkozási intézkedéseket kell bevezetnie, amelyek a hozzárendelt tulajdonságok alapján működnek.
4. A szervezetnek naplóznia kell minden lépést és változást, hogy nyomon követhető legyen a folyamat, és szükség esetén vissza lehessen állítani az EIR korábbi állapotát.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági tulajdonságokat és hozzárendeléseket, hogy biztosítsa azok relevanciáját és hatékonyságát.

6. A szervezetnek biztosítania kell a megfelelő képzést és tudatosságot a személyzet számára a biztonsági tulajdonságok és hozzárendelések fontosságáról, valamint azok sértetlenségének fenntartásáról az EIR-en belül.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-16(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi tulajdonságok illetve az alanyok és objektumok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.93. BIZTONSÁGI TULAJDONSÁGOK – TULAJDONSÁGOK JOGOSULT SZEMÉLYEK ÁLTAL TÖRTÉNŐ TÁRSÍTÁSA

2.93. A szervezet lehetővé teszi a jogosult személyeknek vagy a nevükben eljáró folyamatoknak, a meghatározott biztonsági tulajdonságok és a meghatározott alanyok és objektumok társítását.

MAGYARÁZAT

A rendszerek általában lehetővé teszik a privilegizált felhasználók számára, hogy a rendszer által meghatározott alanyokhoz és objektumokhoz (pl. könyvtárak, fájlok és portok) biztonsági tulajdonságokat rendeljenek. Egyes rendszerek további lehetőséget biztosítanak az általános felhasználók számára, hogy további objektumokhoz (pl. fájlok, e-mailek) rendeljenek biztonsági tulajdonságokat. Az egyes biztonsági tulajdonságok jogosult személyekhez való hozzárendelését a tervezési dokumentáció, pl. a rendszerbiztonsági terv írja le. A rendszerek által nyújtott támogatás magában foglalhatja a felhasználók felhívását az információs objektumokhoz társítandó biztonsági tulajdonságok kiválasztására, automatizált mechanizmusok alkalmazását az információk tulajdonságokkal való kategorizálására, biztonsági osztály megjelölésére meghatározott szabályok alapján, vagy annak biztosítását, hogy a kiválasztott biztonsági tulajdonságok kombinációja érvényes legyen. A szervezetek figyelembe veszik a tulajdonságok létrehozását, törlését vagy módosítását az ellenőrizhető események meghatározásakor.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy mely biztonsági tulajdonságok és alanyok, valamint objektumok társítását engedélyezi.
2. A szervezetnek meg kell határozni, hogy a fenti társítást mely jogosult személyeknek, vagy melyik, a nevükben eljáró folyamatoknak engedélyezi.
3. A szervezetnek biztosítania kell, hogy a biztonsági tulajdonságok egyértelműen azonosíthatók legyenek a kimeneti eszközökön. Ez azt jelenti, hogy a biztonsági tulajdonságoknak világosan és érthetően kell megjelenniük, hogy a felhasználók könnyen azonosíthassák őket.

4. A szervezetnek dokumentálnia kell a biztonsági tulajdonságokat és naplóznia is kell, hogy nyomon követhesse és ellenőrizhesse azokat. Ez magában foglalhatja a rendszeres ellenőrzéseket és a naplók áttekintését, hogy biztosítsák, hogy az EIR megfelelően működik és megfelel a szervezet által meghatározott követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-16(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi tulajdonságok, illetve az alanyok és objektumok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.94. BIZTONSÁGI TULAJDONSÁGOK – TULAJDONSÁGOK MEGJELENÍTÉSE A KIMENETI OBJEKTUMOKON

2.94. A szervezet biztosítja, hogy az EIR az ember által olvasható formában jeleníti meg a biztonsági tulajdonságokat minden olyan objektumra vonatkozóan, amelyet az EIR a kimeneti eszközök felé továbbít, hogy azokon a meghatározott speciális terjesztési, kezelési vagy elosztási utasítások egyértelműen azonosíthatók legyenek.

MAGYARÁZAT

A rendszer kimenetei közé tartoznak a megjelenített adatok, a nyomtatott oldalak, képernyők vagy azzal egyenértékű elemek. A rendszer kimeneti eszközei közé tartoznak a nyomtatók, notebook számítógépek, videókijelzők, okostelefonok és táblagépek. Az EIR az ember által olvasható formában jeleníti meg a biztonsági tulajdonságokat minden olyan objektumra vonatkozóan, melyet a fent említett eszközök felé továbbít, annak érdekében, hogy azokon a meghatározott speciális terjesztési, kezelési vagy elosztási utasítások egyértelműen azonosíthatók legyenek. Fontos törekedni azonban arra, hogy az információk jogosulatlan felfedésével kockázatának teszi ki magát az érintett szervezet, így ennek csökkentése érdekében a teljes értékeket célszerű akkor megjeleníteni, ha azokat a felhasználó felfedte.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR képes legyen az ember által olvasható formában megjeleníteni a biztonsági tulajdonságokat.
2. A szervezetnek gondoskodnia kell arról, hogy az EIR minden olyan objektumra vonatkozóan megjelenítse a biztonsági tulajdonságokat, amelyeket az EIR a kimeneti eszközök felé továbbít. Ez magában foglalhatja a dokumentumokat, fájlokat, adatbázisokat, e-maileket stb.
3. A szervezetnek biztosítania kell, hogy a biztonsági tulajdonságok egyértelműen azonosíthatók legyenek a kimeneti eszközökön. Ez azt jelenti, hogy a biztonsági tulajdonságoknak világosan és érthetően kell megjelenniük, hogy a felhasználók könnyen azonosíthassák őket.
4. A szervezetnek gondoskodnia kell arról, hogy az EIR a biztonsági tulajdonságokat a meghatározott speciális terjesztési, kezelési vagy elosztási utasítások szerint jelenítse meg. Ez

azt jelenti, hogy az EIR-nek képesnek kell lennie arra, hogy a biztonsági tulajdonságokat a megfelelő módon jelenítse meg, attól függően, hogy milyen utasításokat kapott.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-16(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a speciális terjesztési, kezelési vagy elosztási utasítások illetve az ember által olvasható forma meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.95. Biztonsági tulajdonságok – Tulajdonságtársítás karbantartása

2.95. A szervezet arra kötelezi a személyzetet, hogy a meghatározott biztonsági szabályokkal összhangban rendelje hozzá és tartsa fenn a meghatározott biztonsági tulajdonságokat, valamint az alanyok és objektumok meghatározott összekapcsolását.

Magyarázat

A tulajdonság összerendelése megköveteli, hogy az egyes felhasználók a meghatározott biztonsági jellemzők alanyokhoz és objektumokhoz való társításait fenntartsák a rendszerben. Ez azt jelenti, hogy a felhasználóknak gondoskodniuk kell arról, hogy az EIR-ben tárolt adatok megfelelően védettek legyenek, és hogy az adatokhoz való hozzáférés szigorúan szabályozott legyen. A felhasználóknak biztosítaniuk kell, hogy az adatokhoz való hozzáférés csak a megfelelő jogosultságokkal rendelkező személyek számára lehetséges, és hogy az adatokat csak a megfelelő módon használják fel.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a biztonsági tulajdonságokat, amelyeket a személyzetnek hozzá kell rendelnie és fenn kell tartania.
2. A szervezetnek ki kell dolgoznia egy szabályzatot, amely meghatározza, hogyan kell a személyzetnek ezeket a tulajdonságokat hozzárendelni és fenntartani. Ez a szabályzat tartalmazhatja például a tulajdonságok hozzárendelésének folyamatát, a tulajdonságok felülvizsgálatának gyakoriságát stb.
3. A szervezetnek biztosítania kell, hogy a személyzet megértse és betartsa ezt a szabályzatot. Ez magában foglalhatja például a szabályzat ismertetését a személyzettel, a szabályzat betartásának ellenőrzését stb.
4. A szervezetnek rendszeresen naplót kell vezetnie a tulajdonságok hozzárendeléséről és fenntartásáról. Ez a napló segíthet az érintett szervezetnek nyomon követni, hogy a személyzet betartja-e a szabályzatot, és szükség esetén korrigáló intézkedéseket hozni.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a szabályzatot, hogy biztosítsa, hogy az továbbra is megfelel az EIR biztonsági követelményeinek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-16(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi tulajdonságok illetve az alanyok és objektumok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.96. Biztonsági tulajdonságok – Következetes tulajdonságértelmezés

2.96. A szervezet biztosítja az elosztott rendszerelemek között továbbított biztonsági tulajdonságok következetes értelmezését.

Magyarázat

Az elosztott rendszerek több rendszerelemre kiterjedő biztonsági szabályok érvényesítéséhez a szervezetek, a hozzáférési és információáramlási szabályok érvényesítésére vonatkozó döntésekben alkalmazott biztonsági tulajdonságok következetes értelmezését biztosítják. A szervezetek megállapodásokat és folyamatokat hozhatnak létre annak biztosítására, hogy az elosztott rendszerelemek az automatizált hozzáférési és áramlásérvényesítési műveletek során következetesen értelmezett tulajdonságokat alkalmazzanak.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell a biztonsági és adatvédelmi irányelvek következetes értelmezését a rendszerelemek között. Ez magában foglalja az hozzáférés-felügyeleti és az adatáramlás-ellenőrzési döntésekben alkalmazott biztonsági tulajdonságokat.
2. A szervezetnek megállapodásokat és folyamatokat kell létrehoznia, hogy biztosítsa a rendszerelemek következetes értelmezését az automatizált hozzáférés-felügyeleti és adatáramlás-ellenőrzési műveletekben.
3. A szervezetnek naplózásra van szüksége, hogy nyomon követhesse és ellenőrizhesse a biztonsági tulajdonságok következetes értelmezését. A naplózás segíthet azonosítani a potenciális biztonsági réseket és lehetővé teszi a gyors reagálást a biztonsági eseményekre.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági irányelveket, hogy biztosítsa azok relevanciáját és hatékonyságát a rendszerelemek között.
5. A szervezetnek képzést kell biztosítania a munkatársak számára a biztonsági tulajdonságok következetes értelmezéséről, hogy mindenki tisztában legyen a szerepével és felelősségével a biztonsági irányelvek betartásában.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-16(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.97. BIZTONSÁGI TULAJDONSÁGOK – TULAJDONSÁGTÁRSÍTÁSI TECHNIKÁK ÉS TECHNOLÓGIÁK

2.97. A szervezet meghatározott technikákat és technológiákat alkalmaz a biztonsági tulajdonságok információkkal való társítása során.

MAGYARÁZAT

A biztonsági tulajdonságok hozzárendelése a rendszereken belüli információkhoz fontos az automatizált hozzáférés-érvényesítés és az információtáramlás-ellenőrzési műveletek végrehajtásához. Az ilyen tulajdonságok információkhoz való hozzárendelése olyan technológiákkal és technikákkal valósítható meg, amelyek különböző szintű megbízhatóságot biztosítanak. A rendszerek például kriptográfiai úton, hardvereszközök által védett kriptográfiai kulcsokat támogató digitális aláírásokkal kapcsolhatják az adatokat az információkhoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a biztonsági tulajdonságokat, amelyeket az EIR-ben található információkhoz társítani kíván.
2. A szervezetnek automatizált hozzáférési végrehajtási és áramlási végrehajtási műveleteket kell alkalmaznia, amelyek a biztonsági jellemzőkkel társított információkra vonatkoznak.
3. A szervezetnek például kriptográfiai módszerekkel kell társítania a jellemzőket az információkhoz, digitális aláírásokat használva, amelyek támogatják a hardvereszközök által védett kriptográfiai kulcsokat.
4. A szervezetnek dokumentálnia kell a biztonsági jellemzők információkhoz történő társításának folyamatát, hogy nyomon követhető legyen a tevékenység és biztosítható legyen a rendszer sértetlensége.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-16(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a technikák és technológiák meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.98. BIZTONSÁGI TULAJDONSÁGOK – TULAJDONSÁGOK ÁTCSOPORTOSÍTÁSA - ÁTMINŐSÍTÉSI MECHANIZMUSOK

2.98. A szervezet csak meghatározott technikák vagy eljárások segítségével, hitelesített besorolás módosítási mechanizmusok alkalmazásával változtatja meg az információkhoz kapcsolódó biztonsági tulajdonságokat.

MAGYARÁZAT

A hitelesített besorolás egy olyan folyamat, amely által lehetőség nyílik az adatok átminősítésére és újracímkézésére egy meghatározott szabályzatnak megfelelően. A szervezetek hitelesített besorolási mechanizmusokat használnak az egyes jellemzők átminősítési műveleteihez szükséges megbízhatósági szintek biztosítására. Az érvényesítést megkönnyíti annak biztosítása, hogy az átminősítési mechanizmusok korlátozott funkciójúak legyenek. Mivel a biztonsági tulajdonságok változásai közvetlenül befolyásolhatják a szabályok érvényesítési műveleteit, megbízható átminősítési mechanizmusok bevezetése szükséges annak biztosításához, hogy ezek a mechanizmusok következetesen és helyesen működjenek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat a technikákat és eljárásokat, amelyeket a biztonsági tulajdonságok módosítására használni kíván.
2. A szervezetnek hitelesített besorolási módosítási mechanizmusokat kell alkalmaznia.
3. A szervezetnek gondoskodnia kell arról, hogy a besorolási módosítási mechanizmusok korlátozott funkciójúak legyenek. Ez azt jelenti, hogy ezek a mechanizmusok csak a biztonsági jellemzők módosítására használhatók, és nem végeznek más tevékenységeket.
4. A szervezetnek biztosítania kell, hogy az EIR-ben végrehajtott biztonsági tulajdonságok módosításai következetesek legyenek, ezzel támogatva a helyes működését.
5. A szervezetnek dokumentálnia kell a biztonsági tulajdonságok módosításáról. Ez segít a szervezetnek nyomon követni a módosításokat, és biztosítja, hogy a módosítások megfeleljenek a biztonsági követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-16(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a technikák vagy eljárások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.99. Biztonsági tulajdonságok – A tulajdonságok konfigurálása felhatalmazott személyek által

2.99. A szervezet lehetőséget biztosít a jogosult személyek számára, hogy megváltoztassák az alanyokhoz és objektumokhoz társítható biztonsági tulajdonságok típusát és értékét.

Magyarázat

Az biztonsági tulajdonságok tartalma vagy hozzárendelt értékei közvetlenül befolyásolhatják az egyének képességét az érintett szervezet információinak elérésére. Ezért fontos, hogy az EIR képes legyen korlátozni a jogosult személyek számára elérhető attribútumok típusának és értékének létrehozását vagy módosítását. Az érintett szervezetnek biztosítania kell a jogosult személyek számára a lehetőséget, hogy megváltoztassák az alanyokhoz és objektumokhoz társítható biztonsági tulajdonságok típusát és értékét. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie arra, hogy korlátozza az attribútumok létrehozásának és módosításának képességét csak a jogosult személyek számára.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, hogy mely személyek rendelkeznek jogosultsággal a biztonsági tulajdonságok típusának és értékének megváltoztatására az EIR-ben.
2. A szervezetnek implementálnia kell egy rendszert, amely lehetővé teszi a jogosult személyek számára, hogy megváltoztassák a biztonsági tulajdonságokat.
3. A szervezetnek biztosítania kell, hogy a jogosult személyek képesek legyenek megváltoztatni a biztonsági tulajdonságokat anélkül, hogy veszélyeztetnék az EIR biztonságát.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR-ben történő változtatásokat, hogy biztosítsa a biztonsági tulajdonságok megfelelő kezelését. Ez magában foglalhatja a naplók rendszeres áttekintését és a biztonsági események gyors kezelését.
5. A szervezetnek frissítenie kell a biztonsági eljárásait, hogy tükrözzék a jogosult személyek képességét a biztonsági tulajdonságok megváltoztatására. Ez magában foglalhatja a biztonsági szabályok és eljárások dokumentálását, a személyzet képzését és a változások kommunikálását az érintett szervezet egészében.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-16(10)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.100. TÁVOLI HOZZÁFÉRÉS

2.100. A szervezet:

2.100.1. Kidolgozza és dokumentálja az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan a használati korlátozásokat, a konfigurációs vagy csatlakozási követelményeket és az alkalmazási útmutatókat.

2.100.2. Engedélyezési eljárást folytat le a rendszerhez való távoli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően.

MAGYARÁZAT

A távoli hozzáférés olyan hozzáférés, amely az érintett szervezet EIR-jéhez kapcsolódik és amely külső hálózatokon, például az interneten keresztül kommunikál. A szervezet jellemzően titkosított virtuális magánhálózatokat (VPN-eket) használ a távoli kapcsolatok bizalmasságának és integritásának megőrzése érdekében. A titkosított VPN-ek használata elegendő biztosítékot nyújt az érintett szervezet számára arra, hogy hatékonyan kezelje ezeket a kapcsolatokat belső hálózatokként, ha a használt kriptográfiai mechanizmusokat a hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások szerint hajtják végre. A VPN kapcsolatok külső hálózatokon keresztül haladnak át, a titkosított VPN nem növeli a távoli kapcsolatok rendelkezésre állását. A titkosított VPN-ek befolyásolhatják a hálózati kommunikációs forgalom megfelelő monitorozásának képességét a rosszindulatú kódok szempontjából. A távoli hozzáférési szabályok alkalmazása más rendszerekre is vonatkozik, nem csak a nyilvános webkiszolgálókra vagy az olyan EIR-ekre, melyeket úgy terveztek, hogy nyilvánosan hozzáférhetők legyenek. Minden távoli hozzáférési típust engedélyeznie kell a szervezetnek, azt megelőzően, hogy a távoli hozzáférést lehetővé tenné a szervezet. A használati korlátozások mind biztonsági, mind funkcionális korlátozások lehetnek (pl. az átviteli sebességre való tekintettel a streaming szolgáltatások tiltása). A szervezet használhat információcserére, illetve rendszerkapcsolatokra vonatkozó megállapodásokat/szerződéseket, melyekben szabályozzák a távoli hozzáférést is. A említett megállapodásokkal/szerződésekkel kapcsolatos elvárások az "Információcsere" kontrollnál kerültek bővebben kifejtésre. A távoli hozzáférésre vonatkozó korlátozások érvényesítése a "Hozzáférés-ellenőrzés érvényesítése" kontrollnál kerültek bővebben kifejtésre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia és dokumentálnia kell az engedélyezett távoli hozzáférés minden egyes típusára vonatkozó használati korlátozásokat, a konfigurációs vagy csatlakozási követelményeket és az alkalmazási útmutatókat.
2. A szervezetnek titkosított magánhálózatokat (VPN-eket) kell használnia a távoli kapcsolatok bizalmasságának és integritásának megőrzése érdekében.
3. Minden távoli hozzáférési típust engedélyeznie kell a szervezetnek, azt megelőzően, hogy a távoli hozzáférést lehetővé tenné a szervezet.
4. A szervezetnek érvényesítenie kell a távoli hozzáférésre vonatkozó hozzáférési korlátozásokat a biztonsági és a rendelkezésre állási szempontok figyelembevételével.
5. A szervezetnek dokumentálnia kell, hogy mely felhasználók részére került engedélyezésre a távoli hozzáférés.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

2.115. Külső elektronikus információs rendszerek használata

5.6. Információcsere

6.47. A szoftverhasználat korlátozásai

8.2. Azonosítás és hitelesítés

8.10. Eszközök azonosítása és hitelesítése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.13. Távoli hozzáférés

ISO/IEC 27001:2023 REFERENCIA

A.5.14; A.6.7

NIST SP 800-53 REV.5 REFERENCIA

AC-17

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

2.101. TÁVOLI HOZZÁFÉRÉS – FELÜGYELET ÉS IRÁNYÍTÁS

2.101. A szervezet automatizált mechanizmusokat alkalmaz a távoli hozzáférési módok felügyeletére és ellenőrzésére.

MAGYARÁZAT

A távoli hozzáférési módok felügyelete és ellenőrzése lehetővé teszi az érintett szervezet számára a támadások észlelését és segít a távoli hozzáférési eljárások betartásának biztosításában azzal, hogy naplózza a távoli felhasználók kapcsolódási tevékenységeit a különböző rendszerelemeken, beleértve a szervereket, hordozató számítógépeket, munkaállomásokat, okostelefonokat és táblagépeket. Az automatizált mechanizmusok alkalmazása a távoli hozzáférési módok felügyeletére és ellenőrzésére azt jelenti, hogy az érintett szervezet olyan rendszereket használ, amelyek automatikusan nyomon követik és ellenőrzik a távoli hozzáféréseket. Ez magában foglalhatja a hozzáférési kísérletek naplózását, a sikertelen hozzáférési kísérletek észlelését és riasztások küldését, valamint a távoli hozzáférési jogosultságok automatikus korlátozását vagy visszavonását bizonyos feltételek esetén. Az automatizált mechanizmusok használata segíthet a szervezetnek abban, hogy gyorsan reagáljon a potenciális biztonsági fenyegetésekre, minimalizálja a károkat, és megelőzze a jövőbeni biztonsági eseményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie automatizált mechanizmusokat, amelyek képesek nyomon követni és ellenőrizni a távoli hozzáférési módokat.
2. A szervezetnek naplóznia kell a távoli hozzáféréssel kapcsolatos tevékenységeket. Ez segít nyomon követni a felhasználói tevékenységeket, és lehetővé teszi az érintett szervezet számára, hogy azonosítsa a potenciális biztonsági problémákat.
3. A szervezetnek biztosítania kell, hogy a távoli hozzáférés naplózása megfelel a szervezeti elvárásoknak.
4. A szervezetnek meg kell határoznia a naplózási eseményeket. Ez magában foglalja a távoli hozzáférési események, mint például a bejelentkezések, a rendszerhez való hozzáférés és a rendszerből való kilépés naplózását.

5. A szervezetnek rendszeresen ellenőriznie kell a naplókat, hogy időben észlelje a támadásokat és biztosítsa a távoli hozzáférési eljárások betartását. Ez magában foglalhatja a naplók automatizált elemzését és értékelését, valamint a szokatlan vagy gyanús tevékenységek azonnali jelentését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.40. Naplóbejegyzések létrehozása

4.48. Munkaszakasz-ellenőrzés

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.13. Távoli hozzáférés

ISO/IEC 27001:2023 REFERENCIA

A.8.16

NIST SP 800-53 REV.5 REFERENCIA

AC-17(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.102. TÁVOLI HOZZÁFÉRÉS – BIZALMASSÁG ÉS SÉRTETLENSÉG VÉDELME TITKOSÍTÁS ÁLTAL

2.102. A szervezet kriptográfiai mechanizmusokat alkalmaz a távoli hozzáférés biztonságának és sértetlenségének biztosítása érdekében.

MAGYARÁZAT

A szervezet virtuális magánhálózatokat (VPN) használhat a távoli hozzáférési munkaszakaszok bizalmasságának és sértetlenségének biztosítására. A Transport Layer Security (TLS) például egy kriptográfiai protokoll, amely végponttól végpontig biztosítja a kommunikáció biztonságát a hálózatokon, emellett interneten történő kommunikációhoz és online tranzakciók végrehajtásához is használják.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a távoli hozzáféréssel kapcsolatos titkosítás követelményeit.
2. A szervezetnek biztosítania kell a távoli hozzáférés munkaszakaszainak bizalmasságát és sértetlenségét. Ezt megteheti virtuális magánhálózatok (VPN) alkalmazásával, mellyel kapcsolatban meg kell határoznia, hogy milyen kriptográfiai mechanizmust fog alkalmazni.
3. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a kriptográfiai mechanizmusokat, hogy biztosítsa azok működőképességét és hatékonyságát pl.: ha bebizonyosodik, hogy a szervezet által alkalmazott kriptográfiai mechanizmus jogosulatlan személyek által visszafejthető, akkor a szervezetnek egy új, nem visszafejthető kriptográfiai mechanizmust kell alkalmaznia a korábbi helyett.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.40. Az adatátvitel bizalmassága és sértetlensége

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.13. Távoli hozzáférés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-17(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.103. TÁVOLI HOZZÁFÉRÉS – MENEDZSELT HOZZÁFÉRÉS-FELÜGYELETI PONTOK

2.103. A szervezet a távoli hozzáféréseket engedélyezett és menedzselt hálózati hozzáférés-felügyeleti pontokon keresztül irányítja.

MAGYARÁZAT

Az érintett szervezetnek olyan hálózati hozzáférés-felügyeleti pontokat kell létrehoznia és kezelnie, amelyek lehetővé teszik az engedélyezett és menedzselt távoli hozzáférést az EIR-hez. Ezek a pontok lehetővé teszik a szervezet számára, hogy ellenőrizze és menedzselje a távoli hozzáférést, és biztosítsa, hogy csak az arra jogosult felhasználók férhessenek hozzá az EIR-hez és a hozzáférés csak engedélyezett csatornán keresztül valósulhasson meg.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a hálózati hozzáférés-felügyeleti pontokat, amelyeken keresztül a távoli hozzáférések engedélyezhetők, illetve menedzselhetők.
2. A szervezetnek alkalmaznia kell a gyakorlatban egy hozzáférés-felügyeleti eljárást, amely meghatározza, hogy mely felhasználók, milyen körülmények között és milyen eszközökkel férhetnek hozzá az EIR-hez távolról.
3. A szervezetnek biztosítania kell, hogy a hozzáférés-felügyeleti pontok megfelelően védettek legyenek az esetleges támadásokkal szemben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.17. A határok védelme

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.13. Távoli hozzáférés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-17(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.104. TÁVOLI HOZZÁFÉRÉS – PRIVILEGIZÁLT PARANCSOK ÉS HOZZÁFÉRÉS

2.104. A szervezet:

2.104.1. Csak olyan módon engedélyezi a távoli hozzáférést, amely értékelhető bizonyítékot szolgáltat a privilegizált jogosultságot igénylő műveletek végrehajtásához és a biztonságkritikus információk eléréséhez a meghatározott követelményeknek megfelelően, és

2.104.2. a távoli hozzáférés indokoltságát a rendszerbiztonsági tervben dokumentálja.

MAGYARÁZAT

Az EIR-hez történő távoli hozzáférési lehetőség jelentős potenciális sérülékenységet jelenthet, melyet kihasználhatnak a támadók. A távoli hozzáférésen keresztül történő privilegizált parancsok végrehajtásának, valamint a biztonságkritikus információkhoz történő hozzáférés korlátozása és annak monitorozása csökkenti a szervezet kitettségét a távoli hozzáféréshez kapcsolódó fenyegetésekkel szemben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely műveletek igényelnek privilegizált jogosultságot, és mely információk minősülnek biztonsági szempontból kritikusnak az EIR-en belül.
2. A szervezetnek implementálnia kell egy olyan távoli hozzáférési megoldást, amely képes értékelhető bizonyítékot szolgáltatni a privilegizált műveletek végrehajtásáról és a biztonságkritikus információk eléréséről. Ez magában foglalhatja a naplózást, hogy nyomon követhető legyen, ki, mikor és milyen műveleteket hajtott végre.
3. A szervezetnek biztosítania kell, hogy a távoli hozzáférés csak a meghatározott követelményeknek megfelelően lehetséges. Ez magában foglalhatja a kétlépcsős azonosítást, a biztonsági protokollok használatát, és a hozzáférés korlátozását pl.: csak bizonyos IP-címekről vagy eszközökről lehet bejelentkezni.
4. A szervezetnek dokumentálnia kell a távoli hozzáférés indokoltságát a rendszerbiztonsági tervben.

Kapcsolódó intézkedések

2.60. Legkisebb jogosultság elve

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.13. Távoli hozzáférés

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-17(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

2.105. TÁVOLI HOZZÁFÉRÉS – HOZZÁFÉRÉSI MECHANIZMUSRA VONATKOZÓ INFORMÁCIÓK VÉDELME

2.105. Az EIR védi a távoli hozzáférési mechanizmusokra vonatkozó információkat a jogosulatlan felhasználástól és nyilvánosságra hozataltól.

MAGYARÁZAT

A nem szervezethez köthető entitások általi távoli hozzáférés szervezethez köthető információkhoz növeli a jogosulatlan felhasználás és közzététel kockázatát. A szervezet mérlegelheti a távoli hozzáférésre vonatkozó követelmények meghatározását más szervezetekkel kötött információcserével kapcsolatos egyezmény megkötése során. A távoli hozzáférésre vonatkozó követelmények relevánsak lehetnek a "Viselkedési szabályok" és a "Hozzáférési megállapodások" kontrollok vonatkozásában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR megfelelően védi a távoli hozzáférési mechanizmusokra vonatkozó információkat a jogosulatlan felhasználástól és nyilvánosságra hozataltól. Ez magában foglalhatja a hozzáférési jogosultságok szigorú kezelését, a naplók rendszeres felülvizsgálatát, a hozzáférési mechanizmusok biztonsági beállításainak ellenőrzését, illetve az esetleges jelszavak biztonságos tárolását.
2. A szervezetnek be kell építeni a távoli hozzáférési követelményeket az információcserére vonatkozó megállapodásaiba más szervezetekkel, amennyiben ez megoldható.
3. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a távoli hozzáférési mechanizmusokat, hogy biztosítsa azok biztonságát és hatékonyságát.
4. A szervezetnek biztosítania kell, hogy a távoli hozzáférési mechanizmusokat csak a szükséges időtartamra és a szükséges mértékben használják, és hogy a hozzáférési naplókat rendszeresen felülvizsgálják a jogosulatlan hozzáférés jeleinek keresése érdekében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.2. Biztonságtudatossági képzés

3.9. Szerepkör alapú biztonsági képzés

14.9. Hozzáférési megállapodások

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-17(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.106. TÁVOLI HOZZÁFÉRÉS – HOZZÁFÉRÉS MEGSZAKÍTÁSA VAGY LETILTÁSA

2.106. A szervezet biztosítja a rendszerhez való távoli hozzáférés meghatározott időn belüli szétkapcsolásának vagy letiltásának a lehetőségét.

MAGYARÁZAT

A rendszer szétkapcsolásának vagy tiltásának lehetőségét biztosítani kell - a szervezeti célok, ill. az üzleti funkciók kritikusságának figyelembevételével. Ez a követelmény különösen fontos a kiberbiztonsági események esetén, amikor a távoli hozzáférés azonnali letiltása elengedhetetlen a további károk megelőzése érdekében. Az érintett szervezetnek rendelkeznie kell olyan protokollokkal és eszközökkel, amelyek lehetővé teszik számára, hogy gyorsan és hatékonyan reagáljon ilyen helyzetekre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az EIR-hez való távoli hozzáférés kritikusságát és a felhasználás üzleti funkcióit. Ez alapján döntik el, hogy milyen gyorsan kell szétkapcsolni vagy letiltani a távoli hozzáférést.
2. A szervezetnek implementálnia kell egy olyan rendszert, amely képes az EIR-hez való távoli hozzáférés szétkapcsolására vagy letiltására a meghatározott időn belül. Ez magában foglalhatja a hozzáférési jogosultságok ideiglenes felfüggesztését vagy a hozzáférési pontok letiltását.
3. A szervezetnek biztosítania kell, hogy a rendszer képes legyen az azonnali vagy a jövőbeli távoli hozzáférés megszüntetésére, ha szükséges. Ez azt jelenti, hogy a rendszernek képesnek kell lennie azonnali reagálásra, ha a távoli hozzáférés veszélyezteti az EIR biztonságát.
4. A szervezetnek naplóznia kell a távoli hozzáférést, hogy nyomon követhető legyen, ki, mikor és milyen célból fér hozzá az EIR-hez. Ez segít azonosítani a potenciális biztonsági réseket és megelőzni a jövőbeli biztonsági eseményeket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-17(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.107. TÁVOLI HOZZÁFÉRÉS – TÁVOLI PARANCSOK HITELESÍTÉSE

2.107. A szervezet meghatározott mechanizmusokat vezet be a meghatározott parancsok hitelesítésére.

MAGYARÁZAT

A távoli parancsok hitelesítésének megkövetelése védelmet nyújt a nem engedélyezett parancsok és az engedélyezett parancsok visszajátszása ellen. A távoli parancsok hitelesítésének képessége olyan távoli rendszerek esetében fontos, amelyek elvesztése, meghibásodása, eltérítése vagy kihasználása azonnali vagy súlyos következményekkel járna. A távoli parancsok hitelesítési mechanizmusai biztosítják, hogy a rendszerek elfogadják és a tervezett sorrendben hajtsák végre a parancsokat, csak az engedélyezett parancsokat hajtsák végre, és elutasítsák a nem engedélyezett parancsokat. A távoli parancsok hitelesítésére például kriptográfiai mechanizmusok használhatók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezetnek először meg kell határoznia, mely parancsokat kell hitelesíteni. Ez magában foglalhatja a távoli parancsokat, amelyeknél a visszaélés, hibás működés, rossz irányítás vagy kihasználás komoly következményekkel járhat.
2. Az érintett szervezetnek be kell vezetnie a hitelesítési mechanizmusokat a meghatározott parancsok számára. Ezek a mechanizmusok biztosítják, hogy az EIR elfogadja és a megfelelő sorrendben hajtsa végre a parancsokat, valamint csak a hitelesített parancsokat hajtsa végre, és elutasítsa a nem hitelesített parancsokat.
3. Az érintett szervezetnek meg kell határoznia, milyen hitelesítési mechanizmusokat használ. A kriptográfiai mechanizmusok például használhatók a távoli parancsok hitelesítésére.
4. Az érintett szervezetnek implementálnia kell a kiválasztott hitelesítési mechanizmusokat az EIR-ben. Ez magában foglalhatja a szükséges hardver és szoftver beszerzését, telepítését és konfigurálását.

5. Az érintett szervezetnek naplóznia kell a hitelesített parancsokat, hogy nyomon követhető legyen, ki, mikor és milyen célból fér hozzá az EIR-hez. Ez segít azonosítani a potenciális biztonsági réseket és megelőzni a jövőbeli biztonsági eseményeket.

Kapcsolódó intézkedések

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

17.73. Munkaszakasz hitelessége

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-17(10)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a mechanizmusok illetve a távoli parancsok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

2.108. VEZETÉK NÉLKÜLI HOZZÁFÉRÉS

2.108. A szervezet:

2.108.1. A vezeték nélküli hozzáférés minden egyes típusára vonatkozóan konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatást alakít ki.

2.108.2. Engedélyezési eljárást folytat le a rendszerhez való vezeték nélküli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően

MAGYARÁZAT

A vezeték nélküli technológiák közé sorolható a mikrohullám, a nagyon magas- vagy ultra magas rádiós frekvencia, a 802.11x és a Bluetooth. A vezeték nélküli hálózatok hitelesítési protokollokat használnak, amelyek biztosítják a hitelesítő védelmét és a kölcsönös hitelesítést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót kell kidolgoznia minden egyes vezeték nélküli hozzáférési típusra. Ez magában foglalja a mikrohullámú, a nagyon magas- vagy ultra magas frekvenciájú rádió frekvenciákat, a 802.11x-et és a Bluetooth-t is.

2. A szervezetnek engedélyezési eljárást kell lefolytatnia az EIR-hez való vezeték nélküli hozzáférés minden egyes típusára, mielőtt lehetővé tenné ezeket a kapcsolatokat. Ez azt jelenti, hogy az érintett szervezetnek ellenőriznie kell, hogy a vezeték nélküli hozzáférést biztosító technológiák megfelelnek-e a biztonsági követelményeknek, és hogy azokat megfelelően konfigurálták-e.

3. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az általa alkalmazott vezeték nélküli hozzáférési technológiákat, hogy biztosítsa azok naprakészségét és hatékonyságát.

4. A szervezetnek biztosítania kell, hogy a vezeték nélküli hozzáféréshez kapcsolódó biztonsági elvárásokat minden releváns személy megismerje és azokat be is tartsa. Releváns személyek lehetnek a szervezet munkavállalói, alvállalkozói, illetve beszállítói is.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.100. Távoli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

5.24. Belső rendszerkapcsolatok

6.26. Legszűkebb funkcionalitás

8.2. Azonosítás és hitelesítés

8.10. Eszközök azonosítása és hitelesítése

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

13.3.1. Viselkedési szabályok

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.14. Vezeték nélküli hozzáférés

ISO/IEC 27001:2023 referencia

A.5.14; A.8.20

NIST SP 800-53 rev.5 referencia

AC-18

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

2.109. Vezeték nélküli hozzáférés – Hitelesítés és titkosítás

2.109. A szervezet az EIR-ben titkosítással és a felhasználók vagy az eszközök hitelesítésével védi a vezeték nélküli hozzáférést.

Magyarázat

A vezeték nélküli hálózati képességek jelentős sérülékenységet jelenthetnek a szervezet számára, amelyet a támadók kihasználhatnak, hiszen egy esetleges támadás végrehajtásához nem kell fizikálisan kapcsolódniuk az érintett szervezet hálózatához. A felhasználók és az eszközök erős hitelesítése, valamint az erős titkosítás csökkentheti a vezeték nélküli technológiákat felhasználó fenyegetésekkel szembeni sebezhetőséget.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az EIR-hez köthető vezeték nélküli hozzáférési pontokat. Ez magában foglaljhatja a vezeték nélküli hozzáférést biztosító routereket, hálózati adaptereket és más vezeték nélküli eszközöket.
2. A szervezetnek be kell vezetnie egy erős hitelesítési rendszert a felhasználók és az eszközök számára. Ez magában foglalhatja a többtényezős hitelesítést, amely a felhasználói név és jelszó kombinációján túl további hitelesítési lépéseket igényel. Emellett a felhasználóktól egy több szekvenciás, megfelelő hosszúságú jelszót is megkövetelhet a szervezet.
3. A szervezetnek be kell vezetnie a vezeték nélküli hozzáférés titkosítását az EIR-ben. Ez magában foglalhatja a WPA2 vagy WPA3 használatát, amelyek jelenleg a legbiztonságosabb vezeték nélküli titkosítási protokollok - megfelelő komplexitású és hosszúságú jelszavak használata mellett. Mindemellett érdemes tiltani a WPS funkciót, mert az szintén megkönnyíti az esetleges támadásokat.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR vezeték nélküli hozzáférési pontjait, hogy biztosítsa a hitelesítési és titkosítási protokollok megfelelő működését.
5. A szervezetnek periodikusan cserélni kell a hitelesítéshez szükséges információkat pl.: jelszavak periodikus cseréje.

6. A szervezetnek javasolt úgy konfigurálnia a vezeték nélküli hálózatait, hogy annak neve ne fedjen fel információt a szervezetről, adott esetben az SSID elrejtése is növelheti a biztonságot.
7. A szervezetnek naplóznia kell a vezeték nélküli hálózati hozzáférési kísérleteket. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a hozzáférési kísérleteket, és azonosítsa a potenciális biztonsági fenyegetéseket.

Kapcsolódó intézkedések

17.40. Az adatátvitel bizalmassága és sértetlensége
17.49. Kriptográfiai kulcs előállítása és kezelése
17.53. Kriptográfiai védelem

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.14. Vezeték nélküli hozzáférés

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-18(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

2.110. VEZETÉK NÉLKÜLI HOZZÁFÉRÉS – VEZETÉK NÉLKÜLI HÁLÓZAT LETILTÁSA

2.110. A szervezet a rendszerelemekbe ágyazott vezeték nélküli hálózati hozzáférést letiltja amennyiben annak használata nem szükséges.

MAGYARÁZAT

A rendszerelemekbe ágyazott vezeték nélküli hálózati képességek jelentős potenciális sérülékenységet jelenthetnek, melyet a potenciális támadók kihasználhatnak, ugyanis egy esetleges támadás végrehajtásához nem kell fizikálisan kapcsolódniuk az érintett szervezet hálózatához. A rendszerelemekbe ágyazott vezeték nélküli hálózatok kompromittálásával a támadók hozzáférhetnek a szervezet EIR-jeihez. A vezeték nélküli hálózatot biztosító eszközök kikapcsolása - ha a szervezeti célokhoz vagy funkciókhoz nincs szükség rájuk - csökkentheti a támadókkal szembeni kitettséget.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először fel kell mérnie az EIR komponenseit, hogy megállapítsa, melyek rendelkeznek beépített vezeték nélküli hálózati képességekkel.
2. A szervezetnek meg kell határoznia, hogy mely vezeték nélküli hálózati hozzáférések szükségesek a szervezeti vagy üzleti tevékenységek ellátása szempontjából.
3. A szervezetnek le kell tiltania azokat a vezeték nélküli hálózati hozzáféréseket, amelyek nem szükségesek.
4. A szervezetnek rendszeres méréseket kell végeznie, hogy detektálja a tévesen működő vezeték nélküli hálózatokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-18(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.111. Vezeték nélküli hozzáférés – Felhasználók általi konfiguráció korlátozása

2.111. A szervezet azonosítja és külön engedélyezési eljáráson keresztül jogosítja fel azokat a felhasználókat, akik jogosultak a vezeték nélküli hálózati funkciók önálló konfigurálására.

Magyarázat

A szervezet azonosítja és külön engedélyezési eljáráson keresztül jogosítja fel azokat a felhasználókat, akik jogosultak a vezeték nélküli hálózati funkciók önálló konfigurálására. Ez a folyamat magában foglalja a felhasználói a hozzáférési jogosultságok és korlátozások beállítását, melyet külön engedélyezési eljárás keretében folytat le a szervezet. A szervezet kikényszeríti, hogy egy felhasználó csak akkor legyen képes önállóan módosítani a vezeték nélküli hálózati hozzáférés konfigurációját, ha a szervezet által alkalmazott hozzáférés-felügyeleti mechanizmusok jóváhagyták a hozzáférést.

A követelmény alkalmazásának lépései

1. A szervezetnek ki kell választania és külön engedélyezési eljáráson keresztül fel kell jogosítania azokat a felhasználókat, akik jogosultak a vezeték nélküli hálózati funkciók önálló konfigurálására.
2. A szervezetnek létre kell hoznia egy engedélyezési eljárást, amelyen keresztül a kiválasztott felhasználók jogosultságot kapnak a vezeték nélküli hálózati funkciók konfigurálására. A privilegizált jogosultságot független harmadik félnek kell jóváhagynia.
3. A szervezetnek implementálnia kell az engedélyezési eljárást. Ez magában foglalhatja a felhasználói jogosultságok kezelését, a felhasználói jogosultságok ellenőrzését és a felhasználói jogosultságok naplózását.
4. A szervezetnek naplóznia kell a vezeték nélküli hálózati funkciókban, a felhasználók által elvégzett konfigurálásokat. hozzáférési kísérleteket. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a a vezeték nélküli hálózatok funkcióiban elvégzett konfigurálásokat, és azonosítsa a potenciális biztonsági fenyegetéseket.
5. A szervezetnek meghatározott időközönként felül kell vizsgálnia a kiosztott jogosultságokat és szükség esetén meg kell szüntetnie a munkavégzéshez nem szükséges, illetve esetlegesen

összeférhetetlen jogosultságokat. Emellett a változó és jóváhagyott felelősségek alapján szükség esetén módosítania kell a kiosztott jogosultságokat.

Kapcsolódó intézkedések

17.17. A határok védelme

17.54. Együttműködésen alapuló informatikai eszközök

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.14. Vezeték nélküli hozzáférés

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-18(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

2.112. Vezeték nélküli hozzáférés – Antennák és átviteli teljesítmény

2.112. A szervezet olyan rádióantennákat választ ki és az átviteli teljesítményszinteket oly módon kalibrálja, hogy minimalizálja annak valószínűségét, hogy a vezeték nélküli hozzáférési pontok jelei a szervezet által ellenőrzött határokon túl is foghatók legyenek.

Magyarázat

Az érintett szervezetnek gondoskodnia kell arról, hogy a vezeték nélküli hozzáférési pontok jelei ne legyenek foghatók az általa ellenőrzött határokon túl. Ennek érdekében az érintett szervezet kiválasztja a megfelelő rádióantennákat és kalibrálja az átviteli teljesítményszinteket. A szervezet biztonsági intézkedésként használhat irányított (directional)- és sugárformázó (beamforming) antennákat is. Javasolt a szervezet fizikai határain méréseket végezni, melyek eredményeképpen a szervezet képes finomhangolni a már meglévő berendezéseit, hogy a jeleket a határon túl ne lehessen fogni.

A követelmény alkalmazásának lépései

1. A vezeték nélküli hálózatok telepítésénél a szervezetnek figyelembe kell vennie, hogy a kiválasztott antennák jelei milyen hatótávolságon belül foghatók, és minimalizálnia kell annak esélyét, hogy a jelek az érintett szervezet által felügyelt területeken kívül is foghatók legyenek.
2. A meglévő berendezéseket a szervezetnek úgy kell kalibrálnia, hogy a fenti követelménynek megfeleljen.
3. Az érintett szervezetnek méréseket kell végezni az általa felügyelt terület határain, hogy a követelménynek való megfelelést biztosítsa.

Kapcsolódó intézkedések

12.45. Információszivárgás

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.14. Vezeték nélküli hozzáférés

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-18(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

2.113. MOBIL ESZKÖZÖK HOZZÁFÉRÉS-ELLENŐRZÉSE

2.113. A szervezet:

2.113.1. Kialakítja a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót az általa ellenőrzött mobil eszközök számára, beleértve azokat az eseteket is, amikor ezek az eszközök a szervezet által ellenőrzött területen kívül helyezkednek el.

2.113.2. Engedélykötelessé teszi a szervezet rendszereihez mobil eszközökkel történő kapcsolódást.

MAGYARÁZAT

Az érintett szervezet a mobil eszközök számára kialakítja a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót. Az érintett szervezetnek akkor is gondoskodni kell a mobil eszközök biztonságáról, amikor azok a felhasználók kezelésében, az érintett szervezet által felügyelt helyen kívül vannak. Az érintett szervezetnek ezért megfelelően kell konfigurálnia az eszközöket és szabályzati oldalról intézkedéseket kell foganatosítania, hogy a felhasználók felügyelete alatt is megfelelő biztonságban legyenek az eszközök és a rajtuk tárolt adatok.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell alakítania a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót a mobil eszközök számára, különös tekintettel azokra az esetekre, amikor a mobil eszközök az érintett szervezet által ellenőrzött területen kívül helyezkednek el.

2. A szervezetnek engedélykötelessé kell tennie a mobil eszközökkel történő kapcsolódást az EIR-hez. Ez azt jelenti, hogy a mobil eszközök csak akkor csatlakozhatnak az EIR-hez, ha ezt engedélyezték. Célszerű a kiemelt kockázat miatt az ilyen intézkedési engedélyezéseket az üzemeltetéstől független félnek, például a szervezet elektronikus információs rendszer biztonságáért felelős személyének jóváhagynia.

3. A szervezetnek felügyelnie kell a mobil eszközökkel történő csatlakozásokat, továbbá a mobil eszközökön kikényszerített biztonsági beállítások megfelelő és folyamatos működését pl.: MDM (Mobile Device Management) rendszer használata.

4. A szervezetnek rendszeresen felül kell vizsgálnia a kiadott engedélyeket, és a már nem szükséges engedélyeket vissza kell vonnia.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.71. Sikertelen bejelentkezési kísérletek

2.82. Eszköz zárolása

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

2.115. Külső elektronikus információs rendszerek használata

5.24. Belső rendszerkapcsolatok

6.2. Alapkonfiguráció

6.23. Konfigurációs beállítások

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.15. Mobil eszközök hozzáférés ellenőrzése

ISO/IEC 27001:2023 referencia

A.5.14; A.7.9; A.8.1

NIST SP 800-53 rev.5 referencia

AC-19

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

2.114. Mobil eszközök hozzáférés-ellenőrzése – Teljes eszköz vagy konténer-alapú titkosítás

2.114. A szervezet teljes eszköztitkosítást vagy tárolóalapú titkosítást alkalmaz a meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének védelme érdekében.

Magyarázat

Az érintett szervezet teljes ezköztitkosítást vagy tárolóalapú titkosítást alkalmaz a mobil eszközökön tárolt adatok és információk védelme érdekében. Ez magában foglalja kiválasztott adatszerkezetek, például fájlok, rekordok vagy mezők titkosítását, ezzel biztosítva az adatok bizalmasságát és sértetlenségét. A teljes eszköztitkosítás az egész eszközt titkosítja, beleértve az operációs rendszert és az összes felhasználói adatot. Ez a megközelítés különösen hasznos lehet, ha az eszköz elveszik vagy ellopják, mivel a titkosítás megakadályozza az adatokhoz való jogosulatlan hozzáférést. Ezzel szemben a konténer vagy tároló alapú titkosítás egy környezetet hoz létre az eszközön, ahol a szervezet által felügyelt környezetben vannak az információk, és az a környezet kerül titkosításra. A felhasználó környezete és a védett környezet közötti másolás és átjárhatóság tiltva kell legyen. Az érintett szervezetnek gondosan meg kell fontolnia, hogy melyik titkosítási módszert alkalmazza, figyelembe véve az EIR biztonsági követelményeit és a mobil eszközök használatának kockázatait. A döntés során figyelembe kell venni a titkosítás hatását az EIR teljesítményére és használhatóságára is.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia, mely mobil eszközöket használják az EIR-ben tárolt információkhoz való hozzáféréshez.
2. A szervezetnek ki kell dolgoznia egy előírást a teljes eszköztitkosításra vagy a tárolóalapú titkosításra vonatkozóan, és döntenie kell, hogy melyik megoldást implementálja. A titkosítási módszer kiválasztásánál a szervezetnek az esetleges, erre vonatkozó jogszabályi előírásokat is figyelembe kell vennie.
3. A szervezetnek implementálnia kell a kiválasztott titkosítási módszert. Ez magában foglalhatja a szoftver telepítését, a titkosítási kulcsok kezelését és a titkosítási protokollok beállítását pl.: MDM (Mobile Device Management) rendszer használata.

4. A szervezetnek biztosítania kell, hogy a titkosítás megfelelően működjön, és hogy a titkosított adatok csak az arra jogosult személyek számára legyenek hozzáférhetők.
5. A szervezetnek naplózni kell a titkosítási tevékenységeket, beleértve a titkosítási kulcsok használatát és a titkosított adatokhoz való hozzáférést, továbbá menedzselnie kell a titkosítási hozzáférést.
6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a titkosítási eljárásrendjét és gyakorlatát, hogy biztosítsa azok hatékonyságát és megfelelőségét.
7. A szervezetnek képzést kell biztosítania a munkatársak számára a titkosítási eljárásokról és gyakorlatról, valamint arról, hogyan kell biztonságosan használni a titkosított mobil eszközöket.

Kapcsolódó intézkedések

17.49. Kriptográfiai kulcs előállítása és kezelése
17.53. Kriptográfiai védelem
17.81. Tárolt (at rest) adatok védelme

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.15. Mobil eszközök hozzáférés ellenőrzése

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-19(5)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a mobileszközök meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

2.115. KÜLSŐ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK HASZNÁLATA

2.115. A szervezet:

2.115.1. Meghatározza a felhasználási feltételeket, és megállapítja, hogy az elvárt követelmények megvalósultak-e a külső rendszerekben, összhangban a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel létrehozott bizalmi kapcsolatokkal, amelyek lehetővé teszik az arra jogosult személyek számára, hogy:

2.115.1.1. - hozzáférjenek a rendszerhez külső rendszerekből; és

2.115.1.2. - feldolgozzák, tárolják vagy továbbítsák a szervezet által ellenőrzött információkat külső rendszerek használatával; vagy

2.115.2. megtiltja a meghatározott típusú külső rendszerek használatát.

MAGYARÁZAT

Az érintett szervezet meghatározza a követelmény szerinti felhasználási feltételeket, és megállapítja, hogy az elvárt követelmények megvalósultak-e a külső rendszerekben. A szervezet érvényesíti az elvárásait a külső rendszerrel történő információfeldolgozás és -továbbítás kapcsán, továbbá a szervezet által meghatározott típusú külső rendszerek használatát logikai és adminisztratív úton megtiltja.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a felhasználási feltételeket a külső rendszerekkel kapcsolatban. Ez magában foglalja a specifikus alkalmazásokat, amelyekhez hozzáférhetnek külső rendszerekhez, és a legmagasabb biztonsági kategóriájú információt, amelyet feldolgozhatnak, tárolhatnak vagy továbbíthatnak a külső rendszereken.

2. A szervezetnek bizalmi kapcsolatokat kell létrehoznia a külső rendszereket birtokló, üzemeltető vagy karbantartó szervezetekkel. Ezek a kapcsolatok lehetővé teszik, hogy az arra jogosult személyek hozzáférjenek az EIR-hez külső rendszerekből, és feldolgozzák, tárolják vagy továbbítsák az érintett szervezet által ellenőrzött információkat külső rendszerek használatával.

3. A szervezetnek döntenie kell arról, hogy megtiltja-e a meghatározott típusú külsőrendszerek használatát. Például megtilthatja bármely külső rendszer használatát, amelyet nem a szervezet birtokol, vagy megtilthatja a személyes tulajdonban lévő EIR-ek használatát.
4. Ha a felhasználási feltételeket nem lehet meghatározni a külső rendszerek tulajdonosaival, a szervezet korlátozásokat vezethet be azokkal a személyekkel szemben, akik ezeket a külső rendszereket használják.

Kapcsolódó intézkedések

2.2. Fiókkezelés
2.15. Hozzáférés-ellenőrzés érvényesítése
2.100. Távoli hozzáférés
2.113. Mobil eszközök hozzáférés-ellenőrzése
5.6. Információcsere
13.2. Rendszerbiztonsági terv
13.3.1. Viselkedési szabályok
16.49. Külső elektronikus információs rendszerek szolgáltatásai
17.17. A határok védelme

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.16. Külső elektronikus információs rendszerek használata

ISO/IEC 27001:2023 referencia

A.5.14; A.7.9; A.8.20

NIST SP 800-53 rev.5 referencia

AC-20

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

2.116. KÜLSŐ RENDSZEREK HASZNÁLATA – ENGEDÉLYEZETT HASZNÁLAT KORLÁTOZÁSAI

2.116. A szervezet csak akkor engedélyezi a jogosult személyek számára a külső rendszer használatát, a rendszerhez való hozzáférést, illetve a szervezet által ellenőrzött információk feldolgozását, tárolását vagy továbbítását, ha:

2.116.1. ellenőrzésre került a külső rendszeren alkalmazott védelmi intézkedések végrehajtása, amelyeket a szervezet biztonsági szabályzatai és tervei határoznak meg; vagy

2.116.2. betartja és betartatja a jóváhagyott rendszerkapcsolati vagy feldolgozási megállapodásokat a külső rendszert üzemeltető szervezettel.

MAGYARÁZAT

A külső rendszer biztonsági szintjének és beállításainak ellenőrzése kiemelten fontos a használat engedélyezése előtt. Az érintett szervezetnek meg kell vizsgálnia, hogy a külső rendszeren alkalmazott biztonsági intézkedések megfelelnek-e a szervezet által elvárt követelményeknek, illetve meg kell vizsgálnia továbbá, hogy az elvárt követelmények és intézkedések végrehajtásra kerülnek-e a külső rendszeren. Erre azért van szükség, hogy a szervezet a külső rendszerekre vonatkozó biztonsági követelmények és intézkedések hiánya miatt ne szenvedjen kárt pl.: kompromittáció, szervezethez köthető EIR-ben keletkező kár. Vagy a szervezetnek megállapodásokat kell kötnie a rendszerkapcsolatokat és a feldolgozást illetően, melyek rögzítik és adminisztratív oldalról kikényszerítik az érintett szervezet elvárásait. Ezt követően történhet meg az engedélyezés. A szervezet az elvárt biztonsági követelményeket és intézkedéseket külső, független felmérésekkel vagy a külső rendszert üzemeltető, együttműködő fél részéről tanúsítvány bemutatásával is ellenőrizheti.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a felhasználási feltételeket a külső rendszerekkel kapcsolatban.

2. A szervezetnek ellenőriznie kell a külső rendszeren alkalmazott biztonsági intézkedések végrehajtását. A szervezet az elvárt biztonsági követelményeket és intézkedéseket külső,

független felmérésekkel vagy a külső rendszert üzemeltető, együttműködő fél részéről tanúsítvány bemutatásával is ellenőrizheti.

3. Ha a külső rendszeren alkalmazott biztonsági intézkedések megfelelnek a szervezet biztonsági szabályzatainak és terveinek, akkor a szervezet engedélyezheti a jogosult személyek számára a külső rendszer használatát, az ahhoz történő hozzáférést, illetve az érintett szervezet által ellenőrzött információk feldolgozását, tárolását vagy továbbítását.

4. Alternatív megoldásként, a szervezet megtarthatja a jóváhagyott rendszerkapcsolati vagy feldolgozási megállapodásokat a külső rendszert üzemeltető szervezettel. Ez azt jelenti, hogy a szervezet és a külső rendszert üzemeltető szervezet közötti megállapodásban rögzítik a biztonsági intézkedéseket és a hozzáférési jogosultságokat.

Kapcsolódó intézkedések

5.2. Biztonsági értékelések

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.16. Külső elektronikus információs rendszerek használata

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-20(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

2.117. KÜLSŐ RENDSZEREK HASZNÁLATA – HORDOZHATÓ ADATTÁROLÓK HASZNÁLATÁNAK KORLÁTOZÁSA

2.117. A szervezet a meghatározott feltételek szerint korlátozza a jogosult személyek által külső rendszerekben használt, szervezet által ellenőrzött hordozható adattároló eszközök használatát.

MAGYARÁZAT

A szervezet meghatározza, hogy hogyan és milyen feltételek mellett lehet a szervezet által felügyelt hordozható adathordozókat használni külső rendszerekben. A szervezet által felügyelt hordozható adattárolók külső rendszerekben való használatának korlátozásai közé tartozik az ilyen eszközök használatának teljes tilalma is, azonban a szervezet enyhébb megoldást is alkalmazhat. A használat tilalmát vagy esetleges korlátozását technikai vagy nem technikai módszerekkel érvényesítik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia és dokumentálnia a hordozható adattároló eszközök használatának szabályait és korlátait. Ez magában foglalhatja a teljes tilalmat is, amely megakadályozza az ilyen eszközök használatát külső rendszerben, vagy engedi azt bizonyos kompenzációs kontrollok teljesülése esetén. Ez esetben az érintett szervezetnek dokumentálnia kell a használat feltételeit.
2. A szervezetnek nyilvántartást kell vezetnie az általa felügyelt hordozható adattárolókról, melyet naprakészen kell tartania.
3. A szervezetnek technikai módszereket kell alkalmaznia a tilalom vagy korlátozás érvényesítésére. Ez magában foglalhatja a hordozható adattároló eszközök blokkolását vagy korlátozását amikor nem az érintett szervezet által felügyelt környezetben akarják azt használni a felhasználók.
4. A szervezetnek nem technikai módszereket is alkalmaznia kell a tilalom vagy korlátozás érvényesítésére. Ez magában foglalhatja a szabályok és eljárások kidolgozását, a felhasználók oktatását és tudatosítását a hordozható adattároló eszközök használatának korlátairól és következményeiről, valamint a szabályok betartásának ellenőrzését.

5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a hordozható adattároló eszközök használatának szabályait és korlátait, hogy biztosítsa azok hatékonyságát és relevanciáját.
6. A szervezetnek biztosítania kell, hogy a hordozható adattároló eszközök használatának korlátai és tilalmai összhangban legyenek a szervezet biztonsági céljaival, valamint a vonatkozó jogi és szabályozási követelményekkel.

Kapcsolódó intézkedések

11.14. Adathordozók használata
17.116. Portok, illetve ki- és bemeneti eszközök hozzáférése

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.16. Külső elektronikus információs rendszerek használata

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-20(2)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a korlátozások meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

2.118. KÜLSŐ RENDSZEREK HASZNÁLATA – A NEM SZERVEZETI TULAJDONBAN LÉVŐ RENDSZEREK HASZNÁLATÁNAK KORLÁTOZÁSA

2.118. A szervezet a meghatározott feltételek szerint korlátozza a nem szervezeti tulajdonban lévő rendszerek és rendszerelemek használatát a szervezeti információk feldolgozására, tárolására vagy továbbítására.

MAGYARÁZAT

A szervezet tulajdonán kívül eső rendszerek vagy rendszerelemek közé tartoznak a más szervezetek tulajdonában lévő rendszerek vagy rendszerelemek, valamint a személyes tulajdonban lévő eszközök. A nem szervezeti tulajdonú rendszerek vagy rendszerelemek használata potenciális kockázatokat rejt magában. Bizonyos esetekben a kockázat elég nagy ahhoz, hogy az ilyen használatot megtiltsa a szervezet. Más esetekben az ilyen rendszerek vagy rendszerelemek használata megengedett, de valamilyen módon korlátozott. A korlátozások közé tartozik a nem a szervezet tulajdonában lévő rendszerek és rendszerelemek csatlakozásának engedélyezése előtt jóváhagyott biztonsági követelmények teljesülését vizsgáló ellenőrzések végrehajtásának megkövetelése, az információk, szolgáltatások vagy alkalmazások típusaihoz való hozzáférés korlátozása, virtualizációs technikák alkalmazása a feldolgozási és tárolási tevékenységek szervezet által biztosított szerverekre vagy rendszerelemekre való korlátozása érdekében, és a felhasználási feltételek elfogadása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, mely nem szervezeti tulajdonban lévő EIR-ek és rendszerelemek használatát engedélyezi a szervezet információinak feldolgozására, tárolására vagy továbbítására.
2. A szervezetnek meg kell határoznia a nem szervezeti tulajdonban lévő EIR-ek és rendszerelemek használatának feltételeit. Ez magában foglalhatja a szervezet által jóváhagyott biztonsági követelmények teljesülését vizsgáló ellenőrzések végrehajtásának követelményét a nem szervezeti tulajdonban lévő EIR-ek és rendszerelemek csatlakoztatása előtt.

3. A szervezetnek korlátoznia kell a hozzáférést bizonyos információkhoz, szolgáltatásokhoz vagy alkalmazásokhoz a nem szervezeti tulajdonban lévő EIR-ek és rendszerelemek használata esetén.
4. A szervezetnek ismertetnie kell az érintett munkavállalókkal a nem szervezeti tulajdonban lévő rendszerek és rendszerelemek használatára vonatkozó előírásokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-20(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a korlátozások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.119. KÜLSŐ RENDSZEREK HASZNÁLATA – HÁLÓZATI ADATTÁROLÓK HASZNÁLATÁNAK TILTÁSA

2.119. A szervezet megtiltja a meghatározott hálózati adattároló eszközök használatát külső rendszerekben.

MAGYARÁZAT

A külső rendszerek hálózaton elérhető tárolóeszközei közé tartoznak a nyilvános, hibrid vagy közösségi felhőalapú rendszerek online tárolóeszközei.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, mely hálózati adattároló eszközöket használja jelenleg külső rendszerekben és melyek azok melyek használatát meg szeretné tiltani. Ez magában foglalhatja a nyilvános, hibrid vagy közösségi felhőalapú rendszerekben található hálózati adattároló eszközöket.
2. Miután a szervezet meghatározta, hogy mely eszközöket kívánja letiltani, a tiltást a gyakorlatban is alkalmaznia kell. A szervezetnek ki kell dolgoznia egy eljárást arra az esetre, ha valamely munkavállaló megsértené az előírást.
3. A szervezetnek implementálnia kell az elkészített eljárást a belső szabályzói közé, és biztosítania kell, hogy minden alkalmazott tisztában legyen vele és megértse azt. Ez magában foglalja a képzéseket és a biztonságtudatossági programokat.
4. A szervezetnek rendszeresen ellenőriznie kell, hogy az eljárás betartásra kerül-e.
5. A szervezetnek felül kell vizsgálnia és szükség esetén frissítenie kell az előírásokat és az eljárást, amennyiben az szükséges. Ez magában foglalhatja a megtiltott eszközök listájának frissítését, ha új eszközök kerülnek a piacra, vagy ha a szervezet megváltoztatja az EIR-eket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-20(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hálózaton keresztül elérhető adattárolók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.120. KÜLSŐ RENDSZEREK HASZNÁLATA – HORDOZHATÓ ADATTÁROLÓK HASZNÁLATÁNAK TILTÁSA

2.120. A szervezet megtiltja a szervezet által felügyelt hordozható adattároló eszközöknek a jogosult személyek által külső rendszerekben történő használatát.

MAGYARÁZAT

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

KAPCSOLÓDÓ INTÉZKEDÉSEK

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

ISO/IEC 27001:2023 REFERENCIA

NIST SP 800-53 REV.5 REFERENCIA

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.121. INFORMÁCIÓMEGOSZTÁS

2.121. A szervezet:

2.121.1. Elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói mérlegelés szóba jöhet.

2.121.2. Automatizált mechanizmusokat vagy manuális eljárásokat alkalmaz arra, hogy segítsen a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.

MAGYARÁZAT

Az információmegosztás olyan információkra vonatkozik, amelyek hozzáférését valamilyen formális vagy adminisztratív döntés alapján korlátozhatják. Az ilyen információk például a szerződések bizalmas információi, a speciális hozzáférésű programokhoz vagy fiókokhoz kapcsolódó minősített információk, a privilegizált információk, a szervet által védett információk és a személyes adatok. A biztonsági kockázatértékelések, valamint a szervezetre vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások hasznos segítséget nyújthatnak az információmegosztással kapcsolatos döntésekhez. A körülményektől függően a megosztásban részt vevő partnereket egyéni, csoportos vagy szervezeti szinten definiálhatják. Az információt tartalom, típus, biztonsági kategória vagy speciális hozzáférésű program vagy fiók alapján definiálhatják. A hozzáférési korlátozások magukban foglalhatják a titoktartási megállapodásokat is. Az információáramlást szabályozó technikákat és a biztonsági tulajdonságokat fel lehet használni a felhasználóknak nyújtandó automatizált segítségnyújtásra, melyek segíthetnek a megosztási és együttműködési döntések meghozatalában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek korlátoznia kell az információmegosztást formális vagy adminisztratív intézkedésekkel.

2. A szervezetnek olyan biztonsági követelményeket kell meghatároznia az információmegosztással kapcsolatban, melyek segítenek az arra jogosult felhasználóknak eldönteni, hogy a megosztásban részt vevő partnerhez rendelt jogosultságok megfelelnek-e a

szervezet által meghatározott, információra vonatkozó hozzáférési korlátozásoknak. Erre olyan esetekben van szükség, mikor a felhasználói mérlegelés szóba jöhet.

3. A szervezetnek biztonsági kockázatértékeléseket kell végrehajtania, valamint figyelembe kell vennie a szervezetre vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlásokat mielőtt meghatározza az információmegosztással kapcsolatos korlátozásokat.

4. A szervezetnek az információmegosztásban részt vevő partnereket az egyéni, csoportos vagy szervezeti szinten kell meghatároznia, attól függően, hogy milyen körülmények állnak fenn.

5. A szervezetnek meg kell határoznia az információt tartalom, típus, biztonsági kategória vagy speciális hozzáférési program vagy fiók alapján. Az információhoz történő hozzáférési korlátozások magukban foglalhatják a titoktartási megállapodásokat.

6. A szervezet az információáramlást szabályozó technikákat és a biztonsági tulajdonságokat felhasználhatja a felhasználóknak nyújtandó automatizált segítségnyújtásra, melyek segíthetnek a megosztási és együttműködési döntések meghozatalában.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.89. Biztonsági tulajdonságok

15.4. Kockázatértékelés

17.54. Együttműködésen alapuló informatikai eszközök

41/2015. (VII. 15.) BM rendeleti referencia

3.3.10.17. Információmegosztás

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AC-21

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

2.122. INFORMÁCIÓMEGOSZTÁS – AUTOMATIZÁLT DÖNTÉSTÁMOGATÁS

2.122. A szervezet automatizált mechanizmusokat alkalmaz az információmegosztási döntések érvényesítésére, amelyeket a jogosult felhasználók hajtanak végre, figyelembe véve a megosztásban érintett partnerek hozzáférési jogosultságait és az információhoz való hozzáférés korlátozásait.

MAGYARÁZAT

Amennyiben az érintett szervezet automatizált mechanizmusokat alkalmaz az információmegosztási döntések érvényesítésére, akkor az EIR automatikusan ellenőrzi és hajtja végre azokat a döntéseket, amelyeket a jogosult felhasználók hoznak az információ megosztásával kapcsolatban.

Ez a folyamat figyelembe veszi a megosztásban érintett partnerek hozzáférési jogosultságait és az információhoz való hozzáférés korlátozásait. Például, ha egy felhasználó megpróbál megosztani bizonyos információkat egy másik felhasználóval, az EIR automatikusan ellenőrzi, hogy a másik felhasználónak van-e jogosultsága hozzáférni ehhez az információhoz. Ha nincs, az EIR megakadályozza az információ megosztását.

Ez az automatizált mechanizmus segít a szervezetnek abban, hogy megvédje az érzékeny információkat a nem jogosult hozzáférés ellen, és biztosítsa, hogy csak a megfelelő felhasználók férjenek hozzá azokhoz. Ezenkívül, mivel ez a folyamat automatizált, csökkenti a hibák kockázatát, amelyek manuális ellenőrzéssel történhetnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek a 2.121-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek ki kell dolgoznia és be kell vezetnie automatizált mechanizmusokat, amelyek érvényesítik az információmegosztási szabályokat. Ezek a mechanizmusok lehetnek például szoftverek, amelyek automatikusan ellenőrzik a felhasználók hozzáférési jogosultságait és a rájuk vonatkozó korlátozásokat, mielőtt információt osztanának meg velük.

2. A szervezetnek rendszeresen ellenőriznie kell az EIR-ét, hogy biztosítsa az automatizált mechanizmusok megfelelő működését. Ez magában foglalhatja a mechanizmusok tesztelését és a naplók áttekintését, hogy azonosítsák a potenciális problémákat vagy szabálytalanságokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-21(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.123. INFORMÁCIÓMEGOSZTÁS – INFORMÁCIÓKERESÉS ÉS VISSZAKERESÉS

2.123. A szervezet olyan információkeresési és lekérdezési szolgáltatásokat alkalmaz, amelyek érvényesítik a meghatározott információmegosztási korlátozásokat.

MAGYARÁZAT

Az információkeresési és lekérdezési szolgáltatások azonosítják azokat az EIR erőforrásokat, amelyek relevánsak egy adott információs igény szempontjából. Ezek a szolgáltatások kulcsfontosságúak az érintett szervezet számára, mivel lehetővé teszik, hogy a szervezet hatékonyan kezelje és használja fel az EIR-ben tárolt információkat.

A szervezetnek olyan információkeresési és lekérdezési szolgáltatásokat kell alkalmaznia, amelyek érvényesítik a meghatározott információmegosztási korlátozásokat.

Ez a korlátozás történhet felhasználói szinten, ahol csak bizonyos felhasználók férhetnek hozzá bizonyos információkhoz, vagy az információtípus függvényében, ahol csak bizonyos típusú információk érhetők el bizonyos felhasználók számára.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek korlátoznia kell az információmegosztást formális vagy adminisztratív intézkedésekkel.

2. A szervezetnek ki kell választania és be kell vezetnie olyan információkeresési és lekérdezési szolgáltatásokat, amelyek képesek érvényesíteni a meghatározott információmegosztási korlátozásokat.

3. A szervezetnek úgy kell beállítania az EIR-t, hogy az információkeresési és lekérdezési szolgáltatások csak a megfelelő jogosultságokkal rendelkező személyek számára jelenítsenek meg információt.

4. A szervezetnek biztosítania kell, hogy az EIR frissítései és módosításai során megfelelően kezeljék információkeresési és lekérdezési szolgáltatásokat beállításait, pl. új információforrások hozzáadását, a meglévő források módosítását, vagy a források eltávolítását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-21(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információmegosztási korlátozások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.124. NYILVÁNOSAN ELÉRHETŐ TARTALOM

2.124. A szervezet:

2.124.1. Kijelöli azokat a személyeket, akik jogosultak arra, hogy információkat tegyenek nyilvánosan hozzáférhetővé.

2.124.2. Képzést biztosít a jogosult személyek számára, hogy biztosítsa, hogy a nyilvánosan hozzáférhető információk nem tartalmaznak nem nyilvános információkat.

2.124.3. Áttekinti az információ tervezett tartalmát a nyilvánosan hozzáférhető rendszerbe történő közzététel előtt, annak érdekében, hogy biztosítsa, hogy nem tartalmaznak nem nyilvános információkat.

2.124.4. Meghatározott gyakorisággal áttekinti a nyilvánosan hozzáférhető rendszer tartalmát a nem nyilvános információk szempontjából, és eltávolítja az ilyen információkat, ha felfedezik őket.

MAGYARÁZAT

Az érintett szervezet a vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások szerint, nem engedélyezi a nyilvánosság számára a nem nyilvános információkhoz való hozzáférést. A nyilvánosan hozzáférhető tartalom olyan EIR-eket érint, amelyeket az érintett szervezet kontrollál, és amelyek általában azonosítás vagy hitelesítés nélkül hozzáférhetők a nyilvánosság számára. Az információk nem szervezeti rendszerekben történő közzétételét (pl.: nem szervezethez köthető publikusan elérhető weboldalak, fórumok és közösségi média) az érintett szervezet szabályozásában kezelni kell.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell a nyilvános információk közzétételével kapcsolatos feladatok ellátásról. Meg kell határoznia, hogy kik azok a személyek, akik jogosultak nyilvános elérésre szánt információk közzétételére.

2. A szervezetnek tájékoztatást kell nyújtania a jogosult személyeknek annak érdekében, hogy képesek legyenek annak a megállapítására, hogy mely információk tehetők nyilvánosan elérhetővé.

3. A szervezetnek át kell tekintenie az információ tartalmát közzététel előtt és meg kell bizonyosodnia róla, hogy a közzétételre szánt információ nem tartalmaz olyan információt, amely nem minősül nyilvánosnak.

4. A szervezetnek meghatározott gyakorisággal át kell tekintenie a nyilvánosan elérhető tartalmakat, hogy azok tartalmaznak-e nem nyilvános információkat. Amennyiben a szervezet felfedez nyilvánosan elérhető nem nyilvános tartalmat, akkor gondoskodnia kell annak minél hamarabbi eltávolításáról.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

3.2. Biztonságtudatossági képzés

3.9. Szerepkör alapú biztonsági képzés

4.44. Információk kiszivárgásának figyelemmel kísérése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.3.10.18. Nyilvánosan elérhető tartalom

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-22

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

2.125. ADATBÁNYÁSZAT ELLENI VÉDELEM

2.125. A szervezet a meghatározott adattárakon alkalmazza a meghatározott adatbányászatot megelőző és észlelő technikákat, hogy észlelje és védekezzen az engedély nélküli adatbányászat ellen.

MAGYARÁZAT

Az adatbányászat egy analitikai folyamat, amely nagy adathalmazokban keres összefüggéseket vagy mintázatokat bizonyos adatok vagy ismeretek felfedezése érdekében. Az adattároló objektumok közé tartoznak az adatbázis rekordok és az adatbázis mezők. Az adatbányászati műveletekből bizalmas információk is kinyerhetők. A kinyert információ lehet személyes adat is, amiből előzetesen nem várt következtetések is levonhatók (pl.: a személy nevének, születési dátumának megállapítása). Az adatbányászati tevékenységek végrehajtása előtt az érintett szervezet megállapítja, hogy ezek a tevékenységek engedélyezettek-e. A szervezetnek figyelembe kell vennie az adatbányászati követelményekre vonatkozó hatályos jogszabályokat, irányelveket, szabályozásokat, szabványokat és ajánlásokat. Az adatbányászat megelőzésére és észlelésére szolgáló technikák közé tartozik az adatbázis-lekérdezések számának és gyakoriságának korlátozása, annak érdekében, hogy növeljék azon erőforrásokat, amelyek szükségesek az adatbázisok tartalmának meghatározásához, emellett az adatbázis-lekérdezésekre adott válaszok típusainak korlátozása is ide sorolható, illetve a személyzet értesítése is, amikor a megszokottól eltérő adatbázis lekérdezések vagy hozzáférések történnek. Az adatbányászat elleni védelem azon információk védelmére összpontosít, amelyek a szervezet adattáraiban találhatók. Ezzel szemben az "Információk kiszivárgásának figyelemmel kísérése" kontroll azon szervezeti információk monitorozására összpontosít, amelyeket esetleg kibányásztak vagy más módon szereztek be az adattárolókból, és nyilvánosan hozzáférhető információk, tehát bárki által megismerhetők külső oldalakon, például közösségi hálózati vagy közösségi média weboldalakon.

A szervezetnek célszerű felállítania egy belső fenyegetések elleni programot, amelynek célja a belső fenyegetések megelőzése, észlelése és enyhítése, beleértve a bizalmas információk védelmét a kihasználás, kompromittálás vagy más engedély nélküli nyilvánosságra hozatal ellen. Az adatbányászat elleni védelem megköveteli a szervezettől, hogy tisztában legyen azokkal a módszerekkel, amelyek a szükségtelen vagy engedély nélküli adatbányászat

megelőzésére és észlelésére szolgálnak. Az adatbányászatot egy belső személy is felhasználhatja a szervezeti információk gyűjtésére, kiszivárogtatás céljából.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy az adatbányászati tevékenységek engedélyezettek-e. Ezt a szervezet jogi tanácsadója és a szervezet adatvédelmi felelőse segítségével célszerű elvégezni, figyelembe véve hatályos jogszabályokat, irányelveket, szabályozásokat, szabványokat és ajánlásokat.
2. A szervezetnek meg kell határoznia az adatbányászat megelőzésére és észlelésére szolgáló módszereket/technikákat. Ezek közé tartozhat az adatbázis-lekérdezések számának és gyakoriságának korlátozása, a lekérdezésekre adott válaszok típusának korlátozása, a homomorf titkosítás alkalmazása, valamint a személyzet értesítése a megszokottól eltérő adatbázis lekérdezésekről vagy hozzáférésekről.
3. A szervezetnek védelmi megoldást kell biztosítania az adatbányászat ellen. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie arra, hogy észlelje és megakadályozza az engedély nélküli adatbányászatot.
4. A szervezetnek célszerű felállítania egy belső fenyegetések elleni programot, amelynek célja a belső fenyegetések megelőzése, észlelése és enyhítése, beleértve a bizalmas információk védelmét a kihasználás, kompromittálás vagy más engedély nélküli nyilvánosságra hozatal ellen. A belső fenyegetések kockázatát csökkentheti a felelősségek megfelelő szétválasztása és a legkisebb jogosultság elvének megfelelő alkalmazása.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az adatbányászat megelőzésére és észlelésére szolgáló technikákat, hogy biztosítsa a szervezeti adattárak védelmét az adatbányászat ellen.

KAPCSOLÓDÓ INTÉZKEDÉSEK

1.13. Belső fenyegetés elleni program

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-23

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az adatbányászatot megelőző és felderítő technikák, illetve az adattárolási objektumok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.126. HOZZÁFÉRÉS-ELLENŐRZÉSRE VONATKOZÓ DÖNTÉSEK

2.126. A szervezet eljárásokat alakít ki, illetve mechanizmusokat valósít meg annak érdekében, hogy a meghatározott hozzáférés-felügyeleti szabályok minden hozzáférési kérelem esetén alkalmazásra kerüljenek a hozzáférés engedélyezését megelőzően.

MAGYARÁZAT

A hozzáférés-felügyeleti döntésekre akkor kerül sor, amikor az engedélyezési információkat konkrét hozzáférésekre alkalmazzák. Ezzel szemben a hozzáférések érvényesítésére akkor kerül sor, amikor a rendszerek érvényesítik a hozzáférés-felügyeleti döntéseket. Bár gyakori, hogy a hozzáférés-felügyeleti döntéseket és a hozzáférés érvényesítését ugyanaz a szervezeti egység hajtja végre, de ez nem kötelező, és nem is mindig optimális megoldás. Egyes architektúrák és elosztott rendszerek esetében a hozzáférés-felügyeleti döntéseket és a hozzáférés érvényesítését különböző szervezeti egységek is végezhetik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet határozza meg a hozzáférés-felügyeleti szabályokat. Ezek a szabályok tartalmazzák, hogy ki, mikor, milyen információhoz férhet hozzá az EIR-ben.
2. A szervezetnek eljárásokat kell kidolgoznia a hozzáférési kérelmek kezelésére. Ez magában foglalja a kérelmek fogadását, értékelését és jóváhagyását vagy elutasítását.
3. A szervezetnek implementálnia kell a hozzáférés-felügyeleti szabályokat az EIR-ben. Ez azt jelenti, hogy a szabályokat be kell építeni az EIR hozzáférés-kezelési mechanizmusába.
4. A szervezetnek biztosítania kell, hogy a hozzáférés-felügyeleti szabályok minden hozzáférési kérelem esetén alkalmazásra kerüljenek a hozzáférés engedélyezése előtt. Ez azt jelenti, hogy minden hozzáférési kérelemet a szabályok alapján kell értékelni.
5. A szervezetnek naplót kell vezetnie minden hozzáférési kérelemről és az azzal kapcsolatos döntésekről. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon kövesse és ellenőrizze a hozzáférési kérelmeket, és biztosítsa a szabályok betartását.

6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a hozzáférés-felügyeleti szabályokat és eljárásokat, hogy biztosítsa azok hatékonyságát és relevanciáját.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.3

NIST SP 800-53 REV.5 REFERENCIA

AC-24

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hozzáférés-ellenőrzési döntések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.127. HOZZÁFÉRÉS-ELLENŐRZÉSI DÖNTÉSEK – HOZZÁFÉRÉSI ENGEDÉLYEK TOVÁBBÍTÁSA

2.127. A szervezet a meghatározott hozzáférés-engedélyezési információkat a meghatározott követelmények szerint továbbítja azokba a rendszerekbe, amelyek a hozzáférés-felügyeleti döntéseket végrehajtják.

MAGYARÁZAT

Az engedélyezési folyamatok és a hozzáférés-felügyeleti döntések a rendszerek különálló részeiben vagy különálló rendszerekben történhetnek. Ilyen esetekben az engedélyezési információkat biztonságosan továbbítják, hogy a megfelelő helyeken időben érvényesíthetőek legyenek a hozzáférés-felügyeleti döntések. Ezen döntések támogatásához szükséges lehet a hozzáférési jogosultság részeként a biztonsági jellemzők alátámasztására szolgáló információk továbbítása. Ennek oka, hogy az elosztott rendszerekben különböző hozzáférés-felügyeleti döntéseket kell hozni, és ezeket a döntéseket a különböző szereplők egymást követően hozzák meg, és mindegyiküknek szüksége van ezekre az ismérvekre a döntések meghozatalához. A hozzáférés engedélyezési információk védelme biztosítja, hogy ezeket az információkat ne lehessen megváltoztatni, meghamisítani vagy felfedni az átvitel során.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a hozzáférési engedélyezési információkat, amelyeket a hozzáférés-felügyeleti döntések végrehajtásához szükséges EIR-be kell továbbítania.
2. A szervezetnek védenie kell a hozzáférés-engedélyezési információkat, így biztosítva, hogy ezeket az információkat ne lehessen megváltoztatni, meghamisítani vagy felfedni az átvitel során pl.: kriptográfiai mechanizmusok használata.
3. A szervezetnek szükség esetén a hozzáférési jogosultság részeként a biztonsági jellemzők alátámasztására szolgáló információkat is továbbítania kell. Ez azért szükséges, mert az elosztott rendszerekben számos hozzáférés-ellenőrzési döntést kell meghozni, és különböző entitások hozzák meg ezeket a döntéseket, így mindegyiknek szüksége van ezekre a jellemzőkre a döntések meghozatalához.

4. A szervezetnek naplóznia kell a hozzáférési engedélyezési információk továbbítását és a hozzáférési ellenőrzési döntések végrehajtását, hogy nyomon követhető legyen a folyamat és szükség esetén vissza lehessen követni a lépéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.33. Letagadhatatlanság

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-24(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hozzáférés engedélyezési információk, illetve a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.128. Felhasználó- vagy a folyamatazonosító ismerete nélküli hozzáférés-ellenőrzési döntések.

2.128. A szervezet a hozzáférés-felügyeleti döntéseket olyan meghatározott biztonsági tulajdonságok alapján hajtja végre, amelyek nem tartalmazzák a felhasználó vagy a felhasználó nevében eljáró folyamat azonosítóját.

Magyarázat

Bizonyos esetekben fontos, hogy a hozzáférés-felügyeleti döntések a kéréseket benyújtó felhasználók személyazonosságára vonatkozó információk nélkül is meghozhatók legyenek. Ezek általában olyan esetek, amikor az egyén személyes adatainak védelme kiemelkedő fontosságú. Más helyzetekben a felhasználó azonosítására vonatkozó információ egyszerűen nem szükséges a hozzáférés-felügyeleti döntésekhez, és különösen az elosztott rendszerek esetében az ilyen információk megfelelő biztonsággal történő továbbítása nagyon költséges vagy nehezen megvalósítható. A kötelező hozzáférés-felügyelet (mandatory access control (MAC)), a szerepkör alapú hozzáférés-felügyelet (role based access control (RBAC), tulajdonság alapú hozzáférés-felügyelet (attribute based access control (ABAC)) és a címkéken alapuló ellenőrzési irányelvek például nem feltétlenül tartalmazzák a felhasználói azonosítót, mint jellemzőt.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, azokat a biztonsági tulajdonságokat, melyek alapján hozzáférés-felügyeleti döntéseket hoz és amelyek nem tartalmazzák a felhasználó vagy a felhasználó nevében eljáró folyamat azonosítóját.
2. A szervezetnek implementálnia kell egy hozzáférés-felügyeleti házirendet az EIR-ben, amely a meghatározott biztonsági tulajdonságok alapján hajtja végre a döntéseket. Ez magában foglalhatja a MAC, RBAC, ABAC és címke-alapú felügyeleti szabályokat, amelyek nem tartalmazzák a felhasználó azonosítóját, mint tulajdonságot.
3. A szervezetnek biztosítania kell, hogy az EIR képes legyen a hozzáférés-felügyeleti döntések végrehajtására a meghatározott biztonsági tulajdonságok alapján, anélkül, hogy szükség lenne a felhasználó azonosítóinak továbbítására.

4. A szervezetnek naplózni kell az összes hozzáférés-felügyeleti döntést az EIR-ben, hogy nyomon követhető legyen, hogy a döntések valóban a meghatározott biztonsági tulajdonságok alapján történtek-e.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hozzáférés-felügyeleti szabályokat és a biztonsági tulajdonságokat, hogy biztosítsa az EIR biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-24(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági vagy adatvédelmi tulajdonságok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

2.129. REFERENCIÁNAK VALÓ MEGFELELŐSÉG VIZSGÁLATA

2.129. A szervezet a meghatározott hozzáférés-felügyeleti szabályzat ellenőrzésére olyan megfelelőségellenőrző megoldást valósít meg, amely manipulációbiztos, folyamatba épített és a teljes körű elemzés és tesztelés elvégzéséhez alkalmas terjedelmű.

MAGYARÁZAT

A referenciának való megfelelőség vizsgálata olyan, referencia-érvényesítési mechanizmusra vonatkozó, tervezési követelmények összessége, amely az operációs rendszer kulcsfontosságú összetevőjeként érvényre juttatja a hozzáférés-ellenőrzési szabályokat minden alanyra és objektumra vonatkozóan. A referenciaellenőrzési mechanizmus mindig meghívható, manipulációbiztos, és elég kisméretű ahhoz, hogy elemzés és tesztek tárgyát képezze, illetve a teljeskörűsége is biztosítható. Az információk rendszeren belüli megjelenítése az adatstruktúráknak nevezett absztrakciók segítségével történik. A belső adatszerkezetek különböző típusú entitásokat jelölhetnek, aktív és passzív módon egyaránt. Az aktív entitások, más néven alanyok, egyénekhez, eszközökhöz vagy egyének nevében eljáró folyamatokhoz kapcsolódnak. A passzív entitások, más néven objektumok olyan adatszerkezetekhez kapcsolódnak, mint például az adatrekordok, a memóriák, a kommunikációs portok, a táblaszerkezetek, a fájlok és a folyamatok közötti kapcsolatok.

A megfelelőség ellenőrző megoldások olyan hozzáférés-felügyeleti szabályokat hajtanak végre, amelyek az objektumokhoz való hozzáférést az alanyok vagy azon csoportok azonossága alapján korlátozzák, amelyekhez az alanyok tartoznak. Az EIR a szabályzat által meghatározottak alapján hajtja végre a hozzáférés-felügyeleti szabályokat. A megfelelőség ellenőrző megoldás manipulációbiztos tulajdonsága megakadályozza, hogy a lehetséges támadók veszélyeztessék a referenciaellenőrzési mechanizmus működését. A folyamatosan meghívásra kerülő funkció megakadályozza, hogy a támadók megkerüljék a mechanizmust és megsértsék a biztonsági szabályokat. A kismértékűség révén biztosítható a mechanizmus elemzésének és tesztelésének teljessége, ezáltal felfedhető minden olyan gyengeség vagy hiányosság (például látens hiba), amely megakadályozná a biztonsági szabályok érvényesítését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek implementálnia kell egy referenciaellenőrző megoldást, amely a hozzáférés-felügyeleti szabályokat érvényesíti.
2. A szervezetnek biztosítania kell, hogy a referenciaellenőrző megoldás manipulációbiztos, vagyis a rosszindulatú támadók nem tudják megsérteni vagy megkerülni.
3. A szervezetnek biztosítania kell, hogy a referenciaellenőrző megoldás mindig aktiválódik, így a rosszindulatú támadók nem tudják megkerülni.
4. A szervezetnek teljes körű elemzést és tesztelést kell végeznie a referenciaellenőrző megoldáson, hogy felfedje az esetleges gyengeségeket vagy hiányosságokat.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a referenciaellenőrző megoldást, hogy megfeleljen a változó kiberbiztonsági környezetnek és fenyegetéseknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
2.89. Biztonsági tulajdonságok
16.16. Biztonságtervezési elvek
16.87. Fejlesztői biztonsági architektúra és tervezés
17.4. Biztonsági funkciók elkülönítése
17.47. Megbízható útvonal
17.108. A folyamatok elkülönítése
18.68. Előrelátható meghibásodás megelőzése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AC-25

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hozzáférés-ellenőrzési szabályok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024