Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Rendszer- és kommunikációvédelem

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

17.1. Szabályzat és eljárásrendek 9

17.2. Rendszer és felhasználói funkciók szétválasztása 12

17.3. Rendszer és felhasználói funkciók szétválasztása – Nem privilegizált felhasználók interfészei 14

17.4. Biztonsági funkciók elkülönítése 16

17.5. Biztonsági funkciók elkülönítése – Hardver szintű 18

17.6. Biztonsági funkciók elkülönítése – Hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő biztonsági funkciók 20

17.7. Biztonsági funkciók elkülönítése – Nem biztonsági funkciók számának minimalizálása 22

17.8. Biztonsági funkciók elkülönítése – Modulok összekapcsolása és összetartása 24

17.9. Biztonsági funkciók elkülönítése – Réteges szerkezetek 26

17.10. Információk az osztott használatú rendszererőforrásokban 28

17.11. Információk az osztott használatú rendszererőforrásokban – Többszintű vagy időszakos feldolgozás 30

17.12. Szolgáltatásmegtagadással járó támadások elleni védelem 32

17.13. Szolgáltatásmegtagadással járó támadások elleni védelem – Más rendszerek megtámadásának korlátozása 34

17.14. Szolgáltatásmegtagadással járó támadások elleni védelem – Kapacitás, sávszélesség, redundancia 36

17.15. Szolgáltatásmegtagadással járó támadások elleni védelem – Észlelés és felügyelet 38

17.16. Erőforrások rendelkezésre állása 40

17.17. A határok védelme 42

17.18. A határok védelme – Hozzáférési pontok 45

17.19. A határok védelme – Külső infokommunikációs szolgáltatások 47

17.20. A határok védelme – Alapértelmezés szerinti elutasítás és kivétel alapú engedélyezés 50

17.21. A határok védelme – Megosztott csatornahasználat távoli eszközök esetén 52

17.22. A határok védelme – A forgalom átirányítása hitelesített proxykiszolgálókra 55

17.23. A határok védelme – Korlátozza a fenyegető kimenő kommunikációs forgalmat 57

17.24. A határok védelme – Információ kiszivárgásának megakadályozása 59

17.25. A határok védelme – A bejövő kommunikációs forgalom korlátozása 61

17.26. A határok védelme – Hosztalapú védelem 63

17.27. A határok védelme – A biztonsági eszközök, mechanizmusok és támogató rendszerelemek elkülönítése 65

17.28. A határok védelme – Védelem az engedély nélküli fizikai kapcsolatok kialakítása ellen 67

17.29. A határok védelme – Hálózati privilegizált hozzáférések 69

17.30. A határok védelme – Rendszerelemek felfedezésének megakadályozása 71

17.31. A határok védelme – A protokoll formátumok betartása 73

17.32. A határok védelme – Biztonságos állapot fenntartása 75

17.33. A határok védelme – Kommunikáció blokkolása nem szervezeti konfigurációval rendelkező gépekről 77

17.34. A határok védelme – Dinamikus elszigetelés és elkülönítés 79

17.35. A határok védelme – Rendszerelemek elkülönítése 81

17.36. A határok védelme – Különálló alhálózatok a különböző biztonsági tartományokhoz való csatlakozáshoz 83

17.37. A határok védelme – Visszajelzés küldésének letiltása a protokoll ellenőrzési hiba esetén 85

17.38. A határok védelme – Nyilvános hálózathoz történő csatlakozás tiltása 87

17.39. A határok védelme – Különálló alhálózatok a funkciók elkülönítéséhez 89

17.40. Az adatátvitel bizalmassága és sértetlensége 91
17.41. Az adatátvitel bizalmassága és sértetlensége – Kriptográfiai védelem 94
17.42. Az adatátvitel bizalmassága és sértetlensége – Az adatok átvitel előtti és utáni kezelése 96
17.43. Az adatátvitel bizalmassága és sértetlensége – Üzenetek kriptográfiai védelme külső fogadó fél esetén..... 98
17.44. Az adatátvitel bizalmassága és sértetlensége – Kommunikáció elrejtése vagy randomizálása..... 100
17.45. Az adatátvitel bizalmassága és sértetlensége – Védett elosztórendszer 102
17.46. A hálózati kapcsolat megszakítása 104
17.47. Megbízható útvonal..... 106
17.48. Megbízható útvonal – Megmásíthatatlan útvonal 109
17.49. Kriptográfiai kulcs előállítása és kezelése 111
17.50. Kriptográfiai kulcs előállítása és kezelése – Rendelkezésre állás..... 113
17.51. Kriptográfiai kulcs előállítása és kezelése – Aszimmetrikus kulcsok..... 115
17.52. Kriptográfiai kulcs előállítása és kezelése – Kulcsok fizikai felügyelete 117
17.53. Kriptográfiai védelem 119
17.54. Együttműködésen alapuló informatikai eszközök..... 121
17.55. Együttműködésen alapuló informatikai eszközök – Fizikai vagy logikai szétkapcsolás 123
17.56. Együttműködésen alapuló informatikai eszközök – Biztonságos munkaterületek . 125
17.57. Együttműködésen alapuló informatikai eszközök – Résztvevők egyértelmű felsorolása..... 127
17.58. Biztonsági tulajdonságok átvitele..... 129
17.59. Biztonsági tulajdonságok átvitele – Sértetlenség ellenőrzése 131
17.60. Biztonsági tulajdonságok átvitele – Megtévesztés elleni mechanizmusok..... 133

17.61. Biztonsági tulajdonságok átvitele – Kriptográfiai kötés 135
17.62. Nyilvános kulcsú infrastruktúra tanúsítványok 137
17.63. Mobilkód korlátozása 139
17.64. Mobilkód korlátozása – Nem elfogadható kód azonosítása és korrektív intézkedések 141
17.65. Mobilkód korlátozása – Beszerzés, fejlesztés és használat 143
17.66. Mobilkód korlátozása – Letöltés és kódvégrehajtás megakadályozása 145
17.67. Mobilkód korlátozása – Automatikus kódvégrehajtás megakadályozása 147
17.68. Mobilkód korlátozása – Csak zárt környezetekben való kódvégrehajtás 149
17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás) 151
17.70. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás) – Adat forrása és bizalmassága 154
17.71. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás) 156
17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén 158
17.73. Munkaszakasz hitelessége 160
17.74. Munkaszakasz hitelessége – Munkaszakasz-azonosítók érvénytelenítése kijelentkezéskor 162
17.75. Munkaszakasz hitelessége – A rendszer által generált egyedi munkaszakasz-azonosítók 164
17.76. Munkaszakasz hitelessége – Engedélyezett tanúsítvány kibocsájtók 166
17.77. Ismert állapotba való visszatérés 168
17.78. Funkcionalitás és információtárolás minimalizálása 170
17.79. Csapdák alkalmazása 172
17.80. Platform-független alkalmazások 174
17.81. Tárolt (at rest) adatok védelme 176

17.82. Tárolt (at rest) adatok védelme – Kriptográfiai védelem 178
17.83. Tárolt (at rest) adatok védelme – Offline tárhely 180
17.84. Tárolt (at rest) adatok védelme – Kriptográfiai kulcsok 182
17.85. A rendszerelemek esetében alkalmazott változatos információs technológiák 184
17.86. Heterogenitás – Virtualizációs technikák 186
17.87. Elfedés és megtévesztés 188
17.88. Elfedés és megtévesztés – Véletlenszerűség 190
17.89. Elfedés és megtévesztés – Feldolgozási és tárolási helyek megváltoztatása 192
17.90. Elfedés és megtévesztés – Félrevezető információ 194
17.91. Elfedés és megtévesztés – Rendszerelemek elrejtése 196
17.92. Rejtett csatornák elemzése 198
17.93. Rejtett csatornák elemzése – Rejtett csatornák tesztelése a kihasználhatóság szempontjából 200
17.94. Rejtett csatornák elemzése – Maximális sávszélesség 202
17.95. Rejtett csatornák elemzése – Sávszélesség mérése éles környezetben 204
17.96. Rendszer felosztása 206
17.97. Rendszer felosztása – Fizikai tartományok különválasztása a privilegizált funkciókhoz 208
17.98. Végrehajtható, de nem módosítható programok 210
17.99. Végrehajtható, de nem módosítható programok – Nem írható tárolóeszköz 212
17.100. Végrehajtható, de nem módosítható programok – Sértetlenség védelme az írásvédett adathordozón 214
17.101. Külső kártékony kódok azonosítása 216
17.102. Elosztott feldolgozás és tárolás 218
17.103. Elosztott feldolgozás és tárolás – Mérési technikák 220
17.104. Elosztott feldolgozás és tárolás – Szinkronizáció 222

17.105. Sávon kívüli csatornák 224
17.106. Sávon kívüli csatornák – Átvitel és továbbítás biztosítása 227
17.107. Működésbiztonság 229
17.108. A folyamatok elkülönítése 231
17.109. Folyamatok elkülönítése – Hardveres elkülönítés 233
17.110. A folyamatok elkülönítése – Külön végrehajtási tartomány szálanként 235
17.111. Vezeték nélküli kapcsolat védelme 237
17.112. Vezeték nélküli kapcsolat védelme – Elektromágneses interferencia 239
17.113. Vezeték nélküli kapcsolat védelme – Felderítés lehetőségének csökkentése 241
17.114. Vezeték nélküli kapcsolat védelme – Utánzó vagy manipulatív megtévesztés 243
17.115. Vezeték nélküli kapcsolat védelme – Jelparaméterek azonosítása 245
17.116. Portok, illetve ki- és bemeneti eszközök hozzáférése 247
17.117. Érzékelő képességei és kapcsolódó adatok 249
17.118. Érzékelő képesség és adatok – Jelentés a kijelölt személyeknek vagy szerepköröknek 251
17.119. Érzékelő képesség és adatok – Engedélyezett felhasználás 253
17.120. Érzékelő képesség és adatok – Adatgyűjtés minimalizálása 255
17.121. Használati korlátozások 257
17.122. Izolált futtatási környezetek 259
17.123. Rendszeridő szinkronizálása 262
17.124. Rendszeridő szinkronizálása – Szinkronizálás a hiteles időforrással 264
17.125. Rendszeridő szinkronizálása – Másodlagos hiteles időforrás 266
17.126. Tartományok közötti szabályok érvényesítése 268
17.127. Alternatív kommunikációs utak 270
17.128. Érzékelő áthelyezése 272

17.129. Érzékelő áthelyezése – Érzékelők vagy felügyeleti képességek dinamikus áthelyezése 274
17.130. Hardver szintű szétválasztás és szabályérvényesítés 276
17.131. Szoftver szintű szétválasztás és szabályérvényesítés 278
17.132. Hardver szintű védelem 280

17.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

17.1. A szervezet:

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

17.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó rendszer- és kommunikációvédelmi szabályzatot, amely

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

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

17.1.1.2. a rendszer- és kommunikációvédelmi eljárásrendet, amely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

17.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a rendszer- és kommunikációvédelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

17.1.3. Felülvizsgálja és frissíti az aktuális rendszer- és kommunikációvédelmi szabályzatot és a rendszer- és kommunikációvédelmi eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

A rendszer- és kommunikációvédelmi szabályzat és eljárások a rendszer- és kommunikációvédelem követelménycsoportba tartozó védelmi intézkedésekkel foglalkoznak, amelyek az EIR-ekben, illetve a szervezetekben bevezetésre kerülnek.

A kockázatkezelési stratégia fontos tényező az ilyen típusú szabályzatok és eljárásrendek létrehozása során. A szabályzatok és eljárásrendek hozzájárulnak a biztonság garantálásához. Ezért fontos, hogy a szervezet információbiztonsági szabályozási környezete, a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó eljárásrendek összhangban legyenek egymással. A szervezeti szintű biztonsági szabályzatok és eljárásrendek általában

előnyösebbek, és szükségtelenné tehetik a szervezeti célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásrendeket. A szabályok helyet kaphatnak egy általános biztonsági szabályzatban (pl.: Információbiztonsági Szabályzat (IBSZ)), illetve több szabályzatban is megjelenhetnek, attól függően, hogy az érintett szervezetnek milyen a felépítése. Amennyiben szükséges, létrehozhatók eljárásrendek az információbiztonsági irányítási rendszer, a szervezeti célok vagy üzleti folyamatok, illetve az EIR-ek támogatására. Az eljárásrendek leírják miként valósulnak meg a szabályok vagy a védelmi intézkedések, és azok hogyan érintik az eljárásrend tárgyát képező egyént vagy szerepkört. Az eljárásrendek képezhetik a rendszerbiztonsági terv részét, illetve egy vagy több külön dokumentumban is helyet kaphatnak. A rendszer- és kommunikációvédelmi szabályzat és eljárásrendek frissítését kiváltó események lehetnek értékelésből vagy (felül)vizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban. Az elvárt védelmi intézkedések egyszerű újraközlése

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell a rendszer- és kommunikációvédelmi szabályzat és eljárásrendek kidolgozásával, dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatok ellátásáról.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a rendszer- és kommunikációvédelmi 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 rendszer- és kommunikációvédelmi 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 rendszer- és kommunikációvédelmi szabályzatot/szabályokat, illetve a kapcsolódó eljárásrendeket a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

1.10. Kockázatkezelési stratégia
14.12. Fegyelmi intézkedések
16.16. Biztonságtervezési elvek
18.67. Információ kezelése és megőrzése

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

3.3.13.1. Rendszer- és kommunikációvédelmi 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.5.31; A.5.36; A.5.37

NIST SP 800-53 REV.5 REFERENCIA

SC-1

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

17.2. RENDSZER ÉS FELHASZNÁLÓI FUNKCIÓK SZÉTVÁLASZTÁSA

17.2. Az EIR szétválasztja a felhasználók által elérhető funkciókat - beleértve a felhasználói interfész szolgáltatásait - a rendszer üzemeltetési funkcióktól.

MAGYARÁZAT

A rendszerüzemeltetési funkciók közé tartoznak például az adatbázisok, a hálózati rendszerelemek, a munkaállomások vagy szerverek kezeléséhez szükséges, jellemzően privilegizált felhasználói hozzáférést igénylő funkciók. A felhasználói funkciók szétválasztása a rendszerüzemeltetési funkcióktól történhet fizikai vagy logikai szinten. A szervezet külön számítógépekkel, különböző központi feldolgozóegységekkel, operációsrendszerek különböző példányaival, külön hálózati címekkel, virtualizációs technikákkal vagy ezek kombinációival valósíthatja meg a rendszerüzemeltetéssel kapcsolatos funkciók szétválasztását a felhasználói funkcióktól. Ez a fajta szétválasztás magában foglalja például a webes adminisztrációs interfészeket, amelyeken az EIR erőforrásainak többi felhasználóiétól eltérő hitelesítési módszereket használnak. A rendszer és a felhasználói funkciók elkülönítése magában foglalhatja az adminisztratív interfészek elkülönítését a különböző tartományokban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a rendszerüzemeltetési funkcióit, valamint az azokhoz szükséges privilegizált felhasználói hozzáféréseket.
2. A szervezetnek szét kell választania felhasználói funkciókat és az EIR rendszerüzemeltetési funkcióit fizikai vagy logikai megoldásokkal.
3. A szervezetnek biztosítania kell a rendszerüzemeltetési funkciók és a felhasználói funkciók szétválasztása magában foglalja a webes adminisztratív interfészeket, amelyek a rendszer bármely más erőforrásának felhasználói számára külön hitelesítési módszereket alkalmaznak. Az EIR és a felhasználói funkciók szétválasztása elérhető a biztonságtervezési alapelveinek alkalmazásával.
4. A szervezetnek dokumentálnia kell a rendszerbiztonsági tervben az általa szétválasztott felhasználói funkciókat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.60. Legkisebb jogosultság elve

16.7. Beszerzések

16.16. Biztonságtervezési elvek

17.4. Biztonsági funkciók elkülönítése

17.17. A határok védelme

17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

17.96. Rendszer felosztása

17.108. A folyamatok elkülönítése

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

3.3.13.2. Alkalmazás szétválasztás: Az elektronikus információs rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.3. Rendszer és felhasználói funkciók szétválasztása – Nem privilegizált felhasználók interfészei

17.3. Az EIR megakadályozza a rendszerüzemeltetési funkciók megjelenítését a felhasználói interfészeken a nem privilegizált felhasználók számára.

Magyarázat

A rendszerüzemeltetési funkciók nem privilegizált felhasználók számára történő megjelenítésének megakadályozása a felületeken biztosítja, hogy a rendszerüzemeltetési lehetőségek, beleértve a rendszergazdai jogosultságokat is, ne legyenek elérhetőek az általános felhasználók számára. A felhasználói hozzáférés korlátozása megakadályozza az ilyen információk elérhetőségének megszüntetésére általánosan használt grey-out opció használatát is. Az egyik lehetséges megoldás a rendszergazdai beállítások visszatartása mindaddig, amíg a felhasználók rendszergazdai jogosultságokkal rendelkező munkameneteket nem hoznak létre.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, mely felhasználói interfészek jelenítenek meg rendszerüzemeltetési funkciókat. Ez magában foglalhatja a rendszerbeállításokat, az adminisztrátori jogosultságokat és más, a rendszer működéséhez kapcsolódó beállításokat.
2. A szervezetnek meg kell határoznia, mely felhasználók rendelkeznek privilegizált hozzáféréssel.
3. A szervezetnek korlátoznia kell a nem privilegizált felhasználók hozzáférését a rendszerüzemeltetési funkciókhoz.
4. A szervezetnek alkalmaznia kell egy EIR-t, amely csak akkor teszi elérhetővé a rendszerüzemeltetési funkciókat, ha a felhasználók adminisztrátori jogosultságokkal rendelkező munkamenetet indítanak.
5. A szervezetnek naplóznia kell minden hozzáférést és módosítást, amelyet a felhasználók a rendszerüzemeltetési funkciókhoz végeznek. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse, ki fért hozzá ezekhez a funkciókhoz, és milyen változtatásokat hajtottak végre.

6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hozzáférési jogosultságokat, hogy biztosítsa, hogy csak a megfelelő felhasználók férjenek hozzá a rendszerüzemeltetési funkciókhoz.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés 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

SC-2(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.4. BIZTONSÁGI FUNKCIÓK ELKÜLÖNÍTÉSE

17.4. Az EIR elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.

MAGYARÁZAT

Az EIR a biztonsági funkciókat rendszeren belül partíciók és tartományok segítségével megvalósított határokkal különíti el a nem biztonsági funkcióktól. Ez az elkülönítés határozza meg a hozzáférést a biztonsági funkciókat ellátó hardverhez, szoftverhez és firmware-hez, valamint védelmet biztosít ezek számára. Az EIR-ek számos módon valósítják meg az elválasztást (azaz a biztonsági funkciók szétválasztását a nem biztonsági funkcióktól), ilyen például biztonsági mag (security kernel) biztosítása. Nem kernel kód esetében a biztonsági funkció elszigeteltségét gyakran a fájlrendszer védelmével érik el, amellyel védik a kódot a lemezen, és a címtartomány védelmét, amellyel a futtatható kódot védik. Az EIR-ek a biztonsági funkciókhoz való hozzáférést hozzáférés-felügyeleti mechanizmusok és a legkisebb jogosultság elvével képesek korlátozni. Míg az ideális esetben a biztonsági funkció elszigetelési határain belüli összes kód csak biztonsági szempontból releváns kódot tartalmazna, néha szükség lehet rá, hogy nem biztonsági funkciókat is tartsunk az elkülönítési határokon belül.

.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek implementálnia kell egy elkülönítő határt az EIR-en belül, partíciók és domainek segítségével. Ez a határ szabályozza a hozzáférést és védi a hardver, szoftver és firmware integritását, amelyek a rendszerbiztonsági funkcióit végzik.
2. A szervezetnek kódelválasztást kell végrehajtania az EIR-ben, például biztonsági magok biztosításával processzor gyűrűk vagy processzor módok segítségével. A nem magkód esetében a biztonsági funkciók elkülönítése gyakran fájlrendszer-védelmekkel érhető el.
3. A szervezetnek korlátoznia kell a hozzáférést az EIR biztonsági funkcióihoz hozzáférés-felügyeleti mechanizmusok használatával, és a legkisebb jogosultság elvének implementálásával.
4. A szervezetnek néha szükséges a nem biztonsági funkciók kivételként történő bevonását biztosítania.

5. A szervezetnek el kell érnie a biztonsági funkciók és a nem biztonsági funkciók elkülönítését a biztonságtervezési alapelvek alkalmazásával.
6. A szervezetnek dokumentálnia kell az EIR biztonsági és nem biztonsági funkcióinak elkülönítését, hogy bizonyíthassa a követelményeknek való megfelelését.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése
2.60. Legkisebb jogosultság elve
2.129. Referenciának való megfelelőség vizsgálata
6.2. Alapkonfiguráció
6.15. Biztonsági hatásvizsgálatok
16.7. Beszerzések
16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció
16.16. Biztonságtervezési elvek
16.76.1. Fejlesztési folyamat, szabványok és eszközök
16.87. Fejlesztői biztonsági architektúra és tervezés

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

3.3.13.3. Biztonsági funkciók elkülönítése: Az elektronikus információs rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SC-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

17.5. BIZTONSÁGI FUNKCIÓK ELKÜLÖNÍTÉSE – HARDVER SZINTŰ

17.5. Az EIR hardver szintű mechanizmusokat alkalmaz a biztonsági funkciók elkülönítésére.

MAGYARÁZAT

A hardveres szétválasztási mechanizmusok közé tartoznak a mikroprocesszorokban megvalósított hardveres gyűrűarchitektúrák és a hardveres címszegmentálás, amelyet a logikailag elkülönülő, külön attribútumokkal rendelkező tárolóobjektumok támogatására használnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely biztonsági funkciókat kell elkülöníteni az EIR-ben. Ez magában foglalhatja az adatokhoz való hozzáférést, a felhasználói hitelesítést, a naplózást és más fontos biztonsági funkciókat.
2. A szervezetnek ki kell választania és be kell szereznie a szükséges hardvereket, amelyek támogatják a hardver szintű elkülönítési mechanizmusokat. Ez magában foglalhatja a megfelelő mikroprocesszorokat és más hardverelemeket.
3. A szervezetnek implementálnia kell a hardver szintű elkülönítési mechanizmusokat az EIR-ben. Ez magában foglalhatja a hardvergyűrű-architektúrák beállítását és a címszegmensek konfigurálását.
4. A szervezetnek tesztelnie kell az EIR hardver szintű elkülönítési mechanizmusait, hogy biztosítsa, hogy megfelelően működnek és hatékonyan elkülönítik a biztonsági funkciókat.

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

SC-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.6. Biztonsági funkciók elkülönítése – Hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő biztonsági funkciók

17.6. Az EIR elkülöníti a hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő biztonsági funkciókat a nem biztonsági funkcióktól, valamint az egyéb biztonsági funkcióktól.

Magyarázat

A biztonsági funkciók elkülönítése a végrehajtás miatt történik. A funkciók továbbra is vizsgálhatók és ellenőrizhetők. A hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő funkcióktól potenciálisan elszigetelt biztonsági funkciók közé tartoznak a naplózás, a behatolásérzékelés és a rosszindulatú kódok elleni védelmi funkciók.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az EIR-ben lévő biztonsági funkciókat, beleértve a hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő funkciókat, valamint a nem biztonsági funkciókat.
2. A szervezetnek el kell különítenie ezeket a biztonsági funkciókat az EIR-ben. Ez azt jelenti, hogy a hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő funkciókat külön kell kezelni a nem biztonsági funkcióktól és az egyéb biztonsági funkcióktól.
3. A szervezetnek biztosítania kell, hogy a hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő funkciók ne legyenek hozzáférhetők vagy módosíthatók a nem biztonsági funkciók által.
4. A szervezetnek naplózásra és monitorozásra van szüksége, hogy nyomon követhesse és ellenőrizhesse az EIR biztonsági funkcióinak elkülönítését. Ez magában foglalja a hozzáférési naplók, a biztonsági eseményjelentések és a rendszeres biztonsági ellenőrzések kezelését.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR biztonsági funkcióit és azok elkülönítését, hogy biztosítsa a folyamatos kiberbiztonságot és megfeleljen a kiberbiztonsági 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

SC-3(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.7. BIZTONSÁGI FUNKCIÓK ELKÜLÖNÍTÉSE – NEM BIZTONSÁGI FUNKCIÓK SZÁMÁNAK MINIMALIZÁLÁSA

17.7. Az EIR minimalizálja a biztonsági funkciókat tartalmazó izolációs határon belüli nem biztonsági funkciók számát.

MAGYARÁZAT

Ha nem lehetséges a nem biztonsági funkciók szigorú izolációja a biztonsági funkcióktól, akkor olyan intézkedéseket kell hozni, amelyek minimalizálják a nem biztonsági szempontból releváns funkciókat a biztonsági funkciók határán belül. Az izolációs határon belül található nem biztonsági funkciók azért tekinthetők biztonsági szempontból relevánsnak, mert a szoftverben lévő hibák vagy rosszindulatú kódok közvetlenül befolyásolhatják az EIR-ek biztonsági funkcióit. Az alapvető tervezési cél az, hogy az EIR-ek információbiztonságot nyújtó konkrét részei minimális méretűek és összetettségűek legyenek. A nem biztonsági funkciók számának minimalizálása a biztonság szempontjából fontos rendszerelemekben lehetővé teszi a tervezők és a megvalósítók számára, hogy csak azokra a funkciókra összpontosítsanak, amelyek a kívánt biztonsági képesség biztosításához szükségesek. Az izolációs határokon belüli nem biztonsági funkciók minimalizálásával jelentősen csökken az a kódmennyiség, amelyre a biztonsági irányelvek érvényesítését bízzák, ami hozzájárul az érthetőséghez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az EIR-en belüli biztonsági funkciókat és a nem biztonsági funkciókat.
2. A szervezetnek meg kell próbálnia szigorúan izolálni a nem biztonsági funkciókat a biztonsági funkcióktól az EIR-en belül.
3. Amennyiben ez nem lehetséges, akkor a szervezetnek intézkedéseket kell hoznia a nem biztonsági funkciók számának minimalizálására a biztonsági funkciók határain belül.
4. A szervezetnek figyelembe kell vennie, hogy a nem biztonsági funkciók, amelyek az izolációs határon belül találhatók, biztonsági szempontból relevánsak, mert a szoftverben lévő hibák vagy rosszindulatú kódok közvetlenül befolyásolhatják az EIR biztonsági funkcióit.

5. A szervezetnek a tervezés során alapvető célkitűzése az kell legyen, hogy az EIR azon specifikus részei, amelyek az információbiztonságot biztosítják, minimális méretűek és összetettségűek legyenek.
6. A szervezetnek minimalizálnia kell a nem biztonsági funkciók számát az EIR biztonsági elemeiben, hogy a tervezők és implementálók csak azokra a funkciókra összpontosíthassanak, amelyek szükségesek a kívánt biztonsági képesség biztosításához.
7. A szervezetnek minimalizálnia kell a nem biztonsági funkciókat az izolációs határok belül, hogy jelentősen csökkentse a biztonsági szabályok végrehajtására megbízott kód mennyiségét, ezzel hozzájárulva az érthetőséghez.
8. A szervezetnek dokumentálnia kell a fent említett lépéseket, hogy nyomon követhető legyen a folyamat és a változások.

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

SC-3(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.8. BIZTONSÁGI FUNKCIÓK ELKÜLÖNÍTÉSE – MODULOK ÖSSZEKAPCSOLÁSA ÉS ÖSSZETARTÁSA

17.8. Az EIR a biztonsági funkciókat nagymértékben független modulokként valósítja meg, amelyek maximalizálják a modulokon belüli belső összhangot, és minimalizálják a modulok közötti összekapcsoltságot.

MAGYARÁZAT

A modulok közötti kölcsönhatások csökkentése segít a biztonsági funkciók korlátozásában és a komplexitás kezelésében. A szoftvertervezésben a modularitás szempontjából fontosak a csatolás és a kohézió fogalmai. A csatolás azokra a függőségekre utal, amelyekkel egy modul más moduloktól függ. A kohézió a modulon belüli funkciók közötti kapcsolatra utal. A szoftverfejlesztés és a rendszerbiztonsági tervezés legjobb gyakorlatai a komplexitás csökkentése és kezelése érdekében a rétegzésre, a minimalizálásra és a moduláris bontásra támaszkodnak. Ezáltal a szoftvermodulok nagymértékben koherensek és lazán összekapcsoltak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek el kell sajátítania a moduláris tervezés alapelveit, különösen a kapcsolódás és a koherencia fogalmait.
2. A szervezetnek a szoftvertervezés és a rendszer biztonsági tervezés legjobb gyakorlatait kell alkalmaznia, amelyek a rétegezésen, minimalizáláson és moduláris dekompozíción alapulnak a komplexitás kezelésére. Ez olyan szoftvermodulokat eredményez, amelyek nagymértékben koherensek és laza kapcsolatúak.
3. A szervezetnek meg kell terveznie és implementálnia kell az EIR biztonsági funkcióit úgy, hogy azok nagymértékben független modulokként működjenek. Ez azt jelenti, hogy minden modulnak saját, belső összhangban lévő funkciói vannak, és minimális a kapcsolatuk a többi modullal.
4. A szervezetnek dokumentálnia kell az EIR biztonsági funkcióinak megvalósítását és működését. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a modulok közötti összekapcsoltság minimalizálását és a modulokon belüli belső összhang maximalizálását.

5. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell az EIR biztonsági funkcióinak hatékonyságát, hogy biztosítsa a moduláris tervezés elveinek megfelelő működést.

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

SC-3(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.9. BIZTONSÁGI FUNKCIÓK ELKÜLÖNÍTÉSE – RÉTEGES SZERKEZETEK

17.9. A szervezet a biztonsági funkciókat többrétegű struktúraként valósítja meg, minimalizálva a tervezés rétegei közötti kölcsönhatásokat, és elkerülve, hogy az alsóbb rétegek függjenek a magasabb rétegek funkcionalitásától vagy helyességétől.

MAGYARÁZAT

A biztonsági funkciók és a nem hurokszerű rétegek közötti kölcsönhatások minimalizálása lehetővé teszi a biztonsági funkciók elkülönítését és a komplexitás kezelését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azon biztonsági funkciókat, amelyeket többrétegű struktúrában kíván megvalósítani.
2. A szervezetnek minimalizálnia kell a tervezési rétegek közötti kölcsönhatásokat. Ez azt jelenti, hogy a különböző biztonsági funkciók közötti kommunikációt és függőségeket a lehető legkisebbre kell csökkenteni.
3. A szervezetnek biztosítania kell, hogy az alsóbb rétegek ne függjenek a magasabb rétegek funkcionalitásától vagy helyességétől. Ez azt jelenti, hogy minden egyes biztonsági funkció önállóan, a többi funkciótól függetlenül képes legyen működni.
4. A szervezetnek naplóznia kell a biztonsági funkciók működését és az esetlegesen felmerülő problémákat. Ez segít azonosítani a potenciális gyengeségeket és lehetővé teszi a gyors reagálást a biztonsági eseményekre.

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

SC-3(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.10. INFORMÁCIÓK AZ OSZTOTT HASZNÁLATÚ RENDSZERERŐFORRÁSOKBAN

17.10. Az EIR meggátolja a megosztott erőforrásokon keresztül történő jogosulatlan vagy véletlen információátvitelt.

MAGYARÁZAT

Ez az intézkedés megakadályozza, hogy a korábbi felhasználók vagy szerepkörök által végzett tevékenységek információihoz (beleértve a titkosított információkat) hozzáférjenek a megosztott erőforrások (pl. regiszterek, memória, merevlemezek) jelenlegi felhasználói (vagy folyamatai), miután azokat az információs rendszer felszabadította. A megosztott erőforrásokban lévő információ ellenőrzését gyakran objektum-újrafelhasználásnak és maradvány információvédelemnek is nevezik. Ez az intézkedés nem foglalkozik a remanenciával (megmaradt állapot törlés után), amely a névlegesen törölt vagy eltávolított adatok fennmaradó maradvány reprezentációjára utal; a rejtett csatornákkal (beleértve a tárolási és/vagy időzítési csatornákat), ahol a megosztott erőforrásokat manipulálják az információáramlási korlátozások megsértése érdekében; továbbá nem foglalkozik olyan információs rendszereken belüli elemekkel, amelyekhez csak egyetlen felhasználó/szerepkör tartozik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell az EIR-ben használt összes megosztott erőforrást.
2. A szervezetnek be kell vezetnie szabályokat és eljárásokat, amelyek megakadályozzák az információ átadását a megosztott erőforrásokon keresztül, amikor azokat visszaadják az EIR-nek.
3. A szervezetnek biztosítania kell, hogy az EIR-ben tárolt információk, beleértve azok titkosított reprezentációit is, ne legyenek hozzáférhetőek a jelenlegi felhasználók vagy szerepkörök számára, miután az erőforrásokat visszaadták az EIR-nek.
4. A szervezetnek be kell vezetnie a naplózást, hogy nyomon követhesse az információáramlást és azonosíthassa a jogosulatlan hozzáférést vagy információátvitelt.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR biztonsági intézkedéseit, hogy biztosítsa azok hatékonyságát és relevanciáját.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

16.16. Biztonságtervezési elvek

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

3.3.13.4. Információmaradványok: Az elektronikus információs rendszer meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.11. Információk az osztott használatú rendszererőforrásokban – Többszintű vagy időszakos feldolgozás

17.11. Az EIR megakadályozza az engedély nélküli információátvitelt a megosztott erőforrásokon keresztül, a szervezet által meghatározott eljárásokat követve a különböző biztonsági besorolású információk vagy biztonsági osztályok között.

Magyarázat

A feldolgozási szintek változása többszintű vagy időszakos feldolgozás során fordulhat elő, különböző minősítési szinteken vagy biztonsági kategóriákban lévő információkkal. A különböző minősítési szinteken lévő hardverelemek sorozatos újrafelhasználása során is előfordulhat. Az érintett szervezet által meghatározott eljárások magukban foglalhatják az elektronikusan tárolt információk jóváhagyott tisztítási folyamatait.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia azokat az eljárásokat, amelyeket követni fog az információátvitel engedélyezése érdekében. Ezek az eljárások magukban foglalhatják a szanitizációs folyamatokat az elektronikusan tárolt információk számára.
2. Az EIR-nek képesnek kell lennie arra, hogy megakadályozza az engedély nélküli információátvitelt a megosztott erőforrásokon keresztül. Ez azt jelenti, hogy az EIR-nek rendelkeznie kell olyan biztonsági funkciókkal, amelyek képesek blokkolni vagy korlátozni az adatok átadását, ha az nem felel meg az érintett szervezet által meghatározott eljárásoknak.
3. Az EIR-nek képesnek kell lennie arra, hogy különbséget tegyen a különböző biztonsági besorolású információk vagy biztonsági osztályok között. Ez azt jelenti, hogy az EIR-nek rendelkeznie kell olyan funkciókkal, amelyek lehetővé teszik az adatok csoportosítását és szegmentálását biztonsági szintek szerint.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR működését, hogy biztosítsa, hogy az megfelelően működik-e és megakadályozza-e az engedély nélküli információátvitelt. Ez magában foglalhatja a naplók ellenőrzését és elemzését, hogy azonosítsa az esetleges szabálytalanságokat vagy 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

SC-4(2)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az eljárások meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.12. SZOLGÁLTATÁSMEGTAGADÁSSAL JÁRÓ TÁMADÁSOK ELLENI VÉDELEM

17.12. A szervezet:

17.12.1. védekezik a meghatározott szolgáltatásmegtagadással járó támadások ellen, vagy korlátozza azok hatásait; és

17.12.2. alkalmazza azokat a védelmi intézkedéseket, amelyek segítségével elérheti a szolgáltatásmegtagadással járó támadások elleni védekezés célját.

MAGYARÁZAT

A szolgáltatásmegtagadással járó események számos belső és külső ok miatt következhetnek be, például egy támadás vagy a szervezeti igények támogatására irányuló tervezés hiánya miatt a nem megfelelő szintű kapacitás és a sávszélesség miatt. Ilyen támadások a hálózati protokollok széles skáláján (pl. IPv4, IPv6. fordulhatnak elő. A szolgáltatásmegtagadással járó események keletkezésének és hatásainak korlátozására vagy kiküszöbölésére számos technológia áll rendelkezésre. A határvédelmi eszközök például képesek bizonyos típusú csomagok szűrésére, hogy megvédjék a belső hálózatok rendszerelemeit attól, hogy a szolgáltatásmegtagadással járó támadások közvetlenül érintsék őket, vagy ne legyenek a forrásuk. A megnövelt hálózati kapacitás és sávszélesség alkalmazása a szolgáltatás redundanciával kombinálva szintén csökkenti a szolgáltatásmegtagadással járó eseményekre való fogékonyságot.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell a lehetséges belső és külső okokat, amelyek szolgáltatásmegtagadással járó eseményeket okozhatnak.

2. A szervezetnek elemzést kell végeznie a hálózati protokollok széles skáláján, hogy felderítse, melyik lehet a leginkább kitett a szolgáltatásmegtagadással járó támadásokkal szemben.

3. A szervezetnek különböző technológiákat kell alkalmaznia a szolgáltatásmegtagadással járó események eredetének vagy hatásainak korlátozására vagy megszüntetésére. Például a határvédelmi eszközök képesek szűrni bizonyos típusú csomagokat, hogy megvédjék a

rendszerelemeit a belső hálózatokon a szolgáltatásmegtagadással járó támadások közvetlen hatásaitól vagy forrásaitól.

4. A szervezetnek növelnie kell a hálózati kapacitást és sávszélességet, és szolgáltatás redundanciát kell alkalmaznia, hogy csökkentse az EIR sebezhetőségét a szolgáltatásmegtagadással járó eseményekkel szemben.

5. A szervezetnek naplóznia kell a szolgáltatásmegtagadással járó támadásokat és a hozzájuk kapcsolódó védelmi intézkedéseket annak érdekében, hogy folyamatosan értékelje és javítsa a védelmi stratégiákat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

9.9.1. Biztonsági események kezelése

17.16. Erőforrások rendelkezésre állása

17.17. A határok védelme

17.111. Vezeték nélküli kapcsolat 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

SC-5

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

17.13. SZOLGÁLTATÁSMEGTAGADÁSSAL JÁRÓ TÁMADÁSOK ELLENI VÉDELEM – MÁS RENDSZEREK MEGTÁMADÁSÁNAK KORLÁTOZÁSA

17.13. A szervezet korlátozza az egyének képességét, hogy meghatározott szolgáltatásmegtagadással járó támadásokat indíthassanak más rendszerek ellen.

MAGYARÁZAT

Az egyének szolgáltatásmegtagadással járó támadások indítására való képességének korlátozása megköveteli, hogy az ilyen támadásokhoz általánosan használt mechanizmusok ne legyenek elérhetők. Az aggodalomra okot adó személyek közé tartoznak az ellenséges belső személyek vagy külső ellenfelek, akik behatoltak az EIR-be, vagy veszélyeztették azt, és azt szolgáltatásmegtagadással járó támadás indítására használják. A szervezetek korlátozhatják az egyének csatlakozási és tetszőleges információk továbbítási képességét a szállítóeszközön. A szervezetek korlátozhatják az egyének azon képességét is, hogy túlzott mértékben használják az EIR erőforrásait. A szolgáltatásmegtagadással járó támadások indítására képes egyének elleni védelem megvalósítható bizonyos EIR-eken vagy határeszközökön, amelyek megtiltják a potenciális célrendszerekbe való kilépést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és azonosítania kell azokat a mechanizmusokat, amelyeket a szolgáltatásmegtagadással járó támadások indítására általában használnak, ez magában foglalja a belső és külső fenyegetéseket is.
2. Az érintett szervezetnek korlátoznia kell az egyének képességét arra, hogy önkényesen csatlakozzanak és információt továbbítsanak a szállítási közegen.
3. A szervezetnek korlátoznia kell az egyének képességét arra, hogy túlzott mértékben használják az EIR erőforrásait.
4. A szervezetnek védelmet kell biztosítania az ellen, hogy az egyének képesek legyenek szolgáltatásmegtagadással járó támadásokat indítani. Ez a védelem lehet specifikus az EIR-re, vagy határeszközökre is kiterjedhet, amelyek megakadályozzák a kimenetet a potenciális célpont EIR-ek felé.

5. A szervezetnek naplót kell vezetnie az EIR erőforrásainak túlzott mértékű használatával kapcsolatos tevékenységekről, hogy nyomon követhesse a potenciális támadásokat és azok forrását.

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

SC-5(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szolgáltatásmegtagadással járó támadások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.14. SZOLGÁLTATÁSMEGTAGADÁSSAL JÁRÓ TÁMADÁSOK ELLENI VÉDELEM – KAPACITÁS, SÁVSZÉLESSÉG, REDUNDANCIA

17.14. A szervezet kezeli a kapacitásokat, sávszélességeket, egyéb redundanciákat, hogy korlátozza az információs elárasztás által okozott szolgáltatásmegtagadással járó támadások hatásait.

MAGYARÁZAT

A többletkapacitás kezelése biztosítja, hogy elegendő kapacitás álljon rendelkezésre az információs elárasztás által okozott szolgáltatásmegtagadással járó támadások ellen. A többletkapacitás kezelése magában foglalhatja például a prioritások, kvóták, partíciók vagy terheléselosztás körültekintő kiválasztását és létrehozatalát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a kapacitásokat, sávszélességeket és egyéb redundanciákat, amelyeket kezelni kell. Ez magában foglalja a prioritások, kvóták, partíciók vagy terheléselosztás meghatározását.
2. A szervezetnek meg kell terveznie és implementálnia kell egy kapacitáskezelési stratégiát, amely képes korlátozni az információs elárasztás által okozott szolgáltatásmegtagadással járó támadások hatásait. Ez magában foglalja a kapacitások, sávszélességek és redundanciák monitorozását és szabályozását.
3. A szervezetnek rendszeresen ellenőriznie kell az EIR teljesítményét és kapacitását, hogy időben észlelje a potenciális problémákat és megelőzze a szolgáltatásmegtagadással járó támadásokat.
4. A szervezetnek naplózásra és jelentések készítésére van szüksége, hogy nyomon követhesse az EIR kapacitásának változásait és az esetleges támadásokat. A naplók segítenek azonosítani a rendszeres mintázatokat és a rendellenes viselkedést, ami lehetővé teszi a szervezet számára, hogy gyorsan reagáljon a potenciális fenyegetésekre.

5. Az érintett szervezetnek rendszeres időközönként felül kell vizsgálnia és frissítenie kell a kapacitáskezelési stratégiáját, hogy biztosítsa az EIR hatékony működését és védelmét a szolgáltatásmegtagadással járó támadásokkal szemben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.13.5. Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem: Az elektronikus információs rendszer véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

ISO/IEC 27001:2023 REFERENCIA

A.8.6

NIST SP 800-53 REV.5 REFERENCIA

SC-5(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.15. SZOLGÁLTATÁSMEGTAGADÁSSAL JÁRÓ TÁMADÁSOK ELLENI VÉDELEM – ÉSZLELÉS ÉS FELÜGYELET

17.15. A szervezet:

17.15.1. Olyan, a szervezet által meghatározott felügyeleti eszközöket alkalmaz, amelyek képesek észlelni az EIR ellen vagy az EIR-ből kezdeményezett szolgáltatásmegtagadással járó támadások jeleit.

17.15.2. Figyelemmel kíséri a meghatározott EIR erőforrásait annak megállapítása érdekében, hogy megbizonyosodjon arról, hogy elegendő erőforrás áll-e rendelkezésre a hatékony szolgáltatásmegtagadással járó támadások megakadályozásához.

MAGYARÁZAT

Az érintett szervezetek figyelembe veszik az EIR erőforrásainak kihasználtságát és kapacitását, amikor a rosszindulatú támadások miatti szolgáltatásmegtagadással kapcsolatos kockázatot kezelik. A szolgáltatásmegtagadással járó támadások származhatnak külső vagy belső forrásokból. A szolgáltatásmegtagadással szemben érzékeny rendszererőforrások közé tartozik a fizikai lemeztárolás, a memória és a CPU-ciklusok. A tárolókihasználtsággal és -kapacitással kapcsolatos szolgáltatásmegtagadással járó támadások megelőzésére használt technikák közé tartozik a lemezkvóták bevezetése, az EIR-ek konfigurálása a rendszergazdák automatikus figyelmeztetésére, amikor bizonyos tárolókapacitási küszöbértékeket elérnek, fájltömörítési technológiák alkalmazása a rendelkezésre álló tárolóterület maximalizálása érdekében, valamint külön partíciók létrehozása az EIR és a felhasználói adatok számára.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek figyelembe kell vennie az EIR erőforrásainak felhasználását és kapacitását, amikor a rosszindulatú támadások miatti szolgáltatásmegtagadással járó kockázatot kezeli. A szolgáltatásmegtagadással járó támadások az EIR-ből vagy az EIR ellen indulhatnak. Az EIR erőforrásai, amelyek érzékenyek a szolgáltatásmegtagadásra, a fizikai lemez tároló, a memória és a CPU ciklusok.

2. A szervezetnek biztosítania kell szolgáltatásmegtagadással járó támadások megelőzésére használt technikákat, amelyek közé tartozik a lemezkvóták bevezetése, az EIR konfigurálása

úgy, hogy automatikusan figyelmeztetést küldjön az adminisztrátoroknak, amikor elérnek bizonyos tárolókapacitás-küszöböket, a fájltömörítési technológiák használata a rendelkezésre álló tárolóhely maximalizálása érdekében, és külön partíciók beállítása az EIR és a felhasználói adatok számára.

3. A szervezetnek olyan felügyeleti eszközöket kell alkalmaznia, amelyek képesek észlelni a szolgáltatásmegtagadással járó támadások jeleit. Ezenkívül figyelemmel kell kísérnie a meghatározott EIR erőforrásait annak megállapítása érdekében, hogy elegendő erőforrás áll-e rendelkezésre a szolgáltatásmegtagadással járó támadások megakadályozásához.

4. A szervezetnek biztosítania kell a naplózást, mert fontos szerepe lehet a szolgáltatásmegtagadással járó támadások észlelésében és megelőzésében. A naplók segíthetnek azonosítani a szokatlan vagy gyanús tevékenységeket, amelyek a szolgáltatásmegtagadás jelei lehetnek.

Kapcsolódó intézkedések

5.14. Folyamatos felügyelet

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

SC-5(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.16. ERŐFORRÁSOK RENDELKEZÉSRE ÁLLÁSA

17.16. A szervezet úgy védi erőforrásainak rendelkezésre állását, hogy a szervezet által meghatározott erőforrásokat prioritás, kvóta vagy a szervezet által meghatározott egyéb követelmények alapján osztja szét.

MAGYARÁZAT

Az érintett szervezet prioritási védelmet alkalmaz, amely megakadályozza, hogy az alacsonyabb prioritású folyamatok késleltessék vagy zavarják az EIR-t, amely a magasabb prioritású folyamatokat szolgál ki. A kvóták megakadályozzák, hogy a felhasználók vagy folyamatok meghatározott mennyiségűnél több erőforrást szerezzenek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat az erőforrásokat, amelyeket védeni kíván. Ez magában foglalhatja az EIR-eket, a hálózati eszközöket, a szervereket, az adatbázisokat stb.
2. A szervezetnek prioritási rendszert kell kialakítania az erőforrásokhoz. Azaz meg kell határoznia, mely felhasználók, folyamatok vagy tevékenységek rendelkeznek elsőbbséggel az erőforrásokhoz való hozzáférésben.
3. A szervezetnek kvótákat kell beállítania az erőforrásokhoz. Meg kell határoznia, hogy mennyi erőforrást használhat egy adott felhasználó, folyamat vagy tevékenység egy adott időszakban.
4. A szervezetnek, amennyiben szükséges további követelményeket kell bevezetnie az erőforrások elosztására, például a hozzáférési szintek, a felhasználói jogosultságok vagy a biztonsági protokollok meghatározását.
5. A szervezetnek naplót kell vezetnie az erőforrások használatáról.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az erőforrások elosztásának szabályát, hogy biztosítsa az erőforrások hatékony és biztonságos használatát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.12. Szolgáltatásmegtagadással járó támadások 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

SC-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az erőforrások, illetve a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.17. A HATÁROK VÉDELME

17.17. A szervezet:

17.17.1. Ellenőrzi a kommunikációt a menedzselt külső interfészein, valamint a rendszer kulcsfontosságú menedzselt belső interfészein.

17.17.2. A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól.

17.17.3. Csak a szervezet biztonsági architektúrájával összhangban lévő határvédelmi eszközökön keresztül, menedzselt interfészek segítségével kapcsolódik külső hálózatokhoz vagy külső EIR-ekhez.

MAGYARÁZAT

A menedzselt interfészek közé tartoznak például az átjárók, a routerek, a tűzfalak, a hálózati alapú kártékony kódot elemző és virtualizációs rendszerek, vagy a biztonsági architektúrában megvalósított titkosított alagutak (például a tűzfalakat védő routerek vagy a védett alhálózatokon működő alkalmazás-átjárók). A belső hálózatoktól fizikailag vagy logikailag elválasztott alhálózatokat demilitarizált zónáknak, vagy DMZ-knek nevezzük. A szervezeti EIR-eken belüli interfészek korlátozása vagy tiltása magában foglalja például a külső webes forgalom kijelölt webszerverekre történő korlátozását a felügyelt interfészeken belül, és az olyan külső forgalom tiltását, amely hamisítottnak tűnő címet használ. Az érintett szervezetek figyelembe veszik a kereskedelmi távközlési szolgáltatások megosztott jellegét az ilyen szolgáltatások használatával kapcsolatos biztonsági intézkedések végrehajtásakor. Ezek a szolgáltatások tartalmazhatnak harmadik fél által biztosított hozzáférési vonalakat és egyéb szolgáltatási elemeket is. Az ilyen szolgáltatások a szerződéses biztonsági rendelkezések ellenére fokozott kockázatot jelenthetnek. A határvédelem közös intézkedésként lehet implementálva a szervezet hálózatának egészére vagy egy részére, így a védelmet igénylő határ nagyobb, mint egy EIR-specifikus határ (azaz egy engedélyezési határ).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ellenőriznie kell a kommunikációt a menedzselt külső interfészein és az EIR kulcsfontosságú menedzselt belső interfészein.
2. A szervezetnek biztosítania kell a nyilvánosan hozzáférhető rendszerelemek elhelyezését fizikailag vagy logikailag elkülönített alhálózatokban, amelyeket demilitarizált zónáknak neveznek. Ezek az alhálózatok elkülönülnek a belső hálózattól.
3. A szervezetnek biztosítania kell a a külső hálózatokhoz vagy külső EIR-ekhez történő kapcsolódást menedzselt interfészek segítségével a biztonsági architektúrájával összhangban lévő határvédelmi eszközökön keresztül. Korlátoznia kell vagy letiltania kell az interfészeket az EIR-jében, le kell tiltania a külső forgalmat, amely úgy tűnik, hogy hamisítja a belső címeket, és a belső forgalmat is tiltania kell, abban az esetben, ha úgy tűnik, hogy hamisítja a külső címeket.
4. A szervezetnek naplóznia kell a kommunikációt és az eseményeket a menedzselt interfészekben és az EIR-ben, a kiberbiztonsági események nyomon követése és elemzése érdekében.
5. A szervezetnek kockázatelemzést kell végeznie a harmadik féltől származó szolgáltatásokra, mint például a hozzáférési vonalakra és egyéb szolgáltatási elemekre, amelyek növelhetik a kockázatot.
6. A szervezetnek lehetősége van határvédelmet, mint közös intézkedést implementálni a hálózatának egészére vagy részére, így a védendő határ nagyobb lesz, mint egy EIR-specifikus határ.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.28. Információáramlási szabályok érvényesítése
2.100. Távoli hozzáférés
2.108. Vezeték nélküli hozzáférés
2.113. Mobil eszközök hozzáférés-ellenőrzése
2.115. Külső elektronikus információs rendszerek használata
4.44. Információk kiszivárgásának figyelemmel kísérése
5.6. Információcsere
6.2. Alapkonfiguráció

6.15. Biztonsági hatásvizsgálatok

6.26. Legszűkebb funkcionalitás

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

3.3.13.6. A határok védelme

ISO/IEC 27001:2023 REFERENCIA

A.5.14; A.8.16; A.8.20; A.8.22; A.8.23

NIST SP 800-53 REV.5 REFERENCIA

SC-7

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

17.18. A HATÁROK VÉDELME – HOZZÁFÉRÉSI PONTOK

17.18. A szervezet korlátozza az EIR külső hálózati kapcsolatainak számát.

MAGYARÁZAT

A külső hálózati kapcsolatok számának korlátozása megkönnyíti a bejövő és kimenő kommunikációs forgalom felügyeletét. A külső hálózati kapcsolatok számának korlátozása fontos a régebbi technológiákról az újabbakra való áttérés időszakában (pl. az IPv4-ről az IPv6 hálózati protokollokra való áttérés). Az ilyen átmenetek szükségessé tehetik a régebbi és az újabb technológiák egyidejű bevezetését az átmeneti időszak alatt, és ezáltal növelhetik az EIR-hez való hozzáférési pontok számát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek felül kell vizsgálnia az EIR külső hálózati kapcsolatainak jelenlegi számát és típusát. Ez magában foglalja a fizikai és a logikai kapcsolatokat is.
2. A szervezetnek meg kell határoznia, hogy mely külső hálózati kapcsolatok szükségesek az EIR működéséhez.
3. A szervezetnek meg kell terveznie és végre kell hajtania egy stratégiát a nem szükséges külső hálózati kapcsolatok megszüntetésére. Ez magában foglalhatja a kapcsolatok fizikai megszüntetését, a kapcsolatok logikai megszüntetését, vagy a kapcsolatok biztonsági szintjének növelését.
4. A szervezetnek naplózási és monitorozási rendszert kell alkalmaznia, hogy nyomon követhesse az EIR külső hálózati kapcsolatainak használatát.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a külső hálózati kapcsolatokra vonatkozó szabályait és eljárásait, hogy biztosítsa azok relevanciáját és hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.13.6. A határok védelme

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-7(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.19. A HATÁROK VÉDELME – KÜLSŐ INFOKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK

17.19. A szervezet:

17.19.1. Menedzselt interfészt alkalmaz minden külső infokommunikációs szolgáltatáshoz.

17.19.2. Minden menedzselt interfészhez forgalomáramlási szabályokat alakít ki.

17.19.3. Védi az egyes interfészeken átvitelre kerülő információk bizalmasságát és sértetlenségét.

17.19.4. Dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó működési céllal vagy üzleti igénnyel, valamint az igényelt kivétel időtartamával együtt.

17.19.5. Meghatározott gyakorisággal felülvizsgálja a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket nem támogat valamilyen működési cél vagy üzleti igény.

17.19.6. Megakadályozza a nem engedélyezett vezérlőadat-forgalom (control plane traffic) cseréjét a külső hálózatokkal.

17.19.7. Közzéteszi azokat az információkat, amelyek lehetővé teszik a távoli hálózatok számára a nem engedélyezett vezérlőadat-forgalom (control plane traffic) észlelését a belső hálózatokból.

17.19.8. Szűri a nem engedélyezett vezérlőadat-forgalmat a külső hálózatokból.

MAGYARÁZAT

Az érintett szervezet megakadályozza a nem engedélyezett vezérlőadat-forgalom (control plane traffic) (vezérlőadat forgalmára példa: BGP, DNS és kezelési protokollok) cseréjét a külső hálózatokkal. Ez azt jelenti, hogy az EIR blokkolja azokat az adatokat, amelyeket nem szabadna átvinni a külső hálózatokra.

Az érintett szervezet közzéteszi azokat az információkat, amelyek lehetővé teszik a távoli hálózatok számára a nem engedélyezett vezérlőadat-forgalom (control plane traffic) észlelését a belső hálózatokból. Ez azt jelenti, hogy az EIR megosztja azokat az információkat, amelyek segítenek a külső hálózatoknak észlelni a nem engedélyezett adatforgalmat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek menedzselt interfészt kell alkalmaznia minden külső infokommunikációs szolgáltatáshoz.
2. A szervezetnek minden menedzselt interfészhez forgalomáramlási szabályokat kell kialakítania.
3. A szervezetnek védenie kell az egyes interfészeken átvitelre kerülő információk bizalmasságát és sértetlenségét. Ez azt jelenti, hogy az adatokat titkosítani kell, és biztosítani kell, hogy azokat nem manipulálják vagy módosítják a küldés során.
4. A szervezetnek dokumentálnia kell minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó működési céllal vagy üzleti igénnyel, valamint az igényelt kivétel időtartamával együtt. Más szóval, minden kivételt rögzíteni kell, és indokolni kell, miért van rá szükség.
5. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia a forgalomáramlási szabályok alóli kivételeket, és eltávolítani azokat a kivételeket, amelyeket nem támogat valamilyen működési cél vagy üzleti igény.
6. A szervezetnek blokkolni kell minden olyan adatforgalmat, amely nem engedélyezett.
7. A szervezetnek közzé kell tennie azokat az információkat, amelyek segítségével a távoli hálózatok észlelhetik (control plane traffic) a nem engedélyezett adatforgalmat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

17.40. Az adatátvitel bizalmassága és sértetlensége

17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

17.71. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)

17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

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

3.3.13.6. A határok védelme

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-7(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.20. A HATÁROK VÉDELME – ALAPÉRTELMEZÉS SZERINTI ELUTASÍTÁS ÉS KIVÉTEL ALAPÚ ENGEDÉLYEZÉS

17.20. Az EIR alapértelmezés szerint elutasítja a hálózati kommunikációs forgalmat, és csak kivételként engedélyezi azt a menedzselt interfészeknél.

MAGYARÁZAT

Az EIR menedzselt interfészek esetén alapértelmezés szerint megtagadja és kivételek alapján engedélyezi a bejövő és kimenő hálózati kommunikációs forgalmat. Az alapértelmezés szerinti elutasítás és a kivétel alapú engedélyezés elve biztosítja, hogy csak azok a kapcsolatok legyenek engedélyezve, amelyek elengedhetetlenek és jóváhagyottak. Ezt az alapértelmezés szerinti elutasítást és kivétel alapú engedélyezést a külső EIR-hez csatlakozó EIR-ek esetén is alkalmazni kell.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell állítania az EIR-t úgy, hogy alapértelmezés szerint elutasítsa a bejövő és kimenő hálózati kommunikációs forgalmat, kivéve, ha kifejezetten engedélyezett.
2. A szervezetnek meg kell határoznia és jóvá kell hagynia azokat a kapcsolatokat, amelyek létfontosságúak és szükségesek az EIR működéséhez.
3. A szervezetnek alkalmaznia kell ezt a szabályt az EIR-re is, amely külső rendszerhez csatlakozik. Ez azt jelenti, hogy az EIR alapértelmezés szerint elutasítja a külső rendszertől érkező hálózati kommunikációt, és csak kivételként engedélyezi azt.
4. A szervezetnek naplót kell vezetnie az EIR hálózati kommunikációs forgalmáról. Ez a napló segít a szervezetnek nyomon követni és ellenőrizni az EIR hálózati kommunikációs forgalmát, és biztosítja, hogy csak a jóváhagyott és szükséges kapcsolatok legyenek engedélyezve.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.13.6. A határok védelme

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-7(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.21. A HATÁROK VÉDELME – MEGOSZTOTT CSATORNAHASZNÁLAT TÁVOLI ESZKÖZÖK ESETÉN

17.21. Az EIR megakadályozza a megosztott csatornahasználatot az EIR-ekhez csatlakozó távoli eszközök számára, kivéve, ha a megosztott csatornát biztonságosan konfigurálják a szervezet által meghatározott védelmi intézkedések használatával.

MAGYARÁZAT

Az EIR a távoli eszközök számára megakadályozza, hogy az eszköz egyidejűleg távoli kapcsolatot hozzon létre egy EIR-rel és egyidejűleg egyéb kapcsolat révén kommunikáljon külső hálózatok erőforrásaival.

Ez az intézkedés a távoli eszközökön valósul meg a konfigurációs beállítások segítségével, amelyekkel letiltja a megosztott csatornákat (split tunneling) és megakadályozza, hogy ezek a konfigurációs beállítások könnyen módosíthatók legyenek a felhasználók számára. Ez az intézkedés az EIR-en belül a megosztott csatornák (vagy a megosztott csatornákat lehetővé tevő konfigurációs beállítások) észlelésével valósul meg a távoli eszközön, és tiltja a kapcsolatot, ha a távoli eszköz megosztott csatornákat használ. A megosztott csatornák a távoli felhasználók számára a helyi EIR erőforrásaival, például a nyomtatókkal/fájlszerverekkel való kommunikációhoz hasznosak, azonban a megosztott csatornák lehetővé teszik a jogosulatlan külső kapcsolatokat is, így az EIR sérülékenyebbé válik a támadásokkal - és a szervezeti információk kiszivárgásával szemben. A VPN-ek távoli kapcsolatra való használata - amennyiben megfelelő biztonsági intézkedésekkel rendelkeznek - elegendő biztosítékot nyújthat az érintett szervezetnek, hogy bizalmassági és sértetlenségi szempontokból hatékonyan kezelhesse az ilyen kapcsolatokat nem távoli kapcsolatként. Egy virtuális magánhálózat (VPN) használható a megosztott csatorna biztonságos biztosításához. A biztonságosan biztosított VPN magában foglalja a kizárólagos, menedzselt és nevesített környezetekhez vagy az előre jóváhagyott címek meghatározott csoportjához való csatlakozás lezárását, felhasználói felügyelete nélkül. A VPN-ek tehát távoli eszközök számára teszik lehetővé a hálózathoz való biztonságos csatlakozást. A megfelelően kialakított VPN használata nem szünteti meg a megosztott csatornák megelőzésének szükségességét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely távoli eszközök csatlakozhatnak az EIR-ekhez.
2. A szervezetnek meg kell akadályoznia a megosztott csatorna használatát az EIR-ekhez csatlakozó távoli eszközök számára. Ez megvalósítható a konfigurációs beállítások letiltásával, amelyek lehetővé teszik ezt a képességet a távoli eszközökben, és megakadályozza, hogy ezek a konfigurációs beállítások a felhasználók által konfigurálhatók legyenek.
3. A szervezetnek meg kell határoznia a védelmi intézkedéseket, amelyeket a megosztott csatorna biztonságos konfigurálásához használnak.
4. A szervezetnek csak akkor kell engedélyeznie a megosztott csatorna használatát, ha azt biztonságosan konfigurálják a szervezet által meghatározott védelmi intézkedések használatával.
5. A szervezetnek ellenőriznie kell, hogy a távoli eszközök használják-e a megosztott csatornát, és meg kell tiltania a kapcsolatot, ha a távoli eszköz megosztott csatornát használ.
6. A szervezetnek virtuális privát hálózatot (VPN) kell használnia a megosztott csatorna biztonságos használatának biztosítása érdekében. A biztonságosan előkészített VPN magában foglalja a kapcsolat zárolását kizárólagos, menedzselt és megnevezett környezetekhez, vagy egy adott, előzetesen jóváhagyott címekhez, a felhasználói felügyelet nélkül.
7. A szervezetnek naplót kell vezetnie a megosztott csatorna használatáról és dokumentálnia kell a védelmi intézkedések alkalmazását, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.13.6. A határok védelme

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-7(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a védelmi intézkedések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.22. A HATÁROK VÉDELME – A FORGALOM ÁTIRÁNYÍTÁSA HITELESÍTETT PROXYKISZOLGÁLÓKRA

17.22. Az EIR a meghatározott belső kommunikációs forgalmat a meghatározott külső hálózatok felé a menedzselt interfészeken lévő hitelesített proxykiszolgálókon keresztül irányítja.

MAGYARÁZAT

A külső hálózatok a szervezeti ellenőrzésen kívül esnek. A proxykiszolgáló olyan szerver, amely közvetítő szerepet tölt be az EIR erőforrásait (például fájlokat, kapcsolatokat, weboldalakat vagy szolgáltatásokat) kérő kliensek és más szervezetek szerverei között. A proxy szerverhez való kezdeti kapcsolat során létrehozott kliens kérelmeket értékelik a bonyolultság kezelése érdekében és további védelmet biztosítanak a közvetlen kapcsolatok korlátozásával. A webtartalom szűrők a leggyakoribb proxykiszolgálók, amelyekkel hozzáférést biztosíthatunk az internethez. A proxy szerverek támogatják a TCP kapcsolatok naplózását és az URL-ek, domainnevek és IP címek blokkolását. A webes proxyk beállíthatók az érintett szervezet által, engedélyezett és tiltott webhelyek listájával.

A proxykiszolgálók gátolhatják a VPN használatát, és (a megvalósítástól függően) man-in-the-middle támadások lehetőségét teremthetik meg.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a belső kommunikációs forgalmat, amelyet a külső hálózatok felé irányítani kíván.
2. A szervezetnek meg kell határoznia a menedzselt interfészeket, amelyeken keresztül a kommunikációs forgalmat irányítani fogja.
3. A szervezetnek proxykiszolgálókat kell telepítenie és konfigurálnia a menedzselt interfészekre. Ezek a proxykiszolgálók felelnek majd a belső kommunikációs forgalom külső hálózatok felé történő irányításáért.
4. A szervezetnek hitelesítési mechanizmusokat kell beállítania a proxykiszolgálókon, hogy csak a hitelesített forgalom haladhasson át rajtuk.

5. A szervezetnek naplózási mechanizmusokat kell beállítania a proxykiszolgálókon, hogy nyomon követhető legyen a rajtuk áthaladó forgalom.
6. A szervezetnek biztosítania kell, hogy a proxykiszolgálók konfigurációja megfeleljen a szervezet kiberbiztonsági politikájának / szabályainak és követelményeinek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

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

3.3.13.6. A határok védelme

ISO/IEC 27001:2023 REFERENCIA

A.8.23

NIST SP 800-53 REV.5 REFERENCIA

SC-7(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a belső kommunikációs forgalom illetve a külső hálózatok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.23. A HATÁROK VÉDELME – KORLÁTOZZA A FENYEGETŐ KIMENŐ KOMMUNIKÁCIÓS FORGALMAT

17.23. Az EIR:

17.23.1. észleli és megtagadja a kimenő kommunikációs forgalmat, amely fenyegetést jelent a külső rendszerek számára; és

17.23.2. ellenőrzi a megtagadott kommunikációval kapcsolatos belső felhasználók személyazonosságát.

MAGYARÁZAT

A külső EIR-eket fenyegető, belső műveletekből származó kimenő kommunikációs forgalom észlelését extrúzióérzékelésnek nevezik. Az extrúzióérzékelés az EIR-en belül, a menedzselt interfészeken történik. Az extrúzióérzékelés magában foglalja a bejövő és kimenő kommunikációs forgalom elemzését, miközben a külső EIR-ek biztonságát fenyegető belső fenyegetésekre utaló jelek után kutat. A külső EIR-eket fenyegető belső fenyegetések közé tartozik a szolgáltatásmegtagadással járó támadásokra utaló forgalom, a hamisított forráscímekkel rendelkező forgalom és a rosszindulatú kódot tartalmazó forgalom. Az érintett szervezeteknek kritériumokkal kell rendelkezniük az azonosított fenyegetések meghatározásához, frissítéséhez és kezeléséhez, amelyek az extrúzióérzékeléshez kapcsolódnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek implementálnia kell egy extrusion detection rendszert az EIR-en belül. Ez a rendszer képes lesz észlelni a kimenő kommunikációs forgalmat, amely fenyegetést jelent a külső rendszerek számára.
2. A szervezetnek meg kell határoznia a kritériumokat, amelyek alapján az EIR azonosítja és megtagadja a potenciálisan káros kimenő kommunikációt.
3. A szervezetnek rendszeresen frissítenie és kezelnie kell ezeket a kritériumokat, hogy az EIR mindig naprakész legyen a legújabb fenyegetésekkel szemben.
4. Az EIR-nek képesnek kell lennie a megtagadott kommunikációval kapcsolatos belső felhasználók személyazonosságának ellenőrzésére. Ez azt jelenti, hogy az érintett szervezetnek

implementálnia kell egy olyan rendszert, amely képes azonosítani és naplózni a káros kommunikációt kezdeményező felhasználókat.

5. A szervezetnek rendszeresen ellenőriznie kell az EIR naplóit, hogy azonosítsa a potenciális biztonsági réseket, és szükség esetén frissítse a kritériumokat és az EIR-t.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

17.12. Szolgáltatásmegtagadással járó támadások elleni védelem

17.107. Működésbiztonság

17.122. Izolált futtatási környezetek

18.8. Kártékony kódok elleni védelem

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

SC-7(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.24. A HATÁROK VÉDELME – INFORMÁCIÓ KISZIVÁRGÁSÁNAK MEGAKADÁLYOZÁSA

17.24. A szervezet:

17.24.1. megakadályozza az információk kiszivárgását, és

17.24.2. meghatározott gyakorisággal információszivárgási teszteket hajt végre.

MAGYARÁZAT

A kiszivárgás megakadályozása az információk szándékos és nem szándékos kiszivárgására egyaránt vonatkozik. Az EIR-ekből történő információ kiszivárgás megakadályozására alkalmazott technikák a belső végpontokon, a külső határokon és a menedzselt interfészeken keresztül valósíthatók meg, és magukban foglalják a protokollformátumok betartását, az EIR-ek jelzőtevékenységének nyomon követését, a külső hálózati interfészek lekapcsolását, kivéve, ha kifejezetten szükséges, a forgalmi profilelemzés alkalmazását a várt forgalom mennyiségétől és típusától való eltérések észlelésére, az irányító központok visszahívását, behatolásvizsgálatok elvégzését, a steganográfia nyomon követését, a csomagcímek szét- és újra összerakását, valamint az adatvesztés és adatszivárgás megelőzésére szolgáló eszközök használatát. A protokollformátumok szigorú betartását kikényszerítő eszközök közé tartoznak a mély csomagvizsgálatot végző tűzfalak és az XML (Extensible Markup Language) átjárók. Ezek az eszközök az alkalmazási rétegben ellenőrzik a protokollformátumok és specifikációk betartását, és azonosítják azokat a sebezhetőségeket, amelyeket a hálózati vagy szállítási rétegben működő eszközök nem tudnak felismerni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell akadályoznia az információk szándékos és nem szándékos kiszivárgását. Ezt belső végpontokon, külső határokon és menedzselt interfészeken keresztül lehet megvalósítani.

2. A szervezetnek be kell tartania a protokoll formátumokat, és figyelnie kell az EIR-ből származó jelző tevékenységeket.

3. A szervezetnek le kell kapcsolnia a külső hálózati interfészeket, kivéve, ha azokat kifejezetten szükséges használni.

4. A szervezetnek forgalmi profil elemzést kell végeznie a várható forgalomtípusok és mennyiség eltéréseinek észlelésére.

5. A szervezetnek felül kell vizsgálnia a behatolásvédelmi teszteket.

6. A szervezetnek figyelnie kell a steganográfiát, szét kell szednie és újra össze kell állítania a csomagfejléceket, és használnia kell az adatvesztés és adatszivárgás megelőzési eszközöket.

7. Az érintett szervezetnek olyan eszközöket kell használnia, amelyek szigorúan betartják a protokoll formátumokat. Ezek az eszközök ellenőrzik a protokoll formátumok és specifikációk betartását az alkalmazásrétegen, és azonosítják azokat a sebezhetőségeket, amelyeket a hálózati vagy transzportrétegen működő eszközök nem tudnak észlelni.

8. A szervezetnek meghatározott gyakorisággal információszivárgási teszteket kell végrehajtania.

Kapcsolódó intézkedések

2.2. Fiókkezelés

5.20. Behatolásvizsgálat (penetration testing)

18.8. Kártékony kódok elleni védelem

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.8.12

NIST SP 800-53 rev.5 referencia

SC-7(10)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.25. A HATÁROK VÉDELME – A BEJÖVŐ KOMMUNIKÁCIÓS FORGALOM KORLÁTOZÁSA

17.25. Az EIR csak a szervezet által meghatározott, engedélyezett forrásokból származó bejövő adatforgalmat továbbítja a szervezet által meghatározott, engedélyezett célpontok felé.

MAGYARÁZAT

Általános forráscím-érvényesítési technikákat alkalmaznak az illegális és ki nem osztott forráscímek, valamint a csak az EIR-en belül használható forráscímek használatának korlátozására. A bejövő kommunikációs forgalom korlátozása biztosítja annak megállapítását, hogy a forrás- és célcím-párok engedélyezettek vagy engedélyezett kommunikációt képviselnek. A meghatározás több tényezőn alapulhat, beleértve az ilyen címpárok jelenlétét az engedélyezett vagy megengedett kommunikáció listáin, az ilyen címpárok hiányát a nem engedélyezett vagy tiltott címpárok listáin, vagy az engedélyezett vagy megengedett forrás- és célállomáspárokra vonatkozó általánosabb szabályoknak való megfelelést. A hálózati címek erős hitelesítése nem lehetséges kifejezett biztonsági protokollok használata nélkül, ezért a címek gyakran hamisíthatók. Továbbá, a bejövő forgalom korlátozására azonosítás-alapú módszerek is alkalmazhatók, beleértve a router hozzáférés-felügyeleti listáit és a tűzfalszabályokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek alkalmaznia kell általános cím megerősítési technikákat, hogy korlátozza az illegális és nem kiosztott forráscímek használatát, valamint azokat a forráscímeket, amelyeket csak az EIR-en belül kellene használni.
2. A szervezetnek korlátoznia kell a bejövő kommunikációs forgalmat, hogy meghatározza, hogy a forrás- és cél címpárok engedélyezettek vagy megengedett kommunikációkat képviselnek-e. Az azonosítások több tényezőn alapulhatnak, beleértve a címpárok jelenlétét az engedélyezett vagy megengedett kommunikációk listájában, a címpárok hiányát a nem engedélyezett vagy tiltott párok listájában, vagy általánosabb szabályoknak való megfelelést az engedélyezett vagy megengedett forrás- és cél címpárokra vonatkozóan.

3. A szervezetnek alkalmaznia kell azonosításon alapuló bejövő forgalom korlátozási módszereket, beleértve a router hozzáférési listákat és a tűzfalszabályokat.
4. A szervezetnek naplóznia kell a nyomon követhetőség és ellenőrizhetőség érdekében az EIR-en belüli tevékenységeket, és biztosítsa, hogy csak a meghatározott, engedélyezett forrásokból származó bejövő adatforgalmat továbbítsa a meghatározott, engedélyezett célpontok felé.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés 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

SC-7(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az engedélyezett források illetve az engedélyezett célpontok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.26. A HATÁROK VÉDELME – HOSZTALAPÚ VÉDELEM

17.26. A szervezet az általa meghatározott hosztalapú határvédelmi mechanizmusokat megvalósítja a meghatározott rendszerelemeken.

MAGYARÁZAT

A hosztalapú határvédelmi mechanizmusok közé tartoznak a hosztalapú tűzfalak. A hosztalapú határvédelmi mechanizmusokat alkalmazó rendszerelemek közé tartoznak a szerverek, munkaállomások, laptopok/notebookok és mobil eszközök.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a hosztalapú határvédelmi mechanizmusokat, amelyeket alkalmazni kíván. Ezek a mechanizmusok magukban foglalhatják a hosztalapú tűzfalakat, intrusion detection rendszereket, intrusion prevention rendszereket (IPS) és egyéb biztonsági eszközöket.
2. A szervezetnek meg kell határoznia, mely rendszerelemeken kívánja ezeket a mechanizmusokat alkalmazni ezek lehetnek a szerverek, munkaállomások, laptopok.
3. A szervezetnek implementálnia kell a kiválasztott hosztalapú határvédelmi mechanizmusokat a rendszerelemeken. Ez magában foglalhatja a szoftver telepítését, konfigurálását és tesztelését.
4. A szervezetnek naplóznia és monitoroznia kell a hosztalapú határvédelmi mechanizmusok működését és hatékonyságát. Ez magában foglalhatja a naplófájlok rendszeres felülvizsgálatát és a rendszeres biztonsági auditokat.

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

SC-7(12)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hosztalapú határvédelmi mechanizmusok, illetve a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.27. A HATÁROK VÉDELME – A BIZTONSÁGI ESZKÖZÖK, MECHANIZMUSOK ÉS TÁMOGATÓ RENDSZERELEMEK ELKÜLÖNÍTÉSE

17.27. A szervezet az általa meghatározott információbiztonsági eszközöket, mechanizmusokat és támogató rendszerelemeket fizikailag különálló alhálózatok létrehozásával és menedzselt interfészek alkalmazásával különíti el az EIR többi belső rendszerelemétől.

MAGYARÁZAT

A fizikailag elkülönített, menedzselt interfészekkel rendelkező alhálózatok hasznosak a számítógépes hálózatok védelmének a kritikus üzemi feldolgozóhálózatoktól való elszigetelésében, hogy megakadályozzák, hogy a támadók felfedezzék az érintett szervezetek által alkalmazott elemzési és igazságügyi technikákat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a biztonsági eszközöket, mechanizmusokat és támogató rendszerelemeket, amelyeket el kíván különíteni a többi belső rendszerelemtől.
2. A szervezetnek létre kell hoznia fizikailag különálló alhálózatokat. Ezek az alhálózatok lehetővé teszik az rendszerelemek elkülönítését a többi belső rendszerelemtől.
3. A szervezetnek alkalmaznia kell menedzselt interfészeket. A menedzselt interfészek lehetővé teszik a rendszerelemek közötti kommunikáció szabályozását, így megakadályozva a nem kívánt hozzáférést és adatvesztést.
4. A szervezetnek rendszeresen ellenőriznie kell a fizikailag különálló alhálózatok és a menedzselt interfészek működését, és naplót kell vezetnie a tevékenységekről.
5. A szervezetnek folyamatosan frissítenie és fejlesztenie kell a biztonsági eszközöket, mechanizmusokat és támogató rendszerelemeket, hogy megfeleljen a változó kiberbiztonsági környezetnek és fenyegetéseknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.2. Rendszer és felhasználói funkciók szétválasztása

17.4. Biztonsági funkciók 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

SC-7(13)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információbiztonsági eszközök, mechanizmusok és támogató rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.28. A HATÁROK VÉDELME – VÉDELEM AZ ENGEDÉLY NÉLKÜLI FIZIKAI KAPCSOLATOK KIALAKÍTÁSA ELLEN

17.28. A szervezet védekezik a jogosulatlan fizikai csatlakozások ellen a szervezet által meghatározott menedzselt interfészeknél.

MAGYARÁZAT

A különböző biztonsági kategóriákban vagy minősítési szinteken működő EIR-ek közös fizikai és környezeti védelmi intézkedéseken osztozhatnak, mivel az EIR-ek ugyanazon létesítményeken belül közös helyiségekben működhetnek. A gyakorlatban előfordulhat, hogy ezek a különálló EIR-ek közös helyiségekben használnak közös berendezéseket, kábelszekrényeket és kábelelosztó utakat. Az illetéktelen fizikai csatlakozások elleni védelem úgy érhető el, hogy a menedzselt interfészek mindkét oldalán egyértelműen azonosított és fizikailag elkülönített kábeltálcákat, csatlakozókereteket és patchpaneleket használnak olyan fizikai hozzáférés-felügyeletekkel, amelyek korlátozott engedélyezett hozzáférést biztosítanak ezekhez az elemekhez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fizikai védelmi intézkedéseket kell bevezetnie. Ez magában foglalhatja a kábelek, csatlakozókeretek és patch panelek fizikai elválasztását.
2. A szervezetnek fizikai hozzáférés korlátozási intézkedéseket kell bevezetnie, amelyekhez tartoznak pl.: a zárható szekrényeket, biztonsági kártyás hozzáférést vagy biometrikus azonosítás.
3. A szervezetnek naplózást és monitorozást kell alkalmaznia, hogy nyomon követhesse a fizikai hozzáférési kísérleteket és azonosíthassa a jogosulatlan csatlakozásokat. Ez magában foglalhatja a CCTV rendszereket, hozzáférési naplókat és riasztásokat.
4. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a fizikai védelmi intézkedések hatékonyságát és az EIR biztonságát.
5. A szervezetnek be kell építenie a belsős oktatási anyagába a jogosulatlan fizikai csatlakozások veszélyeit és a megfelelő védelmi intézkedéseket.

Kapcsolódó intézkedések

12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

12.45. Információszivárgás

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

SC-7(14)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a felügyelt interfészek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.29. A HATÁROK VÉDELME – HÁLÓZATI PRIVILEGIZÁLT HOZZÁFÉRÉSEK

17.29. Az EIR a privilegizált hálózati hozzáféréseket a hozzáférés-felügyelete és átvizsgálása céljából egy erre a célra dedikált, menedzselt interfészen keresztül irányítja.

MAGYARÁZAT

A privilegizált hozzáférés nagyobb hozzáférést biztosít a rendszerfunkciókhoz, beleértve a biztonsági funkciókat is. A támadók távoli hozzáférésen keresztül próbálnak privilegizált hozzáférést szerezni az EIR-ekhez, hogy káros hatást gyakoroljanak az ügymenetre vagy az üzletmenetre, például információk kiszivárogtatásával vagy egy kritikus rendszerfunkció leállásával. A hálózati, privilegizált hozzáférési kérelmek dedikált, menedzselt interfészen keresztül történő továbbítása tovább korlátozza a privilegizált hozzáférést a fokozott hozzáférés-felügyelet és naplózás érdekében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely hozzáférések minősülnek privilegizáltnak az EIR-en belül.
2. A szervezetnek létre kell hoznia egy dedikált, menedzselt interfészt, amelyen keresztül az összes privilegizált hálózati hozzáférési kérelem áthalad. Ez az interfész lehet egy szoftver, hardver vagy akár ezek kombinációja, amely képes kezelni és irányítani a hozzáférési kérelmeket.
3. A szervezetnek be kell állítania a hozzáférés-felügyeletet az EIR-en belül. Meg kell határoznia a hozzáférési szabályokat, amelyek rendel-eznek arról, hogy ki, mikor és milyen körülmények között férhet hozzá a rendszerhez.
4. A szervezetnek naplózást kell bevezetnie az EIR-en belül, hogy nyomon követhesse a privilegizált hozzáféréseket, és lehetővé tegye a szervezet számára, hogy gyorsan reagáljon a potenciális biztonsági eseményekre.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

4.2. Naplózható események

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

SC-7(15)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.30. A HATÁROK VÉDELME – RENDSZERELEMEK FELFEDEZÉSÉNEK MEGAKADÁLYOZÁSA

17.30. Az EIR megakadályozza a menedzselt interfészekkel rendelkező konkrét rendszerelemek felderítését.

MAGYARÁZAT

A menedzselt interfészt képviselő rendszerelemek felfedezésének megakadályozása segít megvédeni a rendszerelemek hálózati címeit a hálózatokon lévő eszközök azonosítására használt általános eszközök és technikák felfedezésétől. A hálózati címek nem állnak rendelkezésre a felfedezéshez, és a hozzáféréshez előzetes ismeretekre van szükség. A rendszerelemek és eszközök felfedezésének megakadályozása úgy érhető el, hogy a hálózati címeket nem teszik közzé, hálózati címfordítást használnak, vagy nem adják meg a címeket a tartománynévrendszerekben. Egy másik megelőzési technika a hálózati címek időszakos megváltoztatása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell akadályoznia a hálózati címek felderítését. Ez segít megvédeni azokat az elemeket, amelyek hálózati címeket képviselnek, a felderítéstől, amelyet általános eszközök és technikák használnak az EIR-en belüli eszközök azonosítására.
2. A szervezetnek meg kell akadályoznia az elemek és eszközök felderítését, például a hálózati címek közzététele nélkül, hálózati címfordítás használatával, vagy a címek bevitelének mellőzésével a domainnév-rendszerekbe.
3. A szervezetnek egy másik megelőző technikát is alkalmaznia kell, például időszakosan meg kell változtatnia a hálózati címeket.
4. A szervezetnek dokumentálnia kell a fent említett lépések végrehajtását, hogy bizonyíthassa az EIR kiberbiztonsági követelményeknek való megfelelését.

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

SC-7(16)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.31. A HATÁROK VÉDELME – A PROTOKOLL FORMÁTUMOK BETARTÁSA

17.31. Az EIR kikényszeríti a protokoll formátumok betartását.

MAGYARÁZAT

A protokollformátumokat érvényesítő rendszerelemek közé tartoznak a mély csomagvizsgálatot végző tűzfalak és az XML-átjárók. Ezek az elemek ellenőrzik a protokollformátumok és specifikációk betartását az alkalmazási rétegben, és azonosítják azokat a sebezhetőségeket, amelyeket a hálózati vagy szállítási rétegben működő eszközök nem tudnak észlelni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek implementálnia kell azokat az rendszerelemeket, amelyek képesek kikényszeríteni a protokoll formátumok betartását. Ilyen elemek lehetnek például a mély csomagvizsgálati tűzfalak és az XML átjárók.
2. A szervezetnek be kell állítania ezeket a rendszerelemeket úgy, hogy azok ellenőrizzék a protokoll formátumoknak és specifikációknak való megfelelést az alkalmazás rétegében.
3. A szervezetnek biztosítania kell, hogy a rendszerelemek képesek azonosítani azokat a sebezhetőségeket, amelyeket a hálózati vagy szállítási rétegeknél működő eszközök nem tudnak észlelni.
4. A szervezetnek naplót kell vezetnie a rendszerelemek által végzett ellenőrzésekről és dokumentálnia kell az észlelt sebezhetőségeket.
5. A szervezetnek rendszeres időnként felül kell vizsgálnia a rendszerelemek beállításait, hogy biztosítsa a protokoll formátumoknak való megfelelés folyamatos kikényszerítését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.10. Információk az osztott használatú rendszererőforrásokban

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

SC-7(17)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.32. A HATÁROK VÉDELME – BIZTONSÁGOS ÁLLAPOT FENNTARTÁSA

17.32. A szervezet megakadályozza, hogy az EIR nem biztonságos állapotba kerüljön egy határvédelmi berendezés működési hibája esetén.

MAGYARÁZAT

A biztonságos állapot egy olyan állapot, amely eléréséhez az EIR mechanizmusokat alkalmaz, amelyekkel biztosítható, hogy a menedzselt interfészek határvédelmi eszközeinek működési hibája esetén az EIR nem kerül olyan állapotba, amiben a tervezett biztonsági tulajdonságok már nem állnak fenn. A menedzselt interfészek közé tartoznak a védett alhálózatokon (általában demilitarizált zónáknak nevezett) alhálózatokon található routerek, tűzfalak és alkalmazás-átjárók. A határvédelmi eszközök meghibásodásai nem vezethetnek információk külső eszközbe jutásához, és a meghibásodások nem tehetik lehetővé a jogosulatlan információkiadást.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a határvédelmi berendezések, mint például a routerek, tűzfalak és alkalmazási átjárók, melyek a védett alhálózatokon találhatók, megfelelően működjenek és kezelhetők legyenek.
2. A szervezetnek implementálnia kell olyan mechanizmusokat, melyek biztosítják, hogy a határvédelmi berendezések működési hibái esetén az EIR ne kerüljön nem biztonságos állapotba, ahol a tervezett biztonsági tulajdonságok már nem érvényesülnek.
3. A szervezetnek gondoskodnia kell arról, hogy a határvédelmi berendezések hibái ne vezethessenek olyan helyzetekhez, ahol az eszközökön kívüli információk beléphetnek az eszközökbe, vagy ahol a hibák engedélyezhetik a jogosulatlan információ-kiadást.
4. A szervezetnek naplóznia kell a határvédelmi berendezések működési állapotát és az esetleges hibákat, hogy időben észlelje a problémákat és megelőzze a nem biztonságos állapotok kialakulását az EIR-ben.
5. A szervezetnek folyamatosan frissítenie - és karbantartania kell a határvédelmi berendezéseket, hogy biztosítsa a legmagasabb szintű védelmet az EIR számára.

Kapcsolódó intézkedések

7.2. Üzletmenet-folytonossági terv

7.48. Átállás biztonságosüzemmódra

17.77. Ismert állapot való meghibásodás

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

3.3.13.6. A határok védelme

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SC-7(18)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

17.33. A HATÁROK VÉDELME – KOMMUNIKÁCIÓ BLOKKOLÁSA NEM SZERVEZETI KONFIGURÁCIÓVAL RENDELKEZŐ GÉPEKRŐL

17.33. Az EIR blokkolja a bejövő és a kimenő kommunikációs forgalmat azok között a kliensek között, amelyeket a végfelhasználók és a külső szolgáltatók a szervezettől függetlenül konfigurálnak.

MAGYARÁZAT

A végfelhasználók és a külső szolgáltatók által önállóan konfigurált kommunikációs kliensek közé tartoznak az azonnali üzenetküldő kliensek, valamint a videokonferencia-szoftverek és -alkalmazások. A forgalom blokkolása nem vonatkozik azokra a kommunikációs klienesekre, amelyeket az érintett szervezetek engedélyezett funkciók elvégzésére konfiguráltak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie, milyen önállóan konfigurált kommunikációs klienseket használnak a végfelhasználók és a külső szolgáltatók.
2. A szervezetnek meg kell határoznia az EIR beállításait úgy, hogy blokkolja a bejövő és a kimenő kommunikációs forgalmat azok között a kliensek között, amelyeket a végfelhasználók és a külső szolgáltatók a szervezettől függetlenül konfigurálnak.
3. A szervezetnek implementálnia kell a blokkolási szabályokat az EIR-ben. Ez magában foglalhatja a szabályok beállítását a tűzfalon, a hálózati eszközökön és az EIR-en belüli egyéb biztonsági eszközökön.
4. A szervezetnek tesztelnie kell az EIR blokkolási funkcióját, hogy biztosítsa, hogy a szabályok megfelelően működnek.
5. A szervezetnek naplóznia kell az EIR blokkolási tevékenységeit, hogy nyomon követhesse a blokkolt kommunikációs forgalmat és azonosíthassa a potenciális biztonsági problémákat.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR blokkolási szabályait, hogy valamennyi önállóan konfigurált kommunikációs kliensre kiterjedjen.

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

SC-7(19)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.34. A HATÁROK VÉDELME – DINAMIKUS ELSZIGETELÉS ÉS ELKÜLÖNÍTÉS

17.34. Az EIR képes dinamikusan elkülöníteni a szervezet által meghatározott rendszerelemeket a többi rendszerelemtől.

MAGYARÁZAT

Bizonyos belső rendszerelemek dinamikus elkülönítésének képessége akkor hasznos, ha a megkérdőjelezhető eredetű rendszerelemeket el kell választani vagy el kell különíteni a nagyobb megbízhatósággal rendelkező elemektől. Az elemek elkülönítése csökkenti a szervezeti EIR-ek támadási felületét. A kiválasztott rendszerelemek elkülönítése a sikeres támadásokból származó károkat is korlátozhatja, ha ilyen támadások történnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely rendszerelemeket szeretné elkülöníteni a többi rendszerelemtől. Ez lehet olyan rendszerelem, amelynek eredete kérdéses, vagy amely nagyobb bizalommal bír.
2. A szervezetnek implementálnia kell egy dinamikus elkülönítési képességet az EIR-en belül. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie arra, hogy automatikusan elkülönítse a kijelölt rendszerelemeket a többi rendszerelemtől, amikor szükséges.
3. A szervezetnek felügyelnie kell, hogy az EIR elkülönítési képessége korlátozza a sikeres támadásokból eredő károkat. Sikeres támadás esetén csak az elkülönített rendszerelemek kompromittálódnak és a támadás hatása nem terjed tovább a többi rendszerelemre.
5. A szervezetnek dokumentálnia kell az EIR elkülönítésével kapcsolatos tevékenységeit. Így minden elkülönítési eseményt rögzíteni kell, hogy később vissza lehessen követni, ha szükséges.

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

SC-7(20)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.35. A HATÁROK VÉDELME – RENDSZERELEMEK ELKÜLÖNÍTÉSE

17.35. A szervezet határvédelmi mechanizmusokat alkalmaz a szervezet által meghatározott rendszerelemek elkülönítésére, amelyek a szervezet által meghatározott célokat és üzleti funkciókat támogatják.

MAGYARÁZAT

Az érintett szervezetek elkülöníthetik a különböző ügymeneti vagy üzleti funkciókat ellátó rendszerelemeket. Az ilyen elkülönítés korlátozza a rendszerelemek közötti jogosulatlan információáramlást, és lehetőséget biztosít a kiválasztott elemek nagyobb védelmi szintre való fejlesztésére. A rendszerelemek határvédelmi mechanizmusokkal történő szétválasztása lehetővé teszi az egyes elemek fokozott védelmét és az ezen elemek közötti információáramlás hatékonyabb ellenőrzését. Az ilyen típusú fokozott védelem korlátozza a kibertámadások és hibák okozta lehetséges károkat. Az elkülönítés mértéke a választott mechanizmusoktól függően változik. A határvédelmi mechanizmusok közé tartoznak például a routerek, az átjárók és a tűzfalak, amelyek a rendszerelemeket fizikailag elkülönülő hálózatokra vagy alhálózatokra osztják, az alhálózatokat elválasztó kereszt-tartományú eszközök (tartományokon átnyúló), a virtualizációs technikák és a rendszerelemek közötti információáramlás titkosítása (különböző titkosítási kulcsok segítségével).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a rendszerelemeket, amelyek ügymeneti és üzleti funkciókat támogatnak.
2. A szervezetnek határvédelmi mechanizmusokat kell alkalmaznia a rendszerelemek elkülönítésére. Az elkülönítés korlátozza a nem engedélyezett információáramlást a rendszerelemek között, és lehetőséget biztosít a kiválasztott rendszerelemek nagyobb védelmének kialakítására.
3. A szervezetnek növelnie kell az egyes rendszerelemek védelmét, és hatékonyabban kell ellenőriznie az információáramlást az elemek között.

4. A szervezetnek dokumentálnia kell a határvédelmi mechanizmusok alkalmazását és a rendszerelemek elkülönítését, hogy nyomon követhesse a folyamatot és biztosíthassa a követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.24. Belső rendszerkapcsolatok

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

3.3.13.6. A határok védelme

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-7(21)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek, illetve a meghatározott célok és üzleti funkciók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

17.36. A HATÁROK VÉDELME – KÜLÖNÁLLÓ ALHÁLÓZATOK A KÜLÖNBÖZŐ BIZTONSÁGI TARTOMÁNYOKHOZ VALÓ CSATLAKOZÁSHOZ

17.36. A szervezet különböző hálózati címeket hoz létre a különböző biztonsági tartományokban elhelyezett rendszerekhez való csatlakozáshoz.

MAGYARÁZAT

Az EIR-ek alhálózatokra való bontása segít a megfelelő védelmi szint biztosításában a különböző biztonsági tartományokhoz való hálózati kapcsolatok számára, amelyek különböző biztonsági kategóriájú vagy minősítési szintű információkat tartalmaznak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a különböző biztonsági tartományokat, amelyekben az EIR-ek találhatók. Ezek a tartományok lehetnek például különböző biztonsági szintek vagy osztályozási szintek.
2. A szervezetnek létre kell hoznia különböző hálózati címeket, amelyeket ezekhez a tartományokhoz rendel. Ez azt jelenti, hogy minden egyes tartományhoz külön hálózati cím tartozik.
3. A szervezetnek biztosítania kell, hogy az EIR-ek csak a megfelelő hálózati címeken keresztül csatlakozzanak a hálózathoz, az EIR-eknek csak a hozzájuk rendelt hálózati címeken keresztül tudnak csatlakozni a hálózathoz.
4. A szervezetnek naplóznia kell, hogy nyomon követhesse, mely EIR-ek csatlakoznak a hálózathoz, és milyen hálózati címeken keresztül. Ez biztosítja az ellenőrizhetőségét annak, hogy az EIR-ek csak a megfelelő hálózati címeken keresztül csatlakoznak-e a hálózathoz.
5.A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hálózati címeket és a hozzájuk rendelt EIR-eket, hogy biztosítsa a teljeskörű védelmet.

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

SC-7(22)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.37. A HATÁROK VÉDELME – VISSZAJELZÉS KÜLDÉSÉNEK LETILTÁSA A PROTOKOLL ELLENŐRZÉSI HIBA ESETÉN

17.37. Az EIR letiltja a visszajelzés küldését a feladónak, amennyiben protokollformátum-ellenőrzési hiba lép fel.

MAGYARÁZAT

Ha kommunikáció során protokollformátum-ellenőrzési hiba lép fel, az ezzel kapcsolatos visszajelzés küldését az EIR letiltja, ez pedig megakadályozza, hogy a potenciális támadók olyan információkhoz jussanak, amelyek egyébként nem lennének elérhetők számukra. .

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell állítania az EIR-t úgy, hogy automatikusan tiltsa le a visszajelzés küldését, amikor protokollformátum-ellenőrzési hiba lép fel.
2. A szervezetnek tesztelnie kell az EIR-t, hogy biztosítsa a funkció megfelelő működését. Ez magában foglalhatja a protokollformátum-ellenőrzési hiba szimulálását és a visszajelzés küldésének letiltásának ellenőrzését.
3. A szervezetnek naplózni kell az összes protokollformátum-ellenőrzési hibát és a visszajelzés küldésének letiltását az EIR-ben. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse és elemezze az ilyen eseményeket.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR beállításait, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

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

SC-7(23)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.38. A HATÁROK VÉDELME – NYILVÁNOS HÁLÓZATHOZ TÖRTÉNŐ CSATLAKOZÁS TILTÁSA

17.38. A szervezet tiltja a meghatározott EIR nyilvános hálózathoz történő közvetlen csatlakozását.

MAGYARÁZAT

A közvetlen kapcsolat olyan kapcsolatot jelent, ami közvetlenül fizikailag, vagy virtuális módon valósul meg kettő vagy több rendszer között. Az EIR közvetlen csatlakozása más nyilvánosan hozzáférhető hálózathoz, beleértve az internetet és az érintett szervezet egyéb nyilvános hozzáféréssel rendelkező hálózatait, tilos.

Ez a követelmény a kiberbiztonsági kockázatok csökkentésére irányul. A közvetlen csatlakozások lehetővé teszik a támadók számára, hogy könnyebben hozzáférjenek és támadják meg az EIR-t. A közvetlen csatlakozások korlátozása vagy tiltása segít megakadályozni a nem kívánt hozzáférést és a potenciális adatszivárgást.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely EIR-eket szeretné korlátozni a nyilvános hálózathoz való közvetlen csatlakozástól. Ez kitejedhet valamennyi EIR-re, vagy csak bizonyos kritikus rendszerekre.

2. A szervezetnek implementálnia kell a megfelelő hálózati biztonsági szabályokat és protokollokat, amelyek megakadályozzák az EIR közvetlen csatlakozását a nyilvános hálózathoz. Ez magában foglalhatja a tűzfalak, hálózati szűrők és egyéb biztonsági eszközök használatát.

3. A szervezetnek ellenőriznie kell, hogy az EIR-k megfelelően vannak-e konfigurálva. Ez magában foglalhatja a rendszerbeállítások ellenőrzését, a hálózati forgalom monitorozását és a biztonsági események naplózását.

4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hálózati biztonsági szabályait és protokollokat, hogy biztosítsa az EIR-ek védelmét a legújabb fenyegetésekkel szemben.

5 A szervezetnek rendszeresen felül kell vizsgálnia a naplókat, hogy azonosítsa a potenciális biztonsági eseményeket és reagáljon rájuk. Ez magában foglalhatja a naplók elemzését, a biztonsági események értékelését és a megfelelő válaszintézkedések meghozatalát.

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

SC-7(28)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszer meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.39. A HATÁROK VÉDELME – KÜLÖNÁLLÓ ALHÁLÓZATOK A FUNKCIÓK ELKÜLÖNÍTÉSÉHEZ

17.39. A szervezet fizikailag vagy logikailag elkülönített alhálózatokat alakít ki a szervezet működése szempontjából kritikus rendszerelemek és funkciók elkülönítése érdekében.

MAGYARÁZAT

A kritikus rendszerelemek és funkciók elkülönítése más, nem kritikus rendszerelemektől és funkcióktól külön alhálózatokon keresztül szükséges lehet a katasztrofális vagy gyengítő hatású, rendszerhibát eredményező sérüléssel vagy kompromittálódással szembeni kitettség csökkentéséhez. Például egy kereskedelmi repülőgépen az irányítási és vezérlési funkciónak a fedélzeti szórakoztató funkciótól való fizikai elkülönítése külön alhálózatokon keresztül nagyobb fokú biztonságot nyújt a kritikus rendszerfunkciók megbízhatóságában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, melyek azok a rendszerelemek és funkciók, amelyek kritikusak a működése szempontjából.
2. A szervezetnek fizikailag vagy logikailag elkülönített alhálózatokat kell létrehoznia, amelyekben ezek a kritikus rendszerelemek és funkciók helyezkednek el.
3. A szervezetnek gondoskodnia kell arról, hogy a kritikus és nem kritikus rendszerelemek közötti kommunikáció csak szigorúan ellenőrzött és biztonságos csatornákon történjen.
4. A szervezetnek rendszeresen ellenőriznie kell az alhálózatok biztonságát, és naplózni kell minden eseményt, amely potenciálisan veszélyeztetheti a kritikus rendszerelemeket és funkciókat.

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

SC-7(29)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kritikus rendszerelemek és funkciók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.40. AZ ADATÁTVITEL BIZALMASSÁGA ÉS SÉRTETLENSÉGE

17.40. Az EIR megvédi a továbbított információk bizalmasságát és sértetlenségét.

MAGYARÁZAT

Ez az intézkedés mind a belső, mind a külső hálózatokra és valamennyi információs rendszerelemre vonatkozik, amelyekből az információ továbbítható. A szabályozott határok védelmén kívül eső kommunikációs utak ki vannak téve a lehallgatás és módosítás lehetőségének. A szervezeti információk bizalmasságának és sértetlenségének védelme fizikai eszközökkel (például védett elosztó rendszerek alkalmazásával) vagy logikai eszközökkel (például titkosítási technikák alkalmazásával) valósítható meg. A nem teljesen dedikált (pl. az egyéni kliensek igényeihez rendkívül specializálódott szolgáltatások), hanem kereskedelmi szolgáltatásként igénybe vett átviteli szolgáltatásokra támaszkodó szervezetek nehezen szerezhetik meg a szükséges biztosítékokat az átvitel bizalmasságával és sértetlenségével kapcsolatban elvárt biztonsági intézkedésekről. Ilyen helyzetekben a szervezet meghatározza, hogy szabványos, kereskedelmi távközlési szolgáltatáscsomagokban milyen bizalmassági és sértetlenségi szolgáltatások érhetők el. Ha nem kivitelezhető vagy nem praktikus a szükséges biztonsági ellenőrzéseket és intézkedési hatékonyságot a megfelelő szerződéses eszközzel biztosítani, a szervezet megfelelő kiegészítő biztonsági intézkedéseket vezethet be, vagy elfogadja a megnövekedett kockázatot.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR védi a továbbított információk bizalmasságát és sértetlenségét mind belső, mind külső hálózatokon, valamint minden olyan rendszerelemen, amely képes információt továbbítani, beleértve a szervereket, notebookokat, asztali számítógépeket, mobil eszközöket, nyomtatókat, másolókat.
2. A szervezetnek meg kell védenie a kommunikációs utakat a lehetséges lehallgatás és módosítás ellen. Az információ bizalmasságának és sértetlenségének védelme fizikai vagy logikai eszközökkel is elérhető. A fizikai védelem biztosítható védett elosztó rendszerek használatával. A védett elosztó rendszer olyan vezetékes vagy optikai telekommunikációs rendszer, amely terminálokat és megfelelő elektromágneses, akusztikus, elektromos és fizikai

intézkedéseket tartalmaz, amelyek lehetővé teszik annak használatát titkosítatlan információ továbbítására. A logikai védelem elérhető titkosítási technikák alkalmazásával.

3. A szervezetnek meg kell határoznia, milyen típusú bizalmassági vagy sértetlenségi szolgáltatások állnak rendelkezésre a standard, kereskedelmi telekommunikációs szolgáltatási csomagokban, ha olyan kereskedelmi szolgáltatókra támaszkodnak, akik továbbítási szolgáltatásokat nyújtanak szolgáltatásként, nem pedig teljesen dedikált szolgáltatásként.

4. Ha nem lehetséges a szükséges ellenőrzések és az intézkedési hatékonyság biztosításának megszerzése megfelelő szerződéses eszközökön keresztül, a szervezetnek megfelelő kompenzációs intézkedéseket kell végrehajtania.

5. A szervezetnek dokumentálnia kell az összes lépést, amelyet a továbbított információk bizalmasságának és sértetlenségének védelme érdekében tett, hogy bizonyíthassa a megfelelőséget és az ellenőrzés hatékonyságát.

Kapcsolódó intézkedések

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

4.33. Letagadhatatlanság

8.10. Eszközök azonosítása és hitelesítése

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

8.41. Szolgáltatás azonosítása és hitelesítése

10.11. Távoli karbantartás

12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

16.7. Beszerzések

16.16. Biztonságtervezési elvek

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

3.3.13.7. Az adatátvitel bizalmassága

ISO/IEC 27001:2023 referencia

A.5.10; A.5.14; A.5.33; A.8.20; A.8.26

NIST SP 800-53 rev.5 referencia

SC-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.41. AZ ADATÁTVITEL BIZALMASSÁGA ÉS SÉRTETLENSÉGE – KRIPTOGRÁFIAI VÉDELEM

17.41. Az EIR kriptográfiai mechanizmusokat alkalmaz az adatátvitel során, hogy megelőzze az információk jogosulatlan felfedését, illetve kimutassa az információk módosításait.

MAGYARÁZAT

Az EIR kriptográfiai mechanizmusokat alkalmaz, hogy az adatforgalom bizalmasságáról és sértetlenségéről megbizonyosodjon az adatátvitel során, kivéve, ha azt a szervezet által meghatározott alternatív fizikai védelmi intézkedések segítségével védi.

Az adatátvitel során az adatok titkosítása védi meg az információt a jogosulatlan közzétételtől és a módosítástól. Az információ sértetlenségének védelme érdekében megvalósított kriptográfiai mechanizmusok közé tartoznak például a kriptográfiai lenyomat (hash) függvények, amelyeket a elektronikus aláírásokban is használnak, az ellenőrző kódok és az üzenet hitelesítési kódok. Az alternatív fizikai biztonsági biztosítékok közé tartoznak például a védett elosztó rendszerek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell választania a megfelelő kriptográfiai mechanizmusokat, amelyeket az EIR alkalmazni fog az adatátvitel során. Ez magában foglalhatja a TLS és az IPSec (Internet Protocol Security) protokollokat, amelyek biztosítják az adatok bizalmas és integritását az átvitel során.
2. A szervezetnek implementálnia kell a kiválasztott kriptográfiai mechanizmusokat az EIR-ben. Ez magában foglalhatja a szoftverfrissítéseket, a konfigurációs változtatásokat és a tesztelést annak érdekében, hogy biztosítsa a mechanizmusok megfelelő működését.
3. A szervezetnek naplózni kell az EIR kriptográfiai mechanizmusainak használatát. Ez magában foglalhatja az adatátviteli eseményeket, a kriptográfiai hitelesítési eseményeket és az esetleges biztonsági eseményeket.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR kriptográfiai mechanizmusait, hogy biztosítsa azok hatékonyságát és relevanciáját a változó kiberbiztonsági fenyegetésekkel szemben.

5. A szervezetnek gondoskodnia kell arról, hogy a személyzet megfelelően képzett legyen a kriptográfiai mechanizmusok használatával kapcsolatban.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

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

3.3.13.7. Az adatátvitel bizalmassága

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-8(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.42. AZ ADATÁTVITEL BIZALMASSÁGA ÉS SÉRTETLENSÉGE – AZ ADATOK ÁTVITEL ELŐTTI ÉS UTÁNI KEZELÉSE

17.42. Az EIR fenntartja az információ bizalmasságát és sértetlenségét a továbbítás előkészítése és a fogadás során.

MAGYARÁZAT

Az információ a továbbítás előkészítése vagy a fogadása során, beleértve az aggregálást, a protokoll transzformációs pontokat, valamint a csomagolást és kicsomagolást, az információ véletlenül vagy szándékosan nyilvánosságra kerülhet vagy módosulhat. Az ilyen jogosulatlan felfedések vagy módosítások veszélyeztetik az információ titkosságát vagy sértetlenségét.

Az EIR-nek megfelelő biztonsági intézkedéseket kell bevezetnie és fenntartania annak érdekében, hogy megakadályozza az információ jogosulatlan kiadását vagy módosítását. Valamint a szervezetnek naplóznia kell az EIR-nek az összes releváns tevékenységet, hogy képes legyen azonosítani és kezelni az esetleges biztonsági eseményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek implementálnia kell a megfelelő kiberbiztonsági eszközöket és protokollokat, amelyek biztosítják az információ bizalmasságát és sértetlenségét a továbbítás előkészítése és a fogadás során. Ez magában foglalhatja a titkosítást, az adatintegritás-ellenőrzést és a hitelesítést.
2. A szervezetnek be kell vezetnie a szükséges biztonsági intézkedéseket, hogy megakadályozza az információk jogosulatlan hozzáférését vagy módosítását. Ez magában foglalhatja a hozzáférés-vezérlési szabályokat, a jogosulatlan hozzáférési kísérletek észlelését és a biztonsági események kezelését.
3. A szervezetnek naplót kell vezetnie az EIR-ben történő összes tevékenységről, hogy nyomon követhető legyen minden változás, és azonosítható legyen minden potenciális biztonsági esemény.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági intézkedéseket és protokollokat, hogy biztosítsa az EIR folyamatos védelmét a változó kiberbiztonsági fenyegetésekkel szemben.

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

SC-8(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.43. AZ ADATÁTVITEL BIZALMASSÁGA ÉS SÉRTETLENSÉGE – ÜZENETEK KRIPTOGRÁFIAI VÉDELME KÜLSŐ FOGADÓ FÉL ESETÉN

17.43. A szervezet kriptográfiai mechanizmusokat alkalmaz az üzenetek külső adatainak (például: fejléc) védelmére, kivéve, ha azokat a szervezet által kijelölt alternatív fizikai védelmi mechanizmusok védik.

MAGYARÁZAT

"Üzenetek kriptográfiai védelme külső fogadó fél esetén" követelmény az információk jogosulatlan nyilvánosságra hozatala elleni védelemmel foglalkozik. Az üzenet külső adatai közé tartoznak az üzenetfejlécek és az útvonal-információk. A kriptográfiai védelem megakadályozza az üzenet külső adatainak kihasználását, és olyan belső és külső hálózatokra vagy linkekre vonatkozik, amelyek nem jogosult felhasználók számára is láthatóak lehetnek. A fejléc- és útválasztási információkat néha nyílt szövegben továbbítják, mert a szervezet nem azonosítja ezeket jelentős értékű információknak, vagy mert az információ titkosítása alacsonyabb hálózati teljesítményt vagy magasabb költségeket eredményezhet. Az alternatív fizikai védelmi mechanizmusok közé tartoznak a védett elosztó rendszerek alkalmazása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely üzenetek külső adatait kell védeni.
2. A szervezetnek kriptográfiai mechanizmusokat kell bevezetnie, amelyek megakadályozzák az üzenetek külső adatainak jogosulatlan hozzáférését.
3. A szervezetnek biztosítania kell, hogy a kriptográfiai védelem alkalmazása mind a belső, mind a külső hálózatokra vagy kapcsolatokra vonatkozik, amelyek láthatóak lehetnek a nem jogosult felhasználók számára.
4. A szervezetnek alternatív fizikai védelmi mechanizmusokat kell alkalmaznia, ha a kriptográfiai mechanizmusok alkalmazása nem lehetséges vagy nem kívánatos. Ilyen alternatív fizikai védelmi mechanizmusok lehetnek például a védett elosztó rendszerek.

5. A szervezetnek naplózásra van szüksége, hogy nyomon követhesse a kriptográfiai mechanizmusok és az alternatív fizikai védelmi mechanizmusok hatékonyságát és megfelelőségét.

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

SC-8(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.44. AZ ADATÁTVITEL BIZALMASSÁGA ÉS SÉRTETLENSÉGE – KOMMUNIKÁCIÓ ELREJTÉSE VAGY RANDOMIZÁLÁSA

17.44. A szervezet kriptográfiai mechanizmusokat alkalmaz a kommunikációs mintázatok elrejtésére vagy randomizálására, ha azokat nem védi más, a szervezet által meghatározott alternatív fizikai intézkedés.

MAGYARÁZAT

A kommunikációs minták elrejtése vagy randomizálása az információk jogosulatlan nyilvánosságra hozatala elleni védelemmel foglalkozik. A kommunikációs minták közé tartozik a gyakoriság, az időszakok, a kiszámíthatóság és a mennyiség. A kommunikációs mintázatok változásai értékes hírszerzési információkat tárhatnak fel, különösen, ha a szervezet ügymeneti és üzleti funkcióival kapcsolatos egyéb rendelkezésre álló információkkal kombinálják. A kommunikáció elrejtése vagy randomizálása megakadályozza a kommunikációs mintákon alapuló hírszerzési információk levezetését, és mind a belső, mind a külső hálózatokra vagy kapcsolatokra vonatkozik, amelyek olyan személyek számára is láthatóak lehetnek, akik nem jogosult felhasználók. A kapcsolatok titkosítása és a folyamatos, rögzített vagy véletlenszerű mintákban történő továbbítás megakadályozza az EIR kommunikációs mintáiból történő hírszerzési információk levezetését. Az alternatív fizikai intézkedések közé tartoznak a védett elosztórendszerek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie a jelenlegi kommunikációs mintázatait, beleértve a frekvenciát, időszakokat, kiszámíthatóságot és mennyiséget.
2. A szervezetnek kriptográfiai mechanizmusokat kell alkalmaznia a kommunikációs mintázatok elrejtésére vagy randomizálására. Ez magában foglalhatja a hivatkozások titkosítását és a folyamatos, fix vagy véletlenszerű mintázatokban történő továbbítást.
3. A szervezetnek biztosítania kell, hogy a kriptográfiai mechanizmusok mind a belső, mind a külső hálózatokra vagy linkekre alkalmazhatóak legyenek, amelyek láthatóak lehetnek a jogosulatlan felhasználók számára.

4. A szervezetnek alternatív fizikai intézkedéseket is meg kell határoznia, amennyiben a kommunikációs mintázatokat nem védi más. Ez magában foglalhatja a védett elosztó rendszereket.

5. A szervezetnek dokumentálnia kell a kriptográfiai mechanizmusok alkalmazását és a kommunikációs mintázatok változásait, hogy biztosítsa a folyamatos felülvizsgálatot és a szükséges módosításokat.

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

SC-8(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.45. AZ ADATÁTVITEL BIZALMASSÁGA ÉS SÉRTETLENSÉGE – VÉDETT ELOSZTÓRENDSZER

17.45. A szervezet egy, a szervezet által meghatározott védett elosztórendszert alkalmaz, melynek célja az információ jogosulatlan nyilvánosságra hozatalának megakadályozása, valamint az információban bekövetkező változások észlelése a továbbítás során.

MAGYARÁZAT

Az érintett szervezet által meghatározott védett elosztórendszer célja, hogy megakadályozza, észlelje és/vagy megnehezítse a fizikai hozzáférést azokhoz a kommunikációs vonalakhoz. Az EIR ebben az esetben a védett elosztórendszer részét képezi, melynek feladata az információk biztonságos továbbítása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a védett elosztórendszer hatókörét, és az érintett kommunikációs vonalakat.
2. A szervezetnek biztosítania kell, hogy az EIR képes legyen észlelni az információban bekövetkező változásokat a továbbítás során.
3. A szervezetnek szigorú hozzáférési szabályokat kell bevezetnie az EIR-hez, hogy csak a jogosult felhasználók férhessenek hozzá az információhoz. Ez magában foglalhatja a felhasználói hitelesítést, a jogosultságkezelést és a hozzáférések naplózását.
4. Az érintett szervezetnek biztosítania kell, hogy az EIR frissítve legyen a legújabb biztonsági frissítésekkel és javításokkal, hogy megvédje az információt a legújabb fenyegetésektől.

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

SC-8(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a védett elosztórendszer meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.46. A HÁLÓZATI KAPCSOLAT MEGSZAKÍTÁSA

17.46. Az EIR megszakítja a hálózati kapcsolatot a kommunikációs munkaszakasz befejezésekor vagy meghatározott időtartamú inaktivitás után.

MAGYARÁZAT

Ez az intézkedés mind belső, mind külső hálózatokra vonatkozik. A kommunikációs munkaszakaszokhoz kapcsolódó hálózati kapcsolatok megszakítása például a hozzárendelt TCP/IP-címek/portpárok operációs rendszer szintjén történő szétválasztása, vagy a hálózati hozzárendelések alkalmazás szinten történő megszakítása, ha több alkalmazás-munkamenet egyetlen operációs rendszer-szintű hálózati kapcsolatot használ. Az inaktivitás időtartamát a szervezet állapíthatja meg, mérlegelve például a hálózati hozzáférés típusát vagy az egyes hálózati hozzáférések időtartamát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek a kommunikációs munkaszakasz befejezésekor meg kell szakítania a hálózati kapcsolatot.
2. A szervezetnek meg kell határoznia az inaktivitás időtartamát, amely után szintén meg kell szakítani a hálózati kapcsolatot. Az inaktivitás időtartama lehet általános, minden hálózati hozzáférésre vonatkozó, vagy specifikus, egyes hálózati hozzáférésekhez esetén.
3. A szervezetnek naplózásra van szüksége, hogy nyomon követhesse a hálózati kapcsolatok megszakítását és az inaktivitás időtartamát. A naplózás segíthet az érintett szervezetnek abban, hogy elemezze a hálózati kapcsolatok használatát, és szükség esetén módosítsa a hálózati kapcsolatok megszakításának és az inaktivitás időtartamának szabályait.
4. A szervezetnek rendszeres időnként felül kell vizsgálnia és frissítenie kell a hálózati kapcsolatok megszakításának szabályait.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.100. Távoli hozzáférés

17.73. Munkaszakasz hitelessége

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

3.3.13.9. A hálózati kapcsolat megszakítása: Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, meghatározott időtartamú inaktivitás után.

ISO/IEC 27001:2023 REFERENCIA

A.8.20

NIST SP 800-53 REV.5 REFERENCIA

SC-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.47. MEGBÍZHATÓ ÚTVONAL

17.47. Az EIR:

17.47.1. Egy fizikailag vagy logikailag elkülönített, megbízható kommunikációs útvonalat biztosít a felhasználók és az EIR megbízható elemei közötti kommunikációhoz.

17.47.2. Lehetővé teszi a felhasználók számára, hogy ezt a megbízható kommunikációs útvonalat használják a felhasználók és a rendszer biztonsági funkciói közötti kommunikációra, beleértve a hitelesítést és az újrahitelesítést, valamint további, a szervezet által meghatározott biztonsági funkciókat.

MAGYARÁZAT

A megbízható útvonalak olyan mechanizmusok, amelyek révén a felhasználók közvetlenül kommunikálhatnak (beviteli eszközök, például billentyűzetek használatával) az EIR-ek biztonsági funkcióival, a biztonsági szabályok támogatásához szükséges biztosítékokkal. A megbízható útvonal-mechanizmusokat csak a felhasználók vagy a szervezeti EIR-ek biztonsági funkciói aktiválhatják. A megbízható útvonalakon keresztül érkező felhasználói válaszok védve vannak a nem megbízható alkalmazások általi módosítással és a nem megbízható alkalmazások számára történő közzététellel szemben. Az érintett szervezetek megbízható útvonalakat alkalmaznak a megbízható, magas biztosítékú kapcsolatok biztosítása érdekében az EIR biztonsági funkciói és a felhasználók között, beleértve a rendszerbe való bejelentkezést is. A megbízható útvonalak eredeti megvalósításai egy sávon kívüli (out of band) jelet használtak az útvonal elindítására, például a <BREAK> billenyűt, amely nem továbbít hamisítható karaktereket. A későbbi megvalósításokban olyan billentyűkombinációt használtak, amelyet nem lehet eltéríteni (spoof) (pl. a <CTRL> + <ALT> + <DEL> billentyűk). Az ilyen billenytű-kombinációk azonban platformspecifikusak, és nem biztos, hogy minden esetben biztosítják a megbízható útvonal megvalósítását. A megbízható kommunikációs útvonalak érvényesítését a referenciamonitor koncepciónak megfelelő egyedi megvalósítás biztosítja.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy fizikailag vagy logikailag elkülönített, megbízható kommunikációs útvonalat az EIR megbízható elemei és a felhasználók között. Ez magában

foglalhatja a hálózati infrastruktúra biztonságos konfigurációját, a titkosítási protokollok használatát és a biztonsági rétegek bevezetését.

2. A szervezetnek lehetővé kell tennie a felhasználók számára, hogy ezt a megbízható kommunikációs útvonalat használják az EIR biztonsági funkcióival való kommunikációra. Ez magában foglalhatja a felhasználói jogosultságok és hozzáférési szintek beállítását, valamint a felhasználói interakciók naplózását.

3. A szervezetnek biztosítania kell a hitelesítést és az újrahitelesítést a megbízható kommunikációs útvonalon keresztül.

4. A szervezetnek további biztonsági funkciókat kell meghatároznia és implementálnia, amelyeket a felhasználók a megbízható kommunikációs útvonalon keresztül használhatnak. Ez magában foglalhatja a különböző biztonsági protokollok és szabályok bevezetését, valamint a rendszeres biztonsági ellenőrzések és naplózások elvégzését.

5. A szervezetnek biztosítania kell, hogy a megbízható kommunikációs útvonalat csak a felhasználók vagy az EIR biztonsági funkciói aktiválhatják.

Kapcsolódó intézkedések

2.89. Biztonsági tulajdonságok

2.129. Referenciának való megfelelőség vizsgálata

17.49. Kriptográfiai kulcs előállítása és kezelése

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

SC-11

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.48. MEGBÍZHATÓ ÚTVONAL – MEGMÁSÍTHATATLAN ÚTVONAL

17.48. Az EIR:

17.48.1. egy olyan megbízható kommunikációs útvonalat biztosít, amely egyértelműen megkülönböztethető más kommunikációs útvonalaktól;

17.48.2. kezdeményezi a megbízható kommunikációs útvonalat a rendszer meghatározott biztonsági funkciói és a felhasználó közötti kommunikációhoz.

MAGYARÁZAT

Az EIR-nek a kommunikáció során szükséges biztosítania egy olyan megbízható kommunikációs útvonalat amellyel kapcsolatban egy felhasználó egyértelműen felismeri a kommunikáció forrását, mint egy megbízható rendszerelemet. Például a megbízható útvonalra utaló jel megjelenhet a kijelző egy olyan területén, amelyhez más alkalmazásoknak nincs hozzáférése, vagy alapulhat egy olyan azonosítón, amelyet nem lehet meghamisítani.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A megbízható kommunikációs útvonalnak egyértelműen megkülönböztethetőnek kell lennie más kommunikációs útvonalaktól. Ez azt jelenti, hogy a felhasználónak képesnek kell lennie egyértelműen felismerni a kommunikáció forrását, mint egy megbízható rendszerelemet.

2. A szervezetnek biztosítania kell, hogy a megbízható kommunikációs útvonal megjelenjen egy olyan területen, amelyet más alkalmazások nem érhetnek el, vagy alapuljon egy olyan azonosítón, amelyet nem lehet meghamisítani.

3. A szervezetnek naplózásra van szüksége, hogy nyomon követhesse a megbízható kommunikációs útvonal használatát és biztosítsa annak integritását. Ez magában foglalja a kommunikációs útvonalon keresztül továbbított adatok naplózását, valamint a rendszerben történő változásokat, amelyek befolyásolhatják a megbízható kommunikációs útvonal biztonságát.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a megbízható kommunikációs útvonalat, hogy biztosítsa annak folyamatos megbízhatóságát és biztonságát.

Ez magában foglalja a potenciális biztonsági rések azonosítását és javítását, valamint a rendszer frissítéseit a legújabb biztonsági protokollok és technológiák alkalmazásával.

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

SC-11(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.49. KRIPTOGRÁFIAI KULCS ELŐÁLLÍTÁSA ÉS KEZELÉSE

17.49. A szervezet előállítja és kezeli a kriptográfiai kulcsokat a szervezet által meghatározott előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelményekkel összhangban.

MAGYARÁZAT

A kriptográfiai kulcsok kezelése és létrehozása manuális eljárásokkal támogatott automatizált mechanizmusokkal történhet. Az érintett szervezetek meghatározzák a kulcskezelési követelményeket a vonatkozó jogszabályi előírások, vezetői utasítások és előírások, belső szabályzatok, szabványok és iránymutatások figyelembevételével, meghatározva a megfelelő paramétereket. A szervezet egy bizalmi tárolót tart fenn, amelyben csak jóváhagyott megbízható elemek kerülnek tárolásra. Ez magában foglalja az EIR-ek belső műveletekhez kapcsolódó tanúsítványokat és az EIR-ek külső láthatóságú tanúsítványait.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet először határozza meg a kriptográfiai kulcskezelési követelményeket, amelyek összhangban vannak az alkalmazandó törvényekkel, végrehajtási rendeletekkel, irányelvekkel, szabályozásokkal, szabályokkal, szabványokkal és útmutatókkal.
2. Az érintett szervezetnek döntenie kell a megfelelő opciókról, paraméterekről és szintekről, amelyeket a kriptográfiai kulcskezelés során alkalmaznak.
3. A szervezetnek kezelnie kell a bizalmi tárolókat, hogy biztosítsa, csak a jóváhagyott bizalmi ankerpontok legyenek része ezeknek a tárolóknak. Ez magában foglalja az EIR-en kívüli láthatósággal rendelkező tanúsítványokat, valamint az EIR belső működésével kapcsolatos tanúsítványokat.
4. A szervezetnek elő kell állítania és kezelnie kell a kriptográfiai kulcsokat a szervezet által meghatározott előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelményekkel összhangban.
5. A szervezetnek dokumentálnia kell a kriptográfiai kulcskezelési és generálási folyamatokat, hogy nyomon követhető legyen a kulcsok életciklusa.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.100. Távoli hozzáférés

4.25. Naplóinformációk védelme

4.33. Letagadhatatlanság

6.7. A konfigurációváltozások felügyelete (változáskezelés)

8.10. Eszközök azonosítása és hitelesítése

8.37. Hitelesítés kriptográfiai modul esetén

16.7. Beszerzések

16.16. Biztonságtervezési elvek

16.49. Külső elektronikus információs rendszerek szolgáltatásai

17.40. Az adatátvitel bizalmassága és sértetlensége

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

3.3.13.10. Kriptográfiai kulcs előállítása és kezelése

ISO/IEC 27001:2023 REFERENCIA

A.8.24

NIST SP 800-53 REV.5 REFERENCIA

SC-12

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

17.50. KRIPTOGRÁFIAI KULCS ELŐÁLLÍTÁSA ÉS KEZELÉSE – RENDELKEZÉSRE ÁLLÁS

17.50. A szervezet biztosítja az információk rendelkezésre állását abban az esetben is, amikor a felhasználók elveszítik a kriptográfiai kulcsaikat.

MAGYARÁZAT

A szervezet biztosítja az információk rendelkezésre állását a kriptográfiai kulcsok elvesztése esetén is.
A titkosítási kulcsok letétbe helyezése általános gyakorlat a rendelkezésre állás biztosítására az ilyen jellegű események bekövetkezésekor.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie egy kulcsletételi rendszert. Ez a gyakorlat lehetővé teszi a kriptográfiai kulcsok biztonságos tárolását egy harmadik fél által, így ha a felhasználók elveszítik a kulcsaikat, a kulcsok visszaállíthatók.
2. A szervezetnek biztosítania kell, hogy az EIR rendelkezzen a kulcsletételi rendszerrel való integráció képességével. Ez magában foglalja a kulcsok generálását, tárolását és visszaállítását.
3. A szervezetnek ki kell dolgoznia és be kell vezetnie egy biztonsági protokollt, amely meghatározza, hogyan kezelik a kulcsokat az EIR-ben. Ez magában foglalja a kulcsok generálását, tárolását, visszaállítását és törlését.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR-t, hogy biztosítsa a kulcsletételi rendszer megfelelő működését. Ez magában foglalja a naplók felülvizsgálatát, hogy biztosítsa a kulcsok megfelelő kezelését.
5. A szervezetnek biztosítania kell, hogy a felhasználók kulcsletételi rendszerrel és annak használatával kapcsolatban megfelelően tájékozottak és tudatosak legyenek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.13.10. Kriptográfiai kulcs előállítása és kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-12(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

17.51. KRIPTOGRÁFIAI KULCS ELŐÁLLÍTÁSA ÉS KEZELÉSE – ASZIMMETRIKUS KULCSOK

17.51. A szervezet előállítja, felügyeli és terjeszti az aszimmetrikus kriptográfiai kulcsokat a legjobb iparági gyakorlatnak megfelelő kulcskezelési technológia és kulcskezelési folyamatok alkalmazásával.

MAGYARÁZAT

Az érintett szervezetnek az aszimmetrikus kriptográfiai kulcsok előállítására, felügyeletére és terjesztésére vonatkozó követelménye azt jelenti, hogy az érintett szervezetnek biztosítania kell, hogy a kulcsokat a legjobb iparági gyakorlatnak megfelelően kezeljék. Ez magában foglalja a kulcskezelési technológiát és a kulcskezelési folyamatokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a kulcskezelési technológiát és folyamatokat, amelyeket alkalmazni kíván. Ez magában foglalja az aszimmetrikus kriptográfiai kulcsok előállítását, felügyeletét és terjesztését. Az érintett szervezetnek figyelembe kell vennie a legjobb iparági gyakorlatokat, melyekre számos nemzetközi útmutató, keretrendszer létezik.
2. A szervezetnek implementálnia kell a kiválasztott kulcskezelési technológiát és folyamatokat az EIR-ben. Ez magában foglalja a kulcsok előállítását, tárolását, terjesztését, felügyeletét és végül a kulcsok visszavonását.
3. A szervezetnek biztosítania kell, hogy az EIR-ben alkalmazott kulcskezelési technológia és folyamatok megfelelnek a kiberbiztonsági követelményeknek.
4. A szervezetnek naplózni kell az összes kulcskezelési tevékenységet az EIR-ben. A naplózás segít a szervezetnek nyomon követni és ellenőrizni a kulcskezelési tevékenységeket.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kulcskezelési technológiát és folyamatokat az EIR-ben, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

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

SC-12(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.52. Kriptográfiai kulcs előállítása és kezelése – Kulcsok fizikai felügyelete

17.52. A szervezet megőrzi a kriptográfiai kulcsok fizikai felügyeletét, ha a tárolt információkat külső szolgáltatók titkosítják.

Magyarázat

A külső szolgáltatókat (pl. felhőszolgáltatókat vagy adatközpont-szolgáltatókat) igénybe vevő szervezetek esetében a kriptográfiai kulcsok fizikai felügyelete további biztosítékot nyújt arra, hogy az ilyen külső szolgáltatók által tárolt információkat nem lehet jogosulatlanul felfedni vagy módosítani.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell bizonyosodnia arról, hogy rendelkezik a kriptográfiai kulcsok fizikai felügyeletével. Ez azt jelenti, hogy a szervezetnek képesnek kell lennie arra, hogy hozzáférjen és ellenőrizze ezeket a kulcsokat.
3. A szervezetnek biztosítania kell, hogy a kulcsokat biztonságosan tárolják. Ez magában foglalhatja a kulcsok fizikai tárolását egy zárt helyen, mint például egy széfben, vagy digitális formában, de erős titkosítással a szervezet saját tulajdonú adattárán.
4. A szervezetnek rendszeres naplózást kell végeznie a kulcsok használatáról. Ez magában foglalja a kulcsok hozzáférésének, használatának és módosításának nyomon követését.
5. A szervezetnek biztosítania kell, hogy a kulcsokat csak azok a személyek használják, akiknek erre jogosultságuk van. Ez magában foglalhatja a hozzáférési jogosultságok szigorú kezelését és a személyazonosság ellenőrzését.
6. A szervezetnek biztosítania kell, hogy a külső szolgáltatók is megfelelnek a kriptográfiai kulcsok kezelésének követelményeinek. Ez magában foglalhatja a szolgáltatók auditálását és a szerződéses kötelezettségek beépítését a kulcskezelési követelményekkel kapcsolatban.

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

SC-12(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.53. KRIPTOGRÁFIAI VÉDELEM

17.53. A szervezet:

17.53.1. meghatározza a kriptográfia szervezeten belüli felhasználási területeit; és

17.53.2. megvalósítja az egyes kriptográfiai felhasználási területekhez szükséges kriptográfiai megoldásokat.

MAGYARÁZAT

A kriptográfia számos biztonsági megoldás támogatására alkalmazható, beleértve a minősített és az ellenőrzött, nem minősített információk védelmét, a digitális aláírások biztosítását és végrehajtását, valamint az információk elkülönítésének érvényesítését, amikor a jogosult személyek rendelkeznek a szükséges engedélyekkel, de nincsenek meg a szükséges formális hozzáférési jóváhagyások. A kriptográfia a véletlenszám- és hash-generálás támogatására is használható. Az általánosan alkalmazandó kriptográfiai szabványok közé tartozik az NBSZ által jóváhagyott kriptográfia. Például azok a szervezetek, amelyeknek minősített információkat kell védeniük, előírhatják az NBSZ által jóváhagyott kriptográfia használatát. Azok a szervezetek, amelyeknek digitális aláírásokat kell biztosítaniuk és végrehajtaniuk, szabványos hitelesített kriptográfiát használhatnak. A kriptográfiát a vonatkozó törvényekkel, végrehajtási utasításokkal, irányelvekkel, szabályzatokkal, szabályokkal, szabványokkal és iránymutatásokkal összhangban hajtják végre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezetnek először meg kell határoznia a kriptográfia felhasználási területeit az EIR-en belül. Ez magában foglalhatja a titkosított információk és az ellenőrzött nem titkosított információk védelmét, a digitális aláírások biztosítását és megvalósítását, valamint az információ szeparációjának érvényesítését, amikor a jogosult személyek rendelkeznek a szükséges engedélyekkel, de nincsenek meg a szükséges formális hozzáférési jóváhagyások.

2. A szervezetnek meg kell valósítania a kriptográfiai megoldásokat az egyes kriptográfiai felhasználási területeken. Ez magában foglalhatja az NBSZ által jóváhagyott kriptográfiát.

3. A szervezetnek a kriptográfiát az alkalmazható törvények, rendeletek, irányelvek, szabályozások, szabályok, szabványok és útmutatók szerint kell megvalósítania.

4. A szervezetnek dokumentálnia kell a kriptográfiai megoldások implementációját és használatát, hogy biztosítsa a folyamatok átláthatóságát és a kriptográfiai követelményeknek való megfelelőséget.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.71. Sikertelen bejelentkezési kísérletek

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

4.25. Naplóinformációk védelme

4.33. Letagadhatatlanság

6.49. Felhasználó által telepített szoftver

7.35. Az elektronikus információs rendszer mentései

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

3.3.13.11. Kriptográfiai védelem: Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

ISO/IEC 27001:2023 REFERENCIA

A.8.24; A.8.26

NIST SP 800-53 REV.5 REFERENCIA

SC-13

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

17.54. EGYÜTTMŰKÖDÉSEN ALAPULÓ INFORMATIKAI ESZKÖZÖK

17.54. A szervezet:

17.54.1. tiltja az együttműködésen alapuló számítástechnikai eszközök (például: kamerák, mikrofonok) és alkalmazások távoli aktiválását, a szervezet által meghatározott kivételekkel; és

17.54.2. egyértelmű visszajelzést ad a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

MAGYARÁZAT

Az együttműködésen alapuló számítástechnikai eszközök közé tartoznak például a hálózatba kapcsolt kamerák és mikrofonok. A használat kifejezett jelzése magában foglalja például a felhasználók felé küldött jelzéseket az együttműködésen alapuló számítástechnikai eszközök bekapcsolásakor és használatakor.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat az eszközöket és alkalmazásokat, amelyek az együttműködésen alapuló számítástechnikai eszközök kategóriájába tartoznak. Ilyenek lehetnek például a távoli találkozók eszközei és alkalmazásai, kamerák és mikrofonok.
2. A szervezetnek be kell állítania az EIR-t úgy, hogy tiltsa ezeknek az eszközöknek és alkalmazásoknak a távoli aktiválását, kivéve azokat az eseteket, amelyeket a szervezet kifejezetten meghatározott.
3. A szervezetnek biztosítania kell, hogy az EIR egyértelmű visszajelzést adjon a felhasználóknak, amikor ezek az eszközök és alkalmazások aktiválódnak.
4. A szervezetnek naplóznia kell az eszközök és alkalmazások aktiválását, hogy nyomon követhető legyen, mikor és milyen körülmények között történtek a távoli aktiválások.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.121. Információmegosztás

17.117. Érzékelő képességei és kapcsolódó adatok

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

3.3.13.12. Együttműködésen alapuló számítástechnikai eszközök: Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

ISO/IEC 27001:2023 REFERENCIA

A.5.14

NIST SP 800-53 REV.5 REFERENCIA

SC-15

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

17.55. EGYÜTTMŰKÖDÉSEN ALAPULÓ INFORMATIKAI ESZKÖZÖK – FIZIKAI VAGY LOGIKAI SZÉTKAPCSOLÁS

17.55. A szervezet biztosítja az együttműködésen alapuló számítástechnikai eszközök egyszerű és könnyű fizikai vagy logikai szétkapcsolását.

MAGYARÁZAT

Az együttműködésen alapuló számítástechnikai eszközökről történő szétkapcsolás elmulasztása a szervezeti információk későbbi veszélyeztetéséhez vezethet. Az ilyen eszközökről való leválasztás egyszerű módszereinek biztosítása a közös számítástechnikai munkamenet után biztosítja, hogy a résztvevők bonyolult és fárasztó eljárások nélkül végezzék el a szétkapcsolási műveletet. Az együttműködésen alapuló számítástechnikai eszközökről történő szétkapcsolás történhet manuálisan vagy automatikusan.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat az EIR-eket, amelyek együttműködésen alapuló számítástechnikai eszközökkel vannak összekapcsolva.
2. A szervezetnek biztosítania kell, hogy ezek az EIR-ek egyszerűen és könnyen szét lehessen kapcsolni, akár fizikailag, akár logikailag. Ez magában foglalhatja a kapcsolat bontásának automatizálását, vagy a felhasználók számára egyszerű utasítások biztosítását a kapcsolat bontásához.
3. A szervezetnek ki kell dolgoznia és be kell vezetnie egy szabályzatot és eljárásokat, amelyek előírják az EIR-ek szétválasztását a munkamenetek végén.
4. A szervezetnek naplót kell vezetnie arról, hogy mely EIR-ek vannak összekapcsolva, és mikor vannak szétkapcsolva. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon kövesse és ellenőrizze az EIR-ek használatát, és biztosítsa, hogy a szétválasztási eljárásokat megfelelően végrehajtják.

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

SC-15(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.56. EGYÜTTMŰKÖDÉSEN ALAPULÓ INFORMATIKAI ESZKÖZÖK – BIZTONSÁGOS MUNKATERÜLETEK

17.56. A szervezet letiltja vagy eltávolítja a meghatározott biztonságos munkaterületeken található együttműködésen alapuló számítástechnikai eszközöket és alkalmazásokat a meghatározott EIR-ekből, vagy rendszerelemekből.

MAGYARÁZAT

Ha az együttműködésen alapuló számítástechnikai eszközöket és alkalmazásokat nem kapcsolják ki vagy nem távolítják el az EIR-ekből vagy rendszerelemekből, az információk veszélyeztetéséhez vezethet, beleértve a beszélgetések lehallgatását is. A biztonságos munkaterületre példa az érzékeny információkkal foglalkozó létesítmény (Sensitive Compartmented Information Facility, SCIF).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítottania kell az együttműködésen alapuló eszközöket és alkalmazásokat, meg kell határoznia, hogy melyeket kell letiltani vagy eltávolítani az EIR-ekből. Ez a döntés a szervezet biztonsági szabályán, az alkalmazások biztonsági kockázatán és az EIR-ek védelmének szükségességén alapul.
2. A szervezetnek implementálnia kell a letiltási vagy szétkapcsolási folyamatot. Ez magában foglalhatja a szoftverfrissítéseket, a hozzáférési jogosultságok módosítását, vagy akár az eszközök fizikai eltávolítását is.
3. A szervezetnek naplóznia kell a letiltási vagy szétkapcsolási folyamatot. Ez magában foglalja az érintett eszközök és alkalmazások listáját, a végrehajtott intézkedéseket, valamint a változások időpontját.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a letiltási vagy szétkapcsolási folyamatot, hogy biztosítsa az EIR-ek folyamatos védelmét. Ez magában foglalja a naplók áttekintését, a biztonsági események elemzését, és a szükséges változtatások végrehajtását.

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

SC-15(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek illetve a biztonságos munkaterületek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.57. EGYÜTTMŰKÖDÉSEN ALAPULÓ INFORMATIKAI ESZKÖZÖK – RÉSZTVEVŐK EGYÉRTELMŰ FELSOROLÁSA

17.57. A szervezet biztosítja az általa meghatározott online megbeszéléseken és telefonkonferenciákon a résztvevők egyértelmű felsorolását.

MAGYARÁZAT

Az aktuális résztvevők egyértelmű feltüntetése megakadályozza, hogy illetéktelen személyek a többi résztvevő kifejezett tudta nélkül vegyenek részt az együttműködésen alapuló számítástechnikai munkamenetekben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell határoznia, mely online megbeszéléseken és telefonkonferenciákon szeretné biztosítani a résztvevők egyértelmű felsorolását.
2. A szervezetnek be kell vezetnie egy olyan EIR-t, amely képes nyomon követni és rögzíteni a résztvevőket az online megbeszéléseken és telefonkonferenciákon. Ez lehet egy beépített funkció az online megbeszélési platformon, vagy egy különálló EIR, amely integrálható a használt platformmal.
3. A szervezetnek biztosítania kell, hogy minden résztvevő, aki csatlakozik az online megbeszéléshez vagy telefonkonferenciához, azonosítja magát, és ez az információ rögzítésre kerül az EIR-ben.
4. A szervezetnek be kell állítania az EIR-t úgy, hogy a résztvevők listája mindenki számára látható legyen a megbeszélés alatt.
5. A szervezetnek rendszeresen ellenőriznie kell az EIR naplóját, hogy biztosítsa, nem voltak illetéktelen személyek a megbeszéléseken. Szabálytalanság észlelése esetén azonnali válaszlépéseket kell alkalmaznia.

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

SC-15(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az online egyeztetések és telekonferenciák meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.58. BIZTONSÁGI TULAJDONSÁGOK ÁTVITELE

17.58. A szervezet meghatározott biztonsági tulajdonságokat rendel a rendszerek és rendszerelemek között kicserélt információkhoz.

MAGYARÁZAT

A biztonsági tulajdonságok explicit vagy implicit módon társíthatók a szervezeti EIR-ekben vagy rendszerelemekben található információkhoz. A tulajdonságok olyan absztrakciók, amelyek egy entitás alapvető tulajdonságait vagy jellemzőit képviselik az információk védelme tekintetében. A tulajdonságok jellemzően belső adatstruktúrákhoz kapcsolódnak, beleértve a rendszerben lévő rekordokat, puffereket és fájlokat. A biztonsági tulajdonságok a hozzáférés-felügyelet és az információáramlás-szabályozási irányelvek végrehajtására szolgálnak; különleges terjesztési, kezelési vagy terjesztési utasításokat tükröznek, vagy az információbiztonsági irányelvek egyéb szempontjait támogatják.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonsági tulajdonságokat, amelyeket hozzárendel az EIR-ek és EIR-elemek között kicserélt információkhoz. Ezek a tulajdonságok lehetnek explicit vagy implicit módon társítva az információhoz.
2. A tulajdonságok általában az EIR belső adatszerkezeteihez, beleértve a rekordokat, puffereket és fájlokat, vannak társítva. Ezek a tulajdonságok reprezentálják az entitás alapvető tulajdonságait vagy jellemzőit az információ védelme szempontjából.
3. A biztonsági tulajdonságokat a szervezetnek hozzáférés-felügyeleti és információáramlás-ellenőrzési szabályok megvalósítására kell használnia; tükrözniük kell a speciális terjesztési, kezelési utasításokat, vagy támogatniuk kell az információbiztonsági szabályok más aspektusait.
4. A szervezetnek dokumentálnia kell a biztonsági tulajdonságok hozzárendelését és használatát az EIR-ekhez vagy rendszerelemekhez, hogy nyomon követhető legyen a folyamat és biztosítható legyen a megfelelőség.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

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

SC-16

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.59. BIZTONSÁGI TULAJDONSÁGOK ÁTVITELE – SÉRTETLENSÉG ELLENŐRZÉSE

17.59. Az EIR ellenőrzi a továbbított biztonsági tulajdonságok sértetlenségét.

MAGYARÁZAT

A továbbított információk sértetlenségének ellenőrzéséhez hozzátartozik annak biztosítása, hogy az ilyen információkhoz kapcsolódó biztonsági tulajdonságokat nem módosították jogosulatlanul. A biztonsági tulajdonságok jogosulatlan módosítása a továbbított információ sértetlenségének elvesztését eredményezheti.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR rendelkezzen a megfelelő biztonsági eszközökkel és protokollokkal, amelyek képesek ellenőrizni a továbbított biztonsági tulajdonságok sértetlenségét.
2. A szervezetnek implementálnia kell egy olyan biztonsági szabályt, amely meghatározza, hogy milyen biztonsági tulajdonságokat kell továbbítani, és hogyan kell ezeket ellenőrizni.
3. A szervezetnek biztosítania kell, hogy az EIR képes azonosítani és reagálni a nem engedélyezett módosításokra. Ez magában foglalhatja a nem engedélyezett hozzáférési kísérletek naplózását, a rendellenes hálózati forgalom észlelését és a rendszeres biztonsági ellenőrzéseket.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR-t, hogy meggyőződjön a biztonsági tulajdonságok sértetlenségéről. Ez magában foglalhatja a biztonsági naplók áttekintését, a rendszeres biztonsági auditokat és a biztonsági események utólagos vizsgálatát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.33. Letagadhatatlanság

17.40. Az adatátvitel bizalmassága és sértetlensége

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

SC-16(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.60. Biztonsági tulajdonságok átvitele – Megtévesztés elleni mechanizmusok

17.60. Az EIR hamisítás elleni mechanizmusok alkalmaz annak megakadályozására, hogy a rosszindulatú személyek meghamisítsák a biztonsági eljárás sikeres alkalmazását jelző biztonsági tulajdonságokat.

Magyarázat

Egyes támadási vektorok egy EIR biztonsági tulajdonságainak megváltoztatásával működnek, hogy rosszindulatú szándékkal nem megfelelő biztonsági szintet valósítsanak meg az EIR-ben. A tulajdonságok megváltoztatásával az érintett szervezetek azt feltételezik, hogy a ténylegesnél több biztonsági funkció van érvényben és működik.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia és alkalmaznia kell a megfelelő hamisítás elleni mechanizmusokat az EIR-ben. Ezek a mechanizmusok segítenek megakadályozni, hogy a támadók meghamisítsák a biztonsági eljárás sikeres alkalmazását jelző biztonsági tulajdonságokat.
2. A szervezetnek rendszeresen ellenőriznie kell az EIR biztonsági tulajdonságait, hogy biztosítsa, hogy a hamisítás elleni mechanizmusok hatékonyan működnek és megfelelően védik az EIR-t.
3. A szervezetnek naplóznia és monitoroznia kell, hogy nyomon követhesse a biztonsági tulajdonságok változásait és az esetleges hamisítási kísérleteket.
4. A szervezetnek folyamatosan frissítenie és fejlesztenie kell a hamisítás elleni mechanizmusokat, hogy lépést tudjon tartani a változó kiberbiztonsági fenyegetésekkel és biztosíthassa az EIR hosszú távú védelmét.

Kapcsolódó intézkedések

18.8. Kártékony kódok elleni védelem

18.13. Az EIR monitorozása

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

SC-16(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.61. BIZTONSÁGI TULAJDONSÁGOK ÁTVITELE – KRIPTOGRÁFIAI KÖTÉS

17.61. A szervezet meghatározott mechanizmusokat vagy technikákat alkalmaz, hogy a biztonsági tulajdonságokat az átvitt információhoz kösse.

MAGYARÁZAT

Az érintett szervezet kriptográfiai mechanizmusokat és technikákat alkalmaz, amelyek erős biztonsági és adatvédelmi tulajdonságokat kötnek az átvitt információhoz, ezzel segítve annak integritásának biztosítását. Az EIR adatainak védelme érdekében a szervezetnek biztosítania kell, hogy az átvitt információk megfelelően védettek legyenek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell választania és be kell vezetnie a megfelelő kriptográfiai mechanizmusokat vagy technikákat. Ezek a mechanizmusok segítenek a biztonsági tulajdonságok azonosításában és hozzárendelésében az átvitt információhoz.
2. A szervezetnek biztosítania kell, hogy minden EIR megfelelően integrálja és alkalmazza a kiválasztott kriptográfiai mechanizmusokat. Ez magában foglalja a mechanizmusok beállítását, tesztelését és karbantartását.
3. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a használt kriptográfiai mechanizmusokat és technikákat, hogy biztosítsa azok hatékonyságát és relevanciáját. Ez magában foglalja a legújabb kiberbiztonsági fenyegetések és iparági jógyakorlatok figyelemmel kísérését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.89. Biztonsági tulajdonságok

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

SC-16(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a mechanizmusok vagy technikák meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.62. NYILVÁNOS KULCSÚ INFRASTRUKTÚRA TANÚSÍTVÁNYOK

17.62. A szervezet:

17.62.1. nyilvános kulcsú tanúsítványokat állít ki a szervezet által meghatározott tanúsítványkiadási szabályok szerint, vagy nyilvános kulcsú tanúsítványokat szerez be egy bizalmi szolgáltatótól; és

17.62.2. a szervezet által kezelt tanúsítványtárolókban, csak jóváhagyott, hitelesített tanúsítvány vehető fel.

MAGYARÁZAT

A nyilvános kulcsú infrastruktúra tanúsítványai magukban foglalják a szervezeti rendszereken kívüli láthatósággal rendelkező tanúsítványokat és a rendszerek belső működéséhez kapcsolódó tanúsítványokat is, ilyenek például az alkalmazásspecifikus idővel kapcsolatos szolgáltatások. A hierarchikus felépítésű kriptográfiai rendszerekben bizalmi szempontból "fix pont" egy olyan hiteles forrás (pl. tanúsító hatóság), amely iránt a bizalom feltételezett és nem származtatott. Egy PKI-rendszer gyökér-tanúsítványa egy példa egyfajta bizalmi szempontból fix pontra. A bizalmi tároló vagy tanúsítványtároló a megbízható gyökértanúsítványok listáját tartja nyilván.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a tanúsítványkiadási szabályokat, amelyek alapján nyilvános kulcsú tanúsítványokat fog kiadni.

2. A szervezetnek létre kell hoznia egy tanúsítványkiadó rendszert, amely képes a nyilvános kulcsú tanúsítványok kiadására. Az EIR-nek biztosítania kell, hogy a CA megfelelően védett legyen, hogy a tanúsítványok integritása ne legyen veszélyeztetve.

3. A szervezetnek be kell szereznie a nyilvános kulcsú tanúsítványokat egy bizalmi szolgáltatótól, amennyiben nem saját maga állítja ki őket. A bizalmi szolgáltatótól származó tanúsítványokat az EIR-nek hitelesítenie kell, mielőtt felvenné őket a tanúsítványtárolóba.

4. A szervezetnek létre kell hoznia megfelelően védett tanúsítványtárolókat, amelyekben csak jóváhagyott, hitelesített tanúsítvány vehető fel.

5. A szervezetnek dokumentálnia kell a tanúsítványok kiadását és hitelesítését, hogy nyomon követhető legyen a tanúsítványok életciklusa.
6. A szervezetnek rendszeresen ellenőriznie kell a tanúsítványtárolókat és a tanúsítványkiadó rendszert, hogy biztosítsa a tanúsítványok biztonságát és integritását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.33. Letagadhatatlanság
8.21. A hitelesítésre szolgáló eszközök kezelése
17.49. Kriptográfiai kulcs előállítása és kezelése

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

3.3.13.13. Nyilvános kulcsú infrastruktúra tanúsítványok: Az érintett szervezet nyilvános kulcsú tanúsítványokat állít ki a belső hitelesítési rend szerint, vagy a nyilvános kulcsú tanúsítványokat beszerzi a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatótól.

ISO/IEC 27001:2023 REFERENCIA

A.8.24

NIST SP 800-53 REV.5 REFERENCIA

SC-17

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.63. MOBILKÓD KORLÁTOZÁSA

17.63. A szervezet:

17.63.1. meghatározza az elfogadható és a nem elfogadható mobilkódokat, valamint a mobilkód technológiákat; valamint

17.63.2. engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az EIR-en belül.

MAGYARÁZAT

A mobilkódok szervezeti információs rendszereken belüli alkalmazásával kapcsolatos döntések az esetleges rosszindulatú felhasználás esetén a rendszerben okozott lehetséges kár mértékén alapulnak. A mobilkód-technológiák közé tartozik például a Java, a JavaScript, a HTML5, a WebGL és a VBScript. A használati korlátozások és a kivitelezési iránymutatások mind a szerverekre telepített mobilkódok kiválasztására és használatára, mind az egyes munkaállomásokon és eszközökön letöltött és futtatott mobilkódra vonatkoznak. A mobilkód-irányelvek és eljárások a szervezeti EIR-eken belüli nem elfogadható mobilkódok fejlesztésének, beszerzésének vagy a bevezetésének megakadályozását szolgálják.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az elfogadható és nem elfogadható mobilkódokat.

2. A szervezetnek fel kell térképeznie a használatban lévő mobilkód technológiákat. Ilyen technológiák például a Java appletek, a JavaScript, az HTML5, a WebGL és a VBScript.

3. A szervezetnek korlátozásokat kell bevezetnie a mobilkódok használatára, és irányelveket kell kidolgoznia a mobilkódok kiválasztására és használatára vonatkozóan. Ezek a korlátozások és irányelvek vonatkoznak mind a szervereken telepített mobilkódokra, mind az egyéni munkaállomásokon és eszközökön letöltött és futtatott mobilkódokra, beleértve a notebookokat és okostelefonokat.

4. A szervezetnek szabályozást és eljárásokat kell kidolgoznia a mobilkódokkal kapcsolatban. Ezeknek a szabályozásoknak és eljárásoknak ki kell térniük arra, hogy milyen lépéseket tesznek annak érdekében, hogy megakadályozzák a nem elfogadható mobilkódok fejlesztését, beszerzését és bevezetését az EIR-ben. Például előírhatják, hogy a mobilkódokat digitálisan alá kell írni egy megbízható forrástól.

5. A szervezetnek engedélyeznie, felügyelnie és ellenőriznie kell a mobilkódok használatát az EIR-en belül. Ez magában foglalhatja a mobilkódok használatának naplózását, a mobilkódok használatának ellenőrzését, és a mobilkódok használatának engedélyezését vagy tiltását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.40. Naplóbejegyzések létrehozása

6.2. Alapkonfiguráció

6.23. Konfigurációs beállítások

18.8. Kártékony kódok elleni védelem

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

3.3.13.14. Mobilkód korlátozása

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-18

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.64. MOBILKÓD KORLÁTOZÁSA – NEM ELFOGADHATÓ KÓD AZONOSÍTÁSA ÉS KORREKTÍV INTÉZKEDÉSEK

17.64. A szervezet azonosítja a meghatározott nem elfogadható mobilkódot, majd meghatározott korrekciós intézkedéseket hajt végre.

MAGYARÁZAT

Az érintett szervezet azonosítja a nem elfogadható mobilkódot, majd meghatározott korrekciós intézkedéseket hajt végre. Ezek a korrekciós intézkedések tartalmazhatják a blokkolást, karanténba helyezést vagy az adminisztrátorok értesítését. A blokkolás magában foglalja például a beágyazott makrókkal rendelkező szöveges fájlok továbbításának megakadályozását, amennyiben ezeket a makrókat nem elfogadható mobilkódnak minősítették.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet meghatározza a nem elfogadható mobilkódot. Ez magában foglalhatja a mobilkódok vizsgálatát, a kódok elemzését és a nem elfogadható kódok azonosítását.
2. A szervezetnek a nem elfogadható mobilkódokra korrekciós intézkedéseket kell meghatároznia. Ez magában foglalhatja a mobilkód blokkolását, karanténba helyezését vagy az adminisztrátorok értesítését.
3. A szervezetnek dokumentálnia kell a nem elfogadható mobilkódok azonosítását és a hozzájuk kapcsolódó korrekciós intézkedéseket.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a mobilkódokkal kapcsolatos szabályait és eljárásait.

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

SC-18(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a nem elfogadott mobilkódok illetve a korrekciós intézkedések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.65. MOBILKÓD KORLÁTOZÁSA – BESZERZÉS, FEJLESZTÉS ÉS HASZNÁLAT

17.65. A szervezet ellenőrzi, hogy a rendszerben telepítendő mobilkód beszerzése, fejlesztése és használata megfelel-e a szervezet által meghatározott mobilkódokra vonatkozó követelményeknek.

MAGYARÁZAT

Az érintett szervezetnek gondoskodnia kell arról, hogy a rendszerekben telepítendő mobilkódok beszerzése, fejlesztése és használata megfeleljen az általa meghatározott követelményeknek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a mobilkódokra vonatkozó követelményeket a rendszerekben. Ez magában foglalhatja a mobilkódok biztonsági szintjével, a kompatibilitásával és a teljesítménnyel kapcsolatos követelményeket.
2. A szervezetnek ellenőriznie kell, hogy a beszerzett, fejlesztett vagy épp használatban lévő mobilkódok megfelelnek-e az általa meghatározott követelményeknek. Ez kiterjedhet a kódok tesztelésére, ellenőrzésére és validálására.
3. Ha a mobilkódok nem felelnek meg a követelményeknek, az érintett szervezetnek intézkedéseket kell tennie a problémák kijavítására. Ez magában foglalhatja a kódok módosítását, frissítését vagy cseréjét.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a mobilkódokra vonatkozó követelményeket, hogy biztosítsa az EIR folyamatos biztonságát és hatékony működését.

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

SC-18(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a mobilkód követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.66. MOBILKÓD KORLÁTOZÁSA – LETÖLTÉS ÉS KÓDVÉGREHAJTÁS MEGAKADÁLYOZÁSA

17.66. A szervezet megakadályozza az általa meghatározott nem elfogadható mobilkód letöltését és végrehajtását.

MAGYARÁZAT

Az érintett szervezet megakadályozza az általa meghatározott nem elfogadható mobilkód letöltését és végrehajtását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, milyen mobilkódokat tekint nem elfogadhatónak. Ez magában foglalhatja a kártékony kódot tartalmazó mobilkódokat, a nem biztonságos forrásból származó mobilkódokat, stb.
2. A szervezetnek naplózniuk kell és monitorozásra van szüksége, hogy nyomon követhesse a nem elfogadható mobilkódok letöltését és végrehajtását. Ez magában foglalhatja a letöltési naplókat, a rendszeres biztonsági jelentéseket, a rendszeres napló ellenőrzéseket stb.
3. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR biztonsági szabályait, hogy biztosítsa annak hatékonyságát és relevanciáját, a technológiai változásokhoz igazodva.
4. A szervezetnek biztosítania kell, hogy minden munkavállaló megfelelő biztonságtudatossági képzésben részesüljön és tisztában legyenek a nem elfogadható mobilkódokra vonatkozó szabályokkal.

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

SC-18(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a nem elfogadott mobilkódok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.67. MOBILKÓD KORLÁTOZÁSA – AUTOMATIKUS KÓDVÉGREHAJTÁS MEGAKADÁLYOZÁSA

17.67. A szervezet megakadályozza a mobilkódok automatikus végrehajtását a meghatározott szoftverekben, valamint kikényszeríti a meghatározott intézkedések végrehajtását a mobilkódok futtatása előtt.

MAGYARÁZAT

Az érintett szervezet által a mobilkódok automatikus végrehajtásának megakadályozása érdekében meghatározásra kerülő intézkedések közé tartozik a felhasználók figyelmeztetése, mielőtt e-mail mellékleteket nyitnának meg vagy webhivatkozásokra kattintanának. A mobilkódok automatikus végrehajtásának megakadályozása magában foglalja az automatikus végrehajtási funkciók letiltását azon rendszerelemeken, amelyek hordozható tárolóeszközöket használnak, mint például fizikai lemezek, digitális tárolólemezek és USB eszközök. A mobilkódok végrehajtása előtti meghatározott intézkedések végrehajtásának kikényszerítése és a mobilkódok automatikus végrehajtásának megakadályozása segít a szervezetnek megelőzni a kártékony kódok által okozott károkat és biztonsági eseményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, mely esetekben szeretné megakadályozni a mobilkódok automatikus végrehajtását.
2. A szervezetnek el kell végeznie a szükséges beállításokat a mobilkód végrehajtásban érintett rendszerelemeken úgy, hogy azok ne hajtsák végre automatikusan a mobilkódokat. Ez magában foglalhatja az automatikusan végrehajtott funkciók letiltását az érintett rendszerelemeken, és hordozható tárolóeszközökön.
3. A szervezetnek ki kell kényszerítenie a meghatározott intézkedések végrehajtását a mobilkódok futtatása előtt. Ez magában foglalja a felhasználók figyelmeztetését, mielőtt e-mail mellékleteket nyitnának meg vagy webhivatkozásokra kattintanának.

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

SC-18(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szoftver alkalmazások illetve a tevékenységek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.68. MOBILKÓD KORLÁTOZÁSA – CSAK ZÁRT KÖRNYEZETEKBEN VALÓ KÓDVÉGREHAJTÁS

17.68. A szervezet a jóváhagyott mobilkód futtatását kizárólag zárt, virtualizált környezetben engedélyezi.

MAGYARÁZAT

Az érintett szervezet által jóváhagyott mobilkód futtatásának korlátozása kizárólag zárt, virtualizált környezetekre segít megelőzni a rosszindulatú kódok bevezetését más EIR-ekbe és rendszerelemekbe.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy képes legyen virtualizált környezetek létrehozására és kezelésére.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a mobilkódok futtatása csak zárt virtualizált környezetben legyen lehetséges.
3. A szervezetnek dokumentálnia kell a zárt virtuális környezetben történő mobilkódok futtatásának eredményeit.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.122. Izolált futtatási környezetek

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

SC-18(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.69. BIZTONSÁGOS NÉV/CÍM FELOLDÁSI SZOLGÁLTATÁS (HITELES FORRÁS)

17.69. Az EIR:

17.69.1. A név- és címfeloldási kérésekre a hiteles névfeloldási adatokon kívül az információ eredetére és a tartalom sértetlenségére vonatkozó kiegészítő adatokat is biztosít.

17.69.2. Amennyiben egy elosztott, hierarchikus névtér részeként működik, jelzi a gyermektartományok biztonsági állapotát is, és ha azok támogatják a biztonságos névfeloldási szolgáltatásokat, lehetővé teszi a szülő- és gyermektartományok közötti bizalmi lánc ellenőrzését.

MAGYARÁZAT

Ez az intézkedés lehetővé teszi, hogy a külső kliensek, beleértve például a távoli internetes klienseket, eredethitelesítéssel és integritás-ellenőrzéssel kapcsolatos biztos információt szerezzenek a hoszt/szolgáltatás név hálózati címre való feloldásával kapcsolatban. A név- és címfeloldási szolgáltatásokat nyújtó információs rendszerek közé tartoznak például a DNS-kiszolgálók. A további lehetőségek közé tartozik például a DNS biztonsági elektronikus aláírások (DNSSEC) és a kriptográfiai kulcsok. A DNS erőforrásrekord (resource record) példa a hiteles adatokra. A gyermektartomány (child zones) biztonsági állapotának jelzésére szolgáló eszközök közé tartozik például a delegáció-aláíró erőforrásrekordok (DS) használata a DNS-ben. Azon EIR-ek számára, amelyek nem DNS-t használnak a hoszt/szolgáltatás nevek hálózati címmel való összerendelésére, más eszközöket használnak a válaszadatok hitelességének és integritásának ellenőrzésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az EIR-nek biztosítania kell a név- és címfeloldási kérésekhez hiteles névfeloldási adatokat, valamint az információ eredetére és a tartalom sértetlenségére vonatkozó kiegészítő adatokat. Ez lehetővé teszi a külső kliensek számára, beleértve a távoli internetes klienseket is, hogy eredet hitelesítéssel és integritás ellenőrzéssel kapcsolatos biztos információt szerezzenek a szolgáltatáson keresztül megszerzett név és hálózati cím feloldással kapcsolatban.

2. Az EIR-nek, amennyiben egy elosztott, hierarchikus névtér részeként működik, vissza kell jeleznie a gyermektartományok biztonsági állapotával kapcsolatosan. Ezt a delegáció aláíró erőforrás rekordok használatával teheti meg a DNS-ben.

3. Az EIR-nek lehetővé kell tennie a szülő- és gyermektartományok közötti bizalmi lánc ellenőrzését, amennyiben a gyermektartományok támogatják a biztonságos névfeloldási szolgáltatásokat.

4. Az EIR-nek, amelyek olyan technológiákat használnak, amelyek nem a DNS-t használják a hoszt és szolgáltatás nevek és hálózati címek közötti leképezéshez, más eszközöket kell biztosítania a válaszadatok hitelességének és integritásának biztosítására.

5. Az EIR-nek további eszközöket kell biztosítania, mint például a DNS Biztonsági Kiterjesztések digitális aláírások és kriptográfiai kulcsok.

6. Az EIR-nek hiteles adatokat kell biztosítania, beleértve a DNS erőforrás rekordokat.

Kapcsolódó intézkedések

4.33. Letagadhatatlanság

17.40. Az adatátvitel bizalmassága és sértetlensége

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

17.71. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)

17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

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

3.3.13.16. Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás): Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-20

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

17.70. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás) – Adat forrása és bizalmassága

17.70. Az EIR biztosítja az adatok eredetiségének és sértetlenségének a védelmét a belső név- és címfeloldási lekérdezések során.

Magyarázat

Az EIR biztosítja az adatok eredetiségének és sértetlenségének a védelmét a belső név- és címfeloldási lekérdezések során.

A követelmény alkalmazásának lépései

1. Az EIR-nek biztosítania kell a név- és címfeloldási kérésekhez hiteles névfeloldási adatokat, valamint az információ eredetére és a tartalom sértetlenségére vonatkozó kiegészítő adatokat. Ez lehetővé teszi a külső kliensek számára, beleértve a távoli internetes klienseket is, hogy eredet hitelesítéssel és sértetlenség ellenőrzéssel kapcsolatos biztos információt szerezzenek a szolgáltatáson keresztül megszerzett név és hálózati cím feloldásisal kapcsolatban.
2. Az EIR-nek, amennyiben egy elosztott, hierarchikus névtér részeként működik, vissza kell jelezni a gyermektartományok biztonsági állapotával kapcsolatosan. Ezt a delegáció aláíró rekordok használatával teheti meg a DNS-ben.
3. Ha a gyermektartományok támogatják a biztonságos névfeloldási szolgáltatásokat, az EIR-nek lehetővé kell tennie a szülő- és gyermektartományok közötti bizalmi lánc ellenőrzését.
4. Azon EIR-ek, amelyek olyan technológiákat használnak, amelyek nem a DNS-t használják a host és szolgáltatás nevek és hálózati címek közötti leképezéshez, más eszközöket kell biztosítania a válaszadatok hitelességének és sértetlenségének biztosítására.
5. Ahol csak lehetséges az EIR-nek további eszközöket kell biztosítania, mint például a DNS biztonsági kiterjesztések digitális aláírások és kriptográfiai kulcsok.
6. Az EIR-nek hiteles adatokat kell biztosítania, beleértve a DNS erőforrás rekordokat.

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

SC-20(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.71. BIZTONSÁGOS NÉV/CÍM FELOLDÓ SZOLGÁLTATÁS (REKURZÍV VAGY GYORSÍTÓTÁRAT HASZNÁLÓ FELOLDÁS)

17.71. Az EIR eredet-hitelesítést és adatsértetlenség-ellenőrzést kér és hajt végre a hiteles forrásból származó név- és címfeloldó válaszokon.

MAGYARÁZAT

A névfeloldási szolgáltatások minden kliense önállóan végzi el ezt az ellenőrzést, vagy hitelesített csatornákkal rendelkezik a megbízható hitelesítési szolgáltatók irányába. A helyi kliensek számára név- és címfeloldási szolgáltatásokat nyújtó információs rendszerek közé tartozik például a rekurzív feloldású vagy gyorsítótárazó domainnév szerverek. A DNS-kliens feloldók elvégzik a DNSSEC-aláírások validálását, vagy a kliensek hitelesített csatornákat használnak az ilyen validálásokat végrehajtó rekurzív feloldókhoz kapcsolódva. A DNS-től eltérő technológiákat használó információs rendszerek a hoszt/szolgáltatásnevek és a hálózati címek közötti összerendeléshez más eszközöket biztosítanak a kliensek számára a válaszadatok hitelességének és sértetlenségének ellenőrzésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy minden név- és címfeloldó szolgáltatásokat igénybe vevő kliens önállóan végezze el ezt a hitelesítést, vagy hitelesített csatornákon keresztül kapcsolódjon a megbízható hitelesítési szolgáltatókhoz.
2. A szervezetnek meg kell határoznia, hogy a DNS kliens feloldóknak vagy el kell végezniük a DNSSEC aláírások hitelesítését, vagy a klienseknek hitelesített csatornákon keresztül kell csatlakozniuk a rekurzív feloldókhoz, amelyek ilyen hitelesítéseket végeznek.
3. Az EIR-nek, amelyek más technológiákat használnak a DNS-nél a host és szolgáltatásnevek és hálózati címek közötti leképezéshez, biztosítania kell valamilyen más módot a kliensek számára, hogy ellenőrizhessék a válaszadatok hitelességét és sértetlenségét.
4. A szervezetnek naplóznia kell a hitelesítési folyamatokat és az adatok sértetlenségét, hogy nyomon követhesse és ellenőrizhesse azokat.

Kapcsolódó intézkedések

17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

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

3.3.13.17. Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsítótárat használó feloldás): Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér, és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SC-21

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

17.72. ARCHITEKTÚRA ÉS TARTALÉKOK NÉV/CÍM FELOLDÁSI SZOLGÁLTATÁS ESETÉN

17.72. A szervezet számára név- és címfeloldási szolgáltatást együttesen biztosító EIR-ek hibatűrő képességgel rendelkeznek, és alkalmazzák a belső és a külső szerepkörök szétválasztását.

MAGYARÁZAT

A név- és címfeloldási szolgáltatásokat nyújtó információs rendszerek közé tartoznak például a DNS-kiszolgálók. A kritikus hibapontok (ún. single points of failure) kiküszöbölése és a redundancia fokozása érdekében a szervezetek legalább két hiteles tartománynév-kiszolgálót alkalmaznak, az egyiket elsődleges kiszolgálóként, a másik pedig másodlagos kiszolgálóként konfigurálva. Ezen túlmenően a szervezetek rendszerint két földrajzilag elkülönített alhálózaton (azaz nem ugyanabban a fizikai létesítményben) telepítik a szervereket. A szerepkör-szétválasztáshoz a belső szerepkörrel rendelkező DNS-kiszolgálók csak a szervezeten belüli (azaz belső kliensektől származó) név- és címfeloldási kérelmeket dolgoznak fel. A külső szerepekkel rendelkező DNS-kiszolgálók csak a szervezeteken kívüli kliensek név- és címfeloldási kéréseit kezelik (azaz külső hálózatokon, beleértve az internetet is). A szervezetek meghatározzák a klienseket, akik bizonyos szerepkörökben elérhetik a hiteles DNS-kiszolgálókat (pl. címtartományok, explicit listák).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR-ek, amelyek név- és címfeloldási szolgáltatást biztosítanak, hibatűrő képességgel rendelkeznek. Ez azt jelenti, hogy legalább két hiteles DNS kiszolgálót kell alkalmazni - az egyiket elsődleges szerverként, a másikat pedig másodlagos szerverként konfigurálva. A hibatűrés növelése érdekében a szervezetnek a kiszolgálókat két földrajzilag elválasztott alhálózatban kell telepítenie.
2. A szervezetnek biztosítania kell, hogy a belső és külső szerepkörök szétválasztása érdekében a kiszolgálók, amelyek belső szerepkörrel rendelkeznek, csak a szervezeten belüli név- és címfeloldási kéréseket dolgozzák fel, míg azon kiszolgálók, amelyek külső szerepkörrel

rendelkeznek, csak a szervezeten kívüli kliensektől érkező név- és címfeloldási információs kéréseket dolgozzák fel (pl. internet irányából).

4. A szervezetnek meg kell határoznia azokat a klienseket, amelyek bizonyos szerepkörökben elérhetnek a hiteles DNS szerverekhez (például címtartományok és explicit listák alapján).

Kapcsolódó intézkedések

17.2. Rendszer és felhasználói funkciók szétválasztása

17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

17.71. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)

17.77. Ismert állapot való meghibásodás

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

3.3.13.18. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén: Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SC-22

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

17.73. MUNKASZAKASZ HITELESSÉGE

17.73. Az EIR védi a kommunikációs munkaszakaszok hitelességét.

MAGYARÁZAT

Ez az intézkedés a kommunikáció védelmét tárgyalja a munkaszakaszra fókuszálva, nem pedig csomagszinten vizsgálva, és megalapozza a bizalmat a résztvevők azonosságával és az átvitt információ érvényességével kapcsolatban a munkaszakaszban a kommunikációban résztvevő mindkét fél esetében. A hitelességgel kapcsolatos védelmi intézkedések magában foglalják például a közbeékelődéses (man-in-the-middle) támadások/munkaszakasz-eltérítések és a hamis információk munkaszakaszba illesztése elleni védelmet is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell vizsgálnia a kommunikációt munkaszakasz szinten, nem a csomagok szintjén.
2. A szervezetnek meg kell védenie a rendszert a közbeékelődéses támadásoktól, a munkaszakasz-eltérítésektől (session hijacking), és a hamis információk munkaszakasz történő beszúrásától.
3. A szervezetnek meg kell bizonyosodnia arról, hogy az összes rendszerben megfelelő biztonsági intézkedések vannak érvényben a munkaszakaszok hitelességének védelmére.
5. A szervezetnek rendszeresen ellenőriznie kell az EIR-t, hogy biztosítsa a munkaszakaszok hitelességének folyamatos védelmét.
6. A szervezetnek folyamatosan képeznie kell a munkatársait a munkaszakaszok hitelességéről, hogy mindenki tisztában legyen a potenciális kockázatokkal és a megfelelő védelmi intézkedésekkel.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.33. Letagadhatatlanság
17.40. Az adatátvitel bizalmassága és sértetlensége
17.46. A hálózati kapcsolat megszakítása
17.47. Megbízható útvonal

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

3.3.13.19. Munkaszakasz hitelessége: Az elektronikus információs rendszer védje meg a munkaszakaszok hitelességét.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-23

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.74. Munkaszakasz hitelessége – Munkaszakasz-azonosítók érvénytelenítése kijelentkezéskor

17.74. Az EIR érvényteleníti a felhasználói munkaszakasz azonosítóját, amikor a felhasználó kijelentkezik, vagy a munkaszakasz más módon befejeződik.

Magyarázat

Az EIR egyik kiberbiztonsági követelménye, hogy érvénytelenítse a felhasználó munkamenet-azonosítóját, amikor a felhasználó kijelentkezik, vagy a munkamenet más módon befejeződik. Ez a követelmény azért fontos, mert korlátozza a rosszindulatú támadók képességét arra, hogy ellopják és újra felhasználják a korábban érvényes munkamenet-azonosítókat.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell, hogy az EIR rendelkezik a felhasználói munkamenet-azonosítók érvénytelenítésére képes funkcióval. Ez a funkció lehet beépített vagy egy különálló biztonsági eszköz része.
2. A szervezetnek be kell állítania az összes rendszert úgy, hogy automatikusan érvénytelenítse a felhasználói munkamenet-azonosítót, amikor a felhasználó kijelentkezik. Ez magában foglalhatja a felhasználói munkamenet-azonosító törlését vagy érvénytelenítését.
3. A szervezetnek be kell állítania, hogy automatikusan érvénytelenítésre kerüljön a felhasználói munkamenet-azonosító, ha a munkamenet bármilyen módon befejeződik. Ez magában foglalhatja a munkamenet időtúllépését, hálózati hiba esetén történő megszakítást, vagy a felhasználói munkamenet-azonosító érvényességi idejének lejártát.

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

SC-23(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.75. Munkaszakasz hitelessége – A rendszer által generált egyedi munkaszakasz-azonosítók

17.75. Az EIR minden munkaszakaszhoz egyedi munkaszakasz-azonosítót hoz létre a szervezet által meghatározott véletlenszerűségi követelményeknek megfelelően, és csak a rendszer által generált munkaszakasz-azonosítókat fogadja el.

Magyarázat

Az egyedi munkamenet-azonosítók létrehozása minden munkamenet esetén korlátozza a támadók képességét arra, hogy korábban érvényes munkamenet-azonosítókat használjanak újra. A véletlenszerűség elvének alkalmazása az egyedi munkamenet-azonosítók generálásában védelmet nyújt a véletlenszerű próbálkozással végrehajtott támadások ellen, amelyek a munkamenet-azonosítók kitalálására irányulnak.

A követelmény alkalmazásának lépései

1. A szervezetnek be kell állítania az EIR-t úgy, hogy minden munkamenethez egyedi munkamenet-azonosítót hozzon létre.
2. A munkamenet-azonosítók generálásánál a szervezetnek figyelembe kell vennie a véletlenszerűségi követelményeket. Ez azt jelenti, hogy az azonosítók nem követhetnek egy előre meghatározott mintát, és nem lehetnek kiszámíthatóak.
3. A szervezetnek be kell állítania az összes szolgáltatást és rendszert úgy, hogy csak a rendszer által generált munkamenet-azonosítókat fogadja el. Ez azt jelenti, hogy a felhasználók vagy harmadik felek által létrehozott azonosítókat el kell utasítani.

Kapcsolódó intézkedések

2.81. Egyidejű munkaszakasz kezelés

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

SC-23(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a véletlenszerűségi követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.76. Munkaszakasz hitelessége – Engedélyezett tanúsítvány kibocsájtók

17.76. A szervezet a védett munkaszakasz létrehozásának ellenőrzésére csak a szervezet által meghatározott tanúsítványkibocsátók tanúsítványainak használatát engedélyezi.

Magyarázat

Az érintett szervezet által meghatározott tanúsítványkibocsátók tanúsítványainak használatával történő védett munkamenet létrehozásának követelményei közé tartozik a Transport Layer Security tanúsítványok használata. Ezek a tanúsítványok, miután a hozzájuk tartozó tanúsítványkibocsátók ellenőrizték őket, lehetővé teszik a védett munkamenetek létrehozását a webes kliensek és a webszerverek között.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia és jóváhagynia azokat a tanúsítványkibocsátókat, amelyeket a védett munkamenet létrehozásának ellenőrzésére használni kíván.
2. A szervezetnek implementálnia kell egy rendszert, amely képes kezelni és ellenőrizni a tanúsítványok használatát. Ez a rendszer képes lesz azonosítani és ellenőrizni a tanúsítványkibocsátók által kiadott tanúsítványokat.
3. A szervezetnek biztosítania kell, hogy az összes szolgáltatás és kommunikációban résztvevő fél csak a meghatározott tanúsítványkibocsátók tanúsítványait fogadja el. Ez azt jelenti, hogy a rendszereknek képesnek kell lennie elutasítani azokat a tanúsítványokat, amelyek nem a meghatározott tanúsítványkibocsátóktól származnak.

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

SC-23(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a tanúsítvány kibocsátók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.77. ISMERT ÁLLAPOTBA VALÓ VISSZATÉRÉS

17.77. A rendszer meghatározott rendszerelemei a meghatározott hibák bekövetkezése estén megőrzik a hiba bekövetkezése előtti ismert rendszerállapotukat.

MAGYARÁZAT

A hiba bekövetkezése előtti ismert állapot megőrzése vagy visszaállítása a szervezeti EIR-ek vagy azok rendszerelemeinek meghibásodása esetén megakadályozza a bizalmasság, az sértetlenség vagy az információ rendelkezésre állásának degradálódását. A hiba bekövetkezése előtti ismert állapot megőrzése megakadályozza, hogy a rendszerek olyan állapotba kerüljenek, amely személyi sérülést vagy vagyonelemek megsemmisülését okozhatja. Az információs rendszer állapotinformációinak megőrzése megkönnyíti a rendszer újraindítását és a szervezetek működésének helyreállását, így kevésbé zavarva a üzleti (ügymeneti) folyamatokat és az alapfunkciókat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azon EIR-eket vagy ezek rendszerelemeit, amelyeknek meg kell őrizniük a hiba bekövetkezése előtti ismert állapotukat.
2. A szervezetnek meg kell határoznia a potenciális hibákat, amelyek bekövetkezése esetén a rendszerelemeknek meg kell őrizniük a hiba előtti állapotukat.
3. A szervezetnek implementálnia kell egy rendszert vagy eljárást, amely lehetővé teszi a rendszerelemeinek, hogy visszatérjenek a hiba előtti állapotba, ha a meghatározott hibák bekövetkeznek.
4. A szervezetnek tesztelnie kell ezt a rendszert vagy eljárást, hogy biztosítsa annak hatékonyságát és megbízhatóságát a hibák bekövetkezése esetén.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

7.13. Üzletmenet-folytonossági terv tesztelése

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

7.48. Átállás biztonságosüzemmódra

16.16. Biztonságtervezési elvek

17.17. A határok védelme

17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

18.68. Előrelátható meghibásodás megelőzése

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

3.3.13.20. Hibát követő ismert állapot: Meghatározott hibatípusokhoz tartozó hibát követően az elektronikus információs rendszer a kijelölt, vagy utolsó ismert állapotba kerül, amely a hiba esetén is megőrzi a rendszerállapot információkat.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SC-24

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az ismert rendszerállapot illetve a rendszerállapot információk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

17.78. FUNKCIONALITÁS ÉS INFORMÁCIÓTÁROLÁS MINIMALIZÁLÁSA

17.78. A szervezet minimális funkcionalitást és információtárolást alkalmaz a meghatározott rendszerelemeken.

MAGYARÁZAT

A rendszerelemek minimális funkcionalitással történő telepítése csökkenti annak szükségességét, hogy minden végpont esetén nagy erőforrásokat kelljen abba fektetni, hogy azok biztonságosak maradjanak, és csökkentheti az információk, a rendszerek, és azoknak szolgáltatásainak támadásoknak való kitettségét. A csökkentett vagy minimális funkcionalitás magában foglalja a lemezolvasó nélküli eszközök használatát és az egyéb vékony kliens technológiákat is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat az elemeket, amelyek minimális funkcionalitást és információtárolást igényelnek.
2. A szervezetnek úgy kell elvégeznie minden telepítést, hogy azok eredményeképpen csak a minimálisan szükséges funkcionalitások és információtárolás legyen biztosított.
3. A szervezetnek biztosítania kell, hogy a rendszerek megfelelően védettek legyenek a támadásokkal szemben, még akkor is, ha csak minimális funkcionalitást és információtárolást biztosítanak.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.87. Elfedés és megtévesztés

17.122. Izolált futtatási környezetek

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

SC-25

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.79. CSAPDÁK ALKALMAZÁSA

17.79. A szervezet kifejezetten rosszindulatú támadások célpontjául szolgáló elemeket épít be a szervezeti EIR-ekbe, hogy az ilyen támadásokat észlelni, elhárítani és elemezni tudja.

MAGYARÁZAT

Az érintett szervezet kifejezetten rosszindulatú támadások célpontjául szolgáló elemeket (ún. honeypot) hoz létre, hogy ezekkel bevonzza a támadókat és elterelje a támadásokat a tényleges, éles, fő rendszerekről, amelyek támogatják a szervezeti alapfeladatokat és alapfunkciókat. A kifejezetten rosszindulatú támadások célpontjául szolgáló elemek használata esetében fontos a megfelelő izoláció annak biztosítására, hogy a rosszindulatú kód ne fertőzze meg az érintett szervezet tényleges rendszereit. A kifejezetten rosszindulatú támadások célpontjául szolgáló elemek használatáti módjától függően előfordulhat, hogy a használatuk és implementálásuk előtt konzultálni kell a megfelelő felelős szervezettel vagy szervezetekkel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először létre kell hoznia a kifejezetten rosszindulatú támadások célpontjául szolgáló elemeket, hogy vonzó célpontot biztosítson az ellenséges támadók számára és elterelje a támadásokat az operatív rendszerekről.
2. A kifejezetten támadások célpontjául szolgáló elemek használatakor a szervezetnek bizonyos izolációs intézkedéseket is implementálnia kell annak biztosítása érdekében, hogy a kártékony kódok ne fertőzzék meg a szervezet éles rendszereit.
3. A rosszindulatú támadások célpontjául szolgáló elem specifikus használatától függően a szervezetnek konzultálnia kell a felelős szervezeti egységekkel és döntéshozókkal.
4. A szervezetnek dokumentálnia kell a támadások célpontjául szolgáló elemek elhelyezését, valamint ezen elemeknek naplóznia kell a támadások észleléséhez, elhárításához és elemzéséhez.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a támadások célpontjául szolgáló elemeket, hogy megfeleljenek a változó kiberbiztonsági fenyegetéseknek.
6. A szervezetnek biztosítania kell a támadások célpontjául szolgáló elemek és az EIR közötti hatékony kommunikációt, hogy gyorsan reagálhasson a potenciális biztonsági eseményekre.

Kapcsolódó intézkedések

15.10. Sérülékenységmonitorozás és szkennelés

17.17. A határok védelme

17.87. Elfedés és megtévesztés

17.101. Külső kártékony kódok azonosítása

17.122. Izolált futtatási környezetek

18.8. Kártékony kódok elleni védelem

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

SC-26

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.80. PLATFORM-FÜGGETLEN ALKALMAZÁSOK

17.80. A platformfüggetlen alkalmazásokat a szervezet az EIR-ek közé sorolja.

MAGYARÁZAT

A platformok olyan hardver-, firmware- és szoftverelemek kombinációi, amelyeket alkalmazások futtatására használnak. A platformok magukban foglalják az operációs rendszereket, az alapul szolgáló számítógép-architektúrákat, vagy épp mindkettőt. A platformfüggetlen alkalmazások olyan alkalmazások, amelyek képesek több különböző platformon is futni. Az ilyen alkalmazások elősegítik a hordozhatóságot és az újra felépítést különböző platformokon. Az alkalmazások hordozhatósága és a képességük az újraalkotásra különböző platformokon növeli a kritikus funkciók rendelkezésre állását olyan helyzetekben, amikor az adott operációs rendszerekkel rendelkező EIR-ek támadás alatt állnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia és kategorizálnia kell az összes platformfüggetlen alkalmazást, amelyeket használatban vannak vagy lesznek.
2. A szervezetnek biztosítania kell, hogy ezek megfelelően védettek legyenek a kiberbiztonsági fenyegetésekkel szemben. Ez magában foglalja a megfelelő tűzfalak, víruskeresők és egyéb biztonsági eszközök használatát.
3. A szervezetnek rendszeresen ellenőriznie kell az alkalmaásokat, hogy biztosítsa azok megfelelő működését és biztonságát. Ez magában foglalja a naplók ellenőrzését is, hogy azonosításra kerüljenek a lehetséges biztonsági események.
4. A szervezetnek rendszeresen frissítenie kell az az alkalmazásokat és azok rendszerelemeit, illetve az azokat kiszolgáló platformokat, hogy biztosítsa a legújabb biztonsági frissítések és javítások telepítését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.85. A rendszerelemek esetében alkalmazott változatos információs technológiák

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

SC-27

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a platform független alkalmazások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.81. TÁROLT (AT REST) ADATOK VÉDELME

17.81. A szervezet megóvja a meghatározott tárolt, illetve archivált (at rest) adatok bizalmasságát és sértetlenségét a feldolgozás vagy továbbítás alatt álló adatokkal megegyező szinten.

MAGYARÁZAT

Ez az intézkedés a tárolt információk bizalmasságának és sértetlenségének védelmét célozza meg. Egyaránt kiterjed a felhasználói információkra és a rendszerinformációkra. A tárolt információk arra az állapotra utalnak, amikor az információk kifejezetten a rendszerösszetevők tárolóeszközein helyezkednek el és éppen nem állnak feldolgozás vagy továbbítás alatt. A védendő, rendszerrel kapcsolatos információk közé tartoznak például a tűzfalak, átjárók, behatolásérzékelő és -megelőző rendszerek, szűrő routerek, valamint a hitelesítői tartalom konfigurációja vagy szabálykészlete. Az érintett szervezet különböző mechanizmusokat használhat a bizalmasság és sértetlenség védelme érdekében, beleértve a kriptográfiai mechanizmusok és a fájlmegosztás-szkennelés használatát. A sértetlenség védelme például egyszer-írható-szokszor-olvasható technológiák alkalmazásával érhető el. Az érintett szervezet más védelmi intézkedést is alkalmazhat, ideértve például az online tárolás helyett az offline tárolást és/vagy folyamatos ellenőrzést a kártékony kód észleléséhez, ha a tárolt információ megfelelő védelme másképp nem érhető el.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely adatokat tekinti "at rest", azaz tárolt vagy archivált adatoknak. Ezek lehetnek belső vagy külső merevlemezek, hálózati tárolóeszközök vagy adatbázisokon található információk.
2. A szervezetnek biztosítania kell az adatok bizalmasságát és sértetlenségét. Ez magában foglalja a felhasználói információkat és a rendszerekkel kapcsolatos információkat is.
3. A szervezetnek különböző mechanizmusokat kell alkalmaznia a bizalmasság és sértetlenség védelmére. A sértetlenség védelme érdekében az érintett szervezet például alkalmazhatja a write-once-read-many technológiákat.
4. Amennyiben az adatok megfelelő védelme másképpen nem biztosítható, a szervezetnek más védelmi intézkedéseket is alkalmaznia kell. Ilyenek lehetnek a gyakori vizsgálatok a nyugvó

állapotban lévő kártékony kódok azonosítására, vagy a biztonságos offline tárolás az online tárolás helyett.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.60. Legkisebb jogosultság elve

2.113. Mobil eszközök hozzáférés-ellenőrzése

5.14. Folyamatos felügyelet

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.23. Konfigurációs beállítások

7.35. Az elektronikus információs rendszer mentései

11.4. Adathordozók tárolása

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

3.3.13.21. A maradvány információ védelme: Az elektronikus információs rendszer védi az érintett szervezet által meghatározott maradvány információk (pl.: átmeneti fájlok) bizalmasságát, sértetlenségét.

ISO/IEC 27001:2023 referencia

A.5.10; A.5.33

NIST SP 800-53 rev.5 referencia

SC-28

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a tárolt adatok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

17.82. TÁROLT (AT REST) ADATOK VÉDELME – KRIPTOGRÁFIAI VÉDELEM

17.82. A szervezet meghatározott rendszerelemek vagy adathordozók esetében kriptográfiai mechanizmusokat alkalmaz a szervezet által meghatározott tárolt vagy archivált adatok jogosulatlan felfedésének és módosításának megelőzésére.

MAGYARÁZAT

A kriptográfiai mechanizmusok kiválasztása az érintett szervezet információinak bizalmasságának és sértetlenségének védelmi szükségletén alapul. A mechanizmus erőssége arányos az információ biztonsági besorolásával. Az érintett szervezetnek képesnek kell lennie a rendszerelemeken vagy adathordozókon történő információ titkosítására, vagy adatszerkezetek titkosítására, beleértve a fájlokat, rekordokat vagy mezőket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, mely rendszerelemeket vagy adathordozókat kell védeni a jogosulatlan hozzáférés és módosítás ellen.
2. A szervezetnek ki kell választania a megfelelő kriptográfiai mechanizmusokat, amelyek megfelelnek az adatbiztonsághoz kapcsolható követelményeknek és iparági jógyakorlatoknak. A mechanizmus erőssége arányban áll a védett információ információbiztonsági besorolásával.
3. A szervezetnek rugalmasan kell alkalmaznia a kriptográfiai mechanizmusokat, lehetőséget adva a rendszerelemek vagy adathordozók információinak titkosítására, vagy az adatszerkezetek, beleértve a fájlokat, rekordokat vagy mezőket, titkosítására.
4. A szervezetnek implementálnia kell a kiválasztott kriptográfiai mechanizmusokat, és biztosítania kell, hogy azok megfelelően működnek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.113. Mobil eszközök hozzáférés-ellenőrzése

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

A.5.33

NIST SP 800-53 REV.5 REFERENCIA

SC-28(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelem vagy adathordozó illetve az információ meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

17.83. TÁROLT (AT REST) ADATOK VÉDELME – OFFLINE TÁRHELY

17.83. A szervezet eltávolítja a meghatározott információkat az online tárhelyekről, és biztonságos offline tárhelyeken tárolja azokat.

MAGYARÁZAT

Az érintett szervezet által az online tárhelyekről információk offline tárhelyre való átmozgatása kiküszöböli annak lehetőségét, hogy rosszindulatú támadók jogosulatlanul, hálózati elérésen keresztül férjenek hozzá az információkhoz. Ezért a szervezetek úgy dönthetnek, hogy az információkat offline tárhelyre helyezik át, ahelyett, hogy azokat online tárhelyen védenék.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania és kategorizálnia kell azokat az információkat, amelyeket offline tárhelyre szeretne áthelyezni. Ez magában foglalhatja a személyes adatokat, a szellemi tulajdonjogokat, a pénzügyi adatokat és más érzékeny információkat.
2. A szervezetnek biztosítania kell, hogy rendelkezésre állnak a megfelelő offline tárhelyek, amelyek képesek tárolni a meghatározott információkat. Ez magában foglalhatja a fizikai tárhelyeket, mint például a széfek, vagy digitális offline tárhelyeket, mint például az adatszalagok vagy a külső merevlemezek.
3. A szervezetnek meg kell terveznie és végre kell hajtania az információk online tárhelyről történő eltávolítását és offline tárhelyre történő átmozgatását. Ennek érdekében az adatok titkosítása a szállítás során szükséges lehet, hogy a szervezet megvédje azokat a lehetséges illetéktelen hozzáféréstől.
4. A szervezetnek dokumentálnia kell az információk áthelyezését, hogy nyomon követhető legyen, mely információk kerültek áthelyezésre, mikor és kik által. Ez segíthet a jövőbeni vizsgálatokban és a kiberbiztonsági események kezelésében.

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

SC-28(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információ meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.84. TÁROLT (AT REST) ADATOK VÉDELME – KRIPTOGRÁFIAI KULCSOK

17.84. A szervezet meghatározott óvintézkedések és hardveres kulcstároló alkalmazásával biztosítja a kriptográfiai kulcsok védett tárolását.

MAGYARÁZAT

Az érintett szervezet kriptográfiai kulcsainak védelmében a Trusted Platform Module egy példa a hardverrel védett adattárolóra, amelyet alkalmazhatunk. A TPM egy mikrochip, amelyet az eszközök alaplapjára integrálnak, és amely képes biztonságosan tárolni a kriptográfiai kulcsokat. Ez a chip speciálisan úgy van kialakítva, hogy ellenálljon a külső támadásoknak, beleértve a fizikai manipulációkat és a szoftveres támadásokat is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a szükséges óvintézkedéseket a kriptográfiai kulcsok védett tárolásához.
2. A szervezetnek hardveres kulcstárolót kell alkalmaznia a kriptográfiai kulcsok védett tárolásához.
3. A szervezetnek be kell állítania és konfigurálnia kell a EIR-eket a hardveres kulcstárolóval való integrációhoz. Ez magában foglalhatja a kulcsok importálását és exportálását, a kulcsok használatát és a kulcsok kezelését.

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

SC-28(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a védelmi intézkedések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.85. A RENDSZERELEMEK ESETÉBEN ALKALMAZOTT VÁLTOZATOS INFORMÁCIÓS TECHNOLÓGIÁK

17.85. A szervezet EIR-ének meghatározott rendszereleimben különböző technológián alapú összetevőket alkalmaz.

MAGYARÁZAT

A használt technológiák sokféleségének növelése az érintett szervezet rendszereiben csökkenti az egyes technológiák kihasználásának vagy kompromittálódásának hatását. Az ilyen jellegű sokféleség védelmet nyújt a hasonló eredetű hibák ellen, beleértve az ellátási lánc támadások által indukált hibákat is. A használt technológiák sokfélesége továbbá csökkenti annak valószínűségét, hogy egy támadó által egy technológia kompromittálására használt eszközök hatékonyak legyenek más használt technológiák ellen, így tovább növelve a tervezett támadások sikeres végrehajtásához szükséges befektetett munkamennyiséget, ezzel akadályozva a rosszindulatú támadót. A sokféleség növelése átfordulhat problémába is, mert növeli a rendszerek bonyolultságát és túlterhelheti a rendszerek menedzseléséért felelős személyeket, ami végül hibákhoz és konfigurációs problémákhoz vezethet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a jelenleg használt technológiákat.
2. A szervezetnek biztosítania kell a technológiai sokféleséget a rendszereiben, hogy védelmet nyújtson az azonos problémán alapuló hibák ellen, beleértve az ellátási lánc támadásokat.
3. A szervezetnek csökkentenie kell a valószínűségét annak, hogy a rosszindulatú támadók által az egyik rendszerelem megtámadására használt eszköz hatékony legyen más rendszerelemek ellen.
4. A szervezetnek figyelembe kell vennie, hogy a sokféleség túlzott növelése bonyolultságot és menedzsment problémákat eredményezhet, amik végül hibákhoz és problémás konfigurációkhoz vezethetnek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.25. Naplóinformációk védelme

13.6. Információbiztonsági architektúra leírás

17.80. Platform-független alkalmazások

17.87. Elfedés és megtévesztés

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

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

SC-29

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.86. HETEROGENITÁS – VIRTUALIZÁCIÓS TECHNIKÁK

17.86. A szervezet meghatározott gyakorisággal frissített virtualizációs technológiákat alkalmaz a különböző operációs rendszerek és alkalmazások telepítésének támogatására.

MAGYARÁZAT

Az operációs rendszerek és alkalmazások gyakori változtatásai konfigurációs menedzsment kihívásokat jelenthetnek, ugyanakkor ezek a változások növelhetik a sikeres támadások kivitelezéséhez szükséges befektetett időt és energiát. A virtuális operációs rendszerek vagy alkalmazások változtatása, a tényleges operációs rendszerek vagy alkalmazások változtatása helyett, virtuális változásokat biztosít, amelyek akadályozzák a támadók sikerességét, miközben csökkentik a konfigurációs menedzsment erőfeszítéseit. A virtualizációs technikák segíthetnek a nem megbízható szoftverek vagy kétes eredetű szoftverek izolálásában, korlátozott végrehajtási környezetekbe helyezésében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a virtualizációs technológiák frissítésének gyakoriságát.
2. A szervezetnek be kell szereznie a legújabb virtualizációs technológiákat, amelyek támogatják a különböző operációs rendszerek és alkalmazások telepítését.
3. A szervezetnek telepítenie kell a virtualizációs technológiákat. Ez magában foglalhatja a szoftver telepítését, konfigurálását és tesztelését.
4. A szervezetnek rendszeresen frissítenie kell a virtualizációs technológiákat, hogy naprakészek maradjanak.
6. A szervezetnek dokumentálnia kell a virtualizációs technológiák frissítéseit, hogy nyomon követhesse a változásokat és bizonyíthassa a kiberbiztonsági követelményeknek való megfelelést.

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

SC-29(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.87. ELFEDÉS ÉS MEGTÉVESZTÉS

17.87. A szervezet meghatározott elrejtési és félrevezetési technikákat alkalmaz a meghatározott EIR-ekben és időszakokban, annak érdekében, hogy összezavarja és félrevezesse az ellenséges szándékú felhasználókat.

MAGYARÁZAT

Bizonyos elrejtési és félrevezetési technikák jelentősen csökkenthetik a támadók számára rendelkezésre álló támadási felületet a támadások kezdeményezésére és befejezésére. Például a virtualizációs technikák lehetővé teszik az érintett szervezetek számára, hogy álcázzák az EIR-eket, potenciálisan csökkentve a sikeres támadások valószínűségét anélkül, hogy több platformra lenne szükség. Az elrejtési és félrevezetési technikák és módszerek - beleértve a véletlenszerűséget, a bizonytalanságot és a virtualizációt - fokozott használata elegendően összezavarhatja és félrevezetheti a támadókat, és ennek következtében segítheti a támadók által indított felderítés és ártó tevékenység beazonosítását. Az elrejtési és félrevezetési technikák további időt biztosíthatnak a fő funkciók üzemeltetésére. Az elrejtési és félrevezetési technikák alkalmazása növelheti az EIR-ek bonyolultságát és a kezeléséhez szükséges adminisztratív munka mennyiségét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat az EIR-eket, amelyek esetén az elrejtési és félrevezetési technikákat alkalmazni kívánja.
2. A szervezetnek ki kell választania és implementálnia kell azokat az elrejtési és félrevezetési technikákat, amelyeket alkalmazni kíván, például a virtualizációs technikák.
3. A szervezetnek növelnie kell az elrejtési és félrevezetési technikák és módszerek - beleértve a véletlenszerűséget, a bizonytalanságot és a virtualizációt - alkalmazását.
4. A szervezetnek biztosítania kell, hogy az elrejtési és félrevezetési technikák alkalmazása során elegendő időt biztosítson a fő üzleti funkciók végrehajtására.
5. A szervezetnek figyelembe kell vennie, hogy az elrejtési és félrevezetési technikák implementálása növelheti az EIR-ek kezelésének bonyolultságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.60. Legkisebb jogosultság elve

17.78. Funkcionalitás és információtárolás minimalizálása

17.79. Csapdák alkalmazása

17.85. A rendszerelemek esetében alkalmazott változatos információs technológiák

17.122. Izolált futtatási környezetek

18.73. Nem állandó rendszerelemek és szolgáltatások

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

SC-30

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek illetve az időszakok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.88. ELFEDÉS ÉS MEGTÉVESZTÉS – VÉLETLENSZERŰSÉG

17.88. A szervezet meghatározott technikákat alkalmaz a véletlenszerűség bevezetésére a szervezeti működésbe és eszközökbe.

MAGYARÁZAT

A véletlenszerűség bevezetése növeli a támadók bizonytalanságát az érintett szervezet védelmi képességeivel és a rendszerek elleni tervezett támadásokkal kapcsolatban. Az ilyen intézkedések akadályozhatják a támadók képességét arra, hogy pontos, célzott támadásokat indítsanak az érintett szervezet fő üzleti funkcióit támogató rendszerelemek ellen. Ez lassíthatja a támadások megkezdését vagy folytatását. A véletlenszerűséget bevezető félrevezető technikák közé tartozik bizonyos rutinszerű tevékenységek különböző időpontokban történő végrehajtása, különböző információs technológiák alkalmazása, különböző beszállítók használata, valamint a szervezet személyzetének szerepkörei és felelősségei rotációja.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a technikákat, amelyekkel kapcsolatban a véletlenszerűség bevezetése indokolt és eredményes lehet.
2. A szervezetnek be kell vezetnie a véletlenszerűséget például bizonyos rutin tevékenységek különböző időpontokban történő végrehajtásával. Ez növeli a támadók számára a bizonytalanságot, mivel nehezebb lesz előre megjósolni a szervezet működését.
3. A szervezetnek változatos információs technológiákat kell alkalmaznia. Ez magában foglalhatja különböző szoftverek, hardverek és hálózati eszközök használatát, amelyek további bizonytalanságot teremtenek a támadók számára.
4. A szervezetnek különböző beszállítókat kell igénybe vennie. Ez megnehezíti a támadók számára, hogy pontosan meghatározzák, milyen eszközök vannak használatban.
5. A szervezetnek rendszeresen változtatnia kell a munkatársak és felelősök szerepeit és felelősségeit.

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

SC-30(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a technikák meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.89. Elfedés és megtévesztés – Feldolgozási és tárolási helyek megváltoztatása

17.89. A szervezet meghatározott gyakorisággal vagy eseti jelleggel módosítja az információk feldolgozási, vagy tárolási helyét.

Magyarázat

A támadók kritikus ügymeneti és üzleti funkciókat, valamint az ezeket támogató rendszereket célozzák meg, miközben igyekeznek minimalizálni a saját létezésük és alkalmazott technikáik felfedezhetőségét. Az érintett szervezetek célba vett rendszereik a statikus, homogén és determinisztikus jellege miatt könnyebben sebezhetők a támadásokkal szemben, kevesebb erőfeszítéssel és költséggel támadhatóak. A feldolgozási és tárolási helyek megváltoztatása (más néven mozgó célpontok elleni védelem) a fejlett tartós fenyegetést (APT) olyan technikákkal kezeli, mint a virtualizáció, az elosztott feldolgozás és a replikáció. Ez lehetővé teszi a szervezetek számára, hogy áthelyezzék a kritikus ügymeneti és üzleti funkciókat támogató rendszerelemeket (pl. feldolgozás, tárolás). A feldolgozási és tárolási helyek megváltoztatása bizonytalanságot okozhat a támadók tevékenységeinek végrehajtása során, ezzel növelve a támadók munkaidejét, valamint megnöveli az esélyét annak, hogy a támadók véletlen felfedik tevékenységük bizonyos aspektusait, miközben a kritikus szervezeti erőforrások után kutatnak.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a kritikus ügymeneti és üzleti funkciókat, valamint az ezeket támogató rendszerelemeket.
2. A szervezetnek implementálnia kell olyan védelmi technikákat, mint például a virtualizáció, a disztribuált feldolgozás és a replikáció.
3. A szervezetnek rendszeresen vagy eseti jelleggel meg kell változtatnia az információk feldolgozási és/vagy tárolási helyét. Ez bevezet egy bizonyos fokú bizonytalanságot a támadók tevékenységeivel kapcsolatban.
4. A szervezetnek dokumentálnia kell az információk feldolgozási és tárolási helyek változtatásait, hogy nyomonkövethető legyen a későbbiekben.

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

SC-30(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a feldolgozó egység vagy adattároló illetve a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.90. ELFEDÉS ÉS MEGTÉVESZTÉS – FÉLREVEZETŐ INFORMÁCIÓ

17.90. A szervezet valósághű, de félrevezető információkat alkalmaz a meghatározott rendszerelemekben azok biztonsági állapotáról vagy helyzetéről.

MAGYARÁZAT

Az érintett szervezet félrevezető információk alkalmazásával próbálja megzavarni a potenciális támadókat az szervezet által alkalmazott védelmi intézkedések természetével és mértékével kapcsolatban. Így a támadók helytelen és hatástalan támadási technikákat alkalmazhatnak. A támadók félrevezetésének egyik módja, hogy az érintett szervezet félrevezető információkat helyez el a konkrétan alkalmazott védelmi intézkedésekről azokban az EIR-ekben, amelyekről ismert, hogy valószínűleg potenciális célpontokká válhatnak. Egy másik technika a megtévesztő hálózatok használata, amelyek utánozzák a szervezet EIR-einek valós aspektusait, de például elavult szoftverkonfigurációkat használnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely rendszerelemek lehetnek potenciális célpontjai a támadóknak.
2. A szervezetnek valósághű, de félrevezető információkat kell létrehoznia ezekről az elemekről. Ez magában foglalhatja a biztonsági állapotukat, a helyzetüket, vagy akár a használt szoftvereket is.
3. A szervezetnek létre kell hoznia egy "deception net"-et, ami utánozza az EIR és a hálózat valós aspektusait, de például direkt elavult szoftverkonfigurációkat használ.
4. A szervezetnek naplóznia kell a támadók tevékenységét, hogy megértsék, melyik félrevezető információ volt hatékony, és melyik nem, és felderítsék a támadásokat.

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

SC-30(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.91. ELFEDÉS ÉS MEGTÉVESZTÉS – RENDSZERELEMEK ELREJTÉSE

17.91. A szervezet meghatározott technikákat alkalmaz a meghatározott rendszerelemek elrejtésére vagy álcázására.

MAGYARÁZAT

Az érintett szervezetek a kritikus rendszerelemek elrejtésével vagy álcázásával csökkenthetik annak valószínűségét, hogy a támadók célba vegyék és sikeresen kompromittálják ezeket az elemeket. A rendszerelemek elrejtésének vagy álcázásának lehetséges módjai közé tartozik a routerek megfelelő, akár támadókat megtévesztő vagy hálózatokat elrejtő konfigurálása vagy a titkosítási vagy virtualizációs technikák alkalmazása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, melyek azok a rendszerelemek, amelyeket el kell rejteni vagy álcázni kell. Ezek általában a kritikus rendszerelemek, amelyeket a támadók célpontul választhatnak.
2. A szervezetnek megfelelő technikákat kell alkalmaznia a rendszerelemek elrejtésére vagy álcázására.
3. A szervezetnek gondoskodnia kell arról, hogy a technikák megfelelően működjenek, és valóban elrejtsék vagy álcázzák a rendszerelemeket. Ez magában foglalhatja a rendszer tesztelését és a naplók ellenőrzését.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a technikákat, hogy biztosítsa a rendszerelemek elrejtésének vagy álcázásának legjobb iparági gyakorlatait. Ez magában foglalhatja a technikák hatékonyságának értékelését és a legújabb technikák nyomon követését.

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

SC-30(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek illetve a technikák meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.92. REJTETT CSATORNÁK ELEMZÉSE

17.92. A szervezet:

17.92.1. Elemzi a rejtett csatornákat a rendszeren belüli kommunikáció azon aspektusainak azonosítása érdekében, amelyek potenciális útvonalak lehetnek a rejtett tároló vagy időzítő csatornák számára.

17.92.2. Megbecsüli a rejtett csatornák maximális sávszélességét.

MAGYARÁZAT

Az érintett szervezet fejlesztői a legalkalmasabbak arra, hogy azonosítsák azokat a potenciális területeket az EIR-eken belül, amelyek rejtett csatornákat tartalmaznak, vagy azok létrehozására használhatóak. A rejtett csatorna elemzést akkor érdemes leginkább elvégezni, ha fennáll lehetősége a jogosulatlan információáramlásnak a rendszerelemek között, mint például azokban az EIR-ekben, amelyek kiexportált információt tartalmaznak és kapcsolatban állnak külső hálózatokkal. A rejtett csatorna elemzés hasznos a többszintű biztonsági rendszerek, a több biztonsági szintű rendszerek és a kereszt-domain rendszerek számára is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet fejlesztői azok, akik a legjobban képesek azonosítani a kontrolponttal kapcsolatos érdekelt területeket az EIR-eken belül, amelyek rejtett csatornákat tartalmazhatnak, vagy rejtett csatorna létrehozására használhatóak.

2. A szervezetnek meg kell becsülnie a rejtett csatornák maximális sávszélességét. Ez segít az érintett szervezetnek felmérni a rejtett csatornák által jelentett potenciális kockázatot.

3. A szervezetnek dokumentálnia kell a rejtett csatornák elemzését és a kapott eredményeket. Ez lehetővé teszi számukra, hogy nyomon kövessék a változásokat, és időben észleljék a potenciális biztonsági réseket.

4. A szervezetnek rendszeresen felül kell vizsgálnia a rejtett csatornák elemzését, hogy biztosítsa az EIR-ek folyamatos védelmét a rejtett csatornákon keresztüli információszivárogtatással szemben.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

16.16. Biztonságtervezési elvek

18.66. Hibakezelés

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

SC-31

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.93. REJTETT CSATORNÁK ELEMZÉSE – REJTETT CSATORNÁK TESZTELÉSE A KIHASZNÁLHATÓSÁG SZEMPONTJÁBÓL

17.93. A szervezet az azonosított rejtett csatornák egy részén tesztelést hajt végre kihasználhatóságuk megállapítása érdekében.

MAGYARÁZAT

Az érintett szervezet az azonosított rejtett csatornák egy részén tesztelést hajt végre kihasználhatóságuk megállapítása érdekében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell a potenciális rejtett csatornákat. Ez magában foglalhatja a hálózati forgalom, a rendszerfolyamatok és az adatátviteli módszerek elemzését.
2. A szervezetnek tesztelnie kell ezeket a csatornákat, hogy megállapítsa, támadhatóak, vagy támadásra használhatóak-e. Ez magában foglalhatja a csatornák különböző forgalmi mintáinak és adatátviteli sebességeinek vizsgálatát.
3. A szervezetnek potenciálisan veszélyt jelentő csatornákat, amennyiben nem szükségesek az ügymeneti vagy üzleti funkciók működtetéséhez meg kell szüntetnie.
4. A szervezetnek dokumentálnia kell a vizsgálatok és tesztelések eredményeit, valamint rendszeres időnként meg kell ismételnie ezeket az eljárásokat.

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

SC-31(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.94. REJTETT CSATORNÁK ELEMZÉSE – MAXIMÁLIS SÁVSZÉLESSÉG

17.94. A szervezet csökkenti az azonosított rejtett (tárolási és időzítési) csatornák maximális sávszélességét.

MAGYARÁZAT

A rejtett csatornák teljes kiküszöbölése általában nem lehetséges jelentős teljesítménybeli hatások nélkül.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell a rejtett csatornákat. Ez magában foglalhatja a rendszerelemzést, a kódellenőrzést és a különféle tesztelési technikákat.
2. A szervezetnek meg kell állapítania a maximális sávszélességet, amit ezek a csatornák jelenleg használnak. Ez lehetővé teszi a szervezet számára, hogy meghatározza a csatornák által okozott potenciális kockázatot.
3. A szervezetnek csökkentenie kell a rejtett csatornák maximális sávszélességét, annak érdekében, hogy minimalizálja a célzott információszivárogtatás kockázatát.
4. A szervezetnek dokumentálnia kell az általa azonosított rejtett csatornákon végrehajtott sávszélesség csökkentéseket.

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

SC-31(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az értékek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.95. Rejtett csatornák elemzése – Sávszélesség mérése éles környezetben

17.95. A szervezet megméri a meghatározott és azonosított rejtett csatornák sávszélességét a rendszer működési környezetében.

Magyarázat

Az érintett szervezetnek mérni szükséges a meghatározott és azonosított rejtett csatornák sávszélességét az éles környezetben. Ez segít a szervezetnek meghatározni, hogy mennyi információ szivároghat ki rejtetten, mielőtt ez károsan befolyásolná a fő folyamatokat vagy az üzleti funkciókat. A rejtett csatornák sávszélessége jelentősen eltérhet, ha azt olyan környezetben mérik, amely nem tükrözi megfelelően a tényleges működést, beleértve a labor környezetet vagy a fejlesztői környezetet.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania kell a rejtett csatornákat a működési környezetben. Ez magában foglalhatja a hálózati forgalom, a rendszerlogok és más releváns adatok elemzését.
2. A szervezetnek meg kell mérnie a sávszélességüket a rejtett csatornáknak. Ez azt jelenti, hogy meg kell határozniuk, mennyi információ képes áthaladni ezeken a csatornákon egy adott időszak alatt, és mik a jellemző értékek az áthaladó információval kapcsolatban.
3. A szervezetnek ki kell értékelnie, hogy a rejtett csatornákon keresztül szivárgó információ mennyisége milyen hatással van a szervezet fő ügymeneti vagy az üzleti funkcióira. Ha a szivárgás mértéke károsan befolyásolja ezeket a funkciókat, akkor a szervezetnek megfelelő intézkedéseket kell hoznia.
4. A szervezetnek dokumentálnia kell a folyamatot, beleértve az azonosított rejtett csatornákat, a sávszélesség mérési eredményeit és a hozott intézkedéseket. Ez segít a jövőbeni ellenőrzések hatékonyságában és a kiberbiztonsági követelményeknek való megfelelés bizonyításában.

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

SC-31(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az azonosított rejtett csatornákra vonatkozó sávszélesség meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.96. RENDSZER FELOSZTÁSA

17.96. A szervezet az EIR-t meghatározott rendszerelemekre osztja fel, amelyek külön fizikai vagy logikai tartományokban vagy környezetekben helyezkednek el, a szervezet által meghatározott elkülönítési körülményeknek megfelelően.

MAGYARÁZAT

Az EIR-ek elemekre bontása a mélyreható védelmi stratégia része. Az érintett szervezetek meghatározzák a rendszerelemek fizikai elkülönítésének mértékét. A fizikai elkülönítési lehetőségek közé tartoznak a fizikailag különböző elemek külön rackekbe helyezése ugyanabban a helyiségben, a kritikus elemek külön helyiségekbe helyezése, vagy a kritikus elemek földrajzi elkülönítése. A biztonsági kategorizálás segíthet az elkülönítésre jelölt elemek kiválasztásában. A menedzselt interfészek korlátozzák vagy tiltják a hálózati hozzáférést és az információáramlást a felosztott rendszerelemek között.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az elkülönítés mértékét, figyelembe véve a fizikai elkülönítési lehetőségeket.
2. A szervezetnek el kell végeznie biztonsági kategorizálást, hogy segítsen az elkülönítésre jelölt elemek kiválasztásában.
3. A szervezetnek menedzselt interfészeket kell alkalmaznia annak érdekében, hogy az felosztott rendszerelemek közötti információáramlást kezelje és felügyelje.
4. A szervezetnek dokumentálnia kell az EIR-ek elemekre bontásának folyamatát és a rendszerelemek közötti információáramlás szabályait.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.28. Információáramlási szabályok érvényesítése
2.60. Legkisebb jogosultság elve
16.16. Biztonságtervezési elvek
17.2. Rendszer és felhasználói funkciók szétválasztása
17.4. Biztonsági funkciók elkülönítése
17.17. A határok védelme

17.102. Elosztott feldolgozás és tárolás

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

SC-32

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek illetve az a rendszerelemek fizikai vagy logikai szétválasztására vonatkozó körülmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.97. Rendszer felosztása – Fizikai tartományok különválasztása a privilegizált funkciókhoz

17.97. A szervezet a privilegizált funkciókat külön fizikai tartományokba osztja szét.

Magyarázat

Az érintett szervezetben a privilegizált funkciók, amelyek egyetlen fizikai tartományban működnek, egyetlen hibapontot jelentenek, ha ez a tartomány kompromittálódik vagy szolgáltatásmegtagadás tapasztalható. Jelen követelmény szerint a szervezetnek szét kell osztania a privilegizált funkciókat különböző fizikai tartományokba.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, mely funkciók minősülnek privilegizáltnak.
2. A szervezetnek fizikai tartományokat kell létrehoznia, amelyekben ezek a privilegizált funkciók működhetnek.
3. A szervezetnek gondoskodnia kell arról, hogy a fizikai tartományok megfelelően el legyenek szeparálva egymástól, hogy a potenciális kibertámadások ne terjedjenek át egyik tartományról a másikra, illetve ha az egyik tartomány kompromittálódik, izolálódjon el a másik tartománytól.
4. A szervezetnek be kell állítania a megfelelő hozzáférési szabályokat és jogosultságokat a fizikai tartományokban, hogy csak a megfelelő személyek férhessenek hozzá a privilegizált funkciókhoz.
5. A szervezetnek naplóznia és monitoroznia kell privilegizált funkciók használatát, hogy nyomon követhesse az esetlegesen felmerülő biztonsági eseményeket vagy 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

SC-32(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.98. VÉGREHAJTHATÓ, DE NEM MÓDOSÍTHATÓ PROGRAMOK

17.98. A szervezet meghatározott rendszerelemek esetében:

17.98.1. a működési környezet betöltését és futtatását csak hardveresen kikényszerített, csak olvasható adathordozóról engedélyezi;

17.98.2. az alkalmazások betöltését és futtatását csak hardveresen kikényszerített, csak olvasható adathordozóról engedélyezi.

MAGYARÁZAT

Egy EIR működési környezete tartalmazza azon kódokat melyek alkalmazásokat működtetnek, ideértve az operációs rendszereket, futtatható állományokat vagy a virtuális gépek felügyeleti eszközeit. Tartalmazhat olyan alkalmazásokat is, amelyek közvetlenül a hardveres platformokon futnak. A hardveresen kikényszerített, csak olvasható adathordozók közé tartozik a CD és DVD meghajtók, valamint az egyszer írható, programozható, csak olvasható memória. A nem módosítható adattároló használata biztosítja a szoftver integritását a csak olvasható állomány létrehozásának pillanatától kezdve. Az újraprogramozható, csak olvasható memória használata elfogadható lehet csak olvasható adathordozóként, amennyiben a sértetlenséget megfelelően védik az írás kezdetétől a memória beillesztéséig az EIR-be, és megbízható hardveres védelmet alkalmaznak a memória újraprogramozása ellen.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat az elemeket, amelyeknél a működési környezet betöltését és futtatását csak hardveresen kikényszerített, csak olvasható adathordozóról engedélyezi.

2. A szervezetnek biztosítania kell, hogy a működési környezet, beleértve az operációs rendszereket, futtatható állományokat vagy virtuális gép felügyeleti eszközöket csak hardveresen kikényszerített, csak olvasható adathordozóról töltődjön be és futtasson.

3. A szervezetnek ugyanezt a követelményt alkalmaznia kell az alkalmazások betöltésére és futtatására is.

4. A szervezetnek olyan adathordozókat kell használnia, amelyek nem módosíthatók.

5. A szervezetnek biztosítania kell, hogy a szoftver integritása megőrződjön a csak olvasható tartalom létrehozásától kezdve.
6. A szervezetnek biztosítania kell az elfogadható a programozható, csak olvasható memória használatát, feltéve, hogy az integritás megfelelően védett a kezdeti írástól kezdve a memória rendszerekbe történő behelyezéséig, valamint rendelkezik hardvervédelemmel a memória újraprogramozása ellen.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
18.42. Szoftver- és információsértetlenség
18.73. Nem állandó rendszerelemek és szolgáltatások

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

SC-34

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.99. VÉGREHAJTHATÓ, DE NEM MÓDOSÍTHATÓ PROGRAMOK – NEM ÍRHATÓ TÁROLÓESZKÖZ

17.99. A szervezet meghatározott rendszerelemek esetében olyan nem írható tárolóeszközöket alkalmaz, amelyek a rendszerelemek újraindítása vagy be- és kikapcsolása után is folyamatosan fennmaradnak.

MAGYARÁZAT

Az írható tárolóeszközök csatlakoztatásának tiltása kiküszöböli a rosszindulatú kód bejuttatásának lehetőségét a meghatározott rendszerelemeken belülre, az írható tárolóeszközökön keresztül. A korlátozás vonatkozik a rögzített és cserélhető tárolóeszközökre, utóbbiak vagy közvetlenül, vagy a mozgatható eszközökre vonatkozó hozzáférési szabályokon keresztül kerülnek korlátozásra.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely rendszerelemeket érinti az írható tárolóeszközök használata. Ez magában foglalhatja a fix és az eltávolítható tárolóeszközöket is.
2. A szervezetnek be kell azonosítania, mely rendszereken szükséges az írható tárolóeszközök mellőzése és tiltása.
3. A szervezetnek be kell szereznie azokat a nem írható tárolóeszközöket, amelyeket a rendszerelemekben használni kíván.
4. A szervezetnek implementálnia kell a beszerzett, nem írható tárolóeszközöket. Ez magában foglalhatja a tárolóeszközök fizikai telepítését, valamint a szükséges szoftverek és illesztőprogramok telepítését és konfigurálását.
5. A szervezetnek be kell állítania a megfelelő hozzáférési szabályokat a nem írható tárolóeszközökkel rendelkező rendszerelemekhez. Ez magában foglalhatja a hozzáférési jogosultságok, a felhasználói fiókok és a hozzáférési naplók kezelését.
6. A szervezetnek dokumentálnia kell a nem írható tárolóeszközökkel rendelkező rendszerelemek implementációját és kezelését. Ez magában foglalhatja a telepítési és konfigurációs dokumentációt, a hozzáférési szabályokat, a karbantartási és ellenőrzési eljárásokat, valamint a napló adatok kezelésének dokumentálását.

Kapcsolódó intézkedések

2.113. Mobil eszközök hozzáférés-ellenőrzése

11.14. Adathordozók használata

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

SC-34(1)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.100. VÉGREHAJTHATÓ, DE NEM MÓDOSÍTHATÓ PROGRAMOK – SÉRTETLENSÉG VÉDELME AZ ÍRÁSVÉDETT ADATHORDOZÓN

17.100. A szervezet gondoskodik az információ sértetlenségének védelméről még az írásvédett adathordozón történő rögzítés előtt, és ellenőrzi az adathordozót, miután adatokat rögzített rá.

MAGYARÁZAT

Az érintett szervezet szabályzatai és működési követelményei, valamint védelmi intézkedései megakadályozzák az adattárolók cseréjét az EIR-ekben, vagy a programozható, csak olvasható adattároló újraprogramozását az EIR-ekbe történő telepítés előtt. Az integritásvédelmi követelmények magukban foglalják a megelőzést, a felismerést és a reagálást.

A megelőzési követelmények közé tartozik a hozzáférési jogosultságok szigorú kezelése, hogy csak a megfelelő személyek férhessenek hozzá az adatokhoz, valamint a rendszeres biztonsági frissítések és javítások alkalmazása. A felismerési követelmények közé tartozik a naplózás és a monitorozás, amelyek segítségével a szervezet nyomon követheti az adatokhoz való hozzáférést és azok módosítását. A reagálási követelmények közé tartozik a rendszeres biztonsági esemény-választerv, amelyet a szervezetnek alkalmaznia kell, ha az adatok integritása veszélybe kerül.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az adattároló cseréje vagy a programozható, csak olvasható adattároló újraprogramozása ne történhessen meg.
2. A szervezetnek be kell vezetnie az integritásvédelmi követelményeket, amelyek magukban foglalják a megelőzést, a felismerést és a reagálást.
3. A szervezetnek ellenőriznie kell az adathordozót, miután adatokat rögzített rá, hogy biztosítsa az adatok sértetlenségét. Ez magában foglalhatja a hash-értékek vagy más digitális ujjlenyomatok használatát, amelyek segítségével az érintett szervezet ellenőrizheti, hogy az adatok nem változtak meg a rögzítés óta.

4. A szervezetnek dokumentálnia kell az adathordozókon végrehajtott műveleteket, valamint a végrehajtásért felelősök adatait, annak érdekében, hogy a későbbiekben a visszakereshetőek legyenek az esetlegesen bekövetkező biztonsági események kezelése szempontjából.

Kapcsolódó intézkedések

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.45. Konfigurációkezelési terv

11.2. Hozzáférés az adathordozókhoz

11.4. Adathordozók tárolása

11.6. Adathordozók szállítása

17.81. Tárolt (at rest) adatok védelme

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

SC-34(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.101. KÜLSŐ KÁRTÉKONY KÓDOK AZONOSÍTÁSA

17.101. Az EIR olyan rendszerelemeket tartalmaz, amelyek proaktívan keresik és azonosítják a hálózat alapú kártékony kódokat vagy kártékony weboldalakat.

MAGYARÁZAT

A külső kártékony kód azonosítási folyamata abból áll, hogy a rendszerelemek aktívan kutatják és figyelik a hálózatokat, beleértve az internetet is, folyamatosan keresve külső weboldalakon található kártékony kódokat. A külső kártékony kód azonosítási technikák alkalmazása néhány támogató izolációs intézkedést igényel annak biztosítására, hogy a keresés során felfedezett és ezután futtatott kártékony kód ne fertőzhesse meg a szervezet EIR-eit. A virtualizáció például egy gyakran alkalmazott technika az ilyen izoláció elérésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell építenie olyan rendszerelemeket, amelyek proaktívan keresik és azonosítják a hálózat alapú kártékony kódokat vagy kártékony weboldalakat.
2. A szervezetnek folyamatosan aktívan kell vizsgálnia a hálózatokat, beleértve az internetet is, a külső weboldalakon található kártékony kódok után kutatva.
3. A szervezetnek be kell vezetnie néhány támogató izolációs intézkedést, hogy biztosítsák, a keresés során felfedezett és esetlegesen futtatott kártékony kódok ne fertőzzék meg az érintett szervezet rendszereit.
4. A szervezetnek meg kell bizonyosodnia különböző technikák alkalmazásával arról, hogy lehetséges az izoláció, pl. virtualizációs környezet alkalmazásával.
5. A szervezetnek dokumentálnia kell a talált és izolált környezetben futtatott rosszindulatú kódokat, a későbbi visszakereshetőség, valamint a kártékony kód elleni védelem fejlesztése érdekében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.17. A határok védelme
17.79. Csapdák alkalmazása
17.122. Izolált futtatási környezetek
18.8. Kártékony kódok elleni védelem
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

SC-35

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.102. ELOSZTOTT FELDOLGOZÁS ÉS TÁROLÁS

17.102. A szervezet a meghatározott adatfeldolgozó és tároló rendszerelemeket több fizikai helyszínen és több logikai tartomány között osztja szét.

MAGYARÁZAT

Az adatfeldolgozó és tároló rendszerelemek több fizikai helyszínen és több logikai tartomány közötti elosztása redundanciát vagy átfedést biztosít az érintett szervezetek számára. A redundancia és az átfedés növeli a támadók számára a szükséges befektetett munkamennyiséget, ahhoz hogy kárt tudjanak okozni a szervezetek működésével kapcsolatosan, vagy negatívan befolyásolják azok eszközeit vagy személyzetét. Az elosztott feldolgozás és tárolás nem feltételezi egyetlen elsődleges feldolgozási vagy tárolási hely létezését. Emiatt lehetővé válik a párhuzamos feldolgozás és tárolás.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a rendszerelemeket, amelyeket több fizikai helyszínen és logikai tartományban lehet elosztani. Ez magában foglalhatja az adatfeldolgozó és tároló rendszereket, valamint azokat a rendszerelemeket, amelyek kritikusak az érintett szervezet működése szempontjából.
2. A szervezetnek meg kell terveznie és implementálnia kell az elosztott feldolgozási és tárolási stratégiákat. Ez magában foglalhatja a redundancia és az átfedés beépítését.
3. A szervezetnek biztosítania kell, hogy az elosztott feldolgozás és tárolás nem jelöl ki egyetlen elsődleges feldolgozási vagy tárolási helyszínt.
4. A szervezetnek dokumentálnia kell a rendszerelemek elosztását és használatát, hogy nyomon követhesse és ellenőrizhesse azokat.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az elosztott feldolgozási és tárolási stratégiáját, hogy biztosítsa annak naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.19. Biztonsági tárolási helyszín

7.23. Alternatív feldolgozási helyszín

13.6. Információbiztonsági architektúra leírás

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

SC-36

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a feldolgozó egység vagy adattároló meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.103. Elosztott feldolgozás és tárolás – Mérési technikák

17.103. A szervezet:

17.103.1. Tesztelési technikákat alkalmaz az elosztott feldolgozó és tároló rendszerelemek lehetséges zavarainak, hibáinak vagy kompromittálódásának azonosítására.

17.103.2. Zavarok, hibák vagy kompromittálódások azonosítása esetén a szervezet által meghatározott válaszintézkedéseket foganatosítja.

Magyarázat

Az elosztott feldolgozás és/vagy tárolás alkalmazása csökkentheti a támadók számára a lehetőségeket az érintett szervezet információinak és EIR-einek kompromittálására. Azonban a feldolgozó és tároló elemek elosztása nem akadályozza meg a rosszindulatú támadókat abban, hogy kompromittáljanak egy vagy több rendszerelemet. A megfelelő analítikai mérések és tesztelési technikák alkalmazása során a szervezet összehasonlítja az elosztott elemek feldolgozási eredményeit és/vagy a tároló elemek tartalmát, majd az eredmények alapján megfelelő válaszintézkedéseket indít. A megfelelő analítikai mérések és tesztelési technikák azonosítják a potenciális zavarokat, kompromittálódásokat vagy hibákat az elosztott feldolgozó és tároló elemekben.

A követelmény alkalmazásának lépései

1. A szervezetnek megfelelő tesztelési technikákat kell alkalmaznia az EIR-ek lehetséges zavarainak, hibáinak vagy kompromittálódásának azonosítására. Ez magában foglalhatja a rendszeres ellenőrzéseket, stressz teszteket és biztonsági auditokat.
2. A szervezetnek be kell azonosítania, mely esetekben érdemes elosztott megoldásokat alkalmazni, hogy a rosszindulatú támadások által okozott problémák kevésbé legyenek kihatással az érintett szervezet EIR-eire.
3. A szerveztnek el kell végeznie elosztott megoldások bevezetése után ismét a megfelelő analítikai méréseket és az eredmények kiértékelését.
4. Ha a tesztelési technikák alkalmazása során zavarok, hibák vagy kompromittálódások kerülnek azonosításra, a szervezetnek korrekciós intézkedéseket kell indítania. Ezek az

intézkedések lehetnek például a hibás elemek javítása, a kompromittált adatok helyreállítása vagy a biztonsági protokollok felülvizsgálata és frissítése.

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

SC-36(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.104. ELOSZTOTT FELDOLGOZÁS ÉS TÁROLÁS – SZINKRONIZÁCIÓ

17.104. A szervezet szinkronizálja az általa meghatározott redundáns rendszereket vagy rendszerelemeket.

MAGYARÁZAT

Az érintett szervezetnek szinkronizálnia kell az általa meghatározott duplikált EIR-eket vagy rendszerelemeket, mely esetén figyelembe kell vennie az elosztott feldolgozás és tárolás követelményét, valamint a redundáns másodlagos rendszer című követelményt. A duplikált és redundáns szolgáltatások, valamint adatok szinkronizációja segít biztosítani, hogy a szervezet ügymeneti vagy üzleti folyamatai szükség esetén használhassák a szétosztott helyszíneken található információkat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely EIR-eket vagy rendszerelemeket érdemes duplikálni és szinkronizálni.
2. A szervezetnek meg kell terveznie és implementálnia kell a duplikációs és szinkronizációs folyamatokat. Ez magában foglalja a megfelelő technológiák és eszközök kiválasztását, valamint a folyamatok automatizálását, ahol lehetséges.
3. A szervezetnek biztosítania kell, hogy a duplikált rendszerek és rendszerelemek szinkronizálva vannak, és naprakészek.
4. A szervezetnek dokumentálnia kell a szinkronizációs folyamatokat, beleértve a sikeres és sikertelen szinkronizációkat, a hibákat és a problémákat. A dokumentum segíthet a szervezetnek a folyamatok javításában és a problémák gyors megoldásában.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.35. Az elektronikus információs rendszer mentései

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

SC-36(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a duplikált rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.105. SÁVON KÍVÜLI CSATORNÁK

17.105. A szervezet meghatározott sávon kívüli (out-of-band) csatornákat alkalmaz a kijelölt információk, rendszerelemek vagy eszközök fizikai szállításához vagy elektronikus továbbításához a kijelölt személyek vagy rendszerek számára.

MAGYARÁZAT

Az out-of-band csatornák olyan helyi, nem hálózati hozzáféréseket jelentenek a rendszerekhez, amelyek fizikailag elkülönülnek a normális, tervezett működéshez használt hálózati útvonalaktól. Emellett jelenthetnek még nem elektronikus utakat, mint például a postai szolgáltatás. A sávon kívüli (out-of-band) csatornáknak más a sebezhetősége és a támadhatósága, mint a sávon belüli (in-band) csatornáknak, ahol rutinszerű ügymeneti forgalom zajlik. Ezért a sávon belüli (in-band) csatornák bizalmasságának, sérthetetlenségének vagy rendelkezésre állásának kompromittálása általában nem fogja kompromittálni vagy hátrányosan befolyásolni a sávon kívüli (out-of-band) csatornákat. A szervezetek alkalmazhatják a sávon kívüli (out-of-band) csatornákat különböző elemek szállítására vagy továbbítására, beleértve az hitelesítőket és hitelesítési adatokat; kriptográfiai kulcskezelési információkat; rendszer- és adatmentéseket; a hardver, firmware vagy szoftver konfigurációs menedzsment változásaival kapcsolatos információkat; biztonsági frissítéseket; karbantartási információkat; és rosszindulatú kódok elleni védelmi frissítéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely információkat, rendszerelemeket vagy eszközöket érdemes fizikailag szállítani vagy elektronikusan továbbítani a sávon kívüli (out-of-band) csatornákon keresztül.
2. A szervezetnek ki kell jelölnie a személyeket vagy rendszereket, akik vagy amelyek a szállítás vagy továbbítás részeként fognak megjelenni.
3. A szervezetnek létre kell hoznia a szükséges sávon kívüli (out-of-band) csatornákat. Ezek lehetnek helyi, nem hálózati hozzáférések a rendszerekhez, fizikailag elkülönített hálózati utak, amelyeket az operatív forgalomhoz használnak, vagy nem elektronikus utak, mint például a postai szolgáltatás.

4. A szervezetnek biztosítania kell, hogy a sávon kívüli (out-of-band) csatornák nem rendelkeznek ugyanazzal a sebezhetőséggel vagy kitettséggel, mint a sávon belüli (in-band) csatornák.

5. A szervezetnek alkalmaznia kell a sávon kívüli (out-of-band) csatornákat a szervezeti elemek szállításában vagy továbbításában.

6. A szervezetnek naplóznia kell a sávon kívüli csatornák információáramlását, valamint monitoroznia kell azt, hogy megelőzze a potenciális biztonsági események kialakulását, továbbá a biztonsági eseményekre hatékonyan tudjon válaszintézkedéseket hozni.

Kapcsolódó intézkedések

2.2. Fiókkezelés

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.26. Legszűkebb funkcionalitás

8.2. Azonosítás és hitelesítés

8.14. Azonosító kezelés

8.21. A hitelesítésre szolgáló eszközök kezelése

10.11. Távoli karbantartás

17.49. Kriptográfiai kulcs előállítása és kezelése

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

SC-37

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az információk, rendszerelemek vagy eszközök illetve a személyek vagy rendszerek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.106. SÁVON KÍVÜLI CSATORNÁK – ÁTVITEL ÉS TOVÁBBÍTÁS BIZTOSÍTÁSA

17.106. A szervezet kontrollmechanizmusokat alkalmaz annak biztosítására, hogy csak a feljogosított személyek vagy rendszerek férhessenek hozzá bizonyos, a szervezet által meghatározott információkhoz, rendszerelemekhez és eszközökhöz.

MAGYARÁZAT

Az érintett szervezeteknek olyan technikákat kell alkalmazniuk, amelyek biztosítják, hogy csak a kijelölt rendszerek vagy személyek kapjanak hozzáférést bizonyos információkhoz, rendszerelemekhez vagy eszközökhöz. Ilyen technikák közé tartozik például a hitelesítők küldése egy jóváhagyott biztonságos csatornán keresztül, de a címzetteknek valamilyen formában érvényes fényképes azonosítót vagy igazolványt kell bemutatniuk az átvétel feltételeként.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely információkhoz, rendszerelemekhez és eszközökhöz férhet hozzá csak megfelelő, feljogosított személy.
2. A szervezetnek be kell vezetnie a szükséges kontrollmechanizmusokat, amelyek biztosítják, hogy csak a feljogosított személyek vagy rendszerek férhetnek hozzá a meghatározott információkhoz, rendszerelemekhez és eszközökhöz. Ez magában foglalhatja a felhasználói hitelesítést, a hozzáférési jogosultságok kezelését, a hozzáférési naplókat és a rendszeres biztonsági ellenőrzéseket.
3. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kontrollmechanizmusokat, hogy biztosítsa azok hatékonyságát és relevanciáját.
4. A szervezetnek biztosítania kell, hogy a feljogosított személyek tisztában vannak a hozzáférési szabályokkal és követelményekkel, és betartják azokat.

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

SC-37(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények, illetve a személyek vagy rendszerek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.107. MŰKÖDÉSBIZTONSÁG

17.107. A szervezet meghatározott működésbiztonsági követelményeket alkalmaz a szervezet működése szempontjából kritikus információk védelme érdekében a rendszerfejlesztési életciklus során.

MAGYARÁZAT

A működésbiztonság (OPSEC) egy olyan folyamat, amelynek segítségével a potenciális támadóktól megtagadható az információ az érintett szervezet képességeiről és szándékairól, azáltal, hogy a szervezet azonosítja, ellenőrzi és védi az olyan fajta titkosítatlan információkat, amelyek kifejezetten a szervezet tevékenységeinek tervezésével és végrehajtásával kapcsolatosak. Az OPSEC folyamat öt lépésből áll: a kritikus információk azonosítása, a fenyegetések elemzése, a sebezhetőségek elemzése, a kockázatok értékelése és a megfelelő ellenintézkedések alkalmazása. Az OPSEC védelmi intézkedéseket a szervezet rendszereire és azokra a környezetekre alkalmazzák, amelyekben ezek az EIR-ek működnek. Az OPSEC vizsgálatok magukban foglalják az információk bizalmasságának védelmét, beleértve az információ megosztásának korlátozását a beszállítókkal, és más, nem szervezeti elemekkel és személyekkel. A szervezet alapfeladatai és üzleti funkciói szempontjából kritikus információk a felhasználói azonosítók, elemek használata, beszállítók, ellátási lánc folyamatok, funkcionális követelmények, biztonsági követelmények, rendszertervezési specifikációk, tesztelési és értékelési protokollok, valamint a biztonsági ellenőrzések végrehajtásának részletei.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell a kritikus információkat a rendszerekben.
2. A szervezetnek elemeznie kell a fenyegetéseket, amelyek a kritikus információkra vonatkoznak.
3. A szervezetnek értékelnie kell a kockázatokat, amelyek a fenyegetésekből adódnak. Ez magában foglalhatja a potenciális adatvesztést, a szolgáltatás megszakítását, vagy a jogi következményeket.
4. A szervezetnek alkalmaznia kell a megfelelő működésbiztonsági (OPSEC) folyamatokat és kontrollokat, hogy az információit biztonságban tudja.

5. Az OPSEC védelmi intézkedéseket a szervezet EIR-eire és annak működési környezetére kell alkalmazni. Az OPSEC intézkedések védelmezik az információk bizalmas voltát.
6. A szervezetnek dokumentálnia kell a kritikus információk védelme érdekében meghatározott működésbiztonsági követelményeket és azok megvalósítását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.2. Biztonsági értékelések
5.14. Folyamatos felügyelet
13.1. Szabályzat és eljárásrendek
1.10. Kockázatkezelési stratégia
1.13. Belső fenyegetés elleni program
15.2. Biztonsági osztályba sorolás
15.4. Kockázatértékelés
15.10. Sérülékenységmonitorozás és szkennelés
17.17. A határok védelme
19.4. Ellátási láncra vonatkozó követelmények és folyamatok

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

SC-38

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a működésbiztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.108. A FOLYAMATOK ELKÜLÖNÍTÉSE

17.108. Az EIR elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

MAGYARÁZAT

Az EIR-eknek minden végrehajtott folyamathoz külön végrehajtási tartományt javasolt fenntartaniuk, azzal, hogy minden egyes folyamatot külön címtartományban hajtanak végre. Mindegyik EIR folyamatnak egy külön címtartománya van, így a folyamatok közötti kommunikáció a biztonsági funkciók által ellenőrzött módon történhet, és az egyik folyamat nem tudja módosítani egy másik folyamat végrehajtó kódját. Az elkülönített végrehajtási tartományok fenntartása a folyamatok végrehajtásához például külön címterek kialakításával érhető el. A folyamat elszigetelési technológiák, beleértve a sandboxingot vagy a virtualizációt, logikailag elválasztják a szoftvert és a firmware-t más szoftverektől, firmware-től és adatoktól. A folyamat elszigetelés segít korlátozni a potenciálisan nem megbízható szoftverek hozzáférését más rendszererőforrásokhoz. Ez a lehetőség a legtöbb kereskedelmi operációs rendszerben elérhető, amely támogatja a többállapotú processzortechnológiákat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR-ek megfelelő folyamatai számára elkülönített végrehajtási tartományt tartson fenn. Ez azt jelenti, hogy minden ilyen folyamat esetén külön címtartományt kell alkalmazni.
2. A szervezetnek gondoskodnia kell arról, hogy az EIR-ek folyamatai közötti kommunikáció a biztonsági funkciók által szabályozott módon történjen, és egy folyamat ne tudja módosítani egy másik folyamat végrehajtó kódját.
3. A szervezetnek implementálnia kell az elkülönített címtartományokat, hogy biztosítsa a rendszerfolyamatok elkülönített végrehajtási tartományát.
4. A szervezetnek alkalmaznia kell folyamat izolációs technológiákat, mint például a sandboxingot vagy a virtualizációt, hogy logikailag elválassza a szoftvereket és firmware-eket a többi szoftvertől, firmware-től és adattól.

5. A szervezetnek biztosítania kell, hogy az EIR képes legyen fenntartani az elkülönített végrehajtási tartományokat. Ez a képesség rendelkezésre áll a kereskedelemben kapható operációs rendszerekben is.
6. A szervezetnek dokumentálnia kell az általa meghatározott valamennyi végrehajtási tartományt és az azokhoz tartozó végrehajtó folyamatot, melyet rendszeres időnként felül kell vizsgálnia.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése
2.28. Információáramlási szabályok érvényesítése
2.60. Legkisebb jogosultság elve
2.129. Referenciának való megfelelőség vizsgálata
16.16. Biztonságtervezési elvek
17.2. Rendszer és felhasználói funkciók szétválasztása
17.4. Biztonsági funkciók elkülönítése
18.78. Memóriavédelem

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

3.3.13.22. A folyamatok elkülönítése: Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SC-39

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

17.109. FOLYAMATOK ELKÜLÖNÍTÉSE – HARDVERES ELKÜLÖNÍTÉS

17.109. A szervezet a folyamatok elkülönítését elősegítő hardver szintű mechanizmusokat alkalmaz.

MAGYARÁZAT

A hardver szintű elkülönítési mechanizmusok általában kevésbé hajlamosak a kompromittálódásra, mint a szoftver alapú elkülönítés, így nagyobb biztosítékot nyújtanak arra, hogy az elkülönítés előnyei érvényesülhessenek. A hardveres elkülönítési mechanizmusok közé tartozik a hardveres memória kezelés, a processzorok és a memória fizikai elkülönítése, valamint a különböző rendszerelemek közötti kommunikáció korlátozása.

A hardverelemek, valamint hardver szintű mechanizmusok működésbiztonságának fenntartása érdekében a szervezetnek rendszeres karbantartási tevékenységeket kell végeznie, például: a hardverek rendszeres frissítését, a naplók rendszeres ellenőrzését és a rendszer teljesítményének monitorozását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely folyamatokat kell elkülöníteni. Ez magában foglalja az EIR különböző elemeinek, alkalmazásainak és adatbázisainak azonosítását, amelyeket elkülönítetten kell futtatni.
2. A szervezetnek ki kell választania a megfelelő hardver szintű mechanizmusokat, amelyek elősegítik a folyamatok elkülönítését.
3. A szervezetnek implementálnia kell a kiválasztott hardver szintű mechanizmusokat. Ez magában foglalhatja az EIR hardver konfigurációjának módosítását, új hardverek beszerzését és telepítését, valamint a meglévő hardverek frissítését.
4. A szervezetnek ellenőriznie kell, hogy a hardver szintű mechanizmusok megfelelően működnek-e. Ez magában foglalhatja a rendszer tesztelését, a naplók ellenőrzését és a rendszer teljesítményének monitorozását.
5. A szervezetnek folyamatosan karban kell tartania és frissítenie kell a hardver szintű mechanizmusokat, hogy biztosítsa azok hatékonyságát és megbízhatóságát.

6. A szervezetnek dokumentálnia kell a hardver szintű mechanizmusok használatát és karbantartását, hogy bizonyítékot szolgáltasson a kiberbiztonsági követelményeknek való megfelelésről.

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

SC-39(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.110. A FOLYAMATOK ELKÜLÖNÍTÉSE – KÜLÖN VÉGREHAJTÁSI TARTOMÁNY SZÁLANKÉNT

17.110. Az EIR külön végrehajtási tartományt tart fenn minden szálon belül a többszálú feldolgozás esetén.

MAGYARÁZAT

A többszálú feldolgozás (multithreading) egy olyan programozási technika, amely lehetővé teszi, hogy egy alkalmazás egyszerre több feladatot (szálat) hajtson végre. Ezáltal az alkalmazás hatékonyabban tudja kihasználni a rendelkezésre álló számítási erőforrásokat, különösen olyan EIR-ek esetén, amelyek több processzormagot vagy több szálat támogatnak. (pl.: webszerverek, adatbázis-kezelő rendszerek, grafikai alkalmazások...)

A követelmény azt jelenti, hogy a szervezetnek biztosítania kell, hogy minden szálhoz külön végrehajtási tartomány legyen fenntartva, amikor többszálú feldolgozást alkalmaznak. Ezáltal minimalizálhatók az olyan biztonsági kockázatok, mint az adatok véletlen vagy szándékos kereszteződése vagy a szálak közötti nem kívánt befolyásolás.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat az EIR-eket, melyek támogatják a többszálú feldolgozást, valamint azon alkalmazásokat, melyek képesek a többszálú feldolgozásra.
2. A szervezetnek biztosítania kell, hogy minden szálhoz külön végrehajtási tartomány kerüljön meghatározásra.
3. A szervezetnek monitoroznia kell a végrehajtási szálakhoz rendelt végrehajtási tartományok megfelelőségét.

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

SC-39(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a többszálú feldolgozás meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.111. VEZETÉK NÉLKÜLI KAPCSOLAT VÉDELME

17.111. A szervezet védelmet biztosít a meghatározott vezeték nélküli kapcsolatok számára a meghatározott jelparaméter-támadásokkal, valamint az ilyen támadások forrásaira történő hivatkozásokkal szemben.

MAGYARÁZAT

A vezeték nélküli kapcsolatok védelme olyan belső és külső vezeték nélküli kommunikációs kapcsolatokra vonatkozik, amelyek láthatóak lehetnek hozzáférési jogosultsággal nem rendelkező személyek számára is. A támadók kihasználhatják a vezeték nélküli kapcsolatok jelszórását, ha ezek a kapcsolatok nincsennek megfelelően védve. Sokféleképpen támadhatóak a vezeték nélküli kapcsolatok jelparaméterei az információgyűjtés, a szolgáltatás megtagadás vagy a felhasználók megtévesztésének céljából. A vezeték nélküli kapcsolatok védelme csökkenti azoknak a támadásoknak a hatását, amelyek kizárólag a vezeték nélküli rendszerekre jellemzőek. Ha az érintett szervezetek kereskedelmi szolgáltatókra támaszkodnak a továbbítási szolgáltatásokért, nem pedig teljesen dedikált szolgáltatásokat használnak, akkor előfordulhat, hogy nem lehetséges a vezeték nélküli kapcsolatok védelmének megvalósítása a szükséges mértékben a szervezet biztonsági követelményeinek megfelelően.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely belső és külső vezeték nélküli kommunikációs kapcsolatok lehetnek láthatók jogosultsággal nem rendelkező személyek számára.
2. A szervezetnek tudatában kell lennie annak, hogy a vezeték nélküli kapcsolatokat számos módon ki lehet használni információgyűjtésre, szolgáltatás megtagadására vagy a felhasználók megtévesztésére.
3. A szervezetnek meg kell védenie a vezeték nélküli kapcsolatokat különböző védelmi intézkedések alkalmazásával, hogy csökkentse a vezeték nélküli rendszerekre jellemző támadások hatását.
4. A szervezetnek dokumentálnia kell az általa megvalósított biztonsági követelményeket, melyekkel a vezeték nélküli kapcsolatok védelmét hivatott biztosítani.

5. A szervezetnek rendszeres időnként felül kell vizsgálnia a vezeték nélküli kapcsolataira alkalmazott védelmi intézkedéseit, annak érdekében, hogy a valós fenyegetésekkel szemben teljeskörű és naprakész védelmet legyen képes biztosítani.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.108. Vezeték nélküli hozzáférés

17.12. Szolgáltatásmegtagadással járó támadások 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

SC-40

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a vezeték nélküli kapcsolatok, illetve a jelparaméter-támadások, valamint az ilyen támadások forrásaira történő hivatkozások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.112. VEZETÉK NÉLKÜLI KAPCSOLAT VÉDELME – ELEKTROMÁGNESES INTERFERENCIA

17.112. A szervezet olyan kriptográfiai mechanizmusokat valósít meg, amelyek a meghatározott védelmi szint elérését szolgálják a szándékosan előidézett elektromágneses interferencia hatásaival szemben.

MAGYARÁZAT

Az érintett szervezet által megvalósított kriptográfiai mechanizmusok az elektromágneses interferencia elleni védelem céljából képesek védelmet nyújtani a szándékos zavarás ellen, amely megakadályozhatja vagy károsíthatja a kommunikációt. Ezek a mechanizmusok biztosítják, hogy a zavarás elleni védelemre használt vezeték nélküli spektrumterjedési hullámformák ne legyenek előrejelezhetőek jogosulatlan személyek számára. A szervezet által megvalósított kriptográfiai mechanizmusok esetlegesen enyhíthetik a nem szándékos zavarás hatásait is, amelyek ugyanazt a spektrumot használó jogosult adók interferenciájából adódhatnak. A szervezet ügymenetével kapcsolatos követelményei, a várható fenyegetések, a műveletek koncepciója, valamint a törvények, döntéshozói rendeletek, irányelvek és szabályozások határozzák meg a vezeték nélküli kapcsolatok rendelkezésre állásának, a szükséges kriptográfiának és a teljesítménynek a szintjét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a védelmi szintet, amelyet el szeretne érni az elektromágneses interferencia hatásai ellen. Ez a szint számos követelménytől és jogszabálytól függ.
2. A szervezetnek ki kell választania és dokumentálnia kell a megfelelő kriptográfiai mechanizmusokat, amelyek megfelelnek a meghatározott védelmi szintnek. Ezek a mechanizmusok biztosítják, hogy a zavarás elleni védelemre használt vezeték nélküli spektrumszóró hullámformák ne legyenek előrejelezhetők jogosulatlan személyek számára.
3. A szervezetnek implementálnia kell a kiválasztott kriptográfiai mechanizmusokat a rendszerekben. Ez magában foglalja a mechanizmusok beállítását, tesztelését és beüzemelését.

4. A szervezetnek rendszeres időnként felül kell vizsgálnia az alkalmazott kriptográfiai mechanizmusokat, annak érdekében, hogy mindig naprakészek legyenek és megfelelő biztonságot biztosítsanak.

KAPCSOLÓDÓ INTÉZKEDÉSEK

12.47. Elektromágneses impulzus elleni védelem

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

SC-40(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a védelmi szint meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.113. Vezeték nélküli kapcsolat védelme – Felderítés lehetőségének csökkentése

17.113. A szervezet kriptográfiai módszereket alkalmaz annak érdekében, hogy a szervezet által meghatározott szintre csökkentse a vezeték nélküli kapcsolatok észlelési lehetőségét.

Magyarázat

Az érintett szervezet kriptográfiai mechanizmusokat alkalmaz a vezeték nélküli kapcsolatok felderítés lehetőségeinek csökkentése érdekében. Ez használható a kommunikáció elrejtésére és a vezeték nélküli adók geolokációjának védelmére. Ez azt is biztosítja, hogy a szervezet által használt széles spektrumszórású rádióhullámok ne legyenek előrejelezhetőek jogosulatlan személyek számára. Az ilyen rádióhullámok célja, hogy csökkentsék a vezeték nélküli kapcsolatok észlelhetőségét. A vezeték nélküli kapcsolatok észlelhetetlenné tételének szükséges szintjét sok paraméter határozza meg. Ezek: a szervezet alapfeladatai, a várható fenyegetések, valamint az alkalmazandó törvények, rendeletek, irányelvek, szabályozások, szabályok és normák.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a vezeték nélküli kapcsolatok észlelési lehetőségének kívánt szintjét, ezt számos tényező befolyásolja.
2. A szervezetnek ki kell választania a megfelelő kriptográfiai módszereket, amelyeket a vezeték nélküli kapcsolatok felderítés lehetőségének csökkentésére alkalmaz. Ezek a módszerek általában a titkos kommunikációhoz és a vezeték nélküli adók geolokációjának védelméhez használhatók.
3. A szervezetnek implementálnia kell a kiválasztott kriptográfiai módszereket. Ez magában foglalja a szélessávú rádióhullámok használatát, amelyek alacsony észlelési valószínűséget biztosítanak, és nem jósolhatók meg jogosulatlan személyek által.
4. A szervezetnek ellenőriznie kell, hogy az implementált kriptográfiai módszerek megfelelően működnek-e, és elérhető-e a kívánt észlelési szint. Ez magában foglalja a naplózást és a rendszeres tesztelést.

5. A szervezetnek dokumentálnia kell valamennyi alkalmazott kriptográfiai mechanizmust és rendszeres időnként felül kell vizsgálnia, hogy biztosíthassa a meghatározott szintjét a vezeték nélküli kapcsolatok észlelésének.

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

SC-40(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a csökkentési szintjének meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.114. VEZETÉK NÉLKÜLI KAPCSOLAT VÉDELME – UTÁNZÓ VAGY MANIPULATÍV MEGTÉVESZTÉS

17.114. A szervezet olyan kriptográfiai mechanizmusokat alkalmaz, amelyek azonosítják és visszautasítják azokat a vezeték nélküli adatátviteleket, amelyek jelparaméterek figyelembevételével történő elemzés alapján szándékos utánzó vagy manipulatív kommunikációs csalásra utalnak.

MAGYARÁZAT

Az érintett szervezet kriptográfiai mechanizmusokat alkalmaz, amelyek célja az utánzó vagy manipulatív vezeték nélküli kommunikációk azonosítása és visszautasítása. Ezek a mechanizmusok biztosítják, hogy a vezeték nélküli adatátvitel jelparaméterei ne legyenek előre kiszámíthatók jogosulatlan személyek számára. Az ilyen kiszámíthatatlanság csökkenti az utánzó vagy manipulatív kommunikációs csalás valószínűségét, amely kizárólag a jelparamétereken alapul.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és implementálnia kell olyan kriptográfiai mechanizmusokat, amelyek képesek védelmet nyújtani a vezeték nélküli hálózatok utánzó vagy manipulatív kommunikációs támadásaival szemben.
2. A szervezetnek meg kell bizonyosodnia arról, hogy rendelkezik a szükséges hardverrel és szoftverrel, amelyek képesek támogatni ezeket a kriptográfiai mechanizmusokat.
3. A szervezetnek ki kell dolgoznia és be kell vezetnie olyan szabályrendszert és eljárásokat, amelyek meghatározzák, hogyan és mikor kerüljenek alkalmazásra ezek a kriptográfiai mechanizmusok.
4. A szervezetnek rendszeres időnként felül kell vizsgálnia az általa alkalmazott kriptográfiai mechanizmusokat, hogy a szándékos utánzó vagy manipulatív fenyegetésekkel szemben naprakészek legyenek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

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

SC-40(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.115. VEZETÉK NÉLKÜLI KAPCSOLAT VÉDELME – JELPARAMÉTEREK AZONOSÍTÁSA

17.115. A szervezet kriptográfiai mechanizmusokat alkalmaz a meghatározott vezeték nélküli adók jelparamétereinek felhasználásával történő nem kívánt hozzáférés megakadályozására.

MAGYARÁZAT

Az érintett szervezet kriptográfiai mechanizmusokat kell hogy alkalmazzon a vezeték nélküli adók jelparamétereinek beazonosításának megakadályozására, biztosítva, hogy az lehallgatás és letapogatás védelmi módosítások a jelparaméterekben ne legyenek előrejelezhetőek jogosulatlan személyek számára. Ez anonimitást is biztosít, amikor szükséges. A rádióhullám letapogató technikák (ujjlenyomatképzésen alapuló) az adók egyedi jelparamétereit azonosítják, hogy információt nyerjenek ki belőlük, és adatprofilt készítsenek az adókról. Ez a történhet követési célból, vagy akár felhasználó azonosítása céljából.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely vezeték nélküli adók jelparamétereit kívánja védeni a nem kívánt hozzáférés ellen.
2. A szervezetnek ki kell választania a megfelelő kriptográfiai mechanizmusokat, amelyeket alkalmazni kíván a védelemre. Ezeknek a mechanizmusoknak képesnek kell lenniük arra, hogy megakadályozzák a vezeték nélküli adók jelparamétereinek nem kívánt letapogatását.
3. A szervezetnek implementálnia kell a kiválasztott kriptográfiai mechanizmusokat. Ez magában foglalhatja a szoftverfrissítéseket, a hardver módosításait és a rendszerbeállítások módosításait.
4. A szervezetnek tesztelnie kell a kriptográfiai mechanizmusok hatékonyságát.
5. A szervezetnek dokumentálnia kell az alkalmazott kriptográfiai mechanizmusokat és azok rendszeres időnként történő felülvizsgálatát, hogy a jelparaméterek felhasználása ne legyen lehetséges a technológia fejlődésével sem.

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

SC-40(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a vezeték nélküli adók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.116. PORTOK, ILLETVE KI- ÉS BEMENETI ESZKÖZÖK HOZZÁFÉRÉSE

17.116. A szervezet fizikailag vagy logikailag letiltja vagy eltávolítja a meghatározott csatlakozókat, vagy be- és kimeneti eszközöket a meghatározott EIR-eken vagy rendszerelemeken.

MAGYARÁZAT

A csatlakozó portok közé sorolhatóak az univerzális soros busz (USB) kapcsolatok, a Thunderbolt és a Firewire (IEEE 1394). A be- és kimeneti (I/O) eszközök közé tartoznak a CD- és a DVD-meghajtók. Az ilyen portok és I/O eszközök letiltása vagy eltávolítása segít megelőzni az információk kiszivárgását és a rosszindulatú kódok megjelenését ezekről a portokról vagy eszközökről. A portok és/vagy eszközök fizikai letiltása vagy eltávolítása erősebb intézkedés, mint a sima szoftveres vagy logikai tiltás.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a csatlakozókat és be- és kimeneti eszközöket, amelyeket esetében érdemes lehet a letiltáson vagy eltávolításon gondolkozni.
2. A szervezetnek azonosítania kell a letiltandó vagy eltávolítandó csatlakozókat és eszközöket, valamint meg kell határoznia, hogy fizikailag vagy logikailag tiltja-e le vagy távolítja-e el őket. A fizikai letiltás vagy eltávolítás erősebb intézkedés, mivel ez megakadályozza a csatlakozók vagy eszközök fizikai használatát.
3. A szervezet el kell végeznie a letiltást vagy eltávolítást, amennyiben fizikailag tiltja le vagy távolítja el a csatlakozókat vagy eszközöket, akkor ez lehet a csatlakozók lezárása, eltávolítása vagy az eszközök kikapcsolása. Ha logikailag tiltja le vagy távolítja el őket, akkor ez lehet a szoftveres letiltás, például a csatlakozók vagy eszközök használatának letiltása az operációs rendszerben.
4. A szervezetnek ellenőriznie kell, hogy a letiltás vagy eltávolítás sikeres volt-e. Ez magában foglalhatja a csatlakozók vagy eszközök fizikai ellenőrzését, valamint a szoftveres ellenőrzést, hogy a csatlakozók vagy eszközök valóban letiltásra kerültek-e.

5. A szervezetnek nyilvántartást kell vezetnie és rendszeresen felül kell vizsgálnia a letiltott be - és kimeneti eszközöket és csatlakozókat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.115. Külső elektronikus információs rendszerek használata

11.14. Adathordozók használata

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

SC-41

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a csatlakozók, vagy be- és kimeneti eszközök illetve a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.117. ÉRZÉKELŐ KÉPESSÉGEI ÉS KAPCSOLÓDÓ ADATOK

17.117. A szervezet:

17.117.1. megtiltja a meghatározott környezeti érzékelő képességekkel rendelkező eszközök használatát a meghatározott létesítményekben, területeken vagy rendszerekben, továbbá a környezeti érzékelési képességek távoli aktiválását a meghatározott szervezeti EIR-ekben vagy rendszerelemekben, kivéve a szervezet által meghatározott kivételeket; és

17.117.2. egyértelmű jelzést biztosít a szenzor használatáról a meghatározott felhasználói csoport számára.

MAGYARÁZAT

A környezeti érzékelő képességekkel rendelkező eszközökbe, vagy más néven mobil eszközökbe sorolható eszközök például a mobiltelefonok, az okostelefonok és a táblagépek. A mobil eszközök gyakran rendelkeznek olyan érzékelőkkel, amelyek képesek gyűjteni és rögzíteni adatokat a környezetről. Az ilyen mobil eszközökbe épített érzékelők közé tartoznak a mikrofonok, kamerák, a globális helymeghatározó rendszer (GPS) szenzorok és az gyorsulásmérők. Bár a mobil eszközökön található érzékelők fontos funkciót töltenek be, ha titokban aktiválják őket, ezek az eszközök potenciálisan lehetőséget nyújthatnak egy támadó számára, hogy értékes információhoz jussanak az érintett szervezetekről vagy személyről. Például egy mobil eszközön a GPS funkció távoli aktiválása lehetővé teheti egy támadó számára, hogy nyomon kövesse egy személy mozgását. Az érintett szervezetek megtilthatják, hogy az ott dolgozók mobiltelefont vagy digitális kamerát vigyenek be bizonyos kijelölt létesítményekbe vagy ellenőrzött területekre a létesítményeken belül, ahol minősített információkat tárolnak vagy érzékeny beszélgetések zajlanak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely környezeti érzékelő képességekkel rendelkező eszközök használatát tiltja meg és mely meghatározott létesítményekben, területeken vagy rendszerekben.

2. A szervezetnek meg kell tiltania a környezeti érzékelési képességek távoli aktiválását a meghatározott szervezeti EIR-ekben vagy rendszerelemekben, kivéve a szervezet által meghatározott kivételeket.

3. A szervezetnek egyértelmű jelzést kell biztosítania a szenzor használatáról a meghatározott felhasználói csoport számára. Ez magában foglalhatja a felhasználók tájékoztatását arról, hogy mely eszközök használata tiltott, és milyen körülmények között.
4. A szervezetnek dokumentálnia kell a tiltott eszközök használatát, és rendszeres időnként felül kell vizsgálnia a dokumentum tartalmát, valamint ellenőriznie kell a szabályok betartását.

Kapcsolódó intézkedések

17.54. Együttműködésen alapuló informatikai eszközök

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

SC-42

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.118. ÉRZÉKELŐ KÉPESSÉG ÉS ADATOK – JELENTÉS A KIJELÖLT SZEMÉLYEKNEK VAGY SZEREPKÖRÖKNEK

17.118. A szervezet úgy konfigurálja az EIR-t, hogy az csak a jogosult személyek vagy szerepkörök számára továbbítsa a meghatározott érzékelők által gyűjtött adatokat vagy információkat.

MAGYARÁZAT

Az érintett szervezetnek gondoskodnia kell arról, hogy az összes rendszer úgy legyen konfigurálva, hogy csak a jogosult személyek vagy szerepkörök számára továbbítsa a meghatározott érzékelők által gyűjtött adatokat vagy információkat. Azokban a helyzetekben, amikor az érzékelőket jogosult személyek aktiválják, még mindig lehetséges, hogy az érzékelők által gyűjtött adatok vagy információk illetéktelen szervezetekhez kerülnek. Ennek érdekében a szervezetnek rendszeresen ellenőriznie kell az EIR konfigurációját, hogy biztosítsa, hogy csak a jogosult személyek vagy szerepkörök férhetnek hozzá az adatokhoz vagy információkhoz. Ezért a szervezetnek a naplók ellenőrzését, a hozzáférési jogosultságok felülvizsgálatát, és a szoftver beállításainak ellenőrzését is el kell végeznie.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely személyek vagy szerepkörök jogosultak az összegyűjtött adatokhoz vagy információkhoz való hozzáférésre. Ez magában foglalhatja a szervezet belső munkatársait, valamint külső partnereket vagy szolgáltatókat is.
2. A szervezetnek létre kell hoznia egy konfigurációs tervet, amely részletesen leírja, hogy mely személyek vagy szerepkörök jogosultak az adatokhoz vagy információkhoz való hozzáférésre, és milyen körülmények között.
3. A szervezetnek implementálnia kell a konfigurációs tervet. Ez magában foglalhatja a szoftver beállításainak módosítását, a hozzáférési jogosultságok beállítását, és a naplózás beállításait.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR konfigurációját, hogy biztosítsa, hogy csak a jogosult személyek vagy szerepkörök férhetnek hozzá az adatokhoz vagy információkhoz.

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

SC-42(1)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az érzékelők meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.119. ÉRZÉKELŐ KÉPESSÉG ÉS ADATOK – ENGEDÉLYEZETT FELHASZNÁLÁS

17.119. A szervezet meghatározott intézkedéseket alkalmaz annak érdekében, hogy a meghatározott érzékelők által gyűjtött adatokat vagy információkat csak engedélyezett célokra lehessen felhasználni.

MAGYARÁZAT

Az érintett szervezet által meghatározott érzékelők által gyűjtött információkkal kapcsolatban a szervezetnek meg kell bizonyosodnia arról, hogy ezek csak engedélyezett célokra kerülnek felhasználásra, és kerülni kell a nem engedélyezett célokra való felhasználást, mert a gyűjtött adatokkal visszaélhetnek. Például a forgalmi navigáció támogatására használt GPS érzékelőket fel lehetne használni egyének mozgásának nyomon követésére. Az ilyen tevékenységek enyhítésére szolgáló intézkedések közé tartozik a továbbképzés, amely segít biztosítani, hogy a jogosult személyek ne éljenek vissza hatalmukkal, és abban az esetben, ha az érzékelő adatokat külső felek kezelik, szükségesek a szerződéses korlátozások az ilyen adatok használatára.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, milyen jellegű érzékelők gyűjtenek adatokat vagy információkat, és milyen célokra használják fel ezeket az adatokat.
2. A szervezetnek meg kell határoznia, mely személyeknek van hozzáférése gyűjtött adatokhoz, és milyen jogosultságaik vannak ezekkel az adatokkal kapcsolatban.
3. A szervezetnek képzéseket kell szerveznie a jogosult személyek számára, hogy biztosítsa az adatok csak a megengedett célokra fognak felhasználásra kerülni.
4. Amennyiben az adatokat külső felek kezelik, a szervezetnek szerződéses korlátozásokat kell bevezetnie az adatok használatára vonatkozóan.
5. A szervezetnek naplót kell vezetnie az érzékelők által gyűjtött adatok hozzáféréséről és rendszeres időnként felül kell vizsgálnia a naplókat, valamint a jogosultsággal rendelkezők listáját.

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

SC-42(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az érzékelők illetve az intézkedések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.120. Érzékelő képesség és adatok – Adatgyűjtés minimalizálása

17.120. A szervezet olyan érzékelőket alkalmaz, amelyek úgy vannak beállítva, hogy minimalizálják az egyénekről történő szükségtelen információgyűjtést.

Magyarázat

Bár az információgyűjtéssel és annak módjával, menetével kapcsolatos hozzáférési szabályokat lehetséges alkalmazni az információk begyűjtése után is, azonban a nem szükséges információk gyűjtésének mellőzése, és a szükséges információ gyűjtésének minimalizálása csökkenti a adatszivárgási és adatvédelmi kockázatot az EIR belépési pontjain, és csökkenti annak kockázatát, hogy szabályozással kapcsolatos probléma merüljön fel. Például az érintett szervezetnek olyan személyazonosításért felelős érzékelőket kell alkalmaznia, amelyek úgy vannak beállítva, hogy minimalizálják az egyénekről történő szükségtelen információgyűjtést. Ez azt jelenti, hogy az érzékelők csak a szükséges adatokat gyűjtik be, és nem rögzítik az egyének személyes adatait, hacsak ez nem szükséges. Az ilyen beállítások közé tartozik például az arcok vagy más azonosító jellemzők elmosása vagy pixelesítése.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, milyen információk gyűjtése szükséges, és milyenek azok, amelyeket el kell kerülni. Ez magában foglalja a személyes adatok, mint például a személyazonosságot igazoló adatok, a biometrikus adatok és más érzékeny információk vizsgálatát.
2. A szervezetnek be kell állítania az EIR érzékelőit úgy, hogy minimalizálják a szükségtelen információgyűjtést.
3. A szervezetnek biztosítania kell, hogy a szükségtelen információgyűjtés minimalizálása érdekében alkalmazott intézkedések megfelelnek a vonatkozó jogszabályoknak és szervezeti szabályoknak. Ez magában foglalhatja a személyes adatok védelmére vonatkozó jogszabályok, mint például a GDPR, betartását.
4. A szervezetnek folyamatosan monitoroznia kell a jogszabály változásokat, különösen az adatvédelmi vonatkozásban megjelenőket, annak érdekében, hogy az egyénekről történő

információgyűjtési szabályok és eljárások mindig naprakészek legyenek a vonatkozó jogszabályoknak megfelelően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

16.16. Biztonságtervezési elvek

18.67. Információ kezelése és megőrzése

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

SC-42(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az érzékelők meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.121. HASZNÁLATI KORLÁTOZÁSOK

17.121. A szervezet:

17.121.1. kidolgozza a használati korlátozásokat és az alkalmazási irányelveket a szervezet által meghatározott rendszerelemekre; és

17.121.2. engedélyezi, ellenőrzi és szabályozza az ilyen rendszerelemek használatát a rendszeren belül.

MAGYARÁZAT

A használati korlátozások minden rendszerelemre vonatkoznak, beleértve, de nem kizárólag a mobil kódokat, mobil eszközöket, vezeték nélküli hozzáférést, valamint vezetékes és vezeték nélküli perifériás elemeket (pl. másolók, nyomtatók, szkennerek, optikai eszközök ...). A használati korlátozások és az alkalmazási irányelvek a rendszerelemek által az EIR-re gyakorolt potenciális káros hatásokon alapulnak, és segítenek biztosítani, hogy csak az engedélyezett használat történjen az EIR-en belül.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia a használati korlátozásokat a meghatározott rendszerelemekre.

2. A szervezetnek meg kell határoznia az alkalmazási irányelveket, amelyek alapján a rendszerelemek használatát szabályozza. Ezek az irányelvek a rendszerelemek által okozható károk potenciális veszélyeire alapulnak, és segítenek biztosítani, hogy csak az engedélyezett EIR használat történjen.

3. A szervezetnek engedélyeznie kell az rendszerelemek használatát az EIR-en belül a megfelelő korlátok mellett.

4. A szervezetnek ellenőriznie kell a rendszerelemek használatát. Ez azt jelenti, hogy a szervezetnek naplót kell vezetnie a rendszerelemek használatáról, és rendszeresen felül kell vizsgálnia ezt a naplót, hogy biztosítsa a rendszerelemek megfelelő használatát.

Kapcsolódó intézkedések

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

6.23. Konfigurációs beállítások

17.17. A határok védelme

17.63. Mobilkód korlátozása

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

SC-43

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.122. IZOLÁLT FUTTATÁSI KÖRNYEZETEK

17.122. A szervezet elszigetelt programfuttatási környezetet alkalmaz a meghatározott rendszerben, rendszerelemben vagy helyszínen.

MAGYARÁZAT

A "Robbanási kamrák", más néven dinamikus végrehajtási környezetek, lehetővé teszik az érintett szervezetek számára, hogy e-mail mellékleteket nyissanak meg, megbízhatatlan vagy gyanús alkalmazásokat futtassanak, és Universal Resource Locator (URL) kéréseket hajtsanak végre egy elszigetelt környezet vagy virtualizált környezet biztonságában. A védett és elszigetelt végrehajtási környezetek lehetőséget biztosítanak arra, hogy megállapítsák, tartalmaznak-e a hozzájuk kapcsolódó mellékletek vagy alkalmazások kártékony kódot. Bár a megtévesztésen alapuló védelmi technikák közé sorolható, de a dinamikus végrehajtási környezetek alkalmazása nem arra irányul, hogy hosszú távú környezetként működjenek, amelyben egy rosszindulatú támadó működni képes és tevékenységüket meg lehet figyelni. A cél inkább, hogy gyorsan azonosítsák a kártékony kódot, és csökkentsék annak valószínűségét, hogy a kód eljut a felhasználói működési környezetekbe, vagy teljesen megakadályozzák a terjedést.

Az EIR-ekben alkalmazott elszigetelt programfuttatási környezet tehát egy olyan biztonsági intézkedés, amely lehetővé teszi a szervezet számára, hogy biztonságosan vizsgálja meg és tesztelje a potenciálisan kártékony alkalmazásokat és fájlokat. Ez a környezet elszigeteli a tesztelt alkalmazásokat és fájlokat az EIR többi részétől, megakadályozva ezzel a kártékony kódok terjedését. A naplók segítségével a szervezet nyomon követheti és elemezheti a dinamikus végrehajtási környezetekben végrehajtott műveleteket, így további információkat szerezhet a potenciálisan kártékony tevékenységekről.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy elszigetelt programfuttatási környezetet, amelyet robbanási kamrának is neveznek. Így lehetővé válik az e-mailek mellékleteinek megnyitása, a nem megbízható vagy gyanús alkalmazások futtatása, és az url kérések végrehajtása egy biztonságos, elszigetelt környezetben vagy virtualizált környezetben.

2. A szervezetnek biztosítania kell, hogy az elszigetelt programfuttatási környezet képes legyen meghatározni, hogy a kapcsolódó mellékletek vagy alkalmazások tartalmaznak-e kártékony kódot, illetve ezek futtatását és megfigyelését lehetővé tegye.
3. A szervezetnek gondoskodnia kell arról, hogy a robbanási kamrák célja a kártékony kódok gyors azonosítása legyen, valamint csökkentse annak valószínűségét, hogy a kód eljut a felhasználói működési környezetébe.
4. A szervezetnek naplót kell vezetnie a robbanási kamrák használatáról, hogy nyomon követhesse a kártékony kódok azonosítását és kezelését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.17. A határok védelme
17.63. Mobilkód korlátozása
17.78. Funkcionalitás és információtárolás minimalizálása
17.79. Csapdák alkalmazása
17.87. Elfedés és megtévesztés
17.101. Külső kártékony kódok azonosítása
17.108. A folyamatok elkülönítése
18.8. Kártékony kódok elleni védelem
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

SC-44

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszer, rendszerelem vagy helyszín meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.123. RENDSZERIDŐ SZINKRONIZÁLÁSA

17.123. A szervezet szinkronizálja a rendszerórákat a rendszereken belül, valamint a rendszerelemek között.

MAGYARÁZAT

Az érintett szervezet számára elengedhetetlenül fontos a rendszerórák időszinkronizációja, mivel ez számos szolgáltatás helyes működéséhez szükséges, beleértve azonosítási és hitelesítési folyamatokat, amelyek részeként hozzáférési korlátozások és tanúsítványok is beállításra kerülnek. A szolgáltatásmegtagadás vagy lejárt hitelesítő adatok elutasításának hiánya következhet be, ha az EIR-en belül és a rendszerelemek között nincsenek megfelelően szinkronizált órák. Az időt általában Coordinated Universal Time (UTC)-ben, a Greenwichi középidő (GMT)-ben, vagy helyi időben fejezik ki, az UTC-től való eltérés mértékét jelezve. Az időmérések finomsága a rendszerek órái és a referenciaórák, például századmásodpercenként vagy tizedmásodpercenként szinkronizáló órák közötti szinkronizáció mértékére utal. A szervezetek különböző időfinomságokat határozhatnak meg a rendszerelemek számára. Az időszolgáltatás kritikus lehet más biztonsági képességek számára - mint például a hozzáférés-felügyelet és az azonosítás és hitelesítés - attól függően, hogy milyen mechanizmusokat használnak a képességek támogatására.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az időmérés finomságát, vagyis azt, hogy mennyire szorosan kell szinkronizálnia az EIR óráit a referenciaórákkal. Ez lehet például századmásodperces vagy tizedmásodperces szinkronizáció.
2. A szervezetnek implementálnia kell egy időszolgáltatást, amely képes szinkronizálni az EIR óráit a megadott szinten és finomsággal.
3. A szervezetnek dokumentálnia kell az általa használt rendszeridőt és az új rendszerelemek bevezetése során, figyelmet kell fordítania a rendszerelemek, valamint EIR-ek közötti megfelelő rendszeridő szinkronizációra.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

4.24. Időbélyegek

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

SC-45

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.124. Rendszeridő szinkronizálása – Szinkronizálás a hiteles időforrással

17.124.1. A szervezet meghatározott időközönként összehasonlítja a belső rendszerórákat a szervezet által meghatározott hiteles időforrással, és
17.124.2. ha az időkülönbség meghaladja a szervezet által meghatározott időintervallumot, szinkronizálja a belső rendszerórákat a hiteles időforrással.

Magyarázat

Az érintett szervezet számára elengedhetetlenül fontos a rendszerórák időszinkronizációja, mivel ez számos szolgáltatás helyes működéséhez szükséges, beleértve azonosítási és hitelesítési folyamatokat, amelyek részeként hozzáférési korlátozások és tanúsítványok is beállításra kerülnek. A szolgáltatásmegtagadás vagy lejárt hitelesítő adatok elutasításának hiánya következhet be, ha az EIR-en belül és a rendszerelemek között nincsenek megfelelően szinkronizált órák. Az időt általában Coordinated Universal Time (UTC)-ben, a Greenwichi középidő (GMT)-ben, vagy helyi időben fejezik ki, az UTC-től való eltérés mértékét jelezve. Az időmérések finomsága a rendszerek órái és a referenciaórák, például századmásodpercenként vagy tizedmásodpercenként szinkronizáló órák közötti szinkronizáció mértékére utal. A szervezetek különböző időfinomságokat határozhatnak meg a rendszerelemek számára. Az időszolgáltatás kritikus lehet más biztonsági képességek számára - mint például a hozzáférés-felügyelet és az azonosítás és hitelesítés - attól függően, hogy milyen mechanizmusokat használnak a képességek támogatására.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az időmérés finomságát, vagyis azt, hogy mennyire szorosan kell szinkronizálnia az EIR óráit a referenciaórákkal. Ez lehet például századmásodperces vagy tizedmásodperces szinkronizáció.
2. A szervezetnek implementálnia kell egy időszolgáltatást, amely képes szinkronizálni az EIR óráit a megadott szinten és finomsággal.

3. A szervezetnek dokumentálnia kell az általa használt rendszeridőt és az új rendszerelemek bevezetése során, figyelmet kell fordítania a rendszerelemek, valamint EIR-ek közötti megfelelő rendszeridő szinkronizációra.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

4.24. Időbélyegek

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

SC-45

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.125. RENDSZERIDŐ SZINKRONIZÁLÁSA – MÁSODLAGOS HITELES IDŐFORRÁS

17.125.1. A szervezet meghatároz egy olyan másodlagos hiteles időforrást, amely az elsődleges hiteles időforrástól eltérő földrajzi régióban található; és
17.125.2. ha az elsődleges hiteles időforrás nem áll rendelkezésre a belső rendszerórákat a másodlagos hiteles időforráshoz szinkronizálja.

MAGYARÁZAT

Az érintett szervezet számára elengedhetetlenül fontos a rendszerórák időszinkronizációja, mivel ez számos szolgáltatás helyes működéséhez szükséges, beleértve azonosítási és hitelesítési folyamatokat, amelyek részeként hozzáférési korlátozások és tanúsítványok is beállításra kerülnek. A szolgáltatásmegtagadás vagy lejárt hitelesítő adatok elutasításának hiánya következhet be, ha az EIR-en belül és a rendszerelemek között nincsenek megfelelően szinkronizált órák. Az időt általában Coordinated Universal Time (UTC)-ben, a Greenwichi középidő (GMT)-ben, vagy helyi időben fejezik ki, az UTC-től való eltérés mértékét jelezve. Az időmérések finomsága a rendszerek órái és a referenciaórák, például századmásodpercenként vagy tizedmásodpercenként szinkronizáló órák közötti szinkronizáció mértékére utal. A szervezetek különböző időfinomságokat határozhatnak meg a rendszerelemek számára. Az időszolgáltatás kritikus lehet más biztonsági képességek számára - mint például a hozzáférés-felügyelet és az azonosítás és hitelesítés - attól függően, hogy milyen mechanizmusokat használnak a képességek támogatására.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az időmérés finomságát, vagyis azt, hogy mennyire szorosan kell szinkronizálnia az EIR óráit a referenciaórákkal. Ez lehet például századmásodperces vagy tizedmásodperces szinkronizáció.
2. A szervezetnek implementálnia kell egy időszolgáltatást, amely képes szinkronizálni az EIR óráit a megadott szinten és finomsággal.

3. A szervezetnek dokumentálnia kell az általa használt rendszeridőt és az új rendszerelemek bevezetése során, figyelmet kell fordítania a rendszerelemek, valamint EIR-ek közötti megfelelő rendszeridő szinkronizációra.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

4.24. Időbélyegek

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

SC-45

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

17.126. TARTOMÁNYOK KÖZÖTTI SZABÁLYOK ÉRVÉNYESÍTÉSE

17.126. A szervezet fizikai vagy logikai módon érvényesíti a biztonsági szabályzatokat az összekapcsolt biztonsági tartományok fizikai és hálózati interfészei között.

MAGYARÁZAT

Az érintett szervezetnek gondoskodnia kell a megfelelő logikai szétválasztásról, azaz, hogy a különböző interfészek között ne jöjjön létre logikai kapcsolat, mert ez az alkalmazott szabályzat-érvényesítési mechanizmusok megkerüléséhez vezethet. Fizikai szabályzat-érvényesítési mechanizmusok esetén szükség lehet a fizikai izolációra, amelyet a szabályzat-érvényesítés fizikai megvalósítása biztosít, hogy kizárja a rejtett logikai csatornák jelenlétét, amelyek áthatolnak a biztonsági tartományon.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonsági szabályzatokat, amelyeket érvényesíteni kíván az összekapcsolt biztonsági tartományok fizikai és logikai hálózati interfészei között.
2. A szervezetnek implementálnia kell a logikai szabályzat-érvényesítési mechanizmusokat. Ez azt jelenti, hogy el kell kerülniük a logikai útvonalak létrehozását az interfészek között, hogy megakadályozzák a szabályzat-érvényesítési mechanizmus megkerülésének lehetőségét.
3. A szervezetnek fizikai szabályzat-érvényesítési mechanizmusokat is be kell vezetnie. Ez magában foglalja a fizikai izolációt, amelyet a szabályzat-érvényesítés fizikai implementációja biztosít, hogy kizárja a logikai rejtett csatornák jelenlétét.
4. A szervezetnek monitoroznia és naplóznia kell a biztonsági tartományokban lévő interfészek közötti kapcsolatokat, hogy ellenőrizni tudja a megfelelő logikai szétválasztását ezen rendszerelemeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.28. Információáramlási szabályok érvényesítése

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

SC-46

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.127. ALTERNATÍV KOMMUNIKÁCIÓS UTAK

17.127. A szervezet alternatív kommunikációs útvonalakat alakít ki a rendszer működésének szervezeti irányításához és ellenőrzéséhez.

MAGYARÁZAT

Egy biztonsági esemény, legyen az támadó jellegű vagy nem támadó jellegű, képes megzavarni vagy megszakítani a meglévő kommunikációs csatornákat, amelyeket az EIR működéséhez és az érintett szervezet irányításához és ellenőrzéséhez használnak. Az alternatív kommunikációs utak csökkentik annak a kockázatát, hogy minden kommunikációs útvonalat ugyanaz a biztonsági esemény érintsen. A problémát továbbá súlyosbítja, hogy ha a szervezet felelős munkatársai nem képesek időben információt szerezni a zavarokról, vagy nem tudnak időben irányítást adni a működési elemeknek egy kommunikációt támadó biztonsági esemény után, ez befolyásolhatja a szervezet ilyen jellegű biztonsági eseményekre történő időbeni reagálási képességét. Az alternatív kommunikációs utak kialakítása irányítási és ellenőrzési célokra, beleértve az alternatív döntéshozók kijelölését, ha a fő döntéshozók nem érhetők el, és meghatározva cselekvéseik határait és korlátait, nagymértékben elősegítheti a szervezet képességét arra, hogy folyamatosan működjön és megfelelő intézkedéseket hozzon egy biztonsági esemény során.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie a jelenlegi kommunikációs útvonalakat, amelyeket az EIR működéséhez és a szervezeti irányításhoz és ellenőrzéshez használnak.
2. A szervezetnek ki kell dolgoznia alternatív kommunikációs útvonalakat, amelyeket biztonsági események esetén használhatnak. Ezeknek az útvonalaknak képeseknek kell lenniük arra, hogy ellenálljanak és működjenek különböző típusú biztonsági események esetén is.
3. A szervezetnek ki kell jelölnie alternatív döntéshozókat, ha a fő döntéshozók nem érhetők el, és meg kell határoznia az ő cselekvésük határait és korlátait.
4. A szervezetnek tesztelnie kell az alternatív kommunikációs útvonalakat, hogy biztosítsa azok hatékonyságát és megbízhatóságát.
5. A szervezetnek dokumentálnia kell az alternatív kommunikációs útvonalak használatát és annak okát, a biztonsági események kivizsgálási hatékonyságának a növelése céljából.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

7.29. Telekommunikációs szolgáltatások

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

SC-47

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az alternatív kommunikációs utak meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.128. ÉRZÉKELŐ ÁTHELYEZÉSE

17.128. A szervezet a meghatározott érzékelőket és felügyeleti eszközöket a meghatározott helyekre, a meghatározott feltételek és körülmények között dinamikusan helyezi át.

MAGYARÁZAT

A rosszindulatú támadók különböző utakat és megközelítéseket alkalmazhatnak, amikor az érintett szervezeten belül oldalirányban mozognak, hogy elérjék céljaikat, vagy ha megpróbálják kiszivárogtatni az információkat a szervezetből. A szervezetnek gyakran csak korlátozott számú felügyeleti és érzékelő képessége van, és ezek a kritikus vagy valószínűsíthető bemeneti vagy kimeneti irányokra vannak összpontosítva. A támadó növelheti a céljai elérésének esélyét, ha olyan kommunikációs utakat használ, amelyeket a szervezet általában nem ellenőriz. A szervezet akadályozhatja egy támadó céljainak elérését, ha érzékelőit vagy felügyeleti képességeit új helyekre helyezi át. Az érzékelők vagy a felügyeleti képességek áthelyezése történhet a szervezet által megszerzett fenyegetési információk alapján, vagy véletlenszerűen, hogy összezavarja a támadót és nehezítse annak oldalirányú kommunikációját és mozgását az EIR-en vagy a szervezeten belül.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell az érzékelők és a felügyeleti eszközök jelenlegi helyét az EIR-en belül.
2. A szervezetnek fel kell mérnie a potenciális fenyegetéseket és azok valószínűségét, hogy mely utakon próbálnak meg beszivárogni vagy információt kiszivárogtatni.
3. A szervezetnek meg kell határoznia azokat a helyeket az EIR-en belül, ahol az érzékelők és a felügyeleti eszközök áthelyezése a leginkább akadályozhatja az ellenséges szereplők tevékenységét.
4. A szervezetnek dokumentálnia kell az érzékelők és a felügyeleti eszközök áthelyezését, hogy nyomon követhesse a változásokat és értékelje azok hatékonyságát.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén módosítania kell az érzékelők és a felügyeleti eszközök helyét, hogy alkalmazkodjon az új fenyegetésekhez és kihívásokhoz.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

17.17. A határok védelme

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

SC-48

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az érzékelők és felügyeleti eszközök illetve az helyszínek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.129. ÉRZÉKELŐ ÁTHELYEZÉSE – ÉRZÉKELŐK VAGY FELÜGYELETI KÉPESSÉGEK DINAMIKUS ÁTHELYEZÉSE

17.129. A szervezet a meghatározott érzékelőket és felügyeleti eszközöket a meghatározott helyekre, a meghatározott feltételek és körülmények között dinamikusan helyezi át.

MAGYARÁZAT

Az érintett szervezet a meghatározott érzékelőket és felügyeleti eszközöket a meghatározott helyekre, a meghatározott feltételek és körülmények között dinamikusan helyezi át.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell az érzékelők és a felügyeleti eszközök jelenlegi helyét az EIR-en belül.
2. A szervezetnek fel kell mérnie a potenciális fenyegetéseket és azok valószínűségét, hogy mely utakon próbálnak meg beszivárogni, vagy információkat kiszivárogtatni.
3. A szervezetnek folyamatosan monitoroznia kell a helyeket az EIR-en belül, ahol az érzékelők és a felügyeleti eszközök áthelyezése a leginkább akadályozhatja az ellenséges szereplők tevékenységét.
4. A szervezetnek létre kell hoznia kell egy dinamikusan menedzselhető dokumentumot az érzékelők és felügyeleti eszközök EIR-en belüli helyeiről, melyet rendszeresen karban kell tartania.

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

SC-48(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az érzékelők és felügyeleti eszközök illetve az helyszínek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.130. HARDVER SZINTŰ SZÉTVÁLASZTÁS ÉS SZABÁLYÉRVÉNYESÍTÉS

17.130. A szervezet hardverrel kikényszerített szétválasztási és szabály-kikényszerítési mechanizmusokat alkalmaz a szervezet által meghatározott biztonsági tartományok között.

MAGYARÁZAT

A rendszertulajdonosoknak szükséges lehet a használt mechanizmusokat erősíteni és robosztusabbá tenni, hogy biztosítsák a biztonsági tartományok közötti szétválasztást és a szabályok betartását bizonyos típusú fenyegetések és működési környezetek esetén. A hardver szintű szétválasztás és szabályérvényesítés nagyobb mechanizmus erősséget biztosít, mint a szoftverrel kikényszerített szétválasztás és szabály-kikényszerítés.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a biztonsági tartományokat, amelyek között a szétválasztást és szabály-kikényszerítést alkalmazni kívánja.
2. A szervezetnek ki kell választania a megfelelő hardvereszközöket, amelyek képesek a szétválasztás és szabály-kikényszerítés megvalósítására.
3. A szervezetnek tesztelnie kell a hardvereszközök működését, hogy biztosítsa a szétválasztás és szabály-kikényszerítés hatékony működését.
4. A szervezetnek naplóznia kell a hardvereszközök működését, hogy nyomon követhető legyen a szétválasztás és szabály-kikényszerítés folyamata.
5. A szervezetnek biztosítania kell a hardvereszközök felülvizsgálatát, valamint a megfelelő karbantartását és frissítését, hogy fenntartsa a szétválasztás és szabály-kikényszerítés hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.28. Információáramlási szabályok érvényesítése

16.16. Biztonságtervezési elvek

17.131. Szoftver szintű szétválasztás és szabályérvényesítés

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

SC-49

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági tartományok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.131. SZOFTVER SZINTŰ SZÉTVÁLASZTÁS ÉS SZABÁLYÉRVÉNYESÍTÉS

17.131. A szervezet szoftverrel kikényszerített szétválasztási és szabály-kikényszerítési mechanizmusokat alkalmaz a szervezet által meghatározott biztonsági tartományok között.

MAGYARÁZAT

A rendszertulajdonosoknak szükséges biztosítani a biztonsági tartományok szétválasztását és a szabályok kikényszerítését bizonyos fenyegetési típusok és működési környezetek esetén. Ezek a kikényszerített megoldások szoftveresen támogathatóak és megvalósíthatóak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonsági tartományokat, amelyek között szétválasztást és szabály-kikényszerítést szeretne alkalmazni.
2. A szervezetnek ki kell választania és be kell szereznie a szoftvereket, amelyek képesek a szétválasztás és a szabály-kikényszerítés megvalósítására.
3. Az érintett szervezetnek a beállított szoftvereket tesztelnie kell, hogy biztosítsa a szétválasztás és a szabály-kikényszerítés megfelelően működését.
4. A szervezetnek naplózásra és monitorozásra van szüksége, hogy nyomon követhesse a szoftverek működését és észlelje a lehetséges biztonsági problémákat.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a szoftvereket, hogy biztosítsa, hogy a szétválasztás és a szabály-kikényszerítés továbbra is megfelelően működik és megfelel a szervezet biztonsági követelményeinek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
2.28. Információáramlási szabályok érvényesítése
16.16. Biztonságtervezési elvek
17.2. Rendszer és felhasználói funkciók szétválasztása
17.4. Biztonsági funkciók elkülönítése
17.130. Hardver szintű szétválasztás és szabályérvényesítés

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

SC-50

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági tartományok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

17.132. HARDVER SZINTŰ VÉDELEM

17.132. A szervezet:

17.132.1. Hardver szintű írásvédelmet alkalmaz a meghatározott rendszer firmware-elemeken.

17.132.2. Egyedi eljárásokat alkalmaz a jogosult személyek számára a hardveres írásvédelem manuális kikapcsolásához, a firmware módosításaihoz, majd az írásvédelem újbóli bekapcsolásához az üzemi állapotba való visszatérés előtt.

MAGYARÁZAT

Az érintett szervezet kiberbiztonsági követelményei között szerepel, hogy hardver szintű írásvédelmet alkalmazzon a meghatározott firmware-elemeken. Ez azt jelenti, hogy a firmware, vagyis a rendszerek alapvető működését irányító szoftver nem módosítható vagy törölhető, egyszerű módszerekkel, csak bonyolult, speciális eljárások alkalmazása esetén. Ez a védelem segít megelőzni a nem kívánt vagy jogosulatlan módosításokat, amelyek potenciálisan károsíthatják az EIR működését vagy biztonságát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először be kell vezetnie a hardver szintű írásvédelmet a rendszerek firmware-jeivel kapcsolatban.
2. A szervezetnek egyedi eljárásokat kell kidolgoznia a megfelelő jogosult személyek számára a hardveres írásvédelem manuális kikapcsolásához, amennyiben ez szükségessé válna. Ez magában foglalhatja a speciális hozzáférési kódok, jelszavak vagy biometrikus azonosítók használatát.
3. A szervezetnek naplóznia kell az adott EIR firmware-éhez való hozzáféréseket, és amennyiben gyanús eseményeket észlel, haladéktalanul válaszlépéseket kell tennie.
4. A szervezetnek rendszeresen felül kell vizsgálnia a firmware hozzáférésekről készült naplókat, valamint a hozzáférési jogosultsággal rendelkezők listáját.

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

SC-51

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024