Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Rendszer- és szolgáltatásbeszerzés

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

16.1. Szabályzat és eljárásrendek 7

16.2. Erőforrások rendelkezésre állása 10

16.3. A rendszer fejlesztési életciklusa 12

16.4. A rendszer fejlesztési életciklusa – Preprodukciós környezet kezelése 15

16.5. A rendszer fejlesztési életciklusa – A preprodukciós környezetben kezelt adatok 17

16.6. A rendszer fejlesztési életciklusa – Technológiaváltás 19

16.7. Beszerzések 21

16.8. Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai 25

16.9. Beszerzések – Tervezési és megvalósítási információk a védelmi intézkedések teljesüléséhez 27

16.10. Beszerzések – Fejlesztési módszerek, technikák és gyakorlatok 29

16.11. Beszerzések - Rendszer, rendszerelem és szolgáltatás konfigurációk – Rendszer, rendszerelem és szolgáltatás konfigurációk 31

16.12. Beszerzések – Monitorozási terv a biztonsági követelmények teljesülése érdekében 33

16.13. Beszerzések – Használatban lévő funkciók, portok, protokollok és szolgáltatások . 35

16.14. Beszerzések – Adatgazda szerepkör 37

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció 39

16.16. Biztonságtervezési elvek 42

16.17. Biztonságtervezési elvek – Világos fogalomrendszer 45

16.18. Biztonságtervezési elvek – Korlátozott közös működés 47

16.19. Biztonságtervezési elvek – Modularitás és rétegezés 49

16.20. Biztonságtervezési elvek – Részben rendezett függőségek 51

16.21. Biztonságtervezési elvek – Hatékony erőforráshozzáférés közvetítés 53

16.22. Biztonságtervezési elvek – Minimalizált megosztás 55
16.23. Biztonságtervezési elvek – Minimalizált komplexitás 57
16.24. Biztonságtervezési elvek – Biztonságos továbbfejlődés 59
16.25. Biztonságtervezési elvek – Megbízható rendszerelemek 61
16.26. Biztonságtervezési elvek – Hierarchikus bizalom 63
16.27. Biztonságtervezési elvek – Inverz módosítási küszöb 66
16.28. Biztonságtervezési elvek – Hierarchikus védelem 68
16.29. Biztonságtervezési elvek – Biztonsági elemek minimalizálása 70
16.30. Biztonságtervezési elvek – Legkisebb jogosultság 72
16.31. Biztonságtervezési elvek – Feltételhez kötött engedélyezés 75
16.32. Biztonságtervezési elvek – Önfenntartó megbízhatóság 77
16.33. Biztonságtervezési elvek – Biztonságosan elosztott felépítés 79
16.34. Biztonságtervezési elvek – Biztonságos kommunikációs csatornák 81
16.35. Biztonságtervezési elvek – Folyamatos védelem 83
16.36. Biztonságtervezési elvek – Biztonságos metaadatkezelés 86
16.37. Biztonságtervezési elvek – Önellenőrzés 89
16.38. Biztonságtervezési elvek – Elszámoltathatóság és nyomonkövethetőség 91
16.39. Biztonságtervezési elvek – Biztonságos alapbeállítások 94
16.40. Biztonságtervezési elvek – Biztonságos hibakezelés és helyreállítás 97
16.41. Biztonságtervezési elvek – Költséghatékony biztonság 100
16.42. Biztonságtervezési elvek – Teljesítménybiztonság 102
16.43. Biztonságtervezési elvek – Emberi tényezőn alapuló biztonság 105
16.44. Biztonságtervezési elvek – Elfogadható biztonsági szint 108
16.45. Biztonságtervezési elvek – Megismételhető és dokumentált eljárások 110
16.46. Biztonságtervezési elvek – Eljárási szigor 112

16.47. Biztonságtervezési elvek – Biztonságos rendszermódosítás 115

16.48. Biztonságtervezési elvek – Megfelelő dokumentáció 117

16.49. Külső elektronikus információs rendszerek szolgáltatásai 119

16.50. Külső információs rendszerek szolgáltatásai – Kockázatelemzések és szervezeti jóváhagyások 122

16.51. Külső információs rendszerek szolgáltatásai – Funkciók, portok, protokollok és szolgáltatások azonosítása 124

16.52. Külső információs rendszerek szolgáltatásai – Megbízható kapcsolat kialakítása és fenntartása a szolgáltatókkal 126

16.53. Külső információs rendszerek szolgáltatásai – Összhangban lévő érdekek 129

16.54. Külső információs rendszerek szolgáltatásai – Feldolgozás, tárolás és szolgáltatási helyszín 131

16.55. Külső információs rendszerek szolgáltatásai – Felügyelt kriptográfiai kulcsok 133

16.56. Külső információs rendszerek szolgáltatásai – Sértetlenség felügyelete 135

16.57. Külső információs rendszerek szolgáltatásai – Feldolgozási és tárolási helyszín – Magyarország joghatósága 137

16.58. Fejlesztői változáskövetés 139

16.59. Fejlesztői konfigurációkezelés – Szoftver és firmware sértetlenségének ellenőrzése 142

16.60. Fejlesztői konfigurációkezelés – Alternatív konfigurációkezelési folyamatok 144

16.61. Fejlesztői konfigurációkezelés – Hardver sértetlenségének ellenőrzése 146

16.62. Fejlesztői konfigurációkezelés – Megbízható generálás 148

16.63. Fejlesztői konfigurációkezelés – Verziókezelési sértetlenség feltérképezése 150

16.64. Fejlesztői konfigurációkezelés – Megbízható terjesztés 152

16.65. Fejlesztői konfigurációkezelés – Biztonsági felelősök 154

16.66. Fejlesztői biztonsági tesztelés 156

16.67. Fejlesztői biztonsági tesztelés és értékelés – Statikus kódelemzés 159

16.68. Fejlesztői biztonsági tesztelés és értékelés – Fenyegetésmodellezés és sérülékenységelemzések 161

16.69. Fejlesztői biztonsági tesztelés és értékelés – Független ellenőrzés az értékelési tervek és bizonyítékok tekintetében 163

16.70. Fejlesztői biztonsági tesztelés és értékelés – Manuális kódellenőrzés 165

16.71. Fejlesztői biztonsági tesztelés és értékelés – Behatolásvizsgálat 167

16.72. Fejlesztői biztonsági tesztelés és értékelés – Támadási felület értékelések 170

16.73. Fejlesztői biztonsági tesztelés és értékelés – Tesztelés és értékelés hatáskörének ellenőrzése 172

16.74. Fejlesztői biztonsági tesztelés és értékelés – Dinamikus kódelemzés 174

16.75. Fejlesztői biztonsági tesztelés és értékelés – Interaktív alkalmazásbiztonsági tesztelés 176

16.76. Fejlesztési folyamat, szabványok és eszközök 178

16.77. Fejlesztési folyamat, szabványok és eszközök – Minőség mérőszámai 181

16.78. Fejlesztési folyamat, szabványok és eszközök – Biztonsági szempontokat nyomonkövető eszközök 183

16.79. Fejlesztési folyamat, szabványok és eszközök – Kritikussági elemzés 185

16.80. Fejlesztési folyamat, szabványok és eszközök – Támadási felület csökkentése 187

16.81. Fejlesztési folyamat, szabványok és eszközök – Folyamatos továbbfejlesztés 189

16.82. Fejlesztési folyamat, szabványok és eszközök – Automatizált sérülékenységelemzés 191

16.83. Fejlesztési folyamat, szabványok és eszközök – Fenyegetési- és sérülékenységi információk felhasználása 193

16.84. Fejlesztési folyamat, szabványok és eszközök – Biztonsági eseménykezelési terv 195

16.85. Fejlesztési folyamat, szabványok és eszközök – Rendszer vagy rendszerelem archiválása 197

16.86. Szoftverfejlesztők oktatása 199
16.87. Fejlesztői biztonsági architektúra és tervezés 201
16.88. Fejlesztői biztonsági architektúra és tervezés – Formális szabályzati modell 204
16.89. Fejlesztői biztonsági architektúra és tervezés – Biztonsági szempontból kiemelt rendszerelemek 206
16.90. Fejlesztői biztonsági architektúra és tervezés – Formalizált specifikáció 208
16.91. Fejlesztői biztonsági architektúra és tervezés – Nem formalizált specifikáció 211
16.92. Fejlesztői biztonsági architektúra és tervezés – Egyszerű tervezési koncepció 214
16.93. Fejlesztői biztonsági architektúra és tervezés – Tesztelési struktúra 217
16.94. Fejlesztői biztonsági architektúra és tervezés – Struktúra a legkisebb jogosultság elvéhez 219
16.95. Fejlesztői biztonsági architektúra és tervezés – Összehangolás 222
16.96. Fejlesztői biztonsági architektúra és tervezés – Tervezési modellek diverzifikálása 224
16.97. Kritikus rendszerelemek egyedi fejlesztése 226
16.98. Külső fejlesztők háttérellenőrzése 228
16.99. Támogatással nem rendelkező rendszerelemek 231
16.100. Speciális követelmények 234

16.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

16.1. A szervezet:

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

16.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó beszerzési szabályzatot, amely

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

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

16.1.1.2. A beszerzési eljárásrendet, amely a beszerzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

16.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a beszerzési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

16.1.3. Felülvizsgálja és frissíti az aktuális beszerzési szabályzatot és a beszerzési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

A beszerzési szabályzat és eljárások a Beszerzések követelménycsoportba tartozó védelmi intézkedésekkel foglalkoznak, amelyek az EIR-ekben, illetve a szervezetekben bevezetésre kerülnek. A kockázatkezelési stratégia fontos tényező az ilyen szabályok és eljárások létrehozásában. A szabályok és eljárások hozzájárulnak a biztonság garantálásához. Ezért fontos, hogy a szervezet információbiztonsági szabályozási környezete és a beszerzési szabályzat és eljárások összhangban legyenek egymással. A szervezeti szintű biztonsági szabályzatok és eljárásrendek általában előnyösebbek, és szükségtelenné tehetik a működési célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásokat. A szabályokat be lehet illeszteni az általános biztonsági szabályzatba, vagy több szabályzatban is megjelenhetnek, amelyek tükrözik az érintett szervezetek összetett természetét. Eljárásokat

létre lehet hozni az információbiztonsági irányítási rendszer, a működési és üzleti célok, és az EIR-ek támogatására, amennyiben azok szükségesek. Az eljárások leírják, hogy hogyan valósulnak meg a szabályok vagy a védelmi intézkedések, és hogyan vonatkoznak az eljárás tárgyát képező egyénre vagy szerepkörre. Az eljárásokat dokumentálhatják a rendszerbiztonsági tervekben, vagy egy vagy több külön dokumentumban. A beszerzési szabályzat és eljárások frissítését kiváltó események lehetnek értékelési vagy audit megállapítások, biztonsági események vagy változások az alkalmazandó jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban. Az elvárt védelmi intézkedések egyszerű újra közlése nem minősülhet szervezeti szabályzatnak vagy eljárásnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia, dokumentálnia, kiadnia és megismertetnie a szervezet által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és EIR-szintű követelményeket tartalmazó beszerzési szabályzatot.
2. A beszerzési szabályzat meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az érintett szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat.
3. A beszerzési szabályzat összhangban van az érintett szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.
4. A szervezetnek ki kell dolgoznia a beszerzési eljárásrendet, amely a beszerzési szabályzat és az ahhoz kapcsolódó követelmények megvalósítását segíti elő.
5. A szervezetnek ki kell jelölnie egy, a szervezet által meghatározott személyt, aki a beszerzési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.
6. A szervezetnek felül kell vizsgálnia és frissítenie kell az aktuális beszerzési szabályzatot és a beszerzési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

Események, amelyek felülvizsgálatot és frissítést követelhetnek meg lehetnek például audit megállapítások, biztonsági események vagy jogszabályi változások.

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

3.1.3.1. Beszerzési eljárásrend

ISO/IEC 27001:2023 referencia

5.2; 5.3; 7.5.1; 7.5.2; 7.5.3; 8.1; A.5.1; A.5.2; A.5.4; A.5.23; A.5.31; A.5.36; A.5.37

NIST SP 800-53 rev.5 referencia

SA-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

16.2. ERŐFORRÁSOK RENDELKEZÉSRE ÁLLÁSA

16.2. A szervezet:

16.2.1. Az üzletmenet és üzleti folyamatok tervezése során meghatározza az EIR vagy rendszerszolgáltatás magas szintű információbiztonsági követelményeit.

16.2.2. Biztosítja az EIR és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként.

16.2.3. Elkülönített tételként kezeli az EIR-ek biztonságát a beruházás tervezési dokumentumaiban.

MAGYARÁZAT

Az információbiztonság érdekében történő erőforrás tervezés magában foglalja a rendszerrel és rendszerszolgáltatásokkal kapcsolatos beszerzést, fenntartást és az ellátási lánccal kapcsolatos kockázatokat a rendszer fejlesztési életciklusban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek az üzletmenet és alapfunkciók tervezése során meg kell határoznia az EIR vagy rendszerszolgáltatás magas szintű információbiztonsági követelményeit. Ez magában foglalja a kockázatkezelési stratégiák, a biztonsági szabályok és eljárások, valamint a biztonsági technológiák meghatározását.
2. A szervezetnek biztosítania kell az EIR és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként. Ez magában foglalja a szükséges pénzügyi forrásokat, a személyzetet és a technológiai eszközöket.
3. A szervezetnek elkülönített tételként kell kezelnie az EIR-ek biztonságát a beruházás tervezési dokumentumaiban. Ez azt jelenti, hogy a biztonsági költségeket külön kell kezelni a többi költségtől, és külön költségvetési tételként kell szerepeltetni.

KAPCSOLÓDÓ INTÉZKEDÉSEK

13.5. Működési koncepció

1.3. Információbiztonságot érintő erőforrások

1.12. Szervezeti működés és üzleti folyamatok meghatározása

16.49. Külső elektronikus információs rendszerek szolgáltatásai

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

19.13. Beszerzési stratégiák, eszközök és módszerek

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

3.1.3.2. Erőforrás igény felmérés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

16.3. A RENDSZER FEJLESZTÉSI ÉLETCIKLUSA

16.3.1. Az EIR-ek teljes életútján, minden életciklusukban figyelemmel kíséri azok információbiztonsági helyzetét.

16.3.2. A fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket.

16.3.3. Azonosítja az információbiztonsági szerepkörökkel és felelősségi körökkel rendelkező személyeket.

16.3.4. Beépíti a szervezeti információbiztonsági kockázatmenedzsment folyamatot a rendszerfejlesztési életciklus tevékenységeibe.

MAGYARÁZAT

A jól definiált rendszerfejlesztési életciklusok alapját képezik a szervezeti információs rendszerek sikeres fejlesztésének, megvalósításának és üzemeltetésének. A szükséges biztonsági követelmények alkalmazása a rendszerfejlesztési életciklus során az információbiztonság, a fenyegetések, sérülékenységek, kedvezőtlen hatások és kritikus üzleti célok/üzleti funkciók kockázatainak alapvető megértését igényli. A követelmény alapján kialakítandó biztonsági tervezés alapelvei nem alkalmazhatók megfelelően, ha a szakértők, akik az EIR-eket és a rendszerelemeket tervezik, fejlesztik és tesztelik, nem értik a biztonsági elvárásokat. Ezért a szervezetek képzett munkatársakat, például információbiztonsági szakértőket, biztonsági architektúra tervezőket, biztonságtechnikai mérnököket és információbiztonsági felelőst alkalmaznak a rendszerfejlesztési életciklus megvalósításához. A biztonsági követelmények a szervezeti architektúrába történő hatékony implementálása segít annak biztosításában is, hogy a fontos biztonsági szempontok a rendszer teljes életciklusa során érvényesüljenek, és hogy ezek a megfontolások közvetlenül kapcsolódjanak a szervezeti működési célokhoz és az üzleti folyamatokhoz. Ez a folyamat megkönnyíti továbbá az információbiztonsági architektúrák integrálását a szervezeti architektúrába, összhangban a szervezet kockázatkezelési stratégiájával. Mivel egy rendszerfejlesztési életciklusban több szervezet is részt vesz (pl. külső beszállítók, fejlesztők, integrátorok, szolgáltatók), a beszerzési és ellátási lánc kockázatkezelési funkciói és intézkedései jelentős szerepet játszanak az EIR hatékony felügyeletében, annak teljes életciklusa alatt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia az információbiztonsági szerepköröket és felelősségeket az EIR fejlesztési életciklusa során. Ez magában foglalja a szükséges személyek bevonását is az EIR fejlesztési életciklusába, hogy biztosítsák a meghatározott biztonsági követelmények beépítését az EIR-be.

2. A szervezetnek azonosítania kell azokat a személyeket, akik rendelkeznek információbiztonsággal kapcsolatos felelősségi körökkel. Ez magában foglalja a szerepkör-alapú biztonsági képzési programok biztosítását is, hogy a kulcsfontosságú biztonsági szerepkörökkel és felelősségekkel rendelkező személyek rendelkezzenek a szükséges tapasztalattal, készségekkel és szakértelemmel a rendszerfejlesztési életciklus tevékenységeinek végrehajtásához.

3. Az érintett szervezetnek be kell építenie az információbiztonsági kockázatkezelési folyamatot a rendszerfejlesztési életciklus tevékenységeibe. Ez magában foglalja a biztonsági követelmények beépítését a vállalati architektúrába, hogy biztosítsák a releváns biztonsági szempontok figyelembevételét az EIR életciklusa során, és hogy ezek a szempontok közvetlenül kapcsolódjanak az érintett szervezet céljaihoz és üzleti folyamataihoz.

4. Mivel a rendszerfejlesztési életciklus több szervezetet is érint, az érintett szervezetnek figyelembe kell vennie a beszerzési és ellátási lánc kockázatkezelési funkcióit és intézkedéseit az rendszeréletciklusa során történő hatékony kezelés érdekében.

5. A szervezetnek figyelemmel kell kísérnie az EIR információbiztonsági helyzetét az EIR teljes életútján, minden életciklusában. Ez magában foglalja a naplózást és a rendszeres ellenőrzéseket is, hogy biztosítsák az EIR információbiztonsági állapotának megfelelőségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

13.5. Működési koncepció

1.3. Információbiztonságot érintő erőforrások

1.12. Szervezeti működés és üzleti folyamatok meghatározása

16.49. Külső elektronikus információs rendszerek szolgáltatásai

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

19.13. Beszerzési stratégiák, eszközök és módszerek

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

3.3.3.2. A rendszer fejlesztési életciklusa

ISO/IEC 27001:2023 REFERENCIA

A.5.2; A.5.8; A.8.25; A.8.31

NIST SP 800-53 REV.5 REFERENCIA

SA-3

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszer fejlesztési életciklus meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

16.4. A RENDSZER FEJLESZTÉSI ÉLETCIKLUSA – PREPRODUKCIÓS KÖRNYEZET KEZELÉSE

16.4. A szervezet gondoskodik a preprodukciós környezetek kockázatarányos védelméről a rendszer, rendszerelem vagy rendszerszolgáltatás teljes életciklusa során.

MAGYARÁZAT

A preprodukciós környezet magában foglalja a fejlesztési, tesztelési és integrációs környezeteket. A kockázatelemzések és a fejlesztőkre alkalmazott követelmények is hozzájárulnak egy biztonságosabb fejlesztési környezethez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a preprodukciós környezetet, amely magában foglalja a fejlesztési, tesztelési és integrációs környezeteket.
2. A szervezetnek kockázatelemzést kell végeznie, és biztonsági követelményeket kell meghatároznia és alkalmaznia a fejlesztőkre, hogy biztonságosabb EIR preprodukciós környezetet biztosítson.
4. A szervezetnek biztosítania kell a preprodukciós környezetek kockázatarányos védelmét az EIR teljes életciklusa során. Ez magában foglalja a kockázatkezelési stratégiák kidolgozását és alkalmazását, valamint a biztonsági követelmények folyamatos felülvizsgálatát és frissítését.
5. A szervezetnek naplózást kell alkalmaznia a preprodukciós környezetekben, hogy nyomon követhesse a tevékenységeket és az esetleges biztonsági eseményeket. A naplózás segíthet a kockázatok azonosításában és a biztonsági intézkedések hatékonyságának értékelésében.
6. Biztosítania kell a preprodukciós környezetek folyamatos felülvizsgálatát és frissítését, hogy megfeleljen a változó kockázatoknak és a legújabb biztonsági követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció

6.15. Biztonsági hatásvizsgálatok

15.4. Kockázatértékelés

15.21. Rendszerelemek kritikusságának elemzése

16.7. Beszerzések

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

SA-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.5. A RENDSZER FEJLESZTÉSI ÉLETCIKLUSA – A PREPRODUKCIÓS KÖRNYEZETBEN KEZELT ADATOK

16.5. A szervezet:

16.5.1. Jóváhagyja, dokumentálja és ellenőrzi az éles környezetből származó adatok használatát az EIR, rendszerelem vagy rendszerszolgáltatás preprodukciós környezetében.

16.5.2. Biztosítja az EIR, a rendszerelem vagy a rendszerszolgáltatás preprodukciós környezetének védelmét az abban kezelt adatok védelmi igényének megfelelően.

MAGYARÁZAT

Azaz éles rendszerből származó adatok használata preprodukciós környezetben jelentős kockázatokat jelenthet az érintett szervezet számára. Ezenkívül a személyes adatok használata tesztelésben, kutatásban, fejlesztésben és képzésben növeli az ilyen információk jogosulatlan közzétételének vagy visszaélésének kockázatát. Ezért fontos, hogy az érintett szervezet kezelje azokat a további kockázatokat, amelyek az éles rendszerből származó adatok használatából adódhatnak. Az érintett szervezet minimalizálhatja ezeket a kockázatokat azzal, hogy pszeudonimizált, anonimizált vagy fiktív adatokat használ az EIR, a rendszerelemek és a rendszerszolgáltatások tervezése, fejlesztése és tesztelése során. Fel lehet használni kockázatelemzési technikákat annak megállapítására, hogy az éles rendszerből származó adatok használatának kockázata elfogadható-e.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek jóvá kell hagynia az éles környezetből származó adatok használatát az EIR preprodukciós környezetében. Ez azt jelenti, hogy a szervezetnek meg kell határoznia és jóvá kell hagynia azokat az adatokat, amelyeket a preprodukciós környezetben használni kíván.
2. A jóváhagyás után a szervezetnek dokumentálnia kell az adatok használatát. Ez magában foglalja az adatok forrásának, céljának, és a használat módjának rögzítését.
3. A szervezetnek ellenőriznie kell az adatok használatát a preprodukciós környezetben. Ez magában foglalhatja a naplók ellenőrzését, valamint a rendszeres ellenőrzéseket, hogy biztosítsa az adatok megfelelő használatát.

4. A szervezetnek biztosítania kell az EIR preprodukciós környezetének védelmét. Ez magában foglalja a megfelelő biztonsági intézkedések, például tűzfalak alkalmazását.
5.A szervezetnek biztosítania kell, hogy feleljen meg az EIR preprodukciós környezetében kezelt adatok védelme azok védelmi igényének. Ez azt jelenti, hogy a szervezetnek meg kell határoznia az adatok védelmi igényét, és ennek megfelelően kell beállítania a preprodukciós környezet védelmét.

Kapcsolódó intézkedések

15.4. Kockázatértékelés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.8.33

NIST SP 800-53 rev.5 referencia

SA-3(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.6. A RENDSZER FEJLESZTÉSI ÉLETCIKLUSA – TECHNOLÓGIAVÁLTÁS

16.6. A szervezet megtervezi és végrehajtja az EIR technológiaváltási ütemtervét a rendszer teljes életciklusa során.

MAGYARÁZAT

A technológia frissítés tervezése magában foglalhatja a hardvert, a szoftvert, a firmware-t, a folyamatokat, a személyek képességeit, a beszállítókat, a szolgáltatókat és a létesítményeket. Az elavult vagy közel elavult technológia használata növelheti a támogatás nélküli, hamisított vagy újrahasznosított, a biztonsági követelményeket nem teljesítő, lassú vagy működésképtelen, megbízhatatlan forrásból származó elemekkel, nem szándékolt személyi hibával, vagy növekvő komplexitással kapcsolatos biztonsági kockázatokat. A technológiai frissítések általában a rendszerfejlesztési életciklusának üzemeltetési és karbantartási szakaszában történnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie az EIR jelenlegi állapotát, beleértve a hardvert, a szoftvert, a firmware-t, a folyamatokat, a személyzet készségeit, a beszállítókat, a szolgáltatókat és a létesítményeket.
2. A szervezetnek meg kell határoznia az EIR technológiai frissítésének szükségességét, figyelembe véve a közel elavult technológiák használatának kockázatait, mint például a nem támogatott elemeket, hamisított vagy újrahasznosított elemeket, a biztonsági követelményeket nem teljesítő elemeket, a lassú vagy működésképtelen elemeket, a megbízhatatlan forrásból származó elemeket, a személyzet véletlen hibáit, vagy a növekvő komplexitást.
3. A szervezetnek meg kell terveznie az EIR technológiai frissítési ütemtervét, figyelembe véve a rendszerfejlesztési életciklusának működtetési és karbantartási szakaszát.
4. A szervezetnek végre kell hajtania az EIR technológiai frissítési ütemtervet, beleértve a hardver, szoftver, firmware, folyamatok, személyzet készségeinek, beszállítóknak, szolgáltatóknak és létesítményeknek a frissítését.

5. A szervezetnek dokumentálnia kell az EIR technológiai frissítési ütemterv végrehajtását, hogy nyomon követhesse a frissítési folyamatot és biztosíthassa a kiberbiztonsági követelményeknek való megfelelést.

Kapcsolódó intézkedések

10.21. Kellő időben történő karbantartás

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

SA-3(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.7. BESZERZÉSEK

16.7. A szervezet a beszerzési folyamat során - beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is - a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat:

16.7.1. A funkcionális biztonsági követelményeket.

16.7.2. A mechanizmusok erősségére vonatkozó követelményeket.

16.7.3. A biztonság garanciális követelményeit.

16.7.4. Az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket.

16.7.5. A biztonsággal kapcsolatos dokumentációs követelményeket.

16.7.6. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket.

16.7.7. Az EIR fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

16.7.8. A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását.

16.7.9. A teljesítési kritériumokat.

MAGYARÁZAT

Az érintett szervezet a beszerzési folyamat során - beleértve az EIR fejlesztését, adaptálását, követését és karbantartását - a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat:

Funkcionális biztonsági követelmények: Ezek általában magas szintű biztonsági követelményekből származnak. A levezetett követelmények magukban foglalják a biztonsági képességeket, funkciókat és mechanizmusokat.

A mechanizmusok erősségére vonatkozó követelmények: Ezek magukban foglalják a helyesség, teljesség, manipuláció vagy megkerülés elleni ellenállás, valamint a közvetlen támadás elleni ellenállás mértékét.

A biztonság garanciális követelményei: Ezek magukban foglalják a fejlesztési folyamatokat, eljárásokat és módszertanokat, valamint a fejlesztési és értékelési tevékenységekből származó bizonyítékokat, amelyek bizonyosságot nyújt arra, hogy a szükséges funkcionalitás

megvalósításra került, és rendelkezik a szükséges erősségű mechanizmusokkal. Az EIR biztonsági osztályát és az ahhoz tartozó, illetve az érintett szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedések: Ezek a biztonsági célok eléréséhez szükséges biztonsági képességek leírásait tartalmazzák.

A biztonsággal kapcsolatos dokumentációs követelmények: Ezek az EIR fejlesztési életciklusának minden szakaszát lefedik. A dokumentáció felhasználói és adminisztrátori útmutatókat biztosít a követelmények megvalósításához és működtetéséhez.

A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények: Ezek az EIR biztonsági osztályában szükséges képességekre, funkciókra vagy mechanizmusokra való függőség mértékén alapulnak.

Az EIR fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírások: Ezek magukban foglalják az EIR, rendszerelemek és rendszerszolgáltatások elfogadási kritériumait.

A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását: Ezek a fejlesztő és a szervezeti felelősségeket tartalmazzák.

A teljesítési kritériumok: Ezek az érintett szervezet bármely beszerzési vagy fejlesztési kritériumának meghatározását tartalmazzák.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek egységes nyelvezetet kell alkalmaznia a beszerzési folyamat során.
2. A szervezetnek szerződésekben rögzítenie kell a funkcionális biztonsági követelményeket, a mechanizmusok erősségére vonatkozó követelményeket, a biztonság garanciális követelményeit, az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket.
3. A szervezetnek a szerződésekben rögzítenie kell a biztonsággal kapcsolatos dokumentációs követelményeket és a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket.
4. A szervezetnek szerződésekben rögzítenie kell az EIR fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

5. A szervezetnek a szerződésekben rögzítenie kell a felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását.
6. A szervezetnek a szerződésekben rögzíteni kell a teljesítési kritériumokat.
7. A szervezetnek biztosítania kell, hogy a szerződésekben rögzített követelményeket a beszállítók és a fejlesztők is betartsák.
8. A szervezetnek dokumentálnia kell a szerződésekben rögzített követelmények teljesítését, és rendszeresen ellenőriznie, hogy a követelményeket betartják-e.

Kapcsolódó intézkedések

6.23. Konfigurációs beállítások
6.36. Rendszerelem leltár
14.11. Külső személyekhez kapcsolódó biztonsági követelmények
16.3.1. A rendszer fejlesztési életciklusa
16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció
16.16. Biztonságtervezési elvek
16.66. Fejlesztői biztonsági tesztelés
16.76.1. Fejlesztési folyamat, szabványok és eszközök
16.86. Szoftverfejlesztők oktatása
16.87. Fejlesztői biztonsági architektúra és tervezés

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

3.1.3.3. Beszerzések

ISO/IEC 27001:2023 referencia

8.1; A.5.8; A.5.20; A.5.23; A.8.29; A.8.30

NIST SP 800-53 rev.5 referencia

SA-4

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a szerződésben használt nyelv meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

16.8. Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai

16.8. A szervezet megköveteli a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását.

Magyarázat

Az alkalmazandó védelmi intézkedések funkcionális tulajdonságai leírják a funkcionalitást, amelyek a védelmi intézkedések interfészein láthatók, és kifejezetten kizárják a belső működéshez tartozó funkcionalitást és adatszerkezeteket.

A követelmény alkalmazásának lépései

1. A szervezetnek fel kell vennie a kapcsolatot az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjével.
2. A szervezetnek meg kell követelnie a fejlesztőtől, hogy adjon részletes leírást az alkalmazandó védelmi intézkedések funkcionális tulajdonságairól. Ez magában foglalja a biztonsági vagy adatvédelmi képességeket, funkciókat vagy mechanizmusokat, amelyek láthatóak a vezérlők interfészein, és kifejezetten kizárják a vezérlők működésének belső funkcionalitását és adatszerkezeteit.
3. A szervezetnek gondoskodnia kell arról, hogy a fejlesztő által biztosított információk megfelelőek és kielégítőek. Ha szükséges, a szervezetnek további információkat kell kérnie a fejlesztőtől.
4. A szervezetnek be kell építenie ezeket a védelmi intézkedéseket az EIR-be, és gondoskodnia kell arról, hogy megfelelően működjenek.
5. A szervezetnek dokumentálnia kell a folyamatot, beleértve a fejlesztővel folytatott kommunikációt, a kért információkat és a védelmi intézkedések implementálásának folyamatát.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a védelmi intézkedéseket, hogy biztosítsa az EIR folyamatos biztonságát.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SA-4(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

16.9. Beszerzések – Tervezési és megvalósítási információk a védelmi intézkedések teljesüléséhez

16.9. A szervezet megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője biztosítson tervezési és megvalósítási információkat a védelmi intézkedésekhez. Ezek az információk tartalmazzák a biztonsági szempontból releváns külső rendszerinterfészeket, a magas szintű rendszertervet, az alacsony szintű rendszertervet, a forráskódot vagy a hardversémákat, valamint a szervezet által meghatározott részletes tervezési és megvalósítási információkat.

Magyarázat

Az érintett szervezetek eltérő részletességű dokumentációt igényelhetnek az EIR, rendszerelemek vagy rendszerszolgáltatások védelmi intézkedéseinek tervezéséhez és megvalósításához. Mindez az üzleti, a megbízhatósági, valamint az elemzési és tesztelési követelményeken múlik. Az EIR-ek több alrendszerre oszthatók. Minden alrendszer az EIR-en belül tartalmazhat egy vagy több modult. Az EIR magas szintű terve az alrendszerek és az alrendszerek közötti, biztonsági szempontból releváns interfészekből áll. Az EIR alacsony szintű terve a modulok és a modulok közötti, biztonsági szempontból releváns interfészekből áll. A tervezési és megvalósítási dokumentáció tartalmazhatja a gyártót, a verziót, a sorozatszámot, az ellenőrző hash aláírást, a használt szoftverkönyvtárakat, a vásárlás vagy letöltés dátumát, valamint a szállítót vagy a letöltés forrását. A forráskód és a hardverséma reprezentálja az EIR megvalósítását.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a különböző szintű részletességet a dokumentációban az EIR, rendszerelemek vagy EIR szolgáltatások védelmi intézkedéseinek tervezéséhez és megvalósításához, figyelembe véve az ügymeneti és üzleti követelményeket, a rugalmasság és megbízhatóság követelményeit, valamint az elemzési és tesztelési követelményeket.
2. Az EIR-t több alrendszerre lehet osztani. Minden alrendszer az EIR-en belül tartalmazhat egy vagy több modult. Az EIR magas szintű terve az alrendszerek és az alrendszerek közötti, biztonsági szempontból releváns interfészek tekintetében kerül dokumentálásra.

3. Az EIR alacsony szintű terve a modulok és a modulok közötti, biztonsági szempontból releváns interfészek tekintetében kerül dokumentálásra.

4. A tervezési és megvalósítási dokumentáció tartalmazhatja a gyártót, a verziót, a sorozatszámot, az ellenőrző hash aláírást, a használt szoftverkönyvtárakat, a vásárlás vagy letöltés dátumát, valamint a szállító vagy letöltési forrást.

5. A forráskód és a hardver sémák az EIR megvalósítási reprezentációjának tekinthetők.

6. A szervezetnek biztosítania kell a részletes tervezési és megvalósítási információkat, amelyeket az érintett szervezet határoz meg.

7. A szervezetnek naplót kell vezetnie a folyamatról, hogy nyomon követhető legyen a fejlesztés 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

SA-4(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a tervezési és megvalósítási információk illetve a részletességi szint meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

16.10. Beszerzések – Fejlesztési módszerek, technikák és gyakorlatok

16.10. A szervezet megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője bemutassa a rendszerfejlesztési életciklus folyamatának alkalmazását. Ez magában foglalja:

16.10.1. a szervezet által meghatározott rendszertervezési módszereket;

16.10.2. a szervezet által meghatározott rendszerbiztonsági módszereket;

16.10.3. a szervezet által meghatározott szoftverfejlesztési, tesztelési, értékelési, ellenőrzési és érvényesítési módszereket, valamint a minőségellenőrzési eljárásokat.

Magyarázat

Egy rendszer fejlesztési életciklus követése, amely magában foglalja a gyakorlatban alkalmazott korszerű szoftverfejlesztési módszereket, rendszertervezési módszereket, rendszerbiztonsági tervezési módszereket, valamint minőségellenőrzési folyamatokat, hozzájárul a rejtett hibák számának és súlyosságának csökkentéséhez az EIR-ekben, rendszerelemekben és rendszerszolgáltatásokban. Az ilyen jellegű hibák számának és súlyosságának mérséklése egyúttal csökkenti a sérülékenységek számát ezekben az EIR-ekben, elemekben és szolgáltatásokban. A fejlesztők által kiválasztott és alkalmazott módszerek, technikák átláthatósága a rendszertervezési, rendszerbiztonságot és adatvédelmet érintő tervezési, szoftverfejlesztési, elem- és rendszerértékelési, valamint minőségellenőrzési folyamatok terén növeli a beszerzendő EIR, rendszerelem vagy rendszerszolgáltatás iránti bizalmat.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell kérnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjét, hogy mutassa be a rendszerfejlesztési életciklus folyamatát.

2. A rendszerfejlesztési életciklus folyamatának tartalmaznia kell a szervezet által meghatározott EIR tervezési módszereket. Ez magában foglalhatja a szoftverfejlesztési módszereket, a rendszerbiztonsági módszereket, valamint a minőségellenőrzési eljárásokat.

3. A szervezetnek ellenőriznie kell, hogy a fejlesztő által alkalmazásra kerülnek a meghatározott EIR biztonsági módszerek. Ez magában foglalhatja a különböző biztonsági protokollok, szabályok és eljárások alkalmazását.

4. A szervezetnek ellenőriznie kell, hogy a fejlesztő alkalmazza-e a meghatározott szoftverfejlesztési, tesztelési, értékelési, ellenőrzési és érvényesítési módszereket. Ez magában foglalhatja a kódolási szabványok, a tesztelési eljárások, az értékelési módszerek, az ellenőrzési eljárások és az érvényesítési módszerek alkalmazását.

5. A szervezetnek ellenőriznie kell, hogy a fejlesztő által alkalmazásra kerülnek a meghatározott minőségellenőrzési eljárások. Ez magában foglalhatja a minőségellenőrzési eljárások, a naplózás és a dokumentáció alkalmazását.

6. A szervezetnek ellenőriznie kell, hogy a fejlesztő transzparens-e a választott módszerek és technikák alkalmazásában. Ez magában foglalhatja a fejlesztési, tesztelési, értékelési, ellenőrzési és érvényesítési módszerek, valamint a minőségellenőrzési eljárások dokumentálását és bemutatását.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.8.28

NIST SP 800-53 rev.5 referencia

SA-4(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.11. Beszerzések - Rendszer, rendszerelem és szolgáltatás konfigurációk – Rendszer, rendszerelem és szolgáltatás konfigurációk

16.11. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.11.1. Az EIR, rendszerelem vagy szolgáltatás szállítása a meghatározott biztonsági konfigurációk alkalmazásával történjen.

16.11.2. Minden EIR, rendszerelem vagy szolgáltatás későbbi újratelepítése vagy frissítése során az alapkonfigurációkat használják.

Magyarázat

Az alapkonfigurációknak figyelembe kell venniük az érintett szervezetre vonatkozó irányelveket, jogszabályi követelményeket és minden limitációt a funkciók, portok, protokollok és szolgáltatások vonatkozásában. A biztonsági követelmények között megjelenhet az alapértelmezett jelszavak megváltoztatásának szükségessége.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a biztonsági konfigurációkat, amelyeket az EIR, rendszerelem vagy szolgáltatás szállításánál alkalmazni kíván.

2. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy szolgáltatás fejlesztőjétől, hogy a szállítás során alkalmazza ezeket a meghatározott biztonsági konfigurációkat.

3. A szervezetnek biztosítania kell, hogy minden EIR, rendszerelem vagy szolgáltatás újratelepítése vagy frissítése során az alapkonfigurációkat használják. Ez azt jelenti, hogy minden újratelepítés vagy frissítés során vissza kell térni a biztonsági konfigurációkhoz, amelyeket eredetileg meghatároztak és alkalmaztak.

4. A szervezetnek ellenőriznie kell, hogy az EIR, rendszerelem vagy szolgáltatás fejlesztője betartja-e ezeket a követelményeket. Ez magában foglalhatja a naplók ellenőrzését, hogy biztosítsák, a fejlesztő megfelelően alkalmazza a biztonsági konfigurációkat.

5. A szervezetnek szükség esetén intézkedéseket kell hoznia, ha a fejlesztő nem tartja be a követelményeket. Ez magában foglalhatja a fejlesztővel való egyeztetést a problémák megoldása érdekében, vagy akár a fejlesztő cseréjét is, ha a problémák továbbra is fennállnak.

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

SA-4(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

16.12. Beszerzések – Monitorozási terv a biztonsági követelmények teljesülése érdekében

16.12. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan tervet készítsen, amely a szervezet által meghatározott monitorozási programmal összhangban van, és amely a védelmi intézkedések hatékonyságának monitorozását szolgálja.

Magyarázat

A monitorozási tervek célja annak megállapítása, hogy az EIR-ben, a rendszerelemben vagy a rendszerszolgáltatásban tervezett, szükséges és megvalósított biztonsági intézkedések továbbra is hatékonyak-e az elkerülhetetlen változások megvalósítását követően. A fejlesztők által készített monitorozási terveknek kellően részletesnek kell lenniük ahhoz, hogy az információkat be lehessen építeni az érintett szervezet által megvalósított monitorozási folyamatokba. A monitorozási tervek tartalmazhatják a tervezett biztonsági intézkedések és monitorozási tevékenységek típusait, az biztonsági intézkedések monitorozásának gyakoriságát, és a teendőket, ha a biztonsági intézkedések sikertelenné vagy hatástalanná válnak.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy EIR szolgáltatás fejlesztőjétől, hogy készítsen egy folyamatos monitorozási tervet. Ez a terv összhangban kell legyen a szervezet által meghatározott monitorozási programmal.
2. A folyamatos monitorozási tervnek tartalmaznia kell a tervezett, szükséges és bevezetett ellenőrző intézkedéseket az EIR-ben, rendszerelemekben vagy rendszerszolgáltatásban, és azt, hogy ezek az intézkedések idővel hatékonyak maradnak-e a szükségszerű változásokat követően.
3. A fejlesztő által készített folyamatos monitorozási tervnek elegendő részletességgel kell rendelkeznie ahhoz, hogy az információkat be lehessen építeni a szervezet által alkalmazott folyamatos monitorozási folyamatokba.

4. A folyamatos monitorozási terv tartalmazhatja a biztonsági intézkedések értékelésének és monitorozásának tervezett típusait, a biztonsági intézkedések monitorozásának gyakoriságát, és a teendőket, ha a biztonsági intézkedések sikertelenné vagy hatástalanná válnának.
5. A szervezetnek dokumentálnia kell a folyamatos monitorozási terv végrehajtását és az eredményeit, hogy biztosítsa a biztonsági intézkedések hatékonyságának folyamatos monitorozását.

Kapcsolódó intézkedések

5.14. Folyamatos felügyelet

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SA-4(8)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.13. BESZERZÉSEK – HASZNÁLATBAN LÉVŐ FUNKCIÓK, PORTOK, PROTOKOLLOK ÉS SZOLGÁLTATÁSOK

16.13. A szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy határozza meg a használatra tervezett funkciókat, portokat, protokollokat és szolgáltatásokat.

MAGYARÁZAT

A funkciók, portok, protokollok és szolgáltatások azonosítása a rendszer fejlesztési életciklusának korai szakaszában lehetővé teszi a szervezetek számára, hogy befolyásolják az EIR, a rendszerelem vagy szolgáltatás tervezését. Ezáltal elkerülhető vagy minimalizálható az olyan funkciók, portok, protokollok vagy szolgáltatások használata, amelyek szükségtelenül nagy kockázatot jelentenek, és felismerhetőek az egyes portok, protokollok vagy szolgáltatások tiltásával járó kompromisszumok. A funkciók, portok, protokollok és szolgáltatások korai azonosítása segít elkerülni az EIR, a rendszerelem vagy a rendszerszolgáltatás implementációja utáni, költséges védelmi intézkedések kialakítását. A szervezetek azonosítják, azon funkciókat, portokat, protokollokat és szolgáltatásokat melyek külső forrásokból biztosítottak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a fejlesztővel vagy szállítóval kötött szerződésben, hogy mely funkciókat, portokat, protokollokat és szolgáltatásokat terveznek használni az EIR-ben.
2. A szervezetnek korai szakaszban, már az EIR fejlesztési életciklusának kezdeti követelménydefiníciós és tervezési szakaszában, be kell azonosítania a funkciókat, portokat, protokollokat és szolgáltatásokat. Ez lehetővé teszi a szervezet számára, hogy befolyásolja az EIR, a rendszerelem vagy a rendszerszolgáltatás tervezését.
3. A szervezetnek el kell kerülnie vagy minimalizálnia kell azoknak a funkcióknak, portoknak, protokolloknak vagy szolgáltatásoknak a használatát, amelyek feleslegesen magas kockázatot jelentenek, és meg kell értenie a különböző portok, protokollok vagy szolgáltatások blokkolásával vagy a szolgáltatók ilyen követelményeknek való megfelelésével járó kompromisszumokat.

4. A szervezetnek azonosítania kell a korai szakaszban a funkciókat, portokat, protokollokat és szolgáltatásokat, hogy elkerülje a drága utólagos kontrollintézkedések bevezetését, miután az EIR, a rendszerelem vagy a rendszerszolgáltatás már implementálásra került.
5. Az érintett szervezetnek meg kell határoznia, mely funkciókat, portokat, protokollokat és szolgáltatásokat szolgáltatják külső forrásokból.
6. A szervezetnek naplózásra van szüksége, hogy nyomon követhesse és ellenőrizhesse az EIR-ben használt funkciókat, portokat, protokollokat és szolgáltatásokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.26. Legszűkebb funkcionalitás
16.49. Külső elektronikus információs rendszerek szolgáltatásai

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

3.1.3.3. Beszerzések

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-4(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

16.14. Beszerzések – Adatgazda szerepkör

16.14. A szervezet:

16.14.1. A szervezet adatkezelési követelményeit beépíti a beszerzési szerződésekbe.

16.14.2. Megköveteli, hogy minden adatot távolítsanak el a vállalkozó EIR-éből, és szolgáltassanak vissza a szervezetnek a szervezet által meghatározott időn belül

Magyarázat

Azon vállalkozók, akik üzemeltetnek olyan EIR-t, amelyben az adatok a szerződést kezdeményező szervezet tulajdonát képezik, rendelkeznek szabályzatokkal és eljárásrendekkel arra vonatkozóan, hogy az adatokat eltávolítsák a tulajdonukban álló EIR-ekből és/vagy visszaszolgáltassák az adatokat a szerződés által meghatározott időkereten belül.

A követelmény alkalmazásának lépései

1. A szervezetnek be kell építenie az adatkezelési követelményeket a beszerzési szerződésekbe. Ez azt jelenti, hogy a szerződésnek tartalmaznia kell a vállalkozó által követendő adatkezelési eljárásokat és szabályokat.
2. A szervezetnek meg kell követelnie, hogy minden adatot távolítsanak el a vállalkozó EIR-jéből, és szolgáltassanak vissza az érintett szervezetnek a szerződésben meghatározott időn belül. Ez azt jelenti, hogy a vállalkozónak rendelkeznie kell egy olyan eljárással, amely lehetővé teszi az adatok gyors és hatékony eltávolítását az EIR-jéből.
3. A szervezetnek ellenőriznie kell, hogy a vállalkozó betartja-e a szerződésben foglalt adatkezelési követelményeket. Ez magában foglalhatja a vállalkozó EIR-jének naplózását, hogy megbizonyosodjon arról, hogy az adatokat időben eltávolították és visszaszolgáltatták.
4. A szervezetnek biztosítania kell, hogy a vállalkozó megfelelően kezeli az adatokat, amíg azok az EIR-jében vannak. Ez magában foglalhatja az adatbiztonsági intézkedések, például a titkosítás és a hozzáférés-felügyelet alkalmazását.
5. A szervezetnek felül kell vizsgálnia és frissítenie kell a beszerzési szerződéseket, hogy biztosítsa, hogy azok továbbra is megfelelnek az adatkezelési követelményeknek és a kiberbiztonsági legjobb gyakorlatoknak.

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

SA-4(12)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.15. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZERRE VONATKOZÓ DOKUMENTÁCIÓ

16.15. A szervezet:

16.15.1. Kidolgozza vagy beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza:

16.15.1.1. az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését;

16.15.1.2. a biztonsági funkciók hatékony használatát és karbantartását; valamint

16.15.1.3. az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.

16.15.2. Kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza:

16.15.2.1. a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját;

16.15.2.2. a felhasználói interakció biztonságos módját;

16.15.2.3. a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.

16.15.3. Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, úgy a szervezet dokumentálja az EIR, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, valamint végrehajtja a szervezet által meghatározott intézkedéseket; és

16.15.4. a dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek.

MAGYARÁZAT

Az EIR-re vonatkozó dokumentáció segít a védelmi intézkedések megvalósításának és működtetésének megértésében. A szervezetek bevezethetnek intézkedéseket a dokumentáció tartalmi minőségének és teljességének javítására. A rendszert leíró dokumentáció felhasználható az ellátási lánc kockázatának, a biztonsági események és egyéb funkciók kezelésének támogatására is. A dokumentációt el kell juttatni az egyes személyeknek vagy

szerepköröknek (például a rendszerek tulajdonosai, a rendszerbiztonsági felelős és a rendszergazdák). A dokumentáció beszerezhető a gyártóktól vagy beszállítókkal való kapcsolatfelvétellel és/ vagy a webes kereséssel. Amennyiben kiderül, hogy a dokumentáció beszerzése nem lehetséges, az jelezheti, hogy a rendszer vagy rendszerelem elavult, fejlesztői/gyártói támogatása megszűnt. Ha a dokumentáció nem szerezhető be, a szervezeteknek újra el kell készíteniük, amennyiben az szükséges a védelmi intézkedések végrehajtásához. A dokumentáció védelme arányos a rendszer biztonsági osztályával vagy besorolásával. Az EIR sérülékenységeit tartalmazó dokumentáció magasabb szintű védelmet igényelhet. A biztonságos működésébe beletartozik a rendszer indítása és a működés újraindítása egy kiesés után.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell szereznie, vagy beszerezhetetlenség esetén ki kell dolgoznia az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját. Ez a dokumentáció tartalmazza az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését, a biztonsági funkciók hatékony használatát és karbantartását, valamint az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.
2. A szervezetnek be kell szereznie, vagy beszerezhetetlenség esetén ki kell dolgozni az EIR, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját. Ez a dokumentáció tartalmazza a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját, a felhasználói interakció biztonságos módját, valamint a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.
3. Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, a szervezetnek dokumentálnia kell az EIR, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, ha szükséges el kell készíteni a dokumentumokat és végre kell hajtania a szervezet által meghatározott intézkedéseket.
4. A szervezetnek el kell juttatnia a dokumentációkat a szervezet által meghatározott személyeknek vagy szerepköröknek. A dokumentáció védelme arányos az EIR biztonsági

osztályával vagy besorolásával. Az EIR sérülékenységeit tárgyaló dokumentáció esetén nagyobb védelmi szintre lehet szükség. Az EIR biztonságos működése magában foglalja az EIR kezdeti indítását és a működés újraindítását egy kiesést követően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.15. Biztonsági hatásvizsgálatok

6.23. Konfigurációs beállítások

6.26. Legszűkebb funkcionalitás

6.36. Rendszerelem leltár

13.2. Rendszerbiztonsági terv

13.3.1. Viselkedési szabályok

13.6. Információbiztonsági architektúra leírás

14.2. Munkakörök biztonsági szempontú besorolása

16.3.1. A rendszer fejlesztési életciklusa

16.7. Beszerzések

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

3.1.3.4. Az elektronikus információs rendszerre vonatkozó dokumentáció

ISO/IEC 27001:2023 REFERENCIA

7.5.1; 7.5.2; 7.5.3; A.5.37

NIST SP 800-53 REV.5 REFERENCIA

SA-5

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

16.16. BIZTONSÁGTERVEZÉSI ELVEK

16.16. A szervezet az általa meghatározott biztonságtervezési elveket alkalmazza és megköveteli a specifikáció, a tervezés, a fejlesztés, a megvalósítás és az EIR, valamint a rendszerelemek módosítása során.

MAGYARÁZAT

A biztonságtervezési elvek szorosan kapcsolódnak a rendszer fejlesztési életciklushoz és annak minden fázisában alkalmazandóak. A szervezetek a biztonságtervezési elveket alkalmazhatják új rendszerek fejlesztésekor vagy fejlesztés alatt álló rendszereken. Meglévő rendszerek esetén a szervezetek a biztonságtervezési elveket alkalmazzák a rendszer fejlesztései és módosításai során - amennyire ez lehetséges - figyelembe véve a rendszereken belüli hardver-, szoftver- és firmware-elemek jelenlegi állapotát. A biztonságtervezési elvek alkalmazása segíti az érintett szervezetet megbízható, biztonságos és ellenálló rendszerek fejlesztésében, csökkenti a zavarokkal, veszélyekkel, fenyegetésekkel szembeni érzékenységet.

A rendszerbiztonság-technikai elvekre példák: többszintű védelem kialakítása, a tervezés és fejlesztés alapjául szolgáló biztonsági irányelvek, architektúra és biztonsági intézkedések kialakítása, a biztonsági követelmények beépítése a rendszerfejlesztési életciklusba, a fizikai és logikai biztonsági határok kijelölése, annak biztosítása, hogy a fejlesztők képzést kapjanak a biztonságos szoftverek létrehozására, az ellenőrzések testre szabása a szervezeti igényeknek megfelelően, és fenyegetésmodellezés a felhasználási esetek, a fenyegető tényezők, a támadási vektorok és minták, a tervezési minták és a kockázat mérsékléséhez szükséges kompenzációs intézkedések azonosítása érdekében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonságtervezési elveit, amelyeket az EIR fejlesztési életciklusa során alkalmazni fog.
2. A szervezetnek alkalmaznia kell ezeket a biztonságtervezési elveket új EIR fejlesztésénél, vagy amikor az EIR frissítésre kerül. A meglévő EIR esetében az érintett szervezetnek a lehető legnagyobb mértékben alkalmaznia kell a biztonságtervezési elveket az EIR frissítésekor és módosításakor, figyelembe véve a hardver, szoftver és firmware elemek jelenlegi állapotát.

3. A szervezetnek a biztonságtervezési elvek alkalmazásával olyan megbízható, biztonságos és ellenálló EIR-t kell kifejlesztenie, amely csökkenti a zavarok, veszélyek, fenyegetések valószínűségét.

4. A szervezetnek például a következő biztonságtervezési elveket kell alkalmaznia: mélységi védelem kialakítása; biztonsági jógyakorlatok alkalmazása, biztonsági architektúra és követelmények létrehozása a tervezés és fejlesztés alapjául; a biztonsági követelmények beépítése az EIR fejlesztési életciklusába; fizikai és logikai biztonsági határok meghatározása; a fejlesztők képzése biztonságos szoftverek fejlesztésére; a védelmi intézkedések szervezeti igényekhez történő igazítása; fenyegetésmodellezés készítése a használati esetek, fenyegetést jelentő szereplők, támadási vektorok és minták, tervezési minták és a kockázat csökkentéséhez szükséges kiegészítő védelmi intézkedések azonosításához.

5. A szervezetnek a biztonságtervezési elvek alkalmazásával elfogadható szintre kell csökkentenie a kockázatot, és tájékozott kockázatkezelési döntéseket kell hoznia.

6. A szervezetnek a biztonságtervezési elveket a beszállítói lánc bizonyos kockázatainak kezelésére is alkalmaznia kell, beleértve a manipuláció ellen védett hardver beépítését a tervezésbe.

7. A szervezetnek naplót kell vezetnie az EIR módosításairól és frissítéseiről, hogy nyomon követhető legyen a biztonságtervezési elvek alkalmazása.

Kapcsolódó intézkedések

13.6. Információbiztonsági architektúra leírás

1.7. Szervezeti architektúra

15.2. Biztonsági osztályba sorolás

15.4. Kockázatértékelés

15.21. Rendszerelemek kritikusságának elemzése

16.3.1. A rendszer fejlesztési életciklusa

16.7. Beszerzések

16.76.1. Fejlesztési folyamat, szabványok és eszközök

16.87. Fejlesztői biztonsági architektúra és tervezés

16.97. Kritikus rendszerelemek egyedi fejlesztése

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

3.1.3.5. Biztonságtervezési elvek: Az érintett szervezet biztonságtervezési elveket dolgoz ki és alkalmaz az elektronikus információs rendszer specifikációjának meghatározása, tervezése, fejlesztése, kivitelezése és módosítása során.

ISO/IEC 27001:2023 REFERENCIA

A.8.27; A.8.28

NIST SP 800-53 REV.5 REFERENCIA

SA-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonságtervezési elvek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

16.17. BIZTONSÁGTERVEZÉSI ELVEK – VILÁGOS FOGALOMRENDSZER

16.17. A szervezet kialakítja a biztonságtervezési elveit, amelyek világos absztrakciókra épülnek.

MAGYARÁZAT

A "Világos Fogalomrendszer" elve azt mondja ki, hogy az EIR-nek egyszerű, jól meghatározott interfészei és funkciói vannak, amelyek következetes és intuitív képet adnak az adatokról és azok kezeléséről. Az interfészek világossága, egyszerűsége, szükségessége és elegendősége - összekapcsolva a funkcionális viselkedésük pontos meghatározásával - elősegíti az elemzés, ellenőrzés és tesztelés könnyedségét, valamint az EIR helyes és biztonságos használatát. A fogalomrendszer világossága szubjektív. Azt példázza, hogy az érintett szervezet hogyan alkalmazza ezt az elvet, hogy kerüli a felesleges, használaton kívüli interfészeket, az információ elrejtését és az interfészek vagy paramétereik szemantikai túlterhelésének elkerülését. Az információ elrejtése egy tervezési minta, amelyet arra használnak, hogy biztosítsák az információ belső reprezentációja egy rendszerelemben ne legyen látható egy másik rendszerelem számára, amely meghivatkozza vagy felhívja az első elemet, így a közzétett absztrakciót nem befolyásolja, hogy az adatokat belsőleg hogyan kezelik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek össze kell gyűjtenie az EIR rendszerelemeit és teljes logikai térképet kell készítenie azok kapcsolatairól.
2. A szervzetnek minden rendszerelem funkcionalitását, valamint a rendszerelemek között húzódó interfészt nyilvántartásba kell vennie és ki kell egészítenie a kezelt adatok által leírt adat útvonalakkal.
3. A szervezetnek minden frissítés alkalmával felül kell vizsgálnia a logikai térképet és szükség esetén ki kell egészítenie az új elemekkel, interfészekkel és adatokkal.

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

SA-8(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.18. BIZTONSÁGTERVEZÉSI ELVEK – KORLÁTOZOTT KÖZÖS MŰKÖDÉS

16.18. A szervezet a korlátozott közös működés (Least Common Mechanism) biztonságtervezési elvét alkalmazza a meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A "Korlátozott Közös Működés" elve azt mondja ki, hogy azon mechanizmusok mennyiségét melyet több felhasználó közösen használt és amelytől minden felhasználó függ, minimalizálni kell. A mechanizmus minimalizálás azt jelenti, hogy az EIR különböző elemei tartózkodnak attól, hogy ugyanazt a mechanizmust használják egy különböző erőforrások eléréséhez. Minden megosztott mechanizmus (különösen a megosztott változókat tartalmazó mechanizmusok) potenciális információs útvonalat képvisel a felhasználók között és gondosan meg kell tervezni, hogy véletlenül se veszélyeztesse a biztonságot (SALTZER75). A "Korlátozott Közös Működés" elvének alkalmazása segít csökkenteni a rendszerállapot különböző programok közötti megosztásának kedvezőtlen következményeit. Egyetlen program, amely megrongálja a megosztott állapotot (beleértve a megosztott változókat is), potenciálisan megrongálhatja azokat a programokat, amelyek az állapottól függnek. A "Korlátozott Közös Működés" elve támogatja a tervezés egyszerűségének elvét és megoldást kínál a rejtett tároló csatornák problémájára (LAMPSON73).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azon rendszerelemeket, amelyeket más rendszerelemek erőforráselérésre használhatnak.
2. A szervezetnek minimalizálnia kell a több rendszerelem által megosztott elérési mechanizmusokat.
3. A szervezetnek minden frissítés során felül kell vizsgálni a rendszertervet és szükség esetén módosítania a megosztott elérési mechanizmusokat, a "Korlátozott Közös Működés" szempontjait figyelembe véve.

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

SA-8(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.19. Biztonságtervezési elvek – Modularitás és rétegezés

16.19. A szervezet a moduláris és rétegezett felépítés biztonságtervezési elvét alkalmazza a meghatározott EIR-ekben vagy rendszerelemekben.

Magyarázat

A "Modularitás és Rétegezés" alapvető koncepciók a rendszertervezési diszciplínákban. A funkcionális dekompozícióból származó modularitás és rétegezés hatékonyan kezeli az EIR komplexitását, lehetővé téve a struktúra megértését. A modularitás funkciókat és kapcsolódó adatszerkezeteket izolál jól definiált logikai egységekbe, a rétegezés pedig lehetővé teszi ezen egységek kapcsolatainak jobb megértését, így a függőségek világosak és a nem kívánt komplexitás elkerülhető. A modularitás biztonságtervezési elve kiterjeszti a funkcionális modularitást a bizalom, megbízhatóság, privilégium és biztonsági szabályzatok alapján történő megfontolásokra. A biztonsági szempontból történő moduláris dekompozíció magába foglalja a szabályzatok hálózatban lévő EIR-ekhez történő hozzárendelését, az alkalmazások folyamatokba történő szétválasztását külön címtartományokkal, az EIR szabályzatok rétegekhez történő hozzárendelését, és a folyamatok szétválasztását alanyokra külön jogosultságokkal, a hardver által támogatott jogosultsági tartományok alapján.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a logikailag elkülöníthető rendszerelemeket és mechanizmusokat.
2. A szervezetnek minden frissítés során felül kell vizsgálnia a rendszertervet és szükség esetén módosítania kell azt új, logikailag elkülönített rendszerelemeket bevezetve amennyiben szükséges.

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

SA-8(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.20. BIZTONSÁGTERVEZÉSI ELVEK – RÉSZBEN RENDEZETT FÜGGŐSÉGEK

16.20. A szervezet a részben rendezett függőségek (Partially Ordered Dependencies) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A "Részben Rendezett Függőségek" elve azt mondja ki, hogy az EIR-ben található szinkronizációs, hívásos és egyéb függőségek részben rendezettek. Az EIR tervezésének alapvető koncepciója a rétegzés, amely során a rendszert jól meghatározott, funkcionálisan összefüggő modulokra vagy elemekre szervezik. A rétegek lineárisan rendezettek a rétegek között függőségek tekintetében, így a magasabb logikai szinten elhelyezkedő rétegek függnek az alacsonyabb szintű rétegektől. Bizonyos rétegek önmagukban is működhetnek és nem függenek az alacsonyabb rétegektől, miközben funkciókat biztosítanak a magasabban lévő rétegek számára. Bár egy adott EIR összes funkciójának részleges rendezése nem lehetséges, ha azonban a körkörös függőségek rétegeken belülre vannak korlátozva, a körkörös függőségek problémái könnyebben kezelhetőek. A részben rendezett függőségek és az EIR rétegezése jelentősen hozzájárul a tervezés egyszerűségéhez és koherenciájához. A részben rendezett függőségek továbbá megkönnyítik a tesztelést és elemzést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a logikailag elkülöníthető rendszerelemeket és mechanizmusokat.
2. A szervezetnek meg kell terveznie az EIR-t úgy, hogy a különböző rendszerelemek részlegesen rendezettek legyenek a "Részben Rendezett Függőségek" elv alapján. Az alacsonyabb logikai szinten álló rétegek szolgáltatásokat biztosítanak a magasabb szinten álló rétegek számára.
3. A szervezetnek korlátoznia kell a körkörös függőségeket a rétegeken belülre.
4. A szervezetnek minden frissítés során felül kell vizsgálnia a rétegzett rendszertervet és szükség esetén módosítania kell azt.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-8(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.21. BIZTONSÁGTERVEZÉSI ELVEK – HATÉKONY ERŐFORRÁSHOZZÁFÉRÉS KÖZVETÍTÉS

16.21. A szervezet a hatékonyan közvetített erőforráshozzáférés (Efficiently Mediated Access) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A hatékonyan közvetített erőforráshozzáférés biztonságtervezési elve azt mondja ki, hogy a szabályzatvégrehajtási mechanizmusok a rendelkezésre álló legkevesebb közös mechanizmust használják, miközben kielégítik az érintett elem által meghatározott követelményeket. Az EIR erőforrásokhoz (például:CPU, memória, eszközök, kommunikációs portok, szolgáltatások, infrastruktúra, adatok és információk) való hozzáférés közvetítése gyakran a biztonságos rendszerek elsődleges biztonsági funkciója. Ez lehetővé teszi a rendszernek az érintett elem számára nyújtott képességek védelmének megvalósítását. Az erőforráshozzáférés közvetítése szűk keresztmetszet lehet a teljesítmény szempontjából, ha az EIR nem megfelelően van tervezve. Például hardvermechanizmusok használatával elérhető a hatékonyan közvetített erőforráshozzáférés. Ha egyszer hozzáférést nyertünk egy alacsony szintű erőforráshoz, mint például a memória, a hardvervédelmi mechanizmusok biztosíthatják, hogy ne történjen a határokon túli hozzáférés.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia a szabályzatot, amely alapján a hozzáférés közvetítés megvalósulhat.
2. A szervezetnek gondosan meg kell terveznie a hatékony erőforráshozzáférés kezelését a létező szabályzat alapján.
3. A szervezetnek naplóznia kell az erőforráshozzáférés eseményeit, hogy nyomon követhesse azok hatásait az EIR-re.
4. A szervezetnek rendszeresen frissítenie kell a szabályrendszert, valamint az erőforráshozzáférés közvetítésének tervezetét a további fejlesztések során.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.129. Referenciának való megfelelőség vizsgálata

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

SA-8(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.22. BIZTONSÁGTERVEZÉSI ELVEK – MINIMALIZÁLT MEGOSZTÁS

16.22. A szervezet a minimalizált megosztás biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A minimalizált megosztás elve azt állítja, hogy egyetlen számítógépes erőforrás sem kerül megosztásra az EIR elemei (például: objektumok, folyamatok, funkciók) között, hacsak nem feltétlenül szükséges. A minimalizált megosztás segít egyszerűsíteni az EIR tervezését és megvalósítását. Annak érdekében, hogy megvédjük a felhasználói tartomány erőforrásait az önkényes aktív entitásoktól, egyetlen erőforrás sem osztható meg, hacsak ezt a megosztást nem kérték és engedélyezték kifejezetten. Az erőforrás-megosztás szükségességét a legkisebb közös mechanizmus tervezési elve indokolhatja a belső entitások esetében, vagy az érintett elemek követelményei vezérelhetik. Azonban a belső megosztást gondosan meg kell terveni, hogy a teljesítménybeli és a rejtett tárolási és időzítési csatornák problémái elkerülhetőek legyenek. A közös mechanizmuson keresztüli megosztás növelheti az adatok és információk jogosulatlan hozzáférésnek, közzétételnek, használatnak vagy módosításnak való kitettségét, és hátrányosan befolyásolhatja az EIR alapvető képességeit. A közös mechanizmusok által igényelt megosztás minimalizálásának érdekében ezeket a mechanizmusokat újra belépővé (reentrant) vagy virtualizálttá tervezhetjük, hogy megőrizzük a szeparációt. A globális adatoknak az információ megosztására történő felhasználását tüzetesen vizsgálni kell, az enkapszuláció (egységbe zárás) hiánya elhomályosíthatja a megosztó entitások közötti kapcsolatokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a rendszerelemeket, amelyek osztott erőforrásokkal dolgoznak, valamint azonosítani kell az erőforrásokat, melyek megosztásra kerülhetnek.
2. A szervezetnek gondosan meg kell terveznie a megosztást, figyelembe véve a "Minimalizált Megosztás" elvének szempontjait.
3. A szervezetnek rendszeresen frissítenie kell a megosztott erőforrásokról, valamint az osztott erőforrásokkal dolgozó rendszerelemek listáját a további fejlesztések során.

4. A szervezetnek naplóznia kell a megosztási tevékenységeket, hogy nyomon követhesse a megosztásokat és azok hatásait az EIR-re.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az erőforrások megosztására készített terveket, hogy biztosítsa annak hatékonyságát és relevanciáját.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.92. Rejtett csatornák elemzése

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

SA-8(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.23. Biztonságtervezési elvek – Minimalizált komplexitás

16.23. A szervezet a minimalizált komplexitás biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

Magyarázat

A minimalizált komplexitás biztonságtervezési elve azt mondja ki, hogy az EIR terve a lehető legegyszerűbb és legkisebb komplexitású legyen. Egy alacsony komplexitású és egyszerű terv könnyebben érthető, jobban elemezhető és kevésbé hajlamos a hibákra. A minimalizált komplexitás elve bármely EIR aspektusra alkalmazható, de különösen fontos a biztonság szempontjából, mivel számos elemzést végeznek annak érdekében, hogy bizonyítékot szerezzenek az EIR esetleges biztonsági állapotáról. Ahhoz, hogy ezen elemzések sikeresek legyenek, elengedhetetlen egy alacsony komplexitású, egyszerű terv. A minimalizált komplexitás elvének alkalmazása támogatja az EIR fejlesztőit a biztonsági funkcióik helyességének és teljességének megértésében. Ez megkönnyíti továbbá a potenciális sérülékenységek kialakulását. A minimalizált komplexitás következménye, hogy az EIR egyszerűsége közvetlenül összefügg a benne található sérülékenységet számával; vagyis az egyszerűbb EIR-ek kevesebb sérülékenységet tartalmaznak. A minimalizált komplexitás egyik előnye, hogy könnyebb megérteni, hogy a tervezett biztonsági szabályzat megvalósult-e az EIR terveiben, és hogy a fejlesztés során valószínűleg kevesebb sérülékenység kerül majd bevezetésre. További előny, hogy bármilyen következtetés a helyességről, teljességről és a sérülékenységek létezéséről nagyobb bizonyossággal vonható le, mint azon esetekben, ahol az EIR terve bonyolultabb. Az idősebb technológiákról az újabb technológiákra való áttérés megkövetelheti az idősebb és újabb technológiák egyidejű alkalmazását az átmeneti időszak alatt (pl.: IPv4-ről az IPv6-ra történő áttérés). Ez ideiglenesen növelheti az EIR komplexitását az átmenet során.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek a rendszer fejlesztésének korai szakaszaitól folyamatosan szem előtt kell tartania a "Minimalizált Komplexitás" elvét.
2. A szervezetnek minden változtatás és frissítés során felül kell vizsgálnia az EIR tervét a "Minimalizált Komplexitás" elvének követése érdekében.

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

SA-8(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.24. BIZTONSÁGTERVEZÉSI ELVEK – BIZTONSÁGOS TOVÁBBFEJLŐDÉS

16.24. A szervezet a biztonságos továbbfejlődés (Secure Evolvability) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A biztonságos továbbfejlődés elve azt mondja ki, hogy egy EIR úgy legyen fejlesztve, hogy megkönnyítse a biztonsági tulajdonságainak karbantartását, amikor változások történnek a struktúrájában, interfészeiben, összeköttetéseiben (azaz az EIR architektúrájában), funkcionalitásában vagy konfigurációjában (azaz a biztonsági szabályzatok érvényesítésben). A változások közé tartozhat egy új, fejlettebb vagy frissített EIR képesség; karbantartási és fenntartási tevékenységek; és az újrakonfigurálás. Bár nem lehetséges minden EIR fejlesztási aspektust előre tervezni, az EIR frissítéseit és változásait előre lehet jelezni az ügymeneti vagy üzleti stratégiai irányzat, a fenyegetési környezet várható változásai, valamint a karbantartási és fenntartási igények elemzésével. Nem lehet elvárni, hogy bonyolult rendszerek biztonságosak maradjanak olyan környezetekben, amelyeket nem láttak elő a fejlesztés során, legyenek ezek az üzemeltetési környezettel vagy a használattal kapcsolatosak. Egy EIR biztonságos lehet bizonyos új környezetekben, de nincs garancia arra, hogy az emergens viselkedése mindig biztonságos marad. Könnyebb a megbízhatóságot már kezdetektől beépíteni egy tervbe. Az EIR megbízhatóságának fenntartása tehát a változásokra való tervezést igényli, nem pedig az ad hoc vagy nem módszeres alkalmazkodást. Ennek az elvnek az előnyei közé tartozik a szállítói életciklus költségeinek csökkentése, a tulajdonlási költségek csökkentése, a rendszerbiztonság javítása, a biztonsági kockázat hatékonyabb kezelése és a kockázati bizonytalanság csökkentése.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek előre kell terveznie az EIR frissítéseit és változásait, az ügymeneti vagy üzleti stratégiai irány, a fenyegetési környezet várható változásai, valamint a karbantartási és fenntartási igények elemzése alapján.
2. A szervezetnek tervet kell készítenie a változások kezelésére.

3. A szervezetnek a frissítéseket és változásokat koordinált módon kell kezelnie a korábban már megtervezett módszerekkel.
4. A szervezetnek rendszeresen felül kell vizsgálnia a változások kezelésére készített terveket és szükség esetén módosítani azokon az üzleti stratégiai irány, a fenyegetési környezet, valamint a karbantartási és fenntartási igények fényében.

Kapcsolódó intézkedések

6.7. A konfigurációváltozások felügyelete (változáskezelés)

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

SA-8(8)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.25. BIZTONSÁGTERVEZÉSI ELVEK – MEGBÍZHATÓ RENDSZERELEMEK

16.25. A szervezet a megbízható rendszerelemek biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A megbízható rendszerelemek biztonságtervezési elve egy biztonságtervezési elv, mely kimondja, hogy hogy egy rendszerelem megbízhatósága legalább olyan szinten van, amely megfelel az általa támogatott biztonsági függőségeknek. Ez az elv lehetővé teszi a rendszerelemek összeállítását úgy, hogy a összesített megbízhatóság nem csökken. Az elv megkövetel egyfajta metrikát, amellyel a rendszerelembe vetett bizalom és a rendszerelem megbízhatósága ugyanazon az absztrakt skálán mérhető. A megbízható rendszerelemek elve különösen releváns olyan EIR-ek és rendszerelemek esetében, ahol bonyolult bizalmi függőségi láncok keletkeznek. A bizalmi függőséget bizalmi kapcsolatnak is nevezik, és léteznek bizalmi kapcsolati láncok is. A megbízható rendszerelemek elve vonatkozik olyan összetett elemekre is, amelyek különböző megbízhatósági szinten álló alkotóelemekből állnak (például egy alrendszer). A feltételezés az, hogy egy összetett rendszerelem megbízhatósága a legkevésbé megbízható alkotóelemének megbízhatóságával egyezik. Lehetséges, hogy adható mérnöki indoklás arra, hogy egy adott összetett rendszerelem megbízhatósága nagyobb, mint a konzervatív feltételezés, azonban minden ilyen indoklás logikai érvelésen alapul, amely egyértelműen megfogalmazza a megbízhatósági célokat, valamint releváns és hiteles bizonyítékokat tartalmaz. Egy összetett rendszerelem megbízhatósága nem azonos a mélységi védelem rétegeinek fokozott alkalmazásával a rendszerelemen belül vagy a rendszerelemek másolataiban. A mélységi védelem nem növeli az egész megbízhatóságát a legkevésbé megbízható rendszerelem felett.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek a szoftverfejlesztési folyamat kezdetei szakaszában, valamint a további változtatások során számon kell tartania minden létező és újonnan elkészített rendszerelemet.
2. A szervezetnek számon kell tartania egy bizalmi térképet az rendszerelemek között, különös tekintettel az összetett rendszerelemekre és azok biztonsági szintjére.
3. A szervezetnek minden változtatás esetén felül kell vizsgálnia az érintett rendszerelemekről alkotott bizalmi térképet és a biztonságtervezési elveket, valamint rendszerspecifikus logikai szabályzat alapján módosítania kell annak elemeit.

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

SA-8(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.26. BIZTONSÁGTERVEZÉSI ELVEK – HIERARCHIKUS BIZALOM

16.26. A szervezet a hierarchikus bizalom biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

Az "Hierarchikus Bizalom" biztonságtervezési elve az EIR-ekben a "Megbízható rendszerelemek" elvére épít és azt állítja, hogy amennyiben a rendszerelemek megőrzik a "Megbízható rendszerelemek" elvét, a biztonsági függőségek egy részleges rendet alkotnak az EIR-ben. A részleges rend a megbízhatósági relácók alapját adja, amikor egy biztonságos EIR-t heterogén megbízhatóságú rendszerelemekből állítanak össze. Egy heterogén megbízhatóságú rendszerelemekből álló EIR megbízhatóságának elemzéséhez elengedhetetlen a körkörös bizalmi függőségek elkerülése. Ha egy alacsonyabb logikai rétegben található, megbízhatóbb rendszerelem függne egy kevésbé megbízható rendszerelemtől a felsőbb logikai rétegben, ez gyakorlatilag ugyanabba a kevésbé megbízható ekvivalenciaosztályba helyezné a rendszerelemeket a "Megbízható rendszerelemek" elve szerint. A bizalmi kapcsolatok, vagy a bizalmi láncok, különböző megjelenési formákat ölthetnek. Például egy tanúsítványhierarchia gyökértanúsítványa a hierarchia legmegbízhatóbb csomópontja, míg a levelek lehetnek a legkevésbé megbízható csomópontok. Egy másik példa egy rétegzett, magas biztosítási szintű EIR-ben fordul elő, ahol a biztonsági kernel, amely az EIR legalacsonyabb rétegében található, a legmegbízhatóbb rendszerelem. A "Hierarchikus Bizalom" elve azonban nem tiltja a "túlzottan" megbízható rendszerelemek használatát. Lehetnek olyan esetek, amikor egy alacsony megbízhatóságú EIR-ben indokolt egy nagyon megbízható rendszerelem alkalmazása egy kevésbé megbízható helyett (például a rendelkezésre állás vagy más költség-haszon reláció miatt). Ilyen esetben a nagy megbízhatóságú rendszerelem bármilyen függősége egy kevésbé megbízható rendszerelemtől nem rontja az eredményül kapott alacsony megbízhatóságú EIR megbízhatóságát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek számon kell tartania a szoftverfejlesztési folyamat kezdetei szakaszában, valamint a további változtatások során minden létező és újonnan elkészített rendszerelemet.
2. A szervezetnek számon kell tartania egy bizalmi térképet a rendszerelemek között, különös tekintettel az összetett rendszerelemekre és azok biztonsági szintjére.
3. A szervezetnek minden változtatás esetén felül kell vizsgálnia az érintett rendszerelemekről alkotott bizalmi térképet és a biztonságtervezési elvek, valamint rendszerspecifikus logikai szabályzat alapján módosítania kell annak elemeit.
4. A szervezetnek mellőznie kell a körkörös bizalmi függőségeket, heterogén megbizhatóságú rendszerelemekből álló EIR összeállítása esetén.
5. A szervezet alkalmazhat nagy megbízhatóságú rendszerelemet egy alacsony megbizhatóságú EIR esetén, a nagy megbízhatóságú rendszerelem függősége egy kevésbé megbízható rendszerelemtől nem rontja az eredményül kapott alacsony megbízhatóságú EIR megbízhatóságát.

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

SA-8(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.27. BIZTONSÁGTERVEZÉSI ELVEK – INVERZ MÓDOSÍTÁSI KÜSZÖB

16.27. A szervezet az inverz módosítási küszöb (Inverse Modification Threshold) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

Az inverz módosítási küszöb elve a megbízható rendszerelemek elvén és a hierarchikus bizalom elvén alapul, és azt állítja, hogy egy rendszerelem által nyújtott védelem arányos a rendszerelembe helyezett bizalommal. Ahogy a rendszerelembe vetett bizalom növekszik, úgy növekszik azonos mértékben a rendszerelem jogosulatlan módosítása elleni védelem is. A jogosulatlan módosítás elleni védelem lehet a rendszerelem saját önvédelme és inherens megbízhatósága, vagy a biztonsági architektúra más elemeitől vagy sajátosságaiból származó védelmek (beleértve a működési környezet védelmét).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek számon kell tartania a szoftverfejlesztési folyamat kezdetei szakaszában, valamint a további változtatások során minden létező és újonnan elkészített rendszerelemet és az azok közötti bizalmi térképet, különösen az összetett EIR-ek esetén.
2. A szervezetnek az inverz módosítási küszöb biztonságtervezési elvének értelmében növelnie kell az adott rendszerelem jogosulatlan módosításával szembeni védelmet, ha az adott rendszerelembe vetett bizalom növekszik.
3. A szervezetnek minden változtatás esetén felül kell vizsgálnia az érintett rendszerelemekről alkotott bizalmi térképet és amennyiben szükséges az inverz módosítási küszöb biztonságtervezési elv, valamint rendszerspecifikus logikai szabályzat alapján módosítania kell az adott elemeket.

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

SA-8(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.28. BIZTONSÁGTERVEZÉSI ELVEK – HIERARCHIKUS VÉDELEM

16.28. A szervezet a hierarchikus védelem biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A hierarchikus védelem elve kimondja, hogy egy rendszerelemet vagy összetevőt nem kell védeni a nála megbízhatóbbnak tekintett elemektől. A legmegbízhatóbb rendszerelem önmagát védi az összes többi rendszerelemmel szemben. Például, ha egy operációs rendszer magját az EIR legmegbízhatóbb elemének tekintjük, akkor önmagát védi az összes nem megbízható alkalmazástól, amit támogat, de az alkalmazásoknak nem kell védelmet biztosítaniuk a maggal szemben. A felhasználók megbízhatósága fontos szempont a hierarchikus védelem elvének alkalmazásakor. Egy megbízható EIR-nek nem kell megvédenie magát egy ugyanolyan megbízható felhasználótól, ami azt tükrözi, hogy nem megbízható EIR-eket használhatnak magas szintű rendszerkörnyezetekben, ahol a felhasználók nagyon megbízhatóak, és ahol más védelmet is bevezetésre kerülnek az EIR magas szintű végrehajtási környezetének körülhatárolására és védelmére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-ek megbízhatóságát. Ez magában foglalja a különböző EIR-ek és rendszerelemek értékelését, hogy meghatározzák, melyik a legmegbízhatóbb.
2. A szervezetnek meg kell határoznia a védelmi szinteket. Az EIR legmegbízhatóbb elemének védenie kell magát az összes többi, kevésbé megbízható elemtől, de a kevésbé megbízható rendszerelemeknek nem kell védeniük magukat a legmegbízhatóbbtól.
3. A szervezetnek figyelembe kell vennie a felhasználók megbízhatóságát. Egy megbízható EIR-nek nem kell védenie magát egy egyenlően megbízható felhasználótól.
4. A szervezetnek további védelmi intézkedéseket kell bevezetnie a legmagasabb szintű EIR környezet védelmére. Ez magában foglalhatja a naplózást, a hozzáférés-felügyeletet és más biztonsági intézkedéseket.

5. Az érintett szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hierarchikus védelmi tervét, hogy biztosítsa az EIR-ek megfelelő védelmét.

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

SA-8(12)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.29. BIZTONSÁGTERVEZÉSI ELVEK – BIZTONSÁGI ELEMEK MINIMALIZÁLÁSA

16.29. A szervezet a biztonsági elemek minimalizálásának biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A biztonsági elemek minimalizálásának elve alapján az EIR-nek nincsenek külső, megbízhatónak tekintett rendszerelemei vagy összetevői. A biztonsági elemek minimalizálásának elve két aspektusra osztható: a biztonsági elemzés teljes költségére és a biztonsági elemzés komplexitására. A megbízható elemek létrehozása és megvalósítása általában költségesebb a fejlesztési folyamatok szigorúbbá válása miatt. A megbízható elemek megbízhatóságának igazolása alaposabb biztonsági elemzést igényel. Annak érdekében, hogy csökkentsék a költségeket és csökkentsék a biztonsági elemzés komplexitását, egy EIR a lehető legkevesebb megbízható elemet tartalmazza. A megbízható elemek más elemekkel történő interakciójának elemzése az EIR biztonsági ellenőrzésének egyik legfontosabb aspektusa. Ha az elemek közötti interakciók feleslegesen bonyolultak, az EIR biztonsági állapota is nehezebben meghatározható, egy olyan EIR-hez képest, amelynek belső megbízható kapcsolatai egyszerűek és hatékonyabban felépítettek. Általánosságban elmondható, hogy kevesebb megbízható rendszerelem kevesebb belső bizalmas kapcsolatot és egyszerűbb EIR-t eredményez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-eket vagy a rendszerelemeket, amelyeket a biztonsági elemek minimalizálásának elve alapján kell kezelni.
2. A szervezetnek fel kell mérnie az EIR-ekben található megbízható elemeket. Ezek általában drágábbak a kialakításuk és implementálásuk miatt, mivel a fejlesztési folyamatok több és szigorúbb követelményeket támasztanak.
3. A szervezetnek csökkentenie kell a megbízható elemek számát az EIR-ekben, hogy csökkentse a költségeket és csökkentse a biztonsági elemzés bonyolultságát.

4. A szervezetnek elemznie kell a megbízható elemek interakcióját az EIR többi elemével. Ez az egyik legfontosabb aspektusa az EIR biztonsági ellenőrzésének. Ha az elemek közötti interakciók feleslegesen bonyolultak, az EIR biztonsága is nehezebben meghatározható, mint egy olyan EIR-é, amelynek belső bizalmi kapcsolatai egyszerűek és átláthatóan kialakítottak.
5. A szervezetnek naplót kell vezetnie az EIR-ekben található megbízható elemekről és azok interakcióiról, hogy nyomon követhesse a változásokat és az esetleges biztonsági problémákat.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR-eket a biztonsági elemek minimalizálásának elve alapján, hogy biztosítsa az EIR-ek folyamatos biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-8(13)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.30. Biztonságtervezési elvek – Legkisebb jogosultság

16.30. A szervezet a legkisebb jogosultság biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

Magyarázat

A legkisebb jogosultság elve alapján minden rendszerelemnek éppen annyi jogosultságot kell biztosítani, hogy a meghatározott funkcióit ellássa. A legkisebb jogosultság elvének alkalmazása korlátozza rendszerelem műveleti területét, ami két jótékony hatással jár: a hiba, illetve a visszaélés biztonsági hatása minimális lesz, és a rendszerelem biztonsági elemzése egyszerűsödik. A legkisebb jogosultság elve a biztonságos EIR tervezés minden aspektusában jelen van. A rendszerelem képességeinek meghívására szolgáló interfészek csak a felhasználói csoport bizonyos részhalmazai számára érhetők el, és a rendszerelem tervezése elegendő jogosultság bontást támogat. Például egy napló mechanizmus esetében lehet egy interfész a naplózás menedzseléséért felelős személy számára, aki konfigurálja a napló beállításait; egy interfész a naplózást üzemeltető személy számára, aki biztosítja, hogy a napló adatok biztonságosan gyűjtődjenek és tárolódjanak; és végül egy másik interfész a naplókat felülvizsgáló személy számára, akinek csak a begyűjtött naplók adatait kell megtekintenie, műveleteket nem kell azokkal végeznie.

A legkisebb jogosultság elvét nem csak a rendszerinterfésznél lehet megfigyelni, hanem az EIR belső szerkezetének irányadó elveként is használható. A belső legkisebb jogosultság egyik aspektusa az, hogy a modulokat úgy kell felépíteni, hogy csak a modulba foglalt elemeket működtetik közvetlenül a modulon belüli funkciók. A modulon kívüli elemek, amelyeket a modul működése befolyásolhat, közvetetten érhetők el azokat tartalmazó modullal történő interakció révén. A belső legkisebb jogosultság másik aspektusa az, hogy egy adott modul vagy elem hatóköre csak azokat a rendszerelemeket tartalmazza, amelyek a funkcionalitásához szükségesek, és az azokhoz való hozzáférési módok (pl. olvasás, írás) minimálisak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-eket vagy rendszerelemeket, amelyekre a legkisebb jogosultság biztonságtervezési elvét alkalmazni kívánja.
2. A szervezetnek meg kell határoznia az egyes EIR-ek vagy rendszerelemek funkcióit, és meg kell határoznia a szükséges jogosultságokat, amelyek elegendőek ezeknek a funkcióknak a végrehajtásához, de nem többek ennél.
3. A szervezetnek korlátoznia kell az EIR-ek vagy rendszerelemek tevékenységeinek hatókörét, hogy minimalizálja a hibák, a korrupció vagy a visszaélések biztonsági hatásait, és egyszerűsítse az EIR-ek vagy rendszerelemek biztonsági elemzését.
4. A szervezetnek biztosítania kell, hogy az EIR-ek vagy rendszerelemek képességeit csak bizonyos felhasználói csoportok hívhatják meg, és az EIR-ek vagy rendszerelemek tervezése támogatja a jogosultságok elegendően részletes felbontását.
5. Az érintett szervezetnek a legkisebb jogosultság elvét kell alkalmaznia az EIR-ek vagy rendszerelemek belső szerkezetének kialakítására is.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.60. Legkisebb jogosultság elve

6.26. Legszűkebb funkcionalitás

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-8(14)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.31. Biztonságtervezési elvek – Feltételhez kötött engedélyezés

16.31. A szervezet a feltételhez kötött engedélyezés (Predicate Permission) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

Magyarázat

A feltételhez kötött engedélyezés elve alapján az EIR tervezői fontolóra veszik több jogosult entitás hozzájárulásának szükségességét, mielőtt egy rendkívül kritikus műveletet vagy a rendkívül érzékeny adatokhoz, információkhoz vagy erőforrásokhoz való hozzáférést engedélyeznének. Eredetileg a feltételhez kötött engedélyezést a jogosultságok szétválasztásának nevezték, amely egyenértékű a szerepkörök szétválasztásával is. A jogosultságok több fél közötti megosztása csökkenti a visszaélés valószínűségét, és biztosítja, hogy egyetlen baleset, megtévesztés vagy bizalommal való visszaélés sem elegendő ahhoz, hogy visszafordíthatatlan és jelentős károkat okozzon. Az ilyen mechanizmus tervezési lehetőségei lehetnek egyidejű cselekvést igénylőek (pl. nukleáris fegyver kilövéséhez két, jogosultsággal rendelkező személynek kell egy kis időablakon belül parancsot adnia), vagy egy műveletsorozatot, ahol minden további cselekvést valamilyen korábbi cselekvés tesz lehetővé, de egyetlen személy sem képes több mint egy cselekvést engedélyezni.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia azokat az EIR-eket vagy rendszerelemeket, amelyeknél a feltételhez kötött engedélyezési elvet alkalmazni kívánja. Ezek általában olyan kritikus műveletek vagy érzékeny adatok, információk vagy erőforrások, amelyekhez csak több jogosult entitás hozzájárulása után lehet hozzáférni.
2. A szervezetnek meg kell terveznie a feltételhez kötött engedélyezési mechanizmust. Ez lehet egyidejű művelet, vagy egy műveletsorozat, ahol minden további műveletet valamilyen előző művelet tesz lehetővé, de egyetlen személy sem képes több mint egy műveletet engedélyezni.
3. A szervezetnek be kell vezetnie a tervezett feltételhez kötött engedélyezési mechanizmust az EIR-ekben vagy rendszerelemekben.

4. A bevezetés után a szervezetnek naplóznia kell a feltételhez kötött engedélyezési műveleteket, hogy nyomon követhető legyen, ki, mikor és milyen műveletet hajtott végre.
5. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a feltételhez kötött engedélyezési mechanizmus működését és hatékonyságát, és szükség esetén módosítania kell azt.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.59. Felelősségek szétválasztása

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

SA-8(15)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.32. BIZTONSÁGTERVEZÉSI ELVEK – ÖNFENNTARTÓ MEGBÍZHATÓSÁG

16.32. A szervezet az önfenntartó megbízhatóság (Self-reliant Trustworthiness) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

Az önfenntartó megbízhatóság elve kimondja, hogy az EIR-ek minimalizálják a függőségüket más EIR-ektől saját megbízhatóságuk érdekében. Egy EIR alapértelmezés szerint megbízható, és minden kapcsolat egy külső entitással az EIR működését egészíti ki. Ha egy EIR-nek fenn kellene tartania a kapcsolatot egy külső entitással a megbízhatóságának fenntartása érdekében, akkor ez az EIR sérülékeny lenne a rosszindulatú és nem rosszindulatú fenyegetésekkel szemben, melyek a kapcsolat elvesztését vagy romlását eredményezhetik. Az önfenntartó megbízhatóság elvének előnye, hogy az EIR elszigetelése kevésbé teszi sérülékennyé a támadásokkal szemben. Ennek az elvnek a következménye az EIR (vagy rendszerelem) azon képességére vonatkozik, hogy elszigetelten működjön, majd újra szinkronizáljon más elemekkel, amennyiben újra összekapcsolják azokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-eket és a rendszerelemeket, amelyekre az önfenntartó megbízhatóság elvét alkalmazni kell.
2. A szervezetnek meg kell terveznie és implementálnia kell az EIR-ek és a rendszerelemek önfenntartó megbízhatóságát biztosító mechanizmusokat.
3. A szervezetnek folyamatosan dokumentálnia kell az önfenntartó megbízhatóságot biztosító mechanizmusokat az EIR-ek és a rendszerelemek megbízhatóságának nyomon követése érdekében.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR-ek és a rendszerelemek megbízhatóságát biztosító mechanizmusokat a változó környezeti és fenyegetési tényezők figyelembevételével.

5. A szervezetnek képzést kell biztosítania a személyzet számára az önfenntartó megbízhatóság elvének megértése és alkalmazása érdekében.

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

SA-8(16)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.33. BIZTONSÁGTERVEZÉSI ELVEK – BIZTONSÁGOSAN ELOSZTOTT FELÉPÍTÉS

16.33. A szervezet a biztonságosan elosztott felépítés (Secure Distributed Composition) tervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A biztonságosan elosztott felépítés tervezési elve kimondja, hogy azonos rendszerbiztonsági szabályzatot kikényszerítő elosztott elemek összeállítása olyan EIR-t eredményez, amely legalább olyan jól kényszeríti ki a szabályzatban előírtakat, mint az egyes elemek. A biztonságos rendszerek tervezési elve azt járja körül, hogy az egyes elemeknek hogyan kellene egymással interakcióba lépniük. Az elosztott elemek felépítéséből származó képesség létrehozása vagy lehetővé tétele iránti igény felerősítheti ezeknek az elveknek a relevanciáját. Különösen a biztonsági szabályzat átültetése önálló rendszerből elosztott rendszerbe vagy rendszerek rendszerébe váratlan eredményeket hozhat. A kommunikációs protokollok és az elosztott adatok konzisztenciát biztosító mechanizmusai segítenek biztosítani a szabályzati előírások következetes kikényszerítését egy elosztott rendszeren belül. Annak érdekében, hogy biztosítva legyen a rendszeren átívelő helyes kikényszerítése a szabályzati elvárásoknak, az elosztott felépítésű EIR biztonsági architektúráját alaposan elemezni kell.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-eket vagy rendszerelemeket, amelyekben a biztonságosan elosztott felépítés tervezési elvét alkalmazni kívánja.
2. A szervezetnek meg kell határoznia a biztonsági szabályokat, amelyeket az EIR-eknek vagy rendszerelemeknek követniük kell. Ezek a szabályok lehetnek meglévő, vagy új, kifejezetten az EIR-ekre vagy rendszerelemekre szabott szabályok.
3. A szervezetnek meg kell terveznie és implementálnia kell a kommunikációs protokollokat és az elosztott adatok konzisztencia mechanizmusait, amelyek biztosítják a következetes szabályok érvényesítését az EIR-eken vagy rendszerelemeken keresztül.

4. Az érintett szervezetnek alaposan elemeznie kell az elosztott felépítésű EIR-ek biztonsági architektúráját, hogy biztosítsa a szabályok helyes érvényesítését az egész EIR-en vagy rendszerelemen belül.
5. A szervezetnek dokumentálnia kell az EIR-ek vagy rendszerelemek biztonsági szabályainak érvényesítését, hogy nyomon követhesse a szabályok betartását és az esetleges biztonsági problémákat.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR-ek vagy rendszerelemek biztonsági szabályait és kommunikációs protokolljait, hogy biztosítsa a szabályok következetes és hatékony érvényesítését.

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

SA-8(17)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.34. BIZTONSÁGTERVEZÉSI ELVEK – BIZTONSÁGOS KOMMUNIKÁCIÓS CSATORNÁK

16.34. A szervezet a biztonságos kommunikációs csatornák biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A biztonságos kommunikációs csatornák elve kimondja, hogy amikor egy olyan EIR-t állítunk össze, ahol potenciális fenyegetés áll fenn az elemek közötti kommunikációval összefüggésben, minden kommunikációs csatorna a támogatott biztonsági függőségekkel arányosan megbízható (azaz, mennyire bíznak más elemek abban, hogy működnek a biztonsági funkciók). A biztonságos kommunikációs csatornákat a kommunikációs csatornához való hozzáférés korlátozásával (a kommunikációban résztvevő végpontok megfelelő szintű megbízhatóságának biztosítására) és a kommunikációs csatornán keresztül továbbított adatok végponttól végpontig történő védelmének kombinációjával valósíthatók meg (védelmet biztosít a lehallgatás és módosítás ellen, illetve további biztosítékot nyújt a megfelelő végponttól végpontig történő kommunikációhoz).

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az EIR-eket vagy rendszerelemeket, amelyekben a biztonságos kommunikációs csatornák biztonságtervezési elvét alkalmazni kívánja.
2. A szervezetnek fel kell mérnie a potenciális fenyegetéseket, amelyek befolyásolhatják az EIR-ek közötti kommunikációt. Ez magában foglalja az EIR-ek közötti összeköttetések vizsgálatát is.
3. A szervezetnek minden kommunikációs csatornát a megfelelő megbízhatósággal kell kezelnie, amely arányban áll a támogatott biztonsági függőségekkel. Ez azt jelenti, hogy mennyire bíznak más rendszerelemek abban, hogy az adott csatorna elvégzi a biztonsági funkcióit.
4. A biztonságos kommunikációs csatornák megvalósításához a szervezetnek korlátoznia kell a kommunikációs csatornához való hozzáférést. Ez biztosítja, hogy a szervezet elfogadható mértékben megbízhat a kommunikációban részt vevő végpontokban.

5. A szervezetnek végponttól végpontig terjedő védelmet kell alkalmaznia azon adatokra, amelyeket a kommunikációs csatornán keresztül továbbítanak.

6. A szervezetnek naplóznia kell a kommunikációs csatornákban zajló tevékenységeket, ezáltal figyelemmel kísérheti az ezzel kapcsolatos biztonsági intézkedések hatékonyságát. Így a szervezet időben képes észlelni a potenciális biztonsági problémákat, és megtenni a szükséges lépéseket a kockázatok kezelésére.

Kapcsolódó intézkedések

17.40. Az adatátvitel bizalmassága és sértetlensége

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SA-8(18)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.35. BIZTONSÁGTERVEZÉSI ELVEK – FOLYAMATOS VÉDELEM

16.35. A szervezet a folyamatos védelem biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A folyamatos védelem elve kimondja, hogy a biztonsági szabályok érvényesítésére használt elemek és adatok megszakítás nélküli védelmet élveznek, amely összhangban van a biztonsági szabályozókkal és a biztonsági architektúrában meghatározottakkal. Amennyiben védelmi hiányosságok vannak, nem lehet biztosítani, hogy az EIR képes biztosítani a tervezési képességének bizalmassági, sértetlenségi és rendelkezésre állási követelményeit. Nem lehetnek olyan időszakok, amikor az adatok és információk az EIR ellenőrzése, és ezáltal védelme nélkül maradnak. A folyamatos védelem megköveteli a referencia-ellenőrzési koncepció (azaz minden kérést a referencia-ellenőrzés validál; a referencia-ellenőrzés képes megvédeni magát a manipulációtól; és a mechanizmus helyességéről és teljességéről elemzés és tesztelés útján kellő bizonyosságot tud szerezni) és a biztonságos hibakezelés és helyreállítás biztonságtervezési elveinek (azaz a biztonságos állapot megőrzése hiba, hiba, meghibásodás és sikeres támadás esetén; a biztonságos állapot megőrzése a normál, csökkentett vagy alternatív üzemmódba történő helyreállítás során) betartását.

A folyamatos védelem a különböző konfigurációkban való működésre tervezett EIR-ekre is vonatkozik, beleértve a teljes működési képességet biztosító és a részleges működési képességet biztosító, csökkentett üzemmódú konfigurációkat. A folyamatos védelem biztonságtervezési elve megköveteli, hogy az EIR biztonságiszabályainak módosításai visszavezethetők legyenek a konfigurációt vezérlő működési igényre, és ellenőrizhetők legyenek (hogy a javasolt módosítások nem hozzák-e az EIR-t bizonytalan állapotba).

A nem megfelelő nyomon követhetőség és ellenőrzés a probléma összetett vagy eldönthetetlen természete miatt inkonzisztens állapotokhoz vagy védelmem megszakadásaihoz vezethet.

Az új biztonsági szabályzókat tükröző, előzetesen ellenőrzött konfigurációs definíciók használata lehetővé teszi annak elemzését, hogy a régi szabályzókról az új szabályzókra történő

áttérés lényegében atomi jellegű legyen, és hogy a régi szabályzó maradványhatásai garantáltan ne kerüljenek konfliktusba az új szabályzóéval.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azon EIR-eket, amelyeket a folyamatos védelem biztonságtervezési elvének megfelelően kell védeni.
2. A szervezetnek biztosítania kell, hogy az EIR-ek és az azokban tárolt adatok védelme megszakítás nélkül, folyamatosan biztosított legyen, összhangban a biztonsági szabályzatokkal és a biztonsági architektúrában meghatározottakkal.
3. A szervezetnek meg kell győződnie arról, hogy nincsenek rések a védelemben, amelyek aláásnák az EIR-ek biztonságát.
4. A szervezetnek biztosítania kell, hogy az adatok és információk folyamatosan védettek legyenek, vagyis nincsenek olyan időszakok, amikor az adatok és információk az EIR ellenőrzése és védelme nélkül maradnak.
5. A szervezetnek alkalmaznia kell a referencia-ellenőrzés előírásait, a biztonságos hibakezelés és helyreállítás biztonságtervezési elvét.
6. A szervezetnek biztosítania kell, hogy az EIR-ek biztonsági szabályozóinak változásai megfeleljenek a működési szükségletnek és ellenőrizhetők legyenek (azaz lehetséges legyen ellenőrizni, hogy a javasolt változások nem teszik az EIR-t valamilyen szempontból védtelenné).
7. A szervezetnek dokumentálnia kell a változásokat és biztosítania kell, hogy a változások ne vezessenek védelmi hiányosságokhoz vagy inkonzisztens állapotokhoz.
8. A szervezetnek biztosítania kell, hogy a folyamatos védelem elvének megfelelően működő EIR-ek életciklusának védelmi igényeit világosan megfogalmazza, mint biztonsági követelményeket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.129. Referenciának való megfelelőség vizsgálata

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

SA-8(19)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.36. BIZTONSÁGTERVEZÉSI ELVEK – BIZTONSÁGOS METAADATKEZELÉS

16.36. A szervezet a biztonságos metaadatkezelés biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A biztonságos metaadatkezelés elve azt mondja ki, hogy a metaadatok ugyanolyan védelmt kell, hogy élvezzenek, mint azok az adatok és információk, amelyeket a metaadat leír. A biztonságos metaadatkezelés elvét az a felismerés vezérli, hogy egy EIR, alrendszer vagy rendszerelem nem érheti el az védett állapotot, hacsak nem védi azokat az adatokat, amelyekre a helyes végrehajtás érdekében támaszkodik. Az adatokat általában nem az az EIR értelmezi, amelyik tárolja őket. Az adatok szemantikai értékkel bírhatnak (azaz információt tartalmaznak) a felhasználók és az adatokat feldolgozó programok számára. Ezzel szemben a metaadatok adatokról szóló információk(például egy fájlnév vagy a fájl létrehozásának dátuma). A metaadatokat a céladatokhoz vannak kötve, amelyeket az EIR értelmezni tud, de nem szükséges, hogy a céladatokon belül vagy közelében tárolják. Lehetnek olyan metaadatok, amelyek célpontja maga a metaadat (például egy fájlnév osztályozási szintje vagy hatásszintje), beleértve az önhivatkozó metaadatokat is.

A metaadatok elégtelen védelmével kapcsolatosan aggodalomra adnak okot a többszintű biztonsági rendszerek (MLS). Az MLS-rendszerek a relatív érzékenységi szintek alapján közvetítik az alanyok objektumokhoz való hozzáférését. Ebből következik, hogy az MLS-rendszer ellenőrzési körébe tartozó valamennyi alany és objektum vagy közvetlenül, vagy közvetve érzékenységi szintekkel van ellátva. A címkézett metaadatok következménye az MLS-rendszerek esetében azt jelenti, hogy a metaadatokat tartalmazó objektumok címkézettek.

Az adatok védelmi szükségleteinek értékeléséhez hasonlóan figyelmet kell fordítani annak biztosítására, hogy a bizalmassági és integritási védelmek egyedileg kerüljenek értékelésre, meghatározásra és hozzárendelésre a metaadatokhoz, ahogyan azt a ügymeneti, üzleti és rendszeradatok esetében is tennék.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az EIR-eket, amelyekben a biztonságos metaadatkezelés biztonságtervezési elvét alkalmazni kívánja.
2. A szervezetnek biztonsági szabályzataiban rendelkeznie kell a metaadatok kezeléséről, amikor a szabályok vagy a teljes információvédelmet, vagy a biztonsági alrendszer védelmét igénylik.
3. A szervezetnek fel kell ismernie, hogy egy EIR, alrendszer vagy rendszerelem nem érheti el a védett állapotot, hacsak nem védi azokat az adatokat, amelyekre a helyes végrehajtás érdekében támaszkodik.
4. A szervezetnek biztosítania kell, hogy a metaadatok, mint az adatokról szóló információk, megfelelő védelemben részesüljenek.
5. A szervezetnek figyelmet kell fordítania arra, hogy a metaadatok védelmének hiánya megsérti a biztonsági szabályzatot, beleértve az információ kiszivárgását is.
6. A szervezetnek biztosítania kell, hogy minden alany és objektum, amely az EIR ellenőrzési körébe tartozik, közvetlenül címkézett vagy közvetett érzékenységi szintekkel rendelkezik.
7. A szervezetnek egyedileg kell értékelnie, meghatároznia és hozzárendelnie a bizalmassági és sértetlenségi biztonsági követelményeket a metaadatokhoz, ahogy azt az ügymeneti, üzleti és rendszeradatok esetében is tenné.

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

SA-8(20)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.37. BIZTONSÁGTERVEZÉSI ELVEK – ÖNELLENŐRZÉS

16.37. A szervezet az önellenőrzés biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

Az önellenőrzés elve kimondja, hogy egy rendszerelem képes korlátozott mértékben értékelni belső állapotát és működését a végrehajtás különböző szakaszaiban, és hogy ez az önellenőrzési képesség arányos az EIR-be fektetett megbízhatósági szinttel. Az EIR szintjén az önelemzés a megbízhatóság hierarchikus - alulról felfelé épitkező értékelésein keresztül érhetők el. Ebben a megközelítésben az alacsonyabb szintű elemek ellenőrzik a magasabb szintű elemek adatintegritását és (korlátozott mértékben) helyes működését.

A gyökérben egy elem önmagát igazolja, ami általában egy axiomatikus vagy környezeti szempontból kikényszerített feltételezést jelent a sértetlenségéről.

Az önelemzések eredményei felhasználhatók a külsőleg előidézett hibák, belső meghibásodások vagy átmeneti hibák elleni védelemre. Ezt az elvet követve egyes egyszerű meghibásodások vagy hibák anélkül észlelhetők, hogy a hiba vagy meghibásodás hatásai az adott elemen kívülre terjednének. Ezenkívül az önellenőrzés felhasználható az elem konfigurációjának tanúsítására, az elvárt konfigurációval kapcsolatos esetleges ellentmondások észlelésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az EIR-eket, amelyeket az önellenőrzés biztonságtervezési elvének alkalmazásával szeretne védeni.

2. A szervezetnek meg kell terveznie és implementálnia kell egy önellenőrzési rendszert, amely képes az EIR belső állapotának és működésének korlátozott mértékű értékelésére a végrehajtás különböző szakaszaiban. Ez az önellenőrzési képesség arányban kell, hogy álljon az EIR-be fektetett megbízhatósággal.

3. A szervezetnek hierarchikus megbízhatósági értékeléseket kell létrehoznia az EIR szintjén, amelyeket alulról felfelé építenek ki. Ebben a megközelítésben az alsó szintű elemek ellenőrzik a magasabb szintű elemek sértetlenségét és helyes működését.

4. A szervezetnek biztosítania kell, hogy az EIR önellenőrzése során az elemek képesek legyenek azonosítani az egyszerű hibákat és működési zavarokat, anélkül, hogy a hiba vagy működési zavar hatásai az elemen kívülre terjednének.
5. A szervezetnek ellenőrzésre kell használnia az önellenőrzés eredményeit, hogy megvédje az EIR-t a külső hibáktól, belső működési hibáktól vagy átmeneti hibáktól.
6. A szervezetnek használnia kell az önellenőrzést az EIR rendszerelemei konfigurációjának igazolására, és észlelnie kell minden lehetséges konfigurációs ellentmondást az elvárt konfigurációval szemben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.14. Folyamatos felügyelet

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-8(21)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.38. BIZTONSÁGTERVEZÉSI ELVEK – ELSZÁMOLTATHATÓSÁG ÉS NYOMONKÖVETHETŐSÉG

16.38. A szervezet az elszámoltathatóság és nyomonkövethetőség biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

Az elszámoltathatóság és nyomonkövethetőség elve azt állítja, hogy lehetséges a biztonsági szempontból releváns tevékenységek (alany-objektum interakciók) nyomon követése azon entitás számára, akinek megbízásából a tevékenység történik. Az elszámoltathatóság és nyomonkövethetőség elve megbízható infrastruktúrát igényel, amely képes rögzíteni a részleteket a biztonságot érintő tevékenységekről (például egy naplózási alrendszer).

Az elszámoltathatóság és a nyomonkövethetőség másik fontos funkciója a biztonsági szabályzat megsértésével kapcsolatos események rutinszerű és igazságügyi (forensic) elemzése. A naplóbejegyzések elemzése további információkkal szolgálhat, amelyek hasznosak lehetnek annak az útvonalnak vagy elemnek a meghatározásában, amely lehetővé tette a biztonsági szabályzat megsértését, valamint a biztonsági szabályzat megsértésével összefüggő személyek tevékenységét.

A tevékenységek részleteinek rögzítéséhez az EIR képes egyedileg azonosítani azt az entitást, akinek a nevében a tevékenységet végrehajtják, valamint rögzíteni a végrehajtott tevékenységek vonatkozó sorozatát. Az elszámoltathatósági szabály azt is megköveteli, hogy maga a naplózási nyomvonal védve legyen a jogosulatlan hozzáféréstől és módosítástól. A legkisebb jogosultság elve segít visszavezetni a tevékenységeket bizonyos entitásokra, mivel növeli az elszámoltathatóság részletességét. Az egyes műveletek rendszeregységekhez és végső soron felhasználókhoz rendelése, valamint a naplózási nyomvonal jogosulatlan hozzáférésekkel és módosításokkal szembeni biztonságossá tétele biztosítja a letagadhatatlanságot, mivel ha egy művelet egyszer már rögzítésre került, a naplózási nyomvonalat nem lehet megváltoztatni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy képes legyen azonosítani azokat az entitásokat, akik nevében a biztonsági intézkedések végrehajtásra kerülnek. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie egyedi azonosítók létrehozására és kezelésére.
2. A szervezetnek létre kell hoznia egy megbízható infrastruktúrát, amely képes rögzíteni a biztonságot érintő tevékenységek részleteit. Ez magában foglalja egy napló alrendszer létrehozását az EIR-en belül.
3. A szervezetnek biztosítania kell, hogy a naplózási nyomvonalat magát is megvédje az illetéktelen hozzáféréstől és módosítástól. Ez azt jelenti, hogy a naplózásra vonatkozó szabályoknak és eljárásoknak meg kell határozniuk, hogy ki férhet hozzá a naplókhoz, és milyen körülmények között.
4. A szervezetnek alkalmaznia kell a legkisebb jogosultság elvét, ami segít a tevékenységek egyes entitásokhoz történő összekapcsolásban, mivel ez növeli az elszámoltathatóság részletességét.
5. A szervezetnek össze kell kapcsolnia a specifikus tevékenységeket az EIR entitásaival, és végül a felhasználókkal. A naplózási nyomvonal biztonságos megőrzése az illetéktelen hozzáférés és módosítások ellen biztosítja a letagadhatatlanságot, mivel egyszer egy tevékenység rögzítésre került, a naplózási nyomvonalat nem lehet megváltoztatni.
6. A szervezetnek rendszeresen és alaposan elemeznie kell a napló bejegyzéseket, különösen a biztonsági szabályok megsértésével kapcsolatos eseményeket. A naplók elemzése további információkat szolgáltathat, amelyek segíthetnek meghatározni a biztonsági szabályzat megsértését lehetővé tevő útvonalat vagy elemet, valamint az ezzel kapcsolatos egyének tevékenységeit.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.60. Legkisebb jogosultság elve
4.2. Naplózható események
4.3. Naplóbejegyzések tartalma
4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
4.25. Naplóinformációk védelme
4.33. Letagadhatatlanság

4.40. Naplóbejegyzések létrehozása

8.2. Azonosítás és hitelesítés

9.9.1. Biztonsági események kezelése

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

SA-8(22)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.39. BIZTONSÁGTERVEZÉSI ELVEK – BIZTONSÁGOS ALAPBEÁLLÍTÁSOK

16.39. A szervezet a biztonságos alapbeállítások biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A biztonságos alapbeállítások elve azt jelenti, hogy egy EIR alapértelmezett konfigurációja tükrözi a biztonsági szabályozók korlátozó és állapotot megőrző jellegét. A biztonságos alapbeállítások elve vonatkozik az EIR kezdeti (azaz alapértelmezett) konfigurációjára, valamint az olyan hozzáférés-felügyeleti és egyéb biztonsági funkciók biztonságtechnikai és tervezési aspektusaira, amelyek a "tilt, hacsak kifejezetten nem engedélyezett" elvet követik. Az elv kezdeti konfigurációs része azt követeli meg, hogy az EIR, alrendszer vagy rendszerelem bármilyen szállítási konfigurációja ne segítse elő a biztonsági szabályozók megsértését, és megakadályozza az EIR működését az alapértelmezett konfigurációban azokban az esetekben, ahol a biztonsági szabályozó maga igényli a működési felhasználó konfigurációját.

A korlátozó alapbeállítás azt jelenti, hogy az EIR a kiszállításkori állapotában megfelelő önvédelemmel működik, és képes lesz megelőzni a biztonság megsértését a tervezett biztonsági szabályzat és a rendszerkonfiguráció kialakítása előtt. Azokban az esetekben, amikor a szállított termék által nyújtott védelem nem elégséges, az érdekelt felek a biztonságos kezdeti állapot kialakítása előtt felmérik és értékelik a használat kockázatát.

A biztonságos alapbeállítások biztonságtervezési elvének betartása garantálja, hogy az EIR a sikeres inicializálás után biztonságos állapotba kerül.

Ezen elv biztonságtechnikai megközelítése szerint a biztonsági mechanizmusok megtagadják a kéréseket, kivéve, ha a kérés jól formázottnak és a biztonsági szabályzattal összhangban lévőnek bizonyul. A nem biztonságos alternatíva az, hogy a kérést engedélyezik, hacsak nem bizonyul a szabályzattal összeegyeztethetetlennek. Egy nagy rendszerben az alapértelmezés szerint megtagadott kérés engedélyezéséhez teljesített feltételek gyakran sokkal tömörebbek és teljesebbek, mint azok, amelyeket ellenőrizni kell egy alapértelmezés szerint jóváhagyott kérés elutasításához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek alkalmaznia kell a biztonságos alapbeállítások elvét az EIR kezdeti konfigurációjára, valamint a hozzáférés-felügyeleti és egyéb biztonsági funkciók biztonsági tervezésére és mérnöki munkájára, amelyek a "tilt, hacsak kifejezetten nem engedélyezett" elvet követnek.

3. A szervezetnek biztosítania kell, hogy az EIR "kiszállított" konfigurációja ne járuljon hozzá a biztonsági szabályzat megsértéséhez, és akadályozza meg az EIR működését az alapértelmezett konfigurációban azokban az esetekben, ahol a biztonsági szabályok előírják a felhasználó általi konfigurálhatóságot.

4. A szervezetnek biztosítania kell, hogy az EIR megfelelő védelemmel üzemeljen a kiszállítás után, és képes legyen megakadályozni a biztonsági szabálysértéseket, mielőtt a meghatározott biztonsági szabályozók és követelmények, valamint az EIR konfiguráció beállításra kerülne.

5. A szervezetnek vizsgálnia kell azt a kockázatot, hogy a kiszállított termék által nyújtott védelem nem elegendő, mielőtt biztonságos kezdeti állapotot hozna létre.

6. A szervezetnek biztosítania kell, hogy az EIR biztonságos állapotban legyen a kezdeti beállítás sikeres befejezése után.

7. A szervezetnek naplót kell vezetnie a biztonsági eseményekről, hogy képes legyen észlelni és helyreállítani a hibákat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció

6.23. Konfigurációs beállítások

16.7. Beszerzések

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

SA-8(23)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.40. BIZTONSÁGTERVEZÉSI ELVEK – BIZTONSÁGOS HIBAKEZELÉS ÉS HELYREÁLLÍTÁS

16.40. A szervezet a biztonságos hibakezelés és helyreállítás biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A biztonságos hibakezelés és helyreállítás elve kimondja, hogy sem egy rendszerfunkció vagy mechanizmus meghibásodása, sem pedig a hibára adott helyreállítási intézkedés nem vezethet a biztonsági szabályok megsértéséhez. Az EIR biztonságos hibakezelés és helyreállítás elve párhuzamosan működik a folyamatos védelem elvével, hogy biztosítsa az EIR képességét a megvalósult és potenciális hibák észlelésére bármely működési szakaszban és megfelelő lépések megtételére annak érdekében, hogy a biztonsági szabályzók ne sérüljenek. Ezenkívül, amikor ez meghatározott, az EIR képes a potenciális vagy megvalósult hibákból helyreállni, hogy folytassa a normál, csökkentett vagy alternatív biztonságos működést, miközben biztosítja, hogy a biztonságos állapotot fenntartja, így a biztonsági szabályok nem sérülnek. A hiba olyan állapot, amikor egy rendszerelem viselkedése eltér a meghatározott vagy várt működéstől egy dokumentált bemenet esetén. Ha egy hibás biztonsági funkciót észlelnek, az EIR újrakonfigurálhatja magát, hogy elkerülje a hibás rendszerelemet, miközben fenntartja a biztonságot és biztosítja az eredeti rendszer teljes vagy részleges funkcionalitását, vagy teljesen leállíthatja magát, hogy megakadályozza a biztonsági szabályok további megsértését. Ennek érdekében az EIR újrakonfigurálási funkcióit úgy tervezték, hogy folyamatosan érvényesítsék a biztonsági szabályokat az újrakonfigurálás különböző szakaszaiban. Egy másik technika, amelyet a hibákból való helyreállásra lehet használni, az, hogy az EIR visszatér egy biztonságos állapothoz (ami lehet az eredeti állapot), ezt követően leállításra vagy cserére kerül a hibás szolgáltatás vagy rendszerelem, hogy a biztonságos működés folytatódhasson.

A biztonságos hibakezelés elve azt jelzi, hogy az elemek olyan állapotban hibásodnak meg, amely inkább megtagadja, semmint megadja a hozzáférést.

Azon hibavédelmi stratégiák, melyek a biztonsági eljárásrendeket kikényszerítő mechanizmusokat alkalmazzák néha mélységi védelemnek is nevezhetők, mert lehetővé teszik, hogy az EIR akkor is biztonságos állapotban maradjon, amikor az egyik mechanizmus nem

képes a rendszert megvédeni. Ha azonban a mechanizmusok hasonlóak, a kiegészítő védelem látszólagos lehet, mivel a támadó egyszerűen sorozatban támadhat. Hasonlóképpen, egy hálózatos rendszerben az egyik EIR vagy szolgáltatás biztonságának feltörése lehetővé teheti a támadó számára, hogy ugyanezt más hasonló replikált EIR-eken és szolgáltatásokon is megtegye. Több olyan védelmi mechanizmus alkalmazásával, amelyek jellemzői jelentősen különböznek egymástól, csökkenthető a támadások megismétlődésének kockázata.

A megnövekedett komplexitás általában csökkenti a megbízhatóságot. Ha egy erőforrás nem védhető folyamatosan, kritikus fontosságú a biztonsági rések felderítése és kijavítása, mielőtt az erőforrást ismét biztonságos környezetben használnák.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR képes legyen a hibák észlelésére és megfelelő lépések megtételére a biztonsági szabályok megsértésének elkerülése érdekében.
2. A szervezetnek meg kell terveznie a hibakezelési folyamatokat, amelyek lehetővé teszik az EIR számára, hogy elkerülje a hibás rendszerelem használatát, miközben fenntartja a biztonságot, és biztosítja az eredeti EIR funkcióinak egy részét vagy egészét.
3. A szervezetnek alkalmaznia kell a meghatározott visszaállítási technikáit, amelyek lehetővé teszik az EIR számára, hogy visszatérjen egy biztonságos állapothoz, majd leállítsa vagy cserélje ki a hibás szolgáltatást vagy rendszerelemet, hogy a biztonságos működés folytatódhasson.
4. A szervezetnek meghatározott hibakezelési technikákat kell alkalmaznia, amelyek az EIR mechanizmusainak másolatai, hogy az EIR biztonságos állapotban maradhasson, még akkor is, ha egy mechanizmus nem tudta megvédeni az EIR-t.
5. A szervezetnek elemzéseket kell végeznie a redundancia technikáinak költségeiről és előnyeiről, figyelembe véve a megnövekedett erőforrás-használatot és a teljes EIR teljesítményére gyakorolt negatív hatásokat.
6. A szervezetnek további elemzéseket kell végeznie, ahogy a védelmi mechanizmusok bonyolultsága növekszik, mivel a bonyolultság növekedése általában csökkenti a megbízhatóságot.

7. A szervezetnek el kell végeznie a kritikus a biztonsági rések észlelését és javítását, mielőtt az erőforrást újra biztonságos kontextusban használnák, abban az esetben ha az erőforrást nem lehet folyamatosan védeni.
8. A szervezetnek naplózásra van szüksége a hibák és a helyreállítási intézkedések nyomon követéséhez, valamint a biztonsági szabályok megsértésének megelőzéséhez.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása
7.48. Átállás biztonságosüzemmódra
17.17. A határok védelme
17.40. Az adatátvitel bizalmassága és sértetlensége
17.77. Ismert állapot való meghibásodás
18.68. Előrelátható meghibásodás megelőzése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-8(24)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.41. BIZTONSÁGTERVEZÉSI ELVEK – KÖLTSÉGHATÉKONY BIZTONSÁG

16.41. A szervezet a költséghatékony biztonság biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A költséghatékony biztonság elve szerint a biztonsági mechanizmusok nem lehetnek drágábbak, mint a biztonság megsértéséből eredő potenciális kár. Ez a kockázatkezelésben használt költség-haszon elemzések biztonsággal kapcsolatos formája. A költség-haszon elemzés költségfeltevései megakadályozzák, hogy az EIR tervezője a szükségesnél erősebb biztonsági mechanizmusokat építsen be, ahol a mechanizmus erőssége arányos a költségekkel. A költséghatékony biztonság elve megköveteli továbbá a biztosítás előnyeinek elemzését a biztosítás költségeihez viszonyítva, a releváns és hiteles bizonyítékok megszerzésére fordított erőforrások, valamint a bizonyítékok értékeléséhez és a megbízhatóság és a kockázatokra vonatkozó következtetések levonásához szükséges elemzések szempontjából.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az EIR-eket vagy rendszerelemeket, amelyekre a költséghatékony biztonság biztonságtervezési elvét alkalmazni kívánja.
2. Az érintett szervezetnek meg kell becsülnie a potenciális károkat, amelyek egy biztonsági esemény következtében bekövetkezhetnek az EIR-ekben.
3. A szervezetnek költség-haszon elemzést kell végeznie, amelyben összehasonlítja a biztonsági mechanizmusok költségeit a potenciális károkkal.
4. A szervezetnek el kell kerülnie olyan biztonsági mechanizmusok beépítését az EIR-ekbe, amelyek költségesek jellemzően ezen mechanizmusok erőssége túlmutat a szükségesen.
5. A szervezetnek elemzést kell végeznie a biztosítás előnyeiről a biztosítás költségéhez képest, figyelembe véve a szükséges erőfeszítéseket a releváns és hiteles bizonyítékok megszerzéséhez, valamint az elemzéseket, amelyek szükségesek a bizonyítékokból levont megbízhatósági és kockázati következtetésekhez.

6. A szervezetnek naplóznia kell az egyes lépéseket, hogy nyomon követhesse a biztonságtervezési elv alkalmazásának hatékonyságát és hatását az EIR-ekre.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.4. Kockázatértékelés

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

SA-8(25)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.42. BIZTONSÁGTERVEZÉSI ELVEK – TELJESÍTMÉNYBIZTONSÁG

16.42. A szervezet a teljesítménybiztonság tervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A teljesítménybiztonság elve szerint a biztonsági mechanizmusokat úgy kell kialakítani, hogy azok ne rontsák szükségtelenül az EIR teljesítményét. Az érdekelt felek a rendszertervezés teljesítményre és biztonságra vonatkozó követelményeit pontosan megfogalmazzák és rangsorolják. Ahhoz, hogy az EIR megvalósítása megfeleljen a tervezési követelményeknek, és az érdekeltek számára elfogadható legyen, a tervezők betartják azokat a meghatározott korlátozásokat, amelyeket a képességek teljesítményigénye állít a védelmi igények elé. A számításigényes biztonsági szolgáltatások (pl. a kriptográfia) általános hatását értékelik és bizonyítják, hogy azok nem gyakorolnak jelentős hatást a magasabb prioritású teljesítmény követelményekre, vagy elfogadható kompromisszumot nyújtanak a teljesítmény és a megbízható védelem között. A kompromisszumos megoldások közé tartoznak a kevésbé számításigényes biztonsági szolgáltatások, kivéve, ha azok nem állnak rendelkezésre vagy nem elégségesek. Egy biztonsági szolgáltatás elégtelenségét a funkcionális képesség és a mechanizmus erőssége határozza meg. A mechanizmus erősségét a biztonsági követelmények, a teljesítménykritikus többletköltségek (pl. kriptográfiai kulcskezelés) és a fenyegetés értékelésének képessége alapján kell kiválasztani.

A teljesítménybiztonság elve olyan funkciók beépítéséhez vezet, amelyek segítik a biztonsági szabályok érvényesítését, de minimális többletköltséggel járnak, például olyan alacsony szintű hardvermechanizmusok, amelyekre magasabb szintű szolgáltatások építhetők. Az ilyen alacsony szintű mechanizmusok általában nagyon specifikusak, nagyon korlátozott funkcionalitással rendelkeznek, és a teljesítményre vannak optimalizálva. Például, ha a memória egy részéhez való hozzáférési jog megadása megtörtént, sok rendszer hardveres mechanizmusokat használ annak biztosítására, hogy minden további hozzáférés a megfelelő memóriacímet és hozzáférési módot használja. Ennek az elvnek az alkalmazása megerősíti annak szükségességét, hogy a biztonságot az alapoktól kezdve tervezzük a rendszerbe, és az

alsóbb szinteken olyan egyszerű mechanizmusokat építsünk be, amelyek a magasabb szintű mechanizmusok építőköveként használhatók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és prioritizálnia kell a teljesítménybiztonsági és az EIR tervezési követelményeket.
2. A szervezetnek a teljesítménybiztonság tervezési elvének követelményeit figyelembe kell vennie és ennek megfelelően kell implementálnia az EIR-t.
3. A szervezetnek figyelembe kell vennie a számítás igényes biztonsági szolgáltatásokat és a kevésbé számításigényes biztonsági szolgáltatásokat, hacsak azok nem állnak rendelkezésre vagy nem elegendőek.
4. A szervezetnek a biztonsági követelmények, a teljesítménykritikus működési költségek és a fenyegetés értékelési képesség alapján kell kiválasztania a mechanizmus erősségét.
5. A szervezetnek be kell építenie olyan funkciókat, amelyek segítenek a biztonsági szabályok érvényesítésében, de minimális működési költségbeli emelkedést okoznak.
6. A szervezetnek naplót kell vezetnie az EIR-ben végrehajtott összes műveletről, beleértve a hozzáférési jogosultságokat és a memóriacímeket, hogy biztosítsa a helyes memóriacím és hozzáférési mód használatát.
7. A szervezetnek a teljesítménybiztonság elvének alkalmazásával biztosítania kell a biztonság beépítését az EIR-be a tervezési fázistól kezdve, és egyszerű mechanizmusokat kell beépítenie az alacsonyabb szinteken, amelyeket építőkockaként lehet használni a magasabb szintű mechanizmusokhoz.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.49. Kriptográfiai kulcs előállítása és kezelése
17.53. Kriptográfiai védelem
18.2. Hibajavítás
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

SA-8(26)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.43. Biztonságtervezési elvek – Emberi tényezőn alapuló biztonság

16.43. A szervezet az emberi tényezőn alapuló biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

Magyarázat

Az emberi tényezőn alapuló biztonságtervezési elv szerint a biztonsági funkciók és a támogató szolgáltatások felhasználói felülete intuitív, felhasználóbarát, és visszajelzést ad a felhasználó olyan műveleteiről, amelyek hatással vannak az ilyen szabályokra és azok érvényesítésére. A biztonsági szabályokat érvényre juttató mechanizmusok nem zavarják a felhasználót, és úgy vannak kialakítva, hogy ne rontsák a felhasználói hatékonyságot. A biztonsági szabályok érvényesítési mechanizmusai értelmes, világos és releváns visszajelzést és figyelmeztetést is adnak a felhasználónak, ha nem biztonságos döntéseket hoz. Különös figyelmet kell fordítani azokra az interfészekre, amelyeken keresztül az EIR adminisztrációjáért és üzemeltetéséért felelős személyzet konfigurálja és beállítja a biztonsági szabályokat. Ideális esetben ez a személyzet képes megérteni döntéseik hatását. Az EIR adminisztrációjáért és üzemeltetéséért felelős személyzet a rendszer indítása előtt konfigurálhatja az EIR-eket, és a futási idő alatt úgy kezelheti azokat, hogy biztos lehet abban, hogy szándékaik helyesen illeszkednek az EIR mechanizmusaihoz. A biztonsági szolgáltatások, funkciók és mechanizmusok nem akadályozzák vagy nem bonyolítják szükségtelenül az EIR rendeltetésszerű használatát. Kompromisszumot kell kötni az EIR használhatósága és a biztonsági irányelvek érvényesítéséhez szükséges szigorúság között. Ha a biztonsági mechanizmusok frusztrálóak vagy nehezen használhatóak, akkor a felhasználók letilthatják, elkerülhetik őket, vagy olyan módon használják őket, amely nincs összhangban azokkal a biztonsági követelményekkel és védelmi igényekkel, amelyek kielégítésére a mechanizmusokat tervezték.

A követelmény alkalmazásának lépései

1. Az érintett szervezetnek először meg kell határoznia az EIR-eket, amelyekben az emberi tényezőn alapuló biztonságtervezési elvet alkalmazni kívánja.

2. Az érintett szervezetnek a felhasználói felületet úgy kell kialakítania, hogy az intuitív, felhasználóbarát legyen, és visszajelzést adjon a felhasználói műveletekről, amelyek befolyásolják a biztonsági szabályokat és azok érvényesítését.
3. Az érintett szervezetnek biztosítania kell, hogy a biztonsági szabályokat érvényesítő mechanizmusok ne legyenek zavaróak a felhasználó számára, és ne rontsák a felhasználó hatékonyságát.
4. Az érintett szervezetnek figyelmet kell fordítania azokra a felületekre, amelyeken keresztül a rendszeradminisztrációs és üzemeltetési feladatokért felelős személyzet konfigurálja és beállítja a biztonsági szabályokat.
5. Az érintett szervezetnek biztosítania kell, hogy a rendszeradminisztrációs és üzemeltetési feladatokért felelős személyzet képes legyen megérteni a döntéseik hatását.
6. Az érintett szervezetnek biztosítania kell, hogy a biztonsági szolgáltatások, funkciók és mechanizmusok ne akadályozzák vagy feleslegesen bonyolítsák az EIR szándékos használatát.
7. Az érintett szervezetnek naplót kell vezetnie a biztonsági mechanizmusok használatáról, hogy nyomon követhesse, ha a felhasználók kikapcsolják őket, megkerülik őket, vagy olyan módon használják őket, amely nincs összhangban a biztonsági követelményekkel és a védelmi szükségletekkel, amelyeket a mechanizmusok kielégítésére terveztek.

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

SA-8(27)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.44. Biztonságtervezési elvek – Elfogadható biztonsági szint

16.44. A szervezet az elfogadható biztonsági szint biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

Magyarázat

Az elfogadható biztonsági szint elve megköveteli, hogy az EIR által biztosított adatvédelem és teljesítmény szintje összhangban legyen és megfeleljen a felhasználók elvárásainak. A személyes adatok védelmének megítélése befolyásolhatja a felhasználók viselkedését, morálját és hatékonyságát. A szervezet szabályai és a rendszertervezés alapján a felhasználóknak képesnek kell lenniük arra, hogy korlátozni tudják műveleteiket a személyes adataik védelme érdekében. Ha az EIR-ek nem biztosítanak intuitív felületeket, vagy nem felelnek meg az adatvédelmi és teljesítménybeli elvárásoknak, a felhasználók vagy teljesen megkerülhetik az EIR-t, vagy olyan módon használhatják, amely nem hatékony vagy nem biztonságos.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az EIR-eket vagy rendszerelemeket, amelyekre a biztonságtervezési elv alkalmazandó.
2. A szervezetnek meg kell határoznia az elfogadható biztonsági szintet, amely összhangban van a felhasználók elvárásaival. Ez magában foglalja a személyes adatvédelmet és a teljesítményt is.
3. A szervezetnek ki kell dolgoznia egy szervezeti adatvédelmi szabályzatot, amely alapján a felhasználók képesek korlátozni tevékenységeiket személyes adataik védelme érdekében.
4. A szervezetnek biztosítania kell, hogy az EIR intuitív felületet biztosítson a felhasználók számára, és megfeleljen az adatvédelmi és teljesítménybeli elvárásoknak.
5. A szervezetnek intézkedéseket kell hoznia annak érdekében, hogy a felhasználók ne kerüljenek olyan helyzetbe, ahol megkerülik az EIR használatát, vagy olyan módon használják azt, ami nem hatékony vagy biztonsági kockázatot jelent, amennyiben az EIR nem felel meg a fenti elvárásoknak,

6. A szervezetnek naplót kell vezetnie az EIR használatáról, hogy nyomon követhesse a felhasználói tevékenységeket és az esetleges biztonsági problémákat. A napló segíthet azonosítani a rendszerben lévő biztonsági réseket és lehetővé teszi a szervezet számára, hogy időben reagáljon 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

SA-8(28)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.45. BIZTONSÁGTERVEZÉSI ELVEK – MEGISMÉTELHETŐ ÉS DOKUMENTÁLT ELJÁRÁSOK

16.45. A szervezet a megismételhető és dokumentált eljárások biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A megismételhető és dokumentált eljárások biztonságtervezési elve szerint a rendszerelem létrehozásához alkalmazott technikák és módszerek lehetővé teszik az adott elem teljes és helyes újraalkotását későbbi időpontban. A megismételhető és dokumentált eljárások támogatják a korábban elkészített elemmel azonos, esetleg széles körben elterjedt elem kifejlesztését. Más rendszerelemek esetében az ismételhetőség a következetességet és az elemek ellenőrizhetőségét támogatja. Az ismételhető és dokumentált eljárásokat különböző szakaszokban lehet bevezetni az EIR fejlesztési életciklusában, és hozzájárulnak az EIR-re vonatkozó megbízhatósági igények értékelhetőségéhez. Példák közé tartoznak a kódfejlesztés és felülvizsgálat rendszerezett eljárásai, az EIR fejlesztési eszközök és elemek konfigurációkezelési eljárásai, valamint az EIR szállítási eljárásai.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat az EIR-eket vagy rendszerelemeket, amelyekre a megismételhető és dokumentált eljárások biztonságtervezési elvét alkalmazni kívánja.
2. A szervezetnek ki kell dolgoznia a megismételhető eljárásokat, amiket dokumentálhat és amelyek lehetővé teszik a rendszerelemek teljes és helyes újraalkotását későbbi időpontban.
3. A szervezetnek be kell vezetnie a megismételhető és dokumentált eljárásokat az EIR fejlesztési életciklusának különböző szakaszaiban.
4. A szervezetnek eljárásokat kell kidolgoznia a kódfejlesztéshez és felülvizsgálathoz, az EIR fejlesztési eszközök és EIR-elemek konfigurációs kezeléséhez, valamint az EIR szállításához.

Kapcsolódó intézkedések

6.1. Szabályzat és eljárásrendek

16.1. Szabályzat és eljárásrendek

16.58. Fejlesztői változáskövetés

16.66. Fejlesztői biztonsági tesztelés

16.76.1. Fejlesztési folyamat, szabványok és eszközök

16.87. Fejlesztői biztonsági architektúra és tervezés

17.1. Szabályzat és eljárásrendek

18.1. Szabályzat és eljárásrendek

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

SA-8(29)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.46. BIZTONSÁGTERVEZÉSI ELVEK – ELJÁRÁSI SZIGOR

16.46. A szervezet a szigorú eljárási rend biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A szigorú eljárási rend biztonságtervezési elve állítja, hogy az EIR életciklusfolyamatának szigorúsága arányos a tervezett megbízhatósággal.Az eljárási szigor határozza meg az EIR életciklus-eljárásainak hatókörét, mélységét és részletességét. Az EIR szigorú életciklus-eljárásai több szempontból is hozzájárulnak annak biztosításához, hogy az EIR helyes és mentes a nem kívánt funkcióktól.

Először is, az eljárások fékeket és ellensúlyokat írnak elő az életciklus-folyamatban, így megakadályozzák a nem meghatározott funkciók bevezetését.

Másodszor, a rendszerbiztonsági mérnöki tevékenységekre alkalmazott szigorú eljárások, amelyek specifikációkat és egyéb rendszertervezési dokumentumokat készítenek, hozzájárulnak az EIR felépítésének megértéséhez, nem pedig abban bíznak, hogy az implementált elem specifikációja a mérvadó.

Végül egy meglévő rendszerelem módosítása könnyebb, ha részletes specifikációk írják le a jelenlegi felépítést, ahelyett, hogy a forráskódot vagy a kapcsolási rajzokat tanulmányoznák, hogy megértsék, hogyan működik. Az eljárási szigor segít annak biztosításában, hogy a biztonsági funkcionális - és biztosítási követelmények teljesüljenek, és hozzájárul a megbízhatóság és a kockázati helyzet meghatározásához szükséges alaposabb információkkal. Az eljárási szigor arányos az EIR által megkívánt megbízhatóság mértékével. Ha az EIR megkövetelt megbízhatósága alacsony, a magas szintű eljárási szigor szükségtelen költségekkel járhat, míg ha a magas megbízhatóság kritikus fontosságú, akkor a magas eljárási szigor költsége indokolt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR életciklusának folyamatait, és biztosítania kell, hogy ezek összhangban vannak az EIR kívánt megbízhatóságával. Az eljárási szigorúság meghatározza az EIR életciklusának eljárásainak hatókörét, mélységét és részletességét.

2. A szervezetnek szigorú eljárásokat kell alkalmaznia az EIR biztonsági mérnöki tevékenységekre, amelyek specifikációkat és más EIR tervezési dokumentumokat hoznak létre. Ez hozzájárul az EIR megértéséhez, ahogy azt megépítették, nem pedig az elem implementált verziójának megbízhatóságára támaszkodva.
3. A szervezetnek részletes specifikációkat kell készítenie az EIR jelenlegi tervezésének leírására. Ez megkönnyíti a meglévő rendszerelem módosítását, mivel nem kell forráskódot vagy rajzokat tanulmányozni annak működésének megértéséhez.
4. A szervezetnek biztosítania kell, hogy az eljárási szigorúság segít abban, hogy az EIR biztonsági funkcionális és biztosítási követelményei teljesüljenek. Ez hozzájárul az EIR megbízhatóságának és kockázati helyzetének meghatározásához.
5. A szervezetnek meg kell határoznia az EIR számára kívánt megbízhatósági szintet. Ha az EIR kívánt megbízhatósága alacsony, a magas szintű eljárási szigorúság felesleges költséget jelenthet, míg ha a magas megbízhatóság kritikus, a magas szintű eljárási szigorúság költsége indokolt.
6. A szervezetnek dokumentálnia kell az EIR életciklusának minden lépését, hogy biztosítsa a szigorú eljárások betartását és a kívánt megbízhatóság elérését.

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

SA-8(30)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.47. BIZTONSÁGTERVEZÉSI ELVEK – BIZTONSÁGOS RENDSZERMÓDOSÍTÁS

16.47. A szervezet a biztonságos rendszermódosítás biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A biztonságos rendszermódosítás biztonságtervezési elve kimondja, hogy a rendszermódosítás fenntartja az EIR biztonságát az érintettek biztonsági követelményei és kockázattűrése tekintetében. Az EIR-ek frissítése vagy módosítása a biztonságos EIR-eket nem biztonságos EIR-ekké alakíthatja. A rendszermódosítási eljárások biztosítják, hogy ha az EIR megbízhatóságának megőrzése érdekében minden rendszerváltozásnál ugyanazt a szigorúságot alkalmazzák, mint a kezdeti fejlesztésnél. Mivel a módosítások befolyásolhatják az EIR azon képességét, hogy megőrizze biztonságos állapotát, a módosítás alapos biztonsági elemzésére van szükség a bevezetés és a telepítés előtt. Ez az elv párhuzamba állítható a biztonságos fejleszthetőség elvével.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonsági követelményeket és a kockázati toleranciát az EIR-ekkel kapcsolatban.
2. A szervezetnek biztosítania kell, hogy az EIR-ek frissítése vagy módosítása ne változtassa meg a biztonságos állapotot. Ez azt jelenti, hogy a módosításoknak nem szabad negatívan befolyásolniuk az EIR-ek biztonságát.
3. A szervezetnek eljárásokat kell kidolgoznia az EIR-ek módosítására. Ezeknek az eljárásoknak biztosítaniuk kell, hogy az EIR-ek megtartsák megbízhatóságukat, és ugyanolyan szigorúan kell alkalmazni őket, mint az eredeti fejlesztés során.
4. Mivel a módosítások befolyásolhatják az EIR-ek képességét a biztonságos állapot fenntartására, a szervezetnek gondos biztonsági elemzést kell végeznie a módosításról annak végrehajtása és telepítése előtt.
5. A szervezetnek naplót kell vezetnie az EIR-ek módosításairól, hogy nyomon követhető legyen a változások hatása az EIR-ek biztonságára.

6. A szervezetnek alkalmaznia kell a biztonságos fejleszthetőség elvét, ami párhuzamos a biztonságos rendszermódosítás elvével. Ez azt jelenti, hogy az EIR-eknek képesnek kell lenniük a biztonságos fejlődésre és módosításra.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.15. Biztonsági hatásvizsgálatok

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

SA-8(31)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.48. BIZTONSÁGTERVEZÉSI ELVEK – MEGFELELŐ DOKUMENTÁCIÓ

16.48. A szervezet a megfelelő dokumentáció biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.

MAGYARÁZAT

A megfelelő dokumentáció biztonságtervezési elve kimondja, hogy az EIR-rel kapcsolatba kerülő, felelős szervezeti személyzet megfelelő dokumentációt és egyéb információkat kapjon, hogy a személyzet hozzájáruljon az EIR biztonságához, ne pedig rontsa azt. Az olyan elveknek való megfelelésre tett kísérletek ellenére, mint az emberi tényezőkre épülő biztonság és az elfogadható biztonság, az EIR-ek természetüknél fogva összetettek, és a biztonsági mechanizmusok használatának tervezési szándéka, valamint a biztonsági mechanizmusok helytelen használatának vagy rossz konfigurálásának következményei nem mindig intuitíven nyilvánvalóak. A tájékozatlan és nem kellően képzett felhasználók hibákat okozhatnak szándékosan vagy véletlenül. A dokumentáció és a képzés rendelkezésre állása segíthet hozzáértő személyzetet biztosítani, akik mindannyian kritikus szerepet játszanak az olyan elvek megvalósításában, mint a folyamatos védelem. A dokumentációt egyértelműen fogalmazva kell megírni, és olyan képzéssel kell támogatni, amely biztosítja a biztonságtudatosságot és a biztonsággal kapcsolatos felelősségek megértését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR-ekkel kapcsolatos feladatokat ellátó személyek rendelkezzenek a megfelelő dokumentációval és egyéb információkkal.
2. A szervezetnek figyelembe kell vennie, hogy az EIR-ek összetettek, és a biztonsági mechanizmusok használatának tervezett célja van, azonban a biztonsági mechanizmusok helytelen használatának vagy konfigurálásának következményei nem mindig nyilvánvalóak.
3. A szervezetnek fel kell készülnie arra, hogy a tájékozatlan és nem kellően képzett felhasználók hibákat követhetnek el, amelyek sebezhetőségeket eredményezhetnek.

4. A szervezetnek gondoskodnia kell arról, hogy a dokumentáció érthető legyen és meg legyen támogatva olyan képzéssel, amely biztonságtudatosságot és a biztonsági feladatok megértését biztosítja.
5. A szervezetnek dokumentálnia kell a folyamatokat, hogy nyomon követhető legyen a fejlődés és a változások. A dokumentum segít az érintett szervezetnek a biztonsági követelményeknek való megfelelés ellenőrzésében és a szükséges változtatások azonosításában.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.2. Biztonságtudatossági képzés
3.9. Szerepkör alapú biztonsági képzés
16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

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

SA-8(32)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.49. KÜLSŐ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI

16.49. A szervezet:

16.49.1. Szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek, és a szervezet által meghatározott védelmi intézkedéseket alkalmazzák.

16.49.2. Meghatározza és dokumentálja a szervezeti felügyelet és a szervezet felhasználóinak feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban.

16.49.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek.

MAGYARÁZAT

A külső EIR szolgáltatásokat külső szolgáltató nyújtja, az érintett szervezetnek nincs közvetlen kontrollja a szükséges intézkedések végrehajtásában, vagy az intézkedések hatékonyságának értékelésében. A szervezetek különféle módokon alakítanak ki kapcsolatokat külső szolgáltatókkal, többek között üzleti partnerségek, szerződések, szervezetek közötti megállapodások, üzletági megállapodások, licenszmegállapodások stb. révén. A külső rendszer szolgáltatások használatából eredő kockázatok kezelésének felelőssége továbbra is az azt jóváhagyó szerepkörnél marad.

A szervezeteken kívüli szolgáltatások esetében a bizalmi lánc megköveteli, hogy a fogyasztó-szolgáltató vonatkozásában minden szolgáltató megfelelő védelmet alakítson ki és biztosítson a szolgáltatásnyújtás során. Ebben a bizalmi láncban a bizalom mértéke és jellege a szervezetek és a külső szolgáltatók közötti kapcsolatok függvényében változik. Az érintett szervezetek dokumentálják a külsős kapcsolataikat, melyek monitorozhatóak. A külső rendszerszolgáltatások dokumentációja tartalmazza a kormányzati, szolgáltatói, felhasználói biztonsági feladatokat és felelősségeket, valamint a szolgáltatási szintre vonatkozó megállapodásokat. A szolgáltatási szintre vonatkozó megállapodások meghatározzák az alkalmazott rendelkezésekkel kapcsolatos elvárásokat, leírják a mérhető eredményeket, és meghatározzák az eljárást valamelyik fél követelményeknek való nem megfelelésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezetnek szerződéses kötelezettségként meg kell követelnie, hogy az általa igénybe vett EIR-ek szolgáltatásai megfeleljenek az érintett szervezet elektronikus információbiztonsági követelményeinek. Ez azt jelenti, hogy a szolgáltatási szerződésben egyértelműen rögzíteni kell a biztonsági követelményeket és a szervezet által meghatározott védelmi intézkedéseket.
2. Az érintett szervezetnek meg kell határoznia és dokumentálnia kell a szervezeti felügyelet és az érintett szervezet felhasználóinak feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban. Ez magában foglalja a felhasználói jogosultságok, a hozzáférési jogok és a biztonsági protokollok meghatározását.
3. Az érintett szervezetnek külső és belső ellenőrzési eszközökkel kell ellenőriznie, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek. Ez magában foglalja a biztonsági események naplózását, a rendszeres biztonsági ellenőrzéseket és a biztonsági protokollok betartásának ellenőrzését.
4. Az érintett szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a külső EIR szolgáltató teljesítményét, hogy biztosítsa a szerződésben meghatározott követelmények betartását. Ez magában foglalja a szolgáltatási szint-megállapodások felülvizsgálatát és a szolgáltató által biztosított biztonsági jelentések elemzését.
5. Az érintett szervezetnek biztosítania kell, hogy a külső EIR szolgáltatóval való kapcsolatát szabályozó szerződés tartalmazza a biztonsági események kezelésére vonatkozó eljárásokat, beleértve a biztonsági események jelentését, a válaszidőt és a helyreállítási terveket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.115. Külső elektronikus információs rendszerek használata
5.6. Információcsere
7.2. Üzletmenet-folytonossági terv
9.9.1. Biztonsági események kezelése
9.31. Segítségnyújtás a biztonsági események kezeléséhez
13.10. Biztonsági követelmények kiválasztása
13.11. Biztonsági követelmények testre szabása
14.11. Külső személyekhez kapcsolódó biztonsági követelmények

16.2. Erőforrások rendelkezésre állása

16.7. Beszerzések

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

3.1.3.6. Külső elektronikus információs rendszerek szolgáltatásai

ISO/IEC 27001:2023 REFERENCIA

A.5.2; A.5.4; A.5.8; A.5.14; A.5.22; A.5.23; A.8.21

NIST SP 800-53 REV.5 REFERENCIA

SA-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

16.50. KÜLSŐ INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI – KOCKÁZATELEMZÉSEK ÉS SZERVEZETI JÓVÁHAGYÁSOK

16.50. A szervezet:

16.50.1. Elvégzi a szervezeti kockázatelemzést az információbiztonsági szolgáltatások beszerzése vagy kiszervezése előtt.

16.50.2. Meghatározott személyek vagy szerepkörök jóváhagyásához köti az információbiztonsági célú szolgáltatások beszerzését vagy kiszervezését.

MAGYARÁZAT

Az információbiztonsági szolgáltatások magukban foglalják a biztonsági eszközök, például tűzfalak vagy kulcsfontosságú menedzsment szolgáltatások üzemeltetését, valamint a biztonsági események nyomon követését, elemzését és kezelését. Az értékelt kockázatok magukban foglalhatják az EIR, az ügymeneti, az üzleti alapfunkciók, a biztonság, az adatvédelem vagy ellátási lánc kockázatait.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek el kell végeznie a szervezeti kockázatértékelést. Ez magában foglalja az EIR kockázatok, az ügymeneti vagy üzleti kockázatok, a biztonsági kockázatok, az adatvédelmi kockázatok, valamint az ellátási lánc kockázatainak értékelését.
2. A kockázatértékelés során a szervezetnek figyelembe kell vennie a potenciális fenyegetéseket és sebezhetőségeket, valamint azok hatását az EIR-re.
3. A kockázatértékelés eredményei alapján a szervezetnek meg kell határoznia a szükséges információbiztonsági szolgáltatásokat.
4. Az érintett szervezetnek meg kell határoznia azokat a személyeket vagy szerepköröket, akik jóváhagyhatják az információbiztonsági szolgáltatások beszerzését vagy kiszervezését.
5. Az érintett szervezetnek biztosítania kell, hogy a jóváhagyott személyek vagy szerepkörök megfelelően képzettek és felkészültek az információbiztonsági szolgáltatások beszerzésének vagy kiszervezésének jóváhagyására.
6. A szervezetnek dokumentálnia kell az információbiztonsági szolgáltatások beszerzését vagy kiszervezését, beleértve a jóváhagyásokat és a kockázatértékelés eredményeit.

7. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kockázatértékelést és a jóváhagyási folyamatot, hogy biztosítsa az EIR védelmét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.11. Engedélyezés

15.4. Kockázatértékelés

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

SA-9(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.51. KÜLSŐ INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI – FUNKCIÓK, PORTOK, PROTOKOLLOK ÉS SZOLGÁLTATÁSOK AZONOSÍTÁSA

16.51. A szervezet megköveteli a szolgáltatóktól, hogy azonosítsák az általuk nyújtott rendszerszolgáltatásokhoz szükséges funkciókat, portokat, protokollokat és szolgáltatásokat.

MAGYARÁZAT

A külső szolgáltatóktól származó, az ilyen szolgáltatások nyújtása során használt konkrét funkciókkal, portokkal, protokollokkal és szolgáltatásokkal kapcsolatos információk hasznosak lehetnek, ha meg kell érteni az egyes funkciók és szolgáltatások korlátozásával vagy bizonyos portok és protokollok blokkolásával járó kompromisszumokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell venni a kapcsolatot a szolgáltatókkal, és tájékoztatást kell kérniük az általuk nyújtott EIR-szolgáltatásokhoz szükséges funkciókról, portokról, protokollokról és szolgáltatásokról.
2. A szervezetnek meg kell határoznia, hogy mely funkciók, portok, protokollok és szolgáltatások kritikusak az EIR működése szempontjából. Ezt követően az érintett szervezetnek meg kell vizsgálnia, hogy melyek azok a funkciók, portok, protokollok és szolgáltatások, amelyeket korlátozni vagy blokkolni kell a kiberbiztonsági kockázatok csökkentése érdekében.
3. A szervezetnek dokumentumot kell vezetnie a szolgáltatóktól kapott információkról, és rendszeresen felül kell vizsgálnia ezeket a dokumentumokat, hogy biztosítsa az EIR kiberbiztonsági követelményeinek megfelelő működést.
4. A szervezetnek biztosítania kell, hogy a szolgáltatók is megfelelnek ezeknek a követelményeknek, és rendszeresen ellenőriznie kell a szolgáltatók által nyújtott információkat.
5. A szervezetnek folyamatosan frissítenie kell a kiberbiztonsági stratégiáját és szabályzatát, hogy megfeleljen a változó kiberbiztonsági környezetnek és fenyegetéseknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.23. Konfigurációs beállítások

6.26. Legszűkebb funkcionalitás

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-9(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a külső rendszer szolgáltatások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

16.52. KÜLSŐ INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI – MEGBÍZHATÓ KAPCSOLAT KIALAKÍTÁSA ÉS FENNTARTÁSA A SZOLGÁLTATÓKKAL

16.52. A szervezet megbízható kapcsolatokat épít ki és tart fenn külső szolgáltatókkal, a meghatározott biztonsági követelmények alapján.

MAGYARÁZAT

Az érintett szervezetek és a külső szolgáltatók közötti bizalmi kapcsolatok azt tükrözik, hogy mennyire bíznak abban, hogy a külső szolgáltatások igénybevételéből eredő kockázat elfogadható szinten van. A bizalmi kapcsolatok segíthetnek a szervezeteknek abban, hogy nagyobb mértékben bízzanak abban, hogy a szolgáltatók megfelelő védelmet nyújtanak az általuk biztosított szolgáltatásokhoz, és hasznosak lehetnek a biztonsági események elhárításakor vagy a frissítések vagy elavulás tervezésekor is. A bizalmi kapcsolatok bonyolultak lehetnek a fogyasztó és a szolgáltató közötti interakciókban részt vevő szervezetek potenciálisan nagy száma, az alárendelt kapcsolatok és bizalmi szintek, valamint a felek közötti interakciók típusai miatt. Bizonyos esetekben a bizalom mértéke azon alapul, hogy a szervezetek milyen szintű ellenőrzést tudnak gyakorolni a külső szolgáltatókra a szolgáltatás, az információ védelméhez szükséges intézkedések tekintetében, valamint a bevezetett ellenőrzések hatékonyságára vonatkozó bizonyítékokon. Az ellenőrzés szintjét a szerződések vagy szolgáltatási szintű megállapodások feltételei határozzák meg.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonsági követelményeket, amelyek alapján a külső szolgáltatókkal való kapcsolatot építi és tartja fenn. Ezek a követelmények tartalmazhatják az adatvédelmi és információbiztonsági előírásokat, a szolgáltatás minőségére vonatkozó elvárásokat, stb.
2. A szervezetnek ki kell választania a megfelelő külső szolgáltatókat, akik képesek megfelelni ezeknek a követelményeknek. Ez magában foglalhatja a szolgáltatók kiválasztását, értékelését és szerződéses megállapodásokat.

3. A szervezetnek meg kell kötnie a szerződéseket vagy szolgáltatási szintű megállapodásokat a kiválasztott szolgáltatókkal. Ezeknek a dokumentumoknak tartalmazniuk kell a biztonsági követelményeket, és meghatározzák az érintett szervezet és a szolgáltató közötti kapcsolatot.
4. A szervezetnek rendszeresen ellenőriznie kell a szolgáltatók teljesítményét és biztonsági állapotát. Ez magában foglalhatja a napló elemzését, a biztonsági események kezelését, és a szolgáltatók által bevezetett biztonsági intézkedések értékelését.
5. A szervezetnek folyamatosan karban kell tartania és fejlesztenie kell a kapcsolatot a szolgáltatókkal. Ez magában foglalhatja a rendszeres kommunikációt, a biztonsági követelmények frissítését, és a szolgáltatók teljesítményének értékelését.
6. A szervezetnek fel kell készülnie arra, hogy reagáljon a potenciális biztonsági eseményekre, és szükség esetén módosítsa a szolgáltatókkal való kapcsolatot. Ez magában foglalhatja a biztonsági eseménykezelési tervek kidolgozását, a szolgáltatókkal való kommunikációt a biztonsági eseményekről, és a szükséges változtatások végrehajtását az EIR-ben.

Kapcsolódó intézkedések

19.2. Ellátási láncra vonatkozó kockázatkezelési szabályzat

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.23

NIST SP 800-53 rev.5 referencia

SA-9(3)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az az elfogadható megbízható kapcsolatok, meghatározó biztonsági és adatvédelmi követelmények, tulajdonságok, tényezők vagy feltételek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.53. KÜLSŐ INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI – ÖSSZHANGBAN LÉVŐ ÉRDEKEK

16.53. A szervezet meghatározott intézkedéseket hajt végre annak érdekében, hogy ellenőrizze, hogy a külső szolgáltatók érdekei sértik-e szervezeti érdeket.

MAGYARÁZAT

A szervezetek egyre gyakrabban vesznek igénybe külső szolgáltatók általi szolgálatatásokat így előfordulhat, hogy a szolgáltatók érdekei eltérnek a szervezeti érdekektől. Ilyen helyzetekben a szükséges technikai, irányítási vagy működési intézkedések egyszerű megléte nem feltétlenül elegendő, ha az ezeket az intézkedéseket végrehajtó és kezelő szolgáltatók nem az igénybevevő szervezetek érdekeivel összhangban működnek. A szervezetek által az ilyen aggályok kezelése érdekében hozott intézkedések közé tartozik a háttérellenőrzés megkövetelése a kiválasztott szolgáltató személyzetéről; a tulajdonosi nyilvántartások vizsgálata; kizárólag megbízható szolgáltatók alkalmazása, például olyan szolgáltatók, amelyekkel a szervezeteknek már volt sikeres bizalmi kapcsolatuk; és rutinszerű, rendszeres, valamint nem tervezett látogatások elvégzése is lehetséges a szolgáltató létesítményeiben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a külső szolgáltatókat, amelyekkel kapcsolatban fennáll a kockázat, hogy érdekeik ellentétesek lehetnek a szervezet érdekeivel.
2. A szervezetnek háttérinformációkat kell gyűjtenie a kiválasztott szolgáltatók személyzetéről. Ez magában foglalhatja a munkavállalók korábbi munkahelyeinek, végzettségének, bűnügyi előéletének stb. ellenőrzését.
3. A szervezetnek meg kell vizsgálnia a szolgáltató tulajdonosi adatait, hogy meggyőződjön arról, hogy nincsenek-e összeférhetetlenségek vagy potenciális érdekellentétek.
4. A szervezetnek csak megbízható szolgáltatókkal kell szerződnie. Ez lehetnek olyan szolgáltatók, amelyekkel a szervezetnek már van sikeres bizalmi kapcsolata.
5. A szervezetnek rendszeres, időszakos, előre be nem jelentett látogatásokat kell tennie a szolgáltató létesítményeiben. Ezek a látogatások lehetőséget adnak a szervezetnek arra, hogy

ellenőrizze, hogy a szolgáltató megfelelően működik-e, és hogy az EIR-jei, valamint azok környezete megfelel-e a szervezet biztonsági követelményeinek.

6. Az érintett szervezetnek naplót kell vezetnie minden ellenőrzésről és látogatásról, hogy nyomon követhesse a szolgáltatók teljesítményét és biztonsági állapotát. Ez a napló segíthet az érintett szervezetnek a jövőbeni döntéshozatalban és a kockázatkezelésben.

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

SA-9(4)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a külső szolgáltatók illetve a tevékenységek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.54. KÜLSŐ INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI – FELDOLGOZÁS, TÁROLÁS ÉS SZOLGÁLTATÁSI HELYSZÍN

16.54. A szervezet a meghatározott helyszínekre korlátozza az információ feldolgozásának helyét, valamint az információk vagy adatok elhelyezését, a szervezet által meghatározott követelmények és feltételek alapján.

MAGYARÁZAT

Az információfeldolgozás, az információ- és adattárolás vagy a rendszerszolgáltatások helye közvetlen hatással lehet a szervezetek azon képességére, hogy sikeresen végrehajtsák ügymeneti és üzleti funkcióikat. A hatás akkor jelentkezik, ha külső szolgáltatók felügyelik a feldolgozás, a tárolás vagy a szolgáltatások helyét. A külső szolgáltatók által a feldolgozás, a tárolás vagy a szolgáltatások helyének kiválasztásához használt kritériumok eltérhetnek az érintett szervezetek által használt kritériumoktól. A szervezetek például kívánhatják, hogy az adatok vagy információk tárolási helyeit bizonyos helyszínekre korlátozzák, hogy elősegítsék az információbiztonsági események vagy jogsértések esetén az azokra való reagálást. Az biztonsági eseményreagálási tevékenységeket, beleértve a törvényszéki elemzéseket és az utólagos vizsgálatokat is, hátrányosan befolyásolhatják a feldolgozás és tárolás helyszínein és/vagy a rendszerszolgáltatások kiindulópontjainak helyszínein érvényesülő jogszabályok, irányelvek vagy protokollok.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a helyszíneket, ahol az információfeldolgozás, az információk és adatok tárolása, valamint az EIR szolgáltatások megengedettek.
2. A szervezetnek meg kell határoznia a követelményeket és feltételeket, amelyek alapján ezeket a helyszíneket kiválasztja. Ezek a követelmények magukban foglalhatják például a biztonsági előírásokat, a jogi követelményeket, vagy az adatvédelmi szabályokat.
3. A szervezetnek biztosítania kell, hogy az EIR szolgáltatások csak a meghatározott helyszíneken legyenek elérhetőek, és hogy az információk és adatok csak ezeken a helyszíneken legyenek tárolva.

4. A szervezetnek ellenőriznie kell, hogy az EIR szolgáltatások, az információfeldolgozás és az adattárolás valóban csak a meghatározott helyszíneken történik-e. Ehhez naplókat kell vezetnie, amelyekben rögzíti az EIR szolgáltatások használatát, az információfeldolgozást és az adattárolást.

5. A szervezetnek rendszeresen felül kell vizsgálnia a helyszínek kiválasztásának követelményeit és feltételeit, és szükség esetén módosítania kell azokat, hogy megfeleljen a változó körülményeknek és követelményeknek.

6. A szervezetnek biztosítania kell, hogy a helyszínek kiválasztásának követelményei és feltételei, valamint az EIR szolgáltatások, az információfeldolgozás és az adattárolás helyszínei összhangban legyenek a szervezet kiberbiztonsági politikájával és stratégiájával.

Kapcsolódó intézkedések

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

19.8. Rendszerelemek és kapcsolódó adatok eredetisége

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

SA-9(5)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az helyszínek illetve a követelmények vagy feltételek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.55. KÜLSŐ INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI – FELÜGYELT KRIPTOGRÁFIAI KULCSOK

16.55. A szervezet kizárólagos ellenőrzést gyakorol a külső rendszerekben tárolt, vagy külső rendszerekbe továbbított titkos adatokhoz tartozó kriptográfiai kulcsok felett.

MAGYARÁZAT

A kriptográfiai kulcsok kizárólagos ellenőrzésének fenntartása egy külső rendszerben megakadályozza, hogy a szervezeti adatokat a külső rendszer munkatársai visszafejtsék. A kriptográfiai kulcsok szervezeti ellenőrzése megvalósítható a szervezeten belüli adatok titkosításával és visszafejtésével, amikor az adatokat a külső rendszerbe küldik és onnan fogadják, vagy egy olyan elem alkalmazásával, amely lehetővé teszi, hogy a titkosítási és visszafejtési funkciók a külső rendszerben helyi szinten legyenek, de kizárólagos szervezeti hozzáférést biztosít a titkosítási kulcsokhoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a külső EIR-ben tárolt vagy külső rendszerbe továbbított titkos adatokhoz tartozó kriptográfiai kulcsok felett kizárólagos ellenőrzést gyakoroljon. Ez megakadályozza, hogy a külső rendszer munkatársai dekódolják a szervezeti adatokat.
2. A szervezetnek implementálnia kell a kriptográfiai kulcsok ellenőrzését úgy, hogy az adatokat a szervezetben titkosítja és dekódolja, amint azokat a külső rendszerbe küldi és onnan fogadja.
3. Alternatív megoldásként az érintett szervezet használhat olyan elemet is, amely lehetővé teszi a titkosítási és dekódolási funkciók helyi használatát a külső rendszerben, de kizárólagos hozzáférést biztosít a titkosítási kulcsokhoz.
4. A szervezetnek naplót kell vezetnie a kriptográfiai kulcsok használatáról, hogy nyomon követhető legyen, ki, mikor és milyen célból használta azokat. Ez segít a szabálytalanságok azonosításában és a biztonsági események megelőzésében.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kriptográfiai kulcsok kezelésére vonatkozó szabályait és eljárásait, hogy biztosítsa azok hatékonyságát és relevanciáját a változó kiberbiztonsági környezetben.

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

SA-9(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.56. KÜLSŐ INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI – SÉRTETLENSÉG FELÜGYELETE

16.56. A EIR képes arra, hogy ellenőrizze a külső rendszerben található információ sértetlenségét.

MAGYARÁZAT

Az érintett szervezet információinak külső rendszeren történő tárolása megnehezíti a külső rendszeren tárolt adatok sértetlenségének monitorozását, ezért az EIR-nek képesnek kell lennie a külső rendszeren tárolt információk integritását a külső rendszerből történő átvitel nélkül ellenőriznie és validálnia, valamint biztosíatani az átáthatóságot. Ez a képesség különösen fontos, mivel az adatok sértetlensége alapvető a biztonságos működéshez. Az adatok sértetlenségének ellenőrzése azt jelenti, hogy az érintett szervezet képes megbizonyosodni arról, hogy az adatok nem változtak meg, vagy nem sérültek meg a külső információs rendszerben. Ez a képesség lehetővé teszi a szervezet számára, hogy gyorsan észlelje és reagáljon a potenciális, adatok integritását sértő biztonsági eseményekre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, milyen információkat tárol külső rendszerben. Ez magában foglalhatja a személyes adatokat, üzleti információkat, vagy bármilyen más érzékeny adatot.
2. A szervezetnek be kell vezetnie egy olyan eljárást, amely meghatározza, hogyan ellenőrzi az információ sértetlenségét a külső rendszerben. Ez magában foglalhatja a naplózást, a hozzáférés-felügyeletet és a rendszeres ellenőrzéseket.
3. A szervezetnek implementálnia kell a megfelelő technológiákat és eszközöket, amelyek lehetővé teszik számára, hogy ellenőrizze az információ sértetlenségét a külső rendszerben. Ez magában foglalhatja a titkosítást, a digitális aláírásokat és az integritás-ellenőrző algoritmusokat.
4. A szervezetnek rendszeresen ellenőriznie kell az információ sértetlenségét a külső rendszerben. Ez magában foglalhatja a naplók áttekintését, a hozzáférési naplók ellenőrzését és az integritás-ellenőrző algoritmusok futtatását.

5. A szervezetnek dokumentálnia kell az ellenőrzési folyamatot, és biztosítania kell, hogy a dokumentáció naprakész és pontos. Ez magában foglalhatja a naplók, jelentések és egyéb releváns információk tárolását.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az ellenőrzési szabályzatát és eljárásait, hogy biztosítsa azok hatékonyságát és relevanciáját.

Kapcsolódó intézkedések

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

SA-9(7)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.57. KÜLSŐ INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI – FELDOLGOZÁSI ÉS TÁROLÁSI HELYSZÍN – MAGYARORSZÁG JOGHATÓSÁGA

16.57. A szervezet az információfeldolgozást és az adattárolást olyan helyszínekre korlátozza, amelyek Magyarország határain belül találhatók.

MAGYARÁZAT

Az információfeldolgozás és az adattárolás földrajzi helye közvetlen hatással lehet az érintett szervezet ügymeneti és üzleti céljainak megvalósulására. A bizalmas információk és EIR-ek kompromittálása súlyos, akár katasztrofális hatással lehet az érintett szervezetre és annak környezetére, más szervezetekre vagy akár a nemzetre nézve is. A magasabb biztonsági besorolás alá tartozó információk feldolgozásának és tárolásának korlátozása olyan helyszínekre, amelyek Magyarország joghatósági határán belül találhatók, nagyobb kontrollt biztosít az ilyen feldolgozás és tárolás felett.

Az érintett szervezetnek biztosítania kell, hogy az EIR-ek és az adatok tárolása és feldolgozása csak Magyarország területén található helyszíneken történjen. Ez magában foglalja az adatok fizikai tárolását, az adatfeldolgozást, valamint az adatokhoz való hozzáférést és azok kezelését is. Az ilyen korlátozások célja, hogy minimalizálják a kiberbiztonsági kockázatokat és megvédjék az érintett szervezet értékes adatait.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie, hogy mely információfeldolgozások és adattárolások történnek jelenleg olyan helyszíneken, amelyek nem találhatók Magyarország határain belül.
2. A szervezetnek meg kell határoznia azokat a magasabb biztonsági besorolású EIR-eket, amelyeket át kell helyezni Magyarország területére.
3. A szervezetnek ki kell dolgoznia egy tervet az EIR-ek áthelyezésére, beleértve a szükséges infrastruktúrát, erőforrásokat és időkeretet.
4. A szervezetnek végre kell hajtania az áthelyezési tervet, és gondoskodnia kell arról, hogy az EIR-ek áthelyezése ne zavarja a szervezet működését.

5. A szervezetnek dokumentálnia kell az áthelyezési folyamatot, hogy bizonyítani tudja a megfelelőséget és nyomon követhető legyen az áthelyezés.
6. A szervezetnek rendszeresen ellenőriznie kell, hogy az információfeldolgozás és adattárolás továbbra is a Magyarország határain belüli helyszíneken történik-e, és dokumentálnia kell az ellenőrzések eredményeit.
7. A szervezetnek biztosítania kell, hogy a jövőbeni magas biztonsági besorolású EIR fejlesztések és változások is megfelelnek ennek a követelménynek, és naplózni kell ezeket a változásokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció
19.8. Rendszerelemek és kapcsolódó adatok eredetisége

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

SA-9(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.58. FEJLESZTŐI VÁLTOZÁSKÖVETÉS

16.58. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.58.1. Alkalmazzon konfigurációkezelési folyamatokat az EIR, rendszerelem vagy szolgáltatás tervezése, fejlesztése, bevezetése, üzemeltetése vagy kivonása (teljes életciklusa) során.

16.58.2. Dokumentálja, kezelje és ellenőrizze a szervezet által a konfigurációkezelés keretében meghatározott konfigurációs elemek változtatásait, és biztosítsa ezek sértetlenségét.

16.58.3. Csak a szervezet által jóváhagyott változtatásokat hajtsa végre az EIR-en, rendszerelemen vagy rendszerszolgáltatáson.

16.58.4. Dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait.

16.58.5. Kövesse nyomon az EIR, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit a szervezet által meghatározott személyeknek.

MAGYARÁZAT

Ez a követelmény a szervezeten belüli EIR fejlesztésekre és integrációkra egyaránt vonatkozik. A szervezet a biztonsági követelmények minőségének és teljességének bizonyítékául a fejlesztők által leadott konfiguráció-kezelést veszi figyelembe. Az intézkedések közé tartozik például az illetéktelen módosítás vagy megsemmisítés elleni védelme azon információknak melyek a rendszer hardvereinek, szoftvereknek és firmwarek-nek kialakításához elengedhetetlenek. Az EIR, rendszerelem vagy a szolgáltatás változásai során a sértetlenség védelme, a változtatások dokumentálása a rendszerfejlesztés teljes életciklusa alatt szükséges az engedélyezett módosítások nyomon követéséhez és az illetéktelen módosítások megelőzéséhez. A vonatkozó konfigurációs elemek, melyek a konfigurációkezelési szabályok alá tartoznak: a rendszer modell; a funkcionális, magas szintű és alacsony szintű rendszertervek; egyéb tervhez kapcsolódó információk; rendszer bevezetési dokumentációk; forráskód és hardver leírások; a gépi kód futtatott változata; eszközök a biztonsági szempontból releváns hardverleírások és a szoftver/firmware forráskód új verzióinak előző verziókkal való összehasonlításához; tesztelő eszközök és dokumentációk. A szervezet igényeitől és a meglévő szerződéses kapcsolatok jellegétől függően a fejlesztők konfiguráció-kezelés támogatást nyújthatnak az életciklus működési és karbantartási fázisaiban is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy alkalmazzon konfigurációkezelési folyamatokat az EIR teljes életciklusa során. Ez magában foglalja a tervezést, fejlesztést, bevezetést, üzemeltetést és kivonást.
2. A szervezetnek biztosítania kell, hogy a fejlesztő dokumentálja, kezelje és ellenőrizze a konfigurációs elemek változásait, amelyeket a szervezet a konfigurációkezelés keretében határoz meg. Emellett biztosítania kell ezeknek az elemeknek a sértetlenségét.
3. A szervezetnek csak azokat a változtatásokat kell engedélyeznie, amelyeket előzetesen jóváhagyott. Ez azt jelenti, hogy a fejlesztőnek nem megengedett saját belátásuk szerint módosítani az EIR-t, rendszerelemet vagy rendszerszolgáltatást.
4. A szervezetnek meg kell kérnie a fejlesztőt, hogy dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait. Ez segít nyomon követni, hogy milyen változtatások történtek, és hogyan befolyásolják ezek a változtatások az EIR biztonságát.
5. A szervezetnek nyomon kell követnie az EIR, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait. A fejlesztőnek jelentenie kell ezeket az észrevételeket a szervezet által meghatározott személyeknek.
6. A szervezetnek dokumentálnia kell a fent említett tevékenységeket, hogy biztosítsa a folyamatok átláthatóságát és ellenőrizhetőségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció
6.7. A konfigurációváltozások felügyelete (változáskezelés)
6.15. Biztonsági hatásvizsgálatok
6.26. Legszűkebb funkcionalitás
6.45. Konfigurációkezelési terv
16.7. Beszerzések
16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció
16.16. Biztonságtervezési elvek
16.76.1. Fejlesztési folyamat, szabványok és eszközök
18.2. Hibajavítás

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

3.3.3.4. Fejlesztői változáskövetés

ISO/IEC 27001:2023 REFERENCIA

A.8.9; A.8.28; A.8.30; A.8.32

NIST SP 800-53 REV.5 REFERENCIA

SA-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

16.59. Fejlesztői konfigurációkezelés – Szoftver és firmware sértetlenségének ellenőrzése

16.59. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a szervezet részére tegye lehetővé a szoftver- és firmware-elemek sértetlenségének ellenőrzését.

Magyarázat

A szoftver- és firmware-elemek sértetlenségének ellenőrzése lehetővé teszi az érintett szervezet számára, hogy a fejlesztő által biztosított eszközök, technikák és mechanizmusok segítségével jogosulatlan változtatásokat keressen a szoftver- és firmware-elemekben. A sértetlenség-ellenőrző mechanizmusok kimutathatják a szoftver- és firmware-elemek hamisítását is. Az érintett szervezet ellenőrzi a szoftver- és firmware-elemek sértetlenségét, például a fejlesztők által biztosított biztonságos egyirányú hash-ek segítségével. A szállított szoftver- és firmware-elemek magukban foglalják az ilyen elemekhez tartozó frissítéseket is.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy tegye lehetővé a szoftver- és firmware-elemek sértetlenségének ellenőrzését.
2. A szervezetnek biztosítania kell, hogy a fejlesztő által biztosított eszközök, technikák és mechanizmusok segítségével képes észlelni a szoftver- és firmware-elemekben történt jogosulatlan változásokat.
3. A szervezetnek gondoskodnia kell arról, hogy az integritás-ellenőrző mechanizmusok képesek legyenek felismerni a szoftver- és firmware-elemek hamisítását is.
4. A szervezetnek ellenőriznie kell a szoftver- és firmware-elemek integritását, például a fejlesztő által biztosított biztonságos egyirányú hash-ek segítségével.
5. A szervezetnek biztosítania kell, hogy a szállított szoftver- és firmware-elemek magukban foglalják a hozzátartozó frissítéseket is.
6. A szervezetnek dokumentálnia kell a szoftver- és firmware-elemek integritásának ellenőrzését és a változásokat.

Kapcsolódó intézkedések

18.42. Szoftver- és információsértetlenség

19.23. Rendszerelem 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

SA-10(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.60. Fejlesztői konfigurációkezelés – Alternatív konfigurációkezelési folyamatok

16.60. A szervezet alternatív konfigurációkezelési folyamatot biztosít a szervezeti munkavállalók bevonásával, amennyiben a szervezet nem rendelkezik dedikált fejlesztői konfigurációkezelő csoporttal.

Magyarázat

Az alternatív konfigurációkezelési folyamatokra akkor lehet szükség, ha az érintett szervezetek kereskedelemben kapható információs technológiai termékeket használnak. Az alternatív konfigurációkezelési folyamatok magukban foglalják a szervezet munkavállalóit, akik áttekintik és jóváhagyják az EIR, a rendszerelemek, rendszerszolgáltatások tervezett változásait, valamint biztonsági és adatvédelmi hatáselemzéseket végeznek az EIR, az elemek vagy a szolgáltatások változtatásainak bevezetése előtt.

A követelmény alkalmazásának lépései

1. A szervezetnek létre kell hoznia egy folyamatot, amely lehetővé teszi a munkavállalók számára, hogy javaslatokat tegyenek az EIR, az EIR-elemek és a rendszerszolgáltatások változtatásaira. Ez magában foglalhatja a változtatások indoklását, a várható hatásokat és a végrehajtás tervezett időpontját.
2. A szervezetnek meg kell határoznia azokat a munkavállalókat, akik részt vesznek az alternatív konfigurációkezelési folyamatban. Ezeknek a munkavállalóknak meg kell érteniük a konfigurációkezelési folyamatot és annak fontosságát az EIR biztonságában.
3. A javasolt változtatásokat a szervezetnek felül kell vizsgálnia és jóvá kell hagynia. Ez magában foglalhatja a biztonsági és adatvédelmi hatáselemzést, hogy bizonyosságot nyerjen, hogy a változások nem veszélyeztetik az EIR biztonságát vagy a felhasználók személyes adatait.
4. A szervezet általi változások jóváhagyását követően, a munkavállalóknak meg kell tervezniük a változások végrehajtását. Ez magában foglalhatja a változások tesztelését egy izolált környezetben, hogy minimalizálják a hibák hatását az EIR-re.

5. A szervezetnek dokumentálnia kell a konfigurációkezelési folyamatot, beleértve a javasolt és végrehajtott változásokat, valamint a változások jóváhagyásának dátumát és időpontját.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az alternatív konfigurációkezelési folyamatot, hogy biztosítsa annak hatékonyságát és relevanciáját az EIR aktuális állapotához képest.

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

SA-10(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.61. Fejlesztői konfigurációkezelés – Hardver sértetlenségének ellenőrzése

16.61. A szervezet megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője lehetővé tegye a hardverelemek sértetlenségének ellenőrzését.

Magyarázat

A hardverelemek sértetlenségének ellenőrzése lehetővé teszi az érintett szervezet számára, hogy azonosítsák a jogosulatlan változtatásokat a hardverelemeken, a fejlesztő által biztosított eszközök, technikák, módszerek és mechanizmusok segítségével. Az érintett szervezet nehezen-másolható címkékkel, a fejlesztő által biztosított ellenőrizhető sorozatszámokkal, és az anti-manipulációs (anti-tampering) technológiák használatának megkövetelésével ellenőrzi a hardverelemek sértetlenségét. A szállított hardverelemek magukban foglalják a hardverelemekhez és a firmware-hez tartozó frissítéseket is.

A hardverelemek sértetlenségének ellenőrzése során a szervezet által vezetett napló segítségével azonosíthatók a nem engedélyezett változtatások, és ezáltal biztosítható az EIR, rendszerelem vagy rendszerszolgáltatás biztonsága.

A követelmény alkalmazásának lépései

1. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy biztosítsa a hardverelemek sértetlenségének ellenőrzését lehetővé tevő eszközöket.
2. A szervezetnek meg kell határoznia és implementálnia kell a hardverelemek sértetlenségének ellenőrzésére szolgáló eszközöket, technikákat, módszereket és mechanizmusokat, amelyeket a fejlesztő biztosít.
3. A szervezetnek ellenőriznie kell a hardverelemek sértetlenségét olyan módszerekkel, mint a nehezen másolható címkék, a fejlesztő által biztosított ellenőrizhető sorozatszámok, és az anti-tamper technológiák használatának követelménye.
4. A szervezetnek naplóznia kell minden hardverelem ellenőrzését, hogy nyomon követhető legyen minden változás és frissítés.

5. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a hardverelemek sértetlenségének ellenőrzési folyamatát, hogy biztosítsa a folyamat hatékonyságát és a hardverelemek biztonságát."

KAPCSOLÓDÓ INTÉZKEDÉSEK

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

SA-10(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.62. Fejlesztői konfigurációkezelés – Megbízható generálás

16.62. A szervezet megköveteli az EIR, rendszerelem és rendszerszolgáltatás fejlesztőjétől, hogy alkalmazzon eszközöket a biztonság szempontjából fontos hardver specifikációk, forráskódok és objektumkódok újonnan generált verzióinak korábbi verziókkal való összehasonlítására.

Magyarázat

Az érintett szervezet elvárja az EIR, rendszerelem és rendszerszolgáltatás fejlesztőjétől, hogy a fejlesztés során a hardver, szoftver és firmware elemek közötti hitelesített változásokat kezelje. A hangsúly a fejlesztő konfigurációs menedzsment folyamatának hatékonyságán van, hogy biztosítsa: a biztonság szempontjából fontos hardver leírások, forráskódok és objektumkódok újonnan generált verziói továbbra is érvényesítik az EIR, rendszerelem vagy rendszerszolgáltatás biztonsági szabályzatát. Ezzel szemben az Szoftver és firmver sértetlenségének ellenőrzésére és a Hardver sértetlenségének ellenőrzésére vonatkozó intézkedések lehetővé teszik a szervezet számára, hogy azonosítsa a hardver, szoftver és firmware elemekben történt jogosulatlan változásokat a fejlesztők által biztosított eszközök, technikák vagy mechanizmusok segítségével.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie az EIR, rendszerelem és rendszerszolgáltatás fejlesztőjétől, hogy alkalmazzon eszközöket a biztonság szempontjából fontos hardver specifikációk, forráskódok és objektumkódok újonnan generált verzióinak korábbi verziókkal való összehasonlítására.
2. A szervezetnek ellenőriznie kell, hogy a fejlesztő által alkalmazott eszközök, technikák vagy mechanizmusok képesek-e észlelni a nem engedélyezett változásokat a hardver, szoftver és firmware elemekben.
3. A szervezetnek naplózást kell alkalmaznia annak érdekében, hogy nyomon követhesse a változásokat és ellenőrizhesse, hogy a fejlesztő betartja-e a követelményeket.

4. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a fejlesztő által alkalmazott eszközök, technikák és mechanizmusok hatékonyságát, hogy biztosítsa a biztonsági 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

SA-10(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.63. Fejlesztői konfigurációkezelés – Verziókezelési sértetlenség feltérképezése

16.63. A szervezet biztosítja a biztonság szempontjából releváns hardver, szoftver és firmware aktuális verzióját leíró törzsadatok és az aktuális verzió adatainak helyszíni másolata közötti összefüggés sértetlenségét.

Magyarázat

A verziókezelési sértetlenség feltérképezése a hardver-, szoftver- és firmware-elemek változásaira irányul mind a kezdeti fejlesztés, mind a rendszerfejlesztési életciklus frissítései során. A biztonság szempontjából releváns hardver, szoftver és firmware törzsadatok és az operatív környezetekben található helyszíni másolatok (mesterpéldányok) közötti összefüggés sértetlenségének fenntartása elengedhetetlen az érintett szervezet olyan EIR-jeinek rendelkezésre állásának biztosításához, amelyek kritikus ügymeneti és üzleti funkciókat támogatnak.

A követelmény alkalmazásának lépései

1. A szervezetnek létre kell hoznia egy törzsadatokat tartalmazó adatbázist, amely leírja a biztonság szempontjából releváns hardver, szoftver és firmware aktuális verzióit.
2. Az érintett szervezetnek biztosítania kell, hogy a törzsadatokat rendszeresen frissítik, és hogy ezek a frissítések megfelelnek a helyszínen található másolatoknak. Ez magában foglalja a hardver, szoftver és firmware frissítéseit és módosításait.
3. A szervezetnek implementálnia kell egy mechanizmust, amely képes nyomon követni és naplózni az összes változást és frissítést, amelyeket a törzsadatokban és a helyszíni másolatokban végeznek.
4. A szervezetnek biztosítania kell, hogy az előző pontban említett mechanizmus rendszeresen ellenőrzi és összehasonlítja a törzsadatokat és a helyszíni másolatokat, hogy biztosítsa azok összefüggésének sértetlenségét.
5. A szervezetnek be kell vezetnie egy biztonsági protokollt, amely meghatározza, hogyan kezelik a törzsadatokat és a helyszíni másolatokat, beleértve a hozzáférési jogosultságokat, a változások jóváhagyását és a naplózást.

6. A szervezetnek rendszeresen ellenőriznie kell a naplókat, hogy azonosítsa és kezelje a lehetséges biztonsági problémákat, és biztosítsa a törzsadatok és a helyszíni másolatok közötti összefüggés sértetlenségét.

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

SA-10(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.64. Fejlesztői konfigurációkezelés – Megbízható terjesztés

16.64. A szervezet előírja az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjének, hogy olyan eljárásokat hajtson végre, amelyek biztosítják, hogy a szervezet számára szétosztott biztonsági szempontból releváns hardver-, szoftver- és firmware-frissítések pontosan megegyeznek a mesterpéldányok által meghatározottakkal.

Magyarázat

A biztonsági szempontból releváns hardver-, szoftver- és firmware-frissítéseknek megbízható terjesztése segít annak elérésben, hogy a frissítések megfeleljenek a mesterpéldányoknak. Ez biztosítja, hogy a frissítések nem változtak meg vagy nem kerültek módosításra a terjesztés során.

Az EIR fejlesztőjének eljárásokat kell végrehajtania, amelyek ellenőrzik a frissítések integritását és hitelességét. Ez magában foglalhatja a frissítések digitális aláírását, a hash-összegek ellenőrzését, a naplók ellenőrzését és más biztonsági intézkedéseket.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia és dokumentálnia azokat az eljárásokat, amelyeket az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjének végre kell hajtania a biztonsági szempontból releváns hardver-, szoftver- és firmware-frissítések terjesztése során.
2. A szervezetnek biztosítania kell, hogy a fejlesztő rendelkezik a mesterpéldányokkal, és hogy ezeket a példányokat használják a frissítések összehasonlítására.
3. A szervezetnek ellenőriznie kell, hogy a fejlesztő megfelelően hajtja-e végre az eljárásokat, és hogy a frissítések pontosan megegyeznek-e a mesterpéldányokkal.
4. A szervezetnek dokumentálnia kell az összes ellenőrzést és az eredményeket, hogy bizonyíték legyen a megfelelőségről.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az eljárásokat, hogy biztosítsa a folyamatos megfelelőséget és a biztonsági szempontból releváns frissítések pontos szétosztását.

6. A szervezetnek biztosítania kell, hogy a fejlesztő megfelelően képzett és felkészült legyen az eljárások végrehajtására, és hogy rendelkezzen a szükséges eszközökkel és erőforrásokkal.

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

SA-10(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.65. Fejlesztői konfigurációkezelés – Biztonsági felelősök

16.65. A szervezet biztosítja a szervezet által meghatározott biztonsági felelősök bevonását a meghatározott konfigurációs változások kezelési és ellenőrzési folyamatába.

Magyarázat

Az információbiztonsági és az adatvédelemi felelősök között lehetnek a rendszerbiztonsági felelősök, az érintett szervezet vezető információbiztonsági felelőse és az EIR adatvédelmi felelősei. Az információbiztonsági és adatvédelmi szakértelemmel rendelkező személyzet képviselete azért fontos, mert a rendszerkonfigurációk módosításának nem szándékos mellékhatásai lehetnek, amelyek közül néhány biztonsági vagy adatvédelmi szempontból is fontos lehet. Az ilyen változtatások korai felismerése segíthet elkerülni a nem szándékos, negatív következményeket, amelyek végső soron az EIR-ek biztonsági és adatvédelmi helyzetét befolyásolhatják. Ebben a követelménypontban szereplő konfigurációváltoztatás-kezelési és ellenőrzési folyamat a szervezetek által az dokumentált, kezelt és ellenőrzött, a konfigurációkezelés keretében meghatározott konfigurációs elemek változtatásai sértetlenségérének folyamatát egészíti ki.

A követelmény alkalmazásának lépései

1. A szervezetnek először ki kell jelölnie a biztonsági felelősöket, akik részt vesznek az EIR konfigurációs változásainak kezelésében és ellenőrzésében. Ezek a személyek lehetnek rendszerbiztonsági felelősök, a szervezet felső szintű információbiztonsági felelősei, a szervezet felső szintű adatvédelmi felelősei, és az EIR adatvédelmi felelősei.
2. A szervezetnek biztosítania kell, hogy a biztonsági és adatvédelmi felelősök rendelkeznek az információbiztonsági és adatvédelmi szakértelemmel, mivel az EIR konfigurációs változásai nem szándékos mellékhatásokat okozhatnak, amelyek biztonsági vagy adatvédelmi szempontból relevánsak lehetnek.
3. A szervezetnek be kell építenie a biztonsági felelősök bevonását a konfigurációs változások kezelési és ellenőrzési folyamatába, hogy korai szakaszban észlelhessék az ilyen változásokat,

és elkerülhessék a nem szándékos, negatív következményeket, amelyek végül befolyásolhatják az EIR biztonsági és adatvédelmi helyzetét.

4. A szervezetnek a konfigurációs változások kezelési és ellenőrzési folyamatát a fejlesztői változáskövetésben meghatározott változáskezelési és ellenőrzési folyamatnak kell meghatároznia.

5. A szervezetnek dokumentálnia kell a konfigurációs változásokat, és a biztonsági felelősöknek rendszeresen ellenőrizniük kell ezeket a feljegyzéseket, hogy biztosítsák az EIR biztonságát és adatvédelmét.

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

SA-10(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági és adatvédelmi felelősök illetve a konfigurációs változásokra vonatkozó kezelési és ellenőrzési folyamatok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.66. FEJLESZTŐI BIZTONSÁGI TESZTELÉS

16.66. A szervezet az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől megköveteli, hogy:

16.66.1. Készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat.

16.66.2. Meghatározott gyakorisággal hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, illetve regressziós tesztelést, és értékelje ki a szervezet által meghatározottak szerint.

16.66.3. Dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit.

16.66.4. Vezessen be egy ellenőrizhető hibajavítási folyamatot.

16.66.5. Javítsa ki a tesztelés és értékelés során azonosított hibákat.

MAGYARÁZAT

A fejlesztői biztonsági tesztelés és értékelés megerősíti, hogy a szükséges biztonsági intézkedések helyesen vannak végrehajtva, rendeltetésszerűen működnek, érvényesítik a kívánt biztonsági és adatvédelmi irányelveket, és megfelelnek a megállapított biztonsági és adatvédelmi követelményeknek. Az EIR-ek biztonsági tulajdonságait és az személyes adatok védelmét befolyásolhatják a rendszerelemek összekapcsolása vagy az azokon végrehajtott változtatások. Az összekapcsolások vagy változások - beleértve az alkalmazások, operációs rendszerek és firmware-ek frissítését vagy cseréjét - hátrányosan befolyásolhatják a korábban bevezetett biztonsági intézkedéseket. A fejlesztés során végzett folyamatos értékelés lehetővé teszi más típusú teszteléseket és értékeléseket, amelyeket a fejlesztők a lehetséges hibák csökkentése vagy kiküszöbölése érdekében végezhetnek. Az egyedi szoftveralkalmazások tesztelése olyan megközelítéseket igényelhet, mint a kézi kódellenőrzés, a biztonsági architektúra felülvizsgálata és a behatolásvizsgálat, valamint statikus elemzés, dinamikus elemzés, bináris elemzés vagy a három elemzési megközelítés hibridje.

A fejlesztők az elemzési megközelítéseket a biztonsági eszközökkel és a fuzzinggal együtt számos eszközben és a forráskód-ellenőrzések során használhatják. A biztonsági és adatvédelmi értékelési tervek tartalmazzák a fejlesztők által tervezett konkrét tevékenységeket, beleértve a szoftver- és firmware-elemek elemzésének, tesztelésének, értékelésének és felülvizsgálatának típusait; az alkalmazandó szigor mértékét; a folyamatos tesztelés és értékelés gyakoriságát;

valamint az e folyamatok során előállított dokumentumok típusait. A tesztelés és értékelés mélysége az értékelési folyamathoz kapcsolódó szigorúságra és részletességre utal. A tesztelés és értékelés lefedettsége az értékelési folyamatba bevont eredménytermékek körére vonatkozik. A szerződések meghatározzák a biztonsági és adatvédelmi értékelési tervek elfogadási kritériumait, a hibaelhárítási folyamatokat, valamint a tervek és folyamatok gondos alkalmazásának bizonyítékát. Az értékelési tervek, bizonyítékok és dokumentáció felülvizsgálatának és védelmének módszerei arányosak az EIR biztonsági kategóriájával vagy minősítési szintjével. A szerződések meghatározhatják a dokumentáció védelmére vonatkozó követelményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy készítsenek egy biztonságértékelési tervet. Ez a terv tartalmazza a végrehajtandó tevékenységeket, beleértve az elemzések, tesztelések, értékelések és a szoftver- és firmware-elemek áttekintésének típusait; a alkalmazandó szigorúság mértékét; a folyamatos tesztelés és értékelés gyakoriságát; és a folyamatok során előállított eredménytermékek típusait.
2. A fejlesztőknek meghatározott gyakorisággal kell végrehajtaniuk egység-, integrációs-, EIR-, illetve regressziós tesztelést, és ki kell értékelniük a szervezet által meghatározottak szerint.
3. A fejlesztőknek dokumentálniuk kell, hogy végrehajtották a biztonságértékelési tervben foglaltakat, és ismertetniük kell a biztonsági tesztelés és értékelés eredményeit.
4. A szervezetnek be kell vezetnie egy ellenőrizhető hibajavítási folyamatot. Ez magában foglalja a hibák azonosítását, a javítások végrehajtását és a javítások hatékonyságának ellenőrzését.
5. A fejlesztőknek ki kell javítaniuk a tesztelés és értékelés során azonosított hibákat.
6. A szervezetnek dokumentálnia kell a folyamatot, beleértve a hibajavítási folyamatot, a tesztelési és értékelési eredményeket. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a fejlesztési folyamatot és biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.2. Biztonsági értékelések

5.14. Folyamatos felügyelet

6.15. Biztonsági hatásvizsgálatok

16.3.1. A rendszer fejlesztési életciklusa

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

18.2. Hibajavítás

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

3.3.3.5. Fejlesztői biztonsági tesztelés

ISO/IEC 27001:2023 REFERENCIA

A.8.29; A.8.30

NIST SP 800-53 REV.5 REFERENCIA

SA-11

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

16.67. Fejlesztői biztonsági tesztelés és értékelés – Statikus kódelemzés

16.67. A szervezet statikus kódelemző eszközöket alkalmaz a gyakori hibák azonosítására, valamint az elemzés eredményeinek dokumentálására.

Magyarázat

A statikus kódelemzés a biztonsági felülvizsgálatok technológiáját és módszertanát biztosítja, és magában foglalja a kód gyenge pontjainak, valamint az ismert sebezhetőségekkel rendelkező vagy elavult és nem támogatott könyvtárak vagy más kódok beépítésének ellenőrzését. A statikus kódelemzés a sebezhetőségek azonosítására és a biztonságos kódolási gyakorlatok érvényesítésére használható. Akkor a leghatékonyabb, ha a fejlesztési folyamat korai szakaszában alkalmazzák, amikor minden egyes kódváltozást automatikusan át lehet vizsgálni a lehetséges gyenge pontok szempontjából. A statikus kódelemzés egyértelmű javítási útmutatást adhat, és azonosíthatja a fejlesztők számára a javítandó hibákat. A statikus elemzés helyes végrehajtásának bizonyítéka lehet a kritikus hibatípusok összesített hibasűrűsége, annak bizonyítéka, hogy a hibákat a fejlesztők vagy a biztonsági szakemberek megvizsgálták, valamint annak bizonyítéka, hogy a hibákat orvosolták. A figyelmen kívül hagyott megállapítások nagy sűrűsége, amelyet általában falspozitív eredményeknek neveznek, az elemzési folyamat vagy az elemző eszköz lehetséges problémájára utal. Ilyen esetekben az érintett szervezetek mérlegelik a bizonyítékok érvényességét a más forrásokból származó bizonyítékokkal szemben.

A követelmény alkalmazásának lépései

1. A szervezetnek statikus kódelemző eszközöket kell bevezetnie. Ezek az eszközök segítenek a gyakori hibák azonosításában, valamint a kód gyengeségeinek és sérülékenységeinek felismerésében.
2. A szervezetnek biztosítania kell, hogy a statikus kódelemzés korai szakaszban kerüljön alkalmazásra az EIR fejlesztési folyamatában. Így minden kódváltozást automatikusan lehet vizsgálni potenciális gyengeségek szempontjából.

3. A szervezetnek dokumentálnia kell az elemzés eredményeit. Ez magában foglalja a kritikus hibatípusok összesített hibasűrűségét, a hibák fejlesztők vagy biztonsági szakemberek általi ellenőrzésének bizonyítékát, valamint a hibák orvoslásának bizonyítékát.
4. A szervezetnek figyelemmel kell kísérnie a figyelmen kívül hagyott eredmények, azaz a falspozitív eredmények sűrűségét. Ha ez a sűrűség magas, az a statikus kódelemzési folyamat vagy az elemző eszköz hibás lehet.
5. A szervezetnek mérlegelnie kell az elemzési eredmények érvényességét más forrásokból származó bizonyítékokkal szemben. Ha a falspozitív eredmények száma magas, az érintett szervezetnek felül kell vizsgálnia a statikus kódelemzési folyamatot vagy az elemző eszközt.
6. A szervezetnek naplót kell vezetnie a statikus kódelemzési folyamatról és az eredményeket dokumentálnia kell, hogy bizonyítékot szolgáltasson a megfelelő kódelemzési gyakorlatok alkalmazásáról.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.8.28

NIST SP 800-53 rev.5 referencia

SA-11(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.68. Fejlesztői biztonsági tesztelés és értékelés – Fenyegetésmodellezés és sérülékenységelemzések

16.68. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy fenyegetésmodellezést és sérülékenységelemzéseket hajtson végre az EIR-en, rendszerelemen vagy szolgáltatáson a fejlesztés, a tesztelés és az értékelés során, amelyek:

16.68.1. a szervezet által a várható hatásra, a működési környezetre, az ismert vagy feltételezett fenyegetésekre és az elfogadható kockázati szintekre meghatározott környezeti információkat használják;

16.68.2. a szervezet által meghatározott eszközöket és módszereket használják;

16.68.3. a modellezéseket és elemzéseket a szervezet által előírt szigorúsági kritériumok (hatókör és mélység) szerint hajtják végre;

16.68.4. olyan bizonyítékot szolgáltatnak, amelyek megfelelnek a szervezet által meghatározott elfogadási kritériumoknak.

Magyarázat

Az EIR-ek, rendszerelemek és rendszerszolgáltatások jelentősen eltérhetnek a rendszerfejlesztési életciklus követelmény- és tervezési szakaszában létrehozott funkcionális és tervezési specifikációktól. Ezért az ilyen EIR-ek, rendszerelemek és rendszerszolgáltatások fenyegetésmodellezésének és sérülékenységelemzésének frissítése a fejlesztés során és a szállítás előtt kritikus fontosságú azok hatékony működésének szempontjából. A rendszerfejlesztési életciklus ezen szakaszában a fenyegetésmodellezés és a sérülékenységelemzések biztosítják, hogy a tervezési és végrehajtási változásokat figyelembe vették, és hogy az e változások miatt keletkezett sebezhetőségeket felülvizsgálták és mérsékelték.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezzen fenyegetésmodellezést és sérülékenységelemzést az EIR-en, rendszerelemen vagy rendszerszolgáltatáson a fejlesztés, a tesztelés és az értékelés során.

2. A szervezetnek biztosítania kell, hogy a fenyegetésmodellezés és a sérülékenységelemzés a szervezet által a várható hatásra, a működési környezetre, az ismert vagy feltételezett fenyegetésekre és az elfogadható kockázati szintekre meghatározott környezeti információkat használja.
3. A szervezetnek használnia kell az általa meghatározott eszközöket és módszereket a modellezések és elemzések végrehajtásához.
4. Az érintett szervezet végezze el a modellezéseket és elemzéseket az általa előírt szigorúsági kritériumok szerint.
5. Az érintett szervezet szolgáltasson olyan bizonyítékot, amelyek megfelelnek az érintett szervezet által meghatározott elfogadási kritériumoknak.
6. A szervezetnek naplóznia és ellenőriznie kell a folyamatot, hogy biztosítsa a követelményeknek való megfelelést.

Kapcsolódó intézkedések

1.16. Szakmai csoportokkal és közösségekkel való kapcsolattartás
15.4. Kockázatértékelés
15.10. Sérülékenységmonitorozás és szkennelés

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

SA-11(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.69. Fejlesztői biztonsági tesztelés és értékelés – Független ellenőrzés az értékelési tervek és bizonyítékok tekintetében

16.69. A szervezet:

16.69.1. A meghatározott kritériumoknak megfelelő független személyt alkalmaz, aki ellenőrzi a fejlesztői biztonsági-értékelési tervek helyes végrehajtását, valamint a tesztelés és értékelés során előállított bizonyítékokat.

16.69.2. Ellenőrzi, hogy a független megbízott elegendő információt kap-e az ellenőrzési folyamat elvégzéséhez, és fel van-e hatalmazva az ilyen információk megszerzésére

Magyarázat

A független személyek rendelkeznek képesítéssel - beleértve a szakértelmet, a készségeket, a képzést, a tanúsítványokat és a tapasztalatot -, hogy ellenőrizzék a fejlesztői biztonsági értékelési tervek helyes végrehajtását.

A követelmény alkalmazásának lépései

1. A szervezetnek ki kell választania egy független személyt, aki megfelel a meghatározott kritériumoknak. Ennek a személynek rendelkeznie kell a szükséges szakértelemmel, készségekkel, képzéssel, tanúsítványokkal és tapasztalattal, hogy ellenőrizni tudja a fejlesztői biztonsági-értékelési tervek helyes végrehajtását.

2. A szervezetnek biztosítania kell, hogy a független megbízott rendelkezzen az összes szükséges információval az ellenőrzési folyamat elvégzéséhez. Ez magában foglalja az EIR-el kapcsolatos adatokat, dokumentációkat, jelentéseket és egyéb releváns információkat.

3. A szervezetnek fel kell hatalmaznia a független megbízottat, hogy hozzáférhessen az összes szükséges információhoz. Ez magában foglalhatja a hozzáférési jogok, hitelesítő adatok és egyéb szükséges eszközök biztosítását.

4. A szervezetnek ellenőriznie kell, hogy a független megbízott megfelelően végzi-e az ellenőrzést. Ez magában foglalhatja a naplók, jelentések és egyéb bizonyítékok áttekintését, amelyek a tesztelés és értékelés során keletkeztek.

5. A szervezetnek értékelnie kell a független megbízott által végzett munkát, és szükség esetén intézkedéseket kell hoznia a folyamatok javítása érdekében. Ez magában foglalhatja a független megbízott visszajelzéseinek figyelembevételét, a biztonsági és értékelési tervek módosítását, valamint a további képzések és erőforrások biztosítását.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

15.10. Sérülékenységmonitorozás és szkennelés

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

SA-11(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.70. Fejlesztői biztonsági tesztelés és értékelés – Manuális kódellenőrzés

16.70. A szervezet előírja, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője köteles manuális kódellenőrzést végrehajtani a szervezet által meghatározott konkrét kódrészleten, a meghatározott folyamatok, eljárások vagy technikák segítségével.

Magyarázat

A kézi kódellenőrzéseket általában az EIR-ek kritikus szoftver- és firmware-elemei számára tartják fenn. A kézi kódvizsgálatok hatékonyan azonosítják azokat a gyenge pontokat, amelyek az alkalmazás követelményeinek vagy kontextusának olyan ismeretét igénylik, amely a legtöbb esetben nem áll rendelkezésre az automatizált elemző eszközök és technikák, például a statikus és dinamikus elemzés számára. A kézi kódvizsgálat előnyei közé tartozik a hozzáférés-felügyeleti mátrixok ellenőrzése az alkalmazás ellenőrzésével, valamint a kriptográfiai implementációk és intézkedések részletes szempontjainak felülvizsgálata.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, mely EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjének kell manuális kódellenőrzést végeznie bizonyos kódrészleteken.
2. A szervezetnek ki kell dolgoznia és be kell vezetnie egy folyamatot, eljárást vagy technikát, amelyet a fejlesztőknek követniük kell a manuális kódellenőrzés során.
3. A szervezetnek biztosítania kell, hogy a fejlesztők megfelelően képzettek és felkészültek a manuális kódellenőrzésre, és megértik a kódellenőrzési folyamatot és annak célját.
4. A szervezetnek naplót kell vezetnie a manuális kódellenőrzésekről, beleértve a kódellenőrzés időpontját, a kódellenőrzést végző személyt, az ellenőrzött kódrészletet és az ellenőrzés eredményét.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a manuális kódellenőrzési folyamatot, eljárást és technikát, hogy biztosítsa azok hatékonyságát és relevanciáját.
6. A szervezetnek biztosítania kell, hogy a manuális kódellenőrzés eredményei beépüljenek az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztési folyamatába, és hogy a kódellenőrzés során azonosított problémákat megfelelően kezeljék és javítsák.

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

SA-11(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a konkrét kód illetve a folyamatok, eljárások és technikák meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.71. Fejlesztői biztonsági tesztelés és értékelés – Behatolásvizsgálat

16.71. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.71.1. A szervezet meghatározza a vizsgálat terjedelmét és mélységét.

16.71.2. A vizsgálatot a szervezet által meghatározott korlátozások mellett kell elvégezni.

Magyarázat

A behatolásvizsgálat olyan értékelési módszer, amelynek során az értékelők a rendelkezésre álló összes információtechnológiai termék- vagy rendszerdokumentációt felhasználva és meghatározott korlátok között dolgozva megpróbálják megkerülni az információtechnológiai termékek és EIR-ek beépített biztonsági tulajdonságait. A behatolásvizsgálatot végző értékelők számára hasznos információk közé tartoznak a termék- és rendszertervezési specifikációk, a forráskód, valamint a rendszergazdai és felhasználói kézikönyvek. A behatolásvizsgálat magában foglalhat white-box, gray-box vagy black-box vizsgálatokat, amelyek során az elemzéseket képzett szakemberek végzik, akik szimulálják a támadók tevékenységeit. A behatolásvizsgálat célja az EIR-ek, rendszerelemek és szolgáltatások olyan sebezhető pontjainak feltárása, amelyek végrehajtási hibákból, konfigurációs hibákból vagy egyéb működési gyengeségekből vagy hiányosságokból erednek. A behatolásvizsgálatokat automatizált és kézi kódvizsgálatokkal együtt lehet elvégezni, hogy a szokásosnál nagyobb szintű elemzést biztosítsanak. Ha a behatolásvizsgálat során felhasználói munkamenet-információkat és egyéb személyazonosításra alkalmas információkat fedeznek fel vagy rögzítenek, ezeket az információkat a vonatkozó adatvédelmi jogszabályoknak megfelelően kezelik.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a vizsgálat szigorúságát, mélységét és terjedelmét. Ez magában foglalja a vizsgálat céljának, a vizsgálandó rendszerelemeknek és a vizsgálat során alkalmazandó módszereknek a meghatározását.

2. A szervezetnek meg kell határoznia a vizsgálat során alkalmazandó korlátozásokat. Ez magában foglalhatja a vizsgálat időtartamát, a vizsgálat során használható eszközöket és technikákat, valamint a vizsgálat során elérhető EIR erőforrásokat.
3. A szervezetnek fel kell kérnie az EIR fejlesztőjét, hogy végezze el a vizsgálatot a meghatározott szigorúság, mélység, terjedelem és korlátozások mellett.
4. A szervezetnek gondoskodnia kell arról, hogy a vizsgálat során keletkező naplókat megfelelően kezeljék. Ez magában foglalja a naplók biztonságos tárolását, a naplókban szereplő személyes adatok védelmét, valamint a naplók felülvizsgálatát a vizsgálat eredményeinek értékelése céljából.
5. A szervezetnek értékelnie kell a vizsgálat eredményeit, és meg kell határoznia a szükséges lépéseket az EIR-ben talált sebezhetőségek kezelésére. Ez magában foglalhatja a sebezhetőségek javítását, a biztonsági intézkedések megerősítését, vagy a vizsgálat során alkalmazott módszerek és technikák felülvizsgálatát.
6. A szervezetnek dokumentálnia kell a vizsgálat eredményeit és a korrekciós intézkedéseket, hogy bizonyítékot szolgáltasson a kiberbiztonsági követelményeknek való megfelelésről.

Kapcsolódó intézkedések

5.20. Behatolásvizsgálat (penetration testing)
1.15. Tesztelés, képzés és felügyelet
16.3.1. A rendszer fejlesztési életciklusa
18.2. Hibajavítás
18.39. Biztonsági funkciók ellenőrzése

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

SA-11(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.72. Fejlesztői biztonsági tesztelés és értékelés – Támadási felület értékelések

16.72. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezze el az EIR támadási felületeire vonatkozó felülvizsgálatokat és értékeléseket.

Magyarázat

Az EIR-ek és rendszerelemek támadási felületei olyan védtelen területek, amelyek az EIR-eket sebezhetőbbé teszik a támadásokkal szemben. A támadási felületek magukban foglalnak minden olyan hozzáférhető területet, ahol a hardver-, szoftver- és firmware-elemek gyengeségei vagy hiányosságai lehetőséget nyújtanak a támadóknak a sebezhetőségek kihasználására. A támadási felület felülvizsgálata biztosítja, hogy a fejlesztők elemezzék az EIR-ek tervezési és végrehajtási változásait, és mérsékeljék a változások eredményeként keletkező támadási vektorokat. Az azonosított hibák kijavítása magában foglalja a nem biztonságos funkciók megszüntetését.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezze el az EIR támadási felületeire vonatkozó felülvizsgálatokat és értékeléseket.
2. A szervezetnek biztosítania kell, hogy a fejlesztők elemezzék a rendszertervezési és implementációs változásokat, és mérsékeljék a változások eredményeként keletkező támadási vektorokat.
3. A szervezetnek el kell végeznie a hibák korrekcióját, beleértve az nem biztonságos funkciók megszüntetését.
4. At szervezetnek dokumentálnia kell a felülvizsgálatokat és értékeléseket, valamint a hibák korrekcióját.
5. A szervezetnek rendszeres időközönként felül kell vizsgálnia és értékelnie kell az EIR támadási felületeit, hogy biztosítsa az EIR biztonságát és védelmét a támadásokkal szemben.

Kapcsolódó intézkedések

16.76.1. Fejlesztési folyamat, szabványok és 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

SA-11(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.73. Fejlesztői biztonsági tesztelés és értékelés – Tesztelés és értékelés hatáskörének ellenőrzése

16.73. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy ellenőrizze a tesztelés és értékelés terjedelmét annak érdekében, hogy teljes körű lefedettséget biztosítson a szükséges biztonsági követelményekre, amelyeket a szervezet határoz meg a tesztelési és értékelési hatókör és mélység alapján.

Magyarázat

Annak ellenőrzése, hogy a tesztelés és értékelés teljes mértékben lefedi-e az előírt követelményeket, az informális és a formális technikák széles skálájával végezhető el. E technikák mindegyike az elemzés formalizáltságának mértékének megfelelő, növekvő szintű biztonságot biztosít. Az intézkedések lefedettségének szigorú bizonyítása a legmagasabb szintű biztonsági biztosítékkal formális modellezési és elemzési technikákkal érhető el, beleértve az ellenőrzések végrehajtása és a megfelelő tesztesetek közötti korrelációt.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia és dokumentálnia kell a tesztelési és értékelési hatókört és mélységet, amelyek a szükséges biztonsági követelményeket tartalmazzák.
2.A szervezetnek fel kell kérnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjét, hogy ellenőrizze a tesztelés és értékelés terjedelmét.
3. Az ellenőrzés során a fejlesztőnek meg kell állapítania, hogy a tesztelés és értékelés teljes körű lefedettséget biztosít a szükséges biztonsági követelményekre.
4. Az ellenőrzési folyamat során a fejlesztőnek alkalmaznia kell különböző analitikai technikákat, amelyek terjedhetnek az informális módszerektől a formálisakig. Minél formálisabb az analízis, annál nagyobb a biztosított biztonsági szint.
5. A legmagasabb biztonsági szint eléréséhez a fejlesztőnek formális modellezési és analízis technikákat kell alkalmaznia, beleértve a biztonsági intézkedések megvalósítása és a megfelelő tesztesetek közötti összefüggés vizsgálatát.

6. A szervezetnek naplót kell vezetnie az ellenőrzési folyamatról, hogy nyomon követhesse a fejlesztő által végzett munkát és ellenőrizhesse, hogy a tesztelés és értékelés megfelel-e a szükséges biztonsági követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

16.76.1. Fejlesztési folyamat, szabványok és 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

SA-11(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az a tesztelésre és értékelésre vonatkozó hatókör és mélység meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.74. FEJLESZTŐI BIZTONSÁGI TESZTELÉS ÉS ÉRTÉKELÉS – DINAMIKUS KÓDELEMZÉS

16.74. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy alkalmazzon dinamikus kódelemző eszközöket, és az eszközök segítségével azonosítsa a gyakori hibákat, valamint dokumentálja az elemzés eredményeit.

MAGYARÁZAT

A dinamikus kódelemzés a szoftverprogramok futásidejű ellenőrzését biztosítja olyan eszközökkel, amelyek képesek a programokat memóriakárosodás, felhasználói jogosultsági problémák és egyéb potenciális biztonsági problémák szempontjából figyelemmel kísérni. A dinamikus kódelemzés futásidejű eszközöket használ annak biztosítására, hogy a biztonsági funkciók a tervezett módon működjenek. A dinamikus elemzés egy típusa, az úgynevezett fuzz tesztelés, programhibákat idéz elő azáltal, hogy szándékosan rosszul formált vagy véletlenszerű adatokat juttat a szoftverprogramokba. A fuzz-tesztelési stratégiák az alkalmazások tervezett felhasználásából, valamint az alkalmazások funkcionális és tervezési specifikációiból származnak. A dinamikus kódelemzés hatókörének és a nyújtott biztosítéknak a megértéséhez a szervezetek fontolóra vehetik a kódlefedettség elemzését (azaz annak ellenőrzését, hogy a kódot milyen mértékben tesztelték olyan mérőszámok segítségével, mint például a tesztelt alprogramok százalékos aránya vagy a tesztcsomag végrehajtása során meghívott programutasítások százalékos aránya) és/vagy a konkordanciaelemzést (azaz a szoftverkódban helytelenül szereplő szavak, például nem angol nyelvű szavak vagy becsmérlő kifejezések ellenőrzését).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy alkalmazzon dinamikus kódelemző eszközöket.
2. A fejlesztőnek ezeket az eszközöket kell használnia a gyakori hibák azonosítására. Ez magában foglalja a memóriakárosodással kapcsolatos -, felhasználói jogosultságok és egyéb potenciális biztonsági problémák monitorozását.

3. A fejlesztőnek alkalmaznia kell a fuzz tesztelést, amely szándékosan hibás vagy véletlenszerű adatokat vezet be a szoftverprogramokba, hogy felszínre hozza a program hibáit. A fuzz tesztelési stratégiákat az alkalmazások tervezett használatából és a funkcionális és tervezési specifikációkból kell levezetni.
4. A szervezetnek meg kell fontolnia a kódlefedettség elemzését is, amely azt ellenőrzi, mennyire tesztelték a kódot.
5. A szervezetnek el kell végeznie a konkordancia elemzést is, amely a szoftverkódban helytelenül elhelyezett szavakat ellenőrzi, például nem angol nyelvű szavakat vagy sértő kifejezéseket.
6. A szervezetnek dokumentálnia kell az elemzés eredményeit, beleértve a hibák azonosítását és a tesztelési folyamatokat. Ez a dokumentum segíthet az érintett szervezetnek a jövőbeni kiberbiztonsági problémák megelőzésében.

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

SA-11(8)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.75. Fejlesztői biztonsági tesztelés és értékelés – Interaktív alkalmazásbiztonsági tesztelés

16.75. A szervezet megköveteli a rendszerfejlesztőtől, hogy alkalmazzon manuális és automatizált alkalmazásbiztonsági tesztelő eszközöket a hibák azonosítására és a tesztelési eredmények dokumentálására.

Magyarázat

Az interaktív alkalmazásbiztonsági tesztelés a sebezhetőségek felderítésére szolgáló módszer, amely a tesztelés során futó alkalmazások megfigyelésével történik. Az eszközök használata a ténylegesen futó alkalmazások közvetlen méréseire támaszkodik, és a kódhoz, a felhasználói interakciókhoz, a könyvtárakhoz, a keretrendszerekhez, a backend-kapcsolatokhoz és a konfigurációkhoz való hozzáférést használja az intézkedés hatékonyságának közvetlen mérésére. Elemzési technikákkal kombinálva az interaktív alkalmazásbiztonsági tesztelés a potenciális sebezhetőségek széles körét azonosíthatja, és megerősítheti az intézkedés hatékonyságát. Az eszközalapú tesztelés valós időben működik, és a rendszerfejlesztési életciklus során folyamatosan használható.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a manuális és automatizált alkalmazásbiztonsági tesztelő eszközöket, amelyeket a rendszerfejlesztőnek alkalmaznia kell.
2. A szervezetnek biztosítania kell, hogy a rendszerfejlesztő megértse és képes legyen alkalmazni ezeket az eszközöket az EIR fejlesztése során.
3. A szervezetnek meg kell követelnie a rendszerfejlesztőtől, hogy a tesztelési folyamat során azonosítsa a hibákat és dokumentálja a tesztelési eredményeket.
4. A szervezetnek ellenőriznie kell, hogy a rendszerfejlesztő megfelelően alkalmazza-e a manuális és automatizált alkalmazásbiztonsági tesztelő eszközöket, és hogy a tesztelési eredményeket megfelelően dokumentálja-e.
5. A szervezetnek naplót kell vezetnie a tesztelési folyamatról és az eredményekről, hogy biztosítsa a folyamat átláthatóságát és a hibák azonosításának hatékonyságát.

6. A szervezetnek biztosítania kell, hogy a rendszerfejlesztő javítja a hibákat, amelyeket a manuális és automatizált alkalmazásbiztonsági tesztelő eszközök azonosítottak az EIR fejlesztése során.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-11(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.76. FEJLESZTÉSI FOLYAMAT, SZABVÁNYOK ÉS ESZKÖZÖK

16.76.1. A szervezet:

16.76.2. Megköveteli a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentált fejlesztési folyamatot kövessen.

16.76.2.1. Kiemelten kezelje a biztonsági követelményeket.

16.76.2.2. Határozza meg a fejlesztés során alkalmazott szabványokat és eszközöket.

16.76.2.3. Dokumentálja a fejlesztés során alkalmazott speciális eszköz konfigurációkat és opciókat.

16.76.2.4. Tartsa nyilván a változtatásokat, és biztosítsa ezek jogosulatlan változtatás elleni védelmét; továbbá

16.76.3. Előírja, hogy az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat

MAGYARÁZAT

A fejlesztési eszközök közé tartoznak például a programozási nyelvek és a számítógéppel támogatott tervezési rendszerek. A fejlesztési folyamatok áttekintése magában foglalhatja például az érettségi modellek használatát az ilyen folyamatok lehetséges hatékonyságának meghatározására. Az eszközök és folyamat változások esetén a sértetlenség fenntartása lehetővé teszi a pontos ellátási lánccal kapcsolatos kockázatértékelést és mérséklést, valamint az életciklus során (beleértve a tervezést, a fejlesztést, a szállítást, az üzembe helyezést és a karbantartást) történő konfigurációs ellenőrzéseket az engedélyezett változtatások nyomon követése és a jogosulatlan változtatások elkerülése érdekében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy kövessen egy dokumentált fejlesztési folyamatot. Ez magában foglalja a fejlesztési eszközök, mint a programozási nyelvek és a számítógéppel segített tervezési rendszerek használatát.

2. A szervezetnek kiemelten kell kezelnie a biztonsági követelményeket. Ez azt jelenti, hogy a fejlesztési folyamat során különös figyelmet kell fordítania a biztonsági szempontokra.

3. A szervezetnek meg kell határoznia a fejlesztés során alkalmazott szabványokat és eszközöket. Ez magában foglalja a fejlesztési eszközök és módszerek kiválasztását és alkalmazását.
4. A szervezetnek dokumentálnia kell a fejlesztés során alkalmazott speciális eszköz konfigurációkat és opciókat. Ez azt jelenti, hogy minden eszköz konfigurációját és beállítását rögzíteni kell, hogy a fejlesztési folyamat reprodukálható legyen.
5. A szervezetnek nyilván kell tartania a változtatásokat, és biztosítania kell ezek jogosulatlan változtatása elleni védelmét. Ez azt jelenti, hogy a változtatásokat naplózni kell, és meg kell akadályozni, hogy illetéktelen személyek módosíthassák őket.
6. A szervezetnek elő kell írnia, hogy a fejlesztő a meghatározott gyakorisággal tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat. Ez azt jelenti, hogy a fejlesztőnek rendszeresen ellenőriznie kell a fejlesztési folyamatot, hogy biztosítsa a biztonsági követelményeknek való megfelelést.

Kapcsolódó intézkedések

10.21. Kellő időben történő karbantartás
16.3.1. A rendszer fejlesztési életciklusa
16.7. Beszerzések
16.16. Biztonságtervezési elvek
16.58. Fejlesztői változáskövetés
16.66. Fejlesztői biztonsági tesztelés
19.4. Ellátási láncra vonatkozó követelmények és folyamatok
19.8. Rendszerelemek és kapcsolódó adatok eredetisége
19.13. Beszerzési stratégiák, eszközök és módszerek
19.16. Beszállítók értékelése és felülvizsgálata

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

3.3.3.6. Fejlesztési folyamat, szabványok és eszközök

ISO/IEC 27001:2023 referencia

A.5.8; A.8.25; A.8.30

NIST SP 800-53 REV.5 REFERENCIA

SA-15

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

16.77. FEJLESZTÉSI FOLYAMAT, SZABVÁNYOK ÉS ESZKÖZÖK – MINŐSÉG MÉRŐSZÁMAI

16.77. A szervezet megköveteli a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.77.1. A fejlesztési folyamat kezdetén határozzon meg minőségi mérőszámokat.

16.77.2. Rendszeresen, meghatározott időközönként és a mérföldkövek elérésekor számoljon be a minőségi mutatók teljesítéséről és nyújtson be bizonyítékot erre vonatkozóan.

16.77.3. A fejlesztett szolgáltatás átadásakor számoljon be a minőségi mutatók teljesítéséről és nyújtson be bizonyítékot erre vonatkozóan.

MAGYARÁZAT

Az érintett szervezetek minőségi mérőszámokat használnak az EIR minőségének elfogadható szintjének megállapítására. A mérőszámok közé tartozhatnak a minőségkapuk, amelyek teljesítési kritériumok vagy elégségességi szabványok gyűjteményei, amelyek a rendszerfejlesztési projekt bizonyos fázisainak kielégítő végrehajtását jelzik. Például egy minőségi kapu megkövetelheti az összes fordítóprogram (compiler) általi figyelmeztetés kiküszöbölését, vagy annak megállapítását, hogy az ilyen figyelmeztetések nem befolyásolják a szükséges biztonsági vagy adatvédelmi képességek hatékonyságát. A fejlesztési projektek végrehajtási fázisaiban a minőségkapuk világos, egyértelmű jelzést adnak az előrehaladásról. Más mérőszámok a teljes fejlesztési projektre vonatkoznak. A mérőszámok közé tartozhat a sebezhetőségek súlyossági küszöbértékeinek meghatározása a szervezeti kockázati toleranciával összhangban, például az, hogy a szállított rendszerben ne legyenek ismert sebezhetőségek, és ne legyen a Közös sebezhetőségi pontozási rendszer (CVSS) súlyossága közepes vagy magas.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR fejlesztőjétől, hogy a fejlesztési folyamat kezdetén határozzon meg minőségi mérőszámokat. Ezek a mérőszámok lehetnek minőségi kapuk, amelyek a fejlesztési projekt bizonyos fázisainak sikeres végrehajtását jelentik.

2. A szervezetnek meg kell követelnie az EIR fejlesztőjétől, hogy rendszeresen, meghatározott időközönként és a mérföldkövek elérésekor számoljon be a minőségi mutatók teljesítéséről és nyújtson be bizonyítékot erre vonatkozóan. A fejlesztési projekt végrehajtási fázisai során a minőségi kapuk egyértelmű jeleket adnak a haladásról.
3. A szervezetnek meg kell követelnie az EIR fejlesztőjétől, hogy a fejlesztett szolgáltatás átadásakor számoljon be a minőségi mutatók teljesítéséről és nyújtson be bizonyítékot erre vonatkozóan. A mérőszámok közé tartozhat a sérülékenységek súlyossági küszöbértékének meghatározása az érintett szervezet kockázattűrésének megfelelően, például a szállított EIR-ben ne legyenek ismert sérülékenységek, amelyek a Common Vulnerability Scoring System (CVSS) súlyossága szerint közepesek vagy magasak.
4. A szervezetnek dokumentálnia kell a minőségi mérőszámok teljesítését, és bizonyítékot kell tárolnia arra vonatkozóan, hogy ezek a mérőszámok teljesültek.

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

SA-15(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.78. Fejlesztési folyamat, szabványok és eszközök – Biztonsági szempontokat nyomonkövető eszközök

16.78. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy válasszon ki és alkalmazzon olyan eszközöket a fejlesztési folyamat során, amelyek alkalmasak a biztonsági szempontok nyomonkövetésére.

Magyarázat

A rendszerfejlesztő csapatok kiválasztják és telepítik a biztonsági szempontokat nyomonkövető eszközöket, beleértve a sebezhetőségi vagy munkaelem-nyomonkövető rendszereket, amelyek megkönnyítik az elkészült munkaelemek vagy a fejlesztési folyamatokhoz kapcsolódó feladatok hozzárendelését, rendezését, szűrését és nyomon követését.

A követelmény alkalmazásának lépései

1. A szervezetnek ki kell jelölnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjét.
2. A szervezetnek meg kell követelnie a fejlesztőtől, hogy válasszon ki és alkalmazzon olyan eszközöket a fejlesztési folyamat során, amelyek alkalmasak a biztonsági szempontok nyomonkövetésére. Ezek az eszközök tartalmazhatnak sebezhetőségi vagy munkaelem-nyomonkövető rendszereket, amelyek lehetővé teszik a fejlesztési folyamatokhoz vagy befejezett munkaelemekhez kapcsolódó feladatok kijelölését, rendezését, szűrését és nyomon követését.
3. A szervezetnek biztosítania kell, hogy a fejlesztők megfelelően használják ezeket az eszközöket, és rendszeresen ellenőriznie kell, hogy a biztonsági szempontokat megfelelően követik-e nyomon.
4. A szervezetnek dokumentálnia kell a fejlesztési folyamat során használt eszközök alkalmazását, és rendszeresen ellenőriznie kell, hogy a fejlesztők megfelelően használják-e ezeket az eszközöket.
5. A szervezetnek értékelnie kell a fejlesztési folyamatot, hogy megbizonyosodjon arról, hogy a biztonsági szempontokat megfelelően követik-e nyomon, és szükség esetén módosításokat kell végrehajtania.

Kapcsolódó intézkedések

16.66. Fejlesztői biztonsági tesztelés

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

SA-15(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.79. Fejlesztési folyamat, szabványok és eszközök – Kritikussági elemzés

16.79. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezzen kritikussági elemzést:

16.79.1. A rendszerfejlesztési életciklus alatt, a szervezet által meghatározott döntési pontokon.

16.79.2. A szervezet által meghatározott szigorúsággal.

Magyarázat

A fejlesztő által végzett kritikussági elemzés hozzájárul bementi információkkal a szervezetek által végzett kritikussági elemzéshez. A fejlesztő hozzájárulása alapvető fontosságú a szervezeti kritikussági elemzéshez, mivel a szervezetek nem feltétlenül férnek hozzá a kereskedelmi forgalomban kapható termékként kifejlesztett rendszerelemek részletes tervdokumentációjához. Az ilyen tervdokumentáció magában foglalja a funkcionális specifikációkat, a magas szintű terveket, az alacsony szintű terveket, a forráskódot és a hardveres vázlatokat. A kritikussági elemzés fontos a nagy értékű eszközként megjelölt szervezeti rendszerek esetében. A magas értékű eszközök mérsékelt vagy magas hatású rendszerekké válhatnak a megnövekedett kiberfenyegetés vagy a potenciálisan káros hatások miatt a szervezetben. A fejlesztők hozzájárulása különösen fontos, amikor a szervezetek ellátási lánc kritikussági elemzéseket végeznek.

A követelmény alkalmazásának lépései

1. A szervezetnek először ki kell jelölnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjét.
2. A szervezetnek meg kell követelnie a fejlesztőtől, hogy végezzen kritikussági elemzést az EIR-en. Ez az elemzés a rendszerfejlesztési életciklus alatt történik.
3. A szervezetnek döntési pontokat kell meghatároznia a rendszerfejlesztési életciklus során, ahol a kritikussági elemzést el kell végezni. Ezek a döntési pontok a szervezet által meghatározottak.
4. A kritikussági elemzésnek meg kell felelnie a szervezet által meghatározott szigorúságnak. Ez azt jelenti, hogy az elemzésnek alaposnak és részletesnek kell lennie.

5. A szervezetnek dokumentálnia kell a kritikussági elemzést, beleértve a fejlesztő által végzett munkát és az elemzés eredményeit.
6. A szervezetnek felül kell vizsgálnia és értékelnie kell a kritikussági elemzést, hogy biztosítsa, hogy az EIR megfelel az érintett szervezet kiberbiztonsági követelményeinek.

Kapcsolódó intézkedések

15.21. Rendszerelemek kritikusságának elemzése

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

SA-15(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

16.80. FEJLESZTÉSI FOLYAMAT, SZABVÁNYOK ÉS ESZKÖZÖK – TÁMADÁSI FELÜLET CSÖKKENTÉSE

16.80. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a szervezet által meghatározott mértékben csökkentse az EIR támadási felületeit.

MAGYARÁZAT

A támadási felület csökkentése szorosan összefügg a fenyegetés- és sebezhetőség-elemzésekkel, valamint az rendszerarchitektúrájával és tervezésével. A támadási felület csökkentése egy olyan eszköz, amely az érintett szervezetek számára kockázatcsökkentést jelent, mivel kevesebb lehetőséget biztosít a támadóknak a gyengeségek vagy hiányosságok kihasználására az EIR-ben, rendszerelemekben és rendszerszolgáltatásokban. A támadási felület csökkentése magában foglalja a többszintű védelem koncepciójának megvalósítását, a legkisebb jogosultság és a legkisebb funkcionalitás elvének alkalmazását, a biztonságos szoftverfejlesztési gyakorlatok alkalmazását, a nem biztonságos funkciók megszüntetését, a jogosultsággal nem rendelkező felhasználók számára elérhető belépési pontok csökkentését, a végrehajtott kód mennyiségének csökkentését és a támadásokkal szemben sebezhető alkalmazásprogramozási interfészek (API-k) megszüntetését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR támadási felületeit. Ez magában foglalja a fenyegetések és sebezhetőségek elemzését, valamint az rendszer architektúrájának és tervezésének vizsgálatát.
2. A szervezetnek meg kell követelnie az EIR fejlesztőjétől, hogy csökkentse az EIR támadási felületeit. Ez magában foglalhatja a többszintű védelmi rendszerek bevezetését, a legkisebb jogosultság és a legkisebb funkcionalitás elveinek alkalmazását, a biztonságos szoftverfejlesztési gyakorlatok alkalmazását, a nem biztonságos funkciók megszüntetését.
3. A szervezetnek továbbá csökkentenie kell azoknak a hozzáférési pontoknak a számát, amelyek a jogosulatlan felhasználók számára elérhetők, csökkentenie kell a végrehajtott kód mennyiségét, és meg kell szüntetnie azokat az alkalmazásprogramozási interfészeket, amelyek támadásokkal szemben sebezhetők.

4. A szervezetnek dokumentálnia kell az EIR támadási felületének csökkentésére irányuló összes intézkedést. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon kövesse a fejlesztő által végrehajtott változtatásokat, és ellenőrizze, hogy azok megfelelnek-e a követelményeknek.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a támadási felület csökkentésére irányuló stratégiáját, hogy biztosítsa az EIR védelmét a legújabb fenyegetésekkel szemben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.60. Legkisebb jogosultság elve
6.26. Legszűkebb funkcionalitás
15.4. Kockázatértékelés
16.66. Fejlesztői biztonsági tesztelés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.28

NIST SP 800-53 REV.5 REFERENCIA

SA-15(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a küszöbértékek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.81. Fejlesztési folyamat, szabványok és eszközök – Folyamatos továbbfejlesztés

16.81. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy egy folyamatot vezessen be a fejlesztési folyamat folyamatos javítására.

Magyarázat

Az EIR-ek, rendszerelemek és rendszerszolgáltatások fejlesztői mérlegelik a fejlesztési folyamataik hatékonyságát és eredményességét a minőségi célkitűzések teljesítése, valamint a biztonsági és adatvédelmi képességek kezelése szempontjából az adott fenyegető környezetekben.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy vezessenek be egy eljárást a fejlesztési folyamat folyamatos javítására.
2. A szervezetnek biztosítania kell, hogy a fejlesztők figyelembe veszik a fejlesztési folyamatok hatékonyságát és eredményességét a minőségi célok elérése és a jelenlegi fenyegetési környezetben lévő biztonsági és adatvédelmi képességek kezelése érdekében.
3. A szervezetnek ellenőriznie kell, hogy a fejlesztők rendszeresen értékelik és frissítik a fejlesztési folyamatot, hogy biztosítsák annak folyamatos javulását.
4. A szervezetnek biztosítania kell, hogy a fejlesztők dokumentálják a fejlesztési folyamatot, beleértve a folyamat javítására tett lépéseket is.
5. A szervezetnek rendszeresen felül kell vizsgálnia a fejlesztési folyamatot és annak javítását, hogy biztosítsa a folyamat hatékonyságát és a minőségi célok elérését.

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

SA-15(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.82. FEJLESZTÉSI FOLYAMAT, SZABVÁNYOK ÉS ESZKÖZÖK – AUTOMATIZÁLT SÉRÜLÉKENYSÉGELEMZÉS

16.82. A szervezet megköveteli a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a fejlesztési folyamat során, a szervezet által elvárt gyakorisággal:

16.82.1. végezze el az automatizált sérülékenységelemzést a szervezet által meghatározott eszközökkel;

16.82.2. határozza meg a felfedezett sérülékenységek kihasználásának módjait és potenciálját;

16.82.3. határozza meg a sérülékenységekre vonatkozó javasolt kockázatcsökkentő lehetőségeket; valamint

16.82.4. adja át a vizsgálat és elemzés eredményeit a szervezet által meghatározott személyeknek vagy szerepköröknek.

MAGYARÁZAT

Az automatizált eszközök hatékonyabban elemezhetik a nagy és összetett EIR-ek kihasználható gyengeségeit vagy hiányosságait, súlyosság szerint rangsorolhatják a sérülékenységeket, és ajánlásokat tehetnek a kockázatcsökkentésre.

Ezt követően a fejlesztő megválasztja a sérülékenységek kezelésének vagy minimalizálásának módszereit, például a szoftverfrissítések alkalmazását, a hálózati biztonsági beállítások módosítását vagy a felhasználói jogosultságok korlátozását alkalmazhatja.

A fejlesztőknek az értékelést és kockázatcsökkentési intézkedéseket tartalmazó dokumentumokat át kell adnia az illetékes szervezeti felelősök részére. Valamint el kell végeznie azon szükséges információk kigyűjtését, melyek a döntéshozóknak és a kockázatkezelő csapatnak hasznosak lehetnek a későbbiekben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezzen automatizált sérülékenységelemzést a szervezet által meghatározott eszközökkel. Ez magában foglalja a szoftverek, hardverek és hálózati elemek ellenőrzését a potenciális sérülékenységek szempontjából.

2. A fejlesztőnek meg kell határoznia a felfedezett sérülékenységek kihasználásának módjait és potenciálját. Ez magában foglalja a támadók által lehetséges módon kihasználható sérülékenységek azonosítását és értékelését.
3. A fejlesztőnek meg kell határoznia a sérülékenységekre vonatkozó kockázatcsökkentő lehetőségeket. Ez magában foglalja a sérülékenységek kezelésének vagy minimalizálásának módszereit.
4. A fejlesztőnek át kell adnia a vizsgálat és elemzés eredményeit a szervezet által meghatározott személyeknek vagy szerepköröknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.10. Sérülékenységmonitorozás és szkennelés
16.66. Fejlesztői biztonsági tesztelés

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

SA-15(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.83. Fejlesztési folyamat, szabványok és eszközök – Fenyegetési- és sérülékenységi információk felhasználása

16.83. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a fejlesztési folyamat támogatása érdekében vegye figyelembe a hasonló rendszerekből, rendszerelemekből vagy rendszerszolgáltatásokból származó fenyegetésmodellezést és sérülékenységelemzéseket.

Magyarázat

A hasonló szoftveralkalmazásokban talált sérülékenységek elemzése tájékoztatást adhat a fejlesztés alatt álló EIR-ek lehetséges tervezési és megvalósítási problémáiról. Hasonló EIR-ek vagy rendszerelemek létezhetnek a fejlesztő szervezeteken belül.

A követelmény alkalmazásának lépései

1. Az érintett szervezetnek először meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy vegye figyelembe a hasonló EIR-ekből, rendszerelemekből vagy rendszerszolgáltatásokból származó fenyegetésmodellezést és sérülékenységelemzéseket.
2. Az érintett szervezetnek biztosítania kell, hogy a fejlesztők rendelkezzenek a szükséges információkkal és erőforrásokkal a fenyegetésmodellezéshez és a sérülékenységelemzéshez. Ez magában foglalhatja a hasonló EIR-ekből, rendszerelemekből vagy rendszerszolgáltatásokból származó adatokhoz való hozzáférést.
3. Az érintett szervezetnek biztosítania kell, hogy a fejlesztők képesek legyenek azonosítani és elemezni a potenciális sérülékenységeket, és ezeket figyelembe venni a fejlesztési folyamat során.
4. Az érintett szervezetnek ellenőriznie kell, hogy a fejlesztők megfelelően alkalmazzák a fenyegetésmodellezést és a sérülékenységelemzést a fejlesztési folyamat során. Ez magában foglalhatja a fejlesztési naplók ellenőrzését és a fejlesztőkkel való rendszeres kommunikációt.
5. Az érintett szervezetnek értékelnie kell a fejlesztési folyamat eredményeit, hogy biztosítsa a fenyegetésmodellezés és a sérülékenységelemzés hatékony alkalmazását. Ez magában

foglalhatja a fejlesztett EIR, rendszerelem vagy rendszerszolgáltatás tesztelését és értékelését, valamint a sérülékenységelemzés eredményeinek felhasználását a további fejlesztési tevékenységekben.

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

SA-15(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.84. FEJLESZTÉSI FOLYAMAT, SZABVÁNYOK ÉS ESZKÖZÖK – BIZTONSÁGI ESEMÉNYKEZELÉSI TERV

16.84. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a fejlesztési folyamat részeként készítse el, vezesse be és tesztelje a rendszer biztonsági eseménykezelési tervét.

MAGYARÁZAT

A fejlesztők által rendelkezésre bocsátott biztonsági eseménykezelési terv olyan információkkal szolgálhat, amelyek a szervezetek számára nem állnak könnyen rendelkezésre, és amelyeket be kell építeni a (teljes) szervezeti biztonsági eseménykezelési tervekbe. Ez magában foglalhatja a tervben leírt válaszstratégiák tesztelését és a terv felülvizsgálatát a tesztelés eredményei alapján. A fejlesztői információk is rendkívül hasznosak lehetnek, például amikor a szervezetek a kereskedelmi forgalomban kapható termékekben található sebezhetőségekre reagálnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a fejlesztési folyamat részeként készítse el a biztonsági eseménykezelési tervet.
2. A fejlesztőnek be kell vezetnie a biztonsági eseménykezelési tervet az EIR fejlesztési folyamatába. Ez magában foglalja a potenciális biztonsági események azonosítását, a válaszstratégiák kidolgozását, és a választervek tesztelését.
3. A fejlesztőnek tesztelnie kell a biztonsági eseménykezelési tervet, hogy biztosítsa annak hatékonyságát és teljességét a potenciális biztonsági eseményekre.
4. A szervezetnek be kell építenie a fejlesztő által biztosított biztonsági eseménykezelési tervet a saját eseménykezelési tervébe.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági eseménykezelési tervet, hogy biztosítsa annak relevanciáját és hatékonyságát a változó biztonsági környezetben.

Kapcsolódó intézkedések

9.34. Biztonsági eseménykezelési terv

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

SA-15(10)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.85. Fejlesztési folyamat, szabványok és eszközök – Rendszer vagy rendszerelem archiválása

16.85. A szervezet megköveteli az EIR vagy rendszerelem fejlesztőjétől, hogy archiválja a kiadásra vagy szállításra kerülő rendszert vagy rendszerelemet a végső biztonsági felülvizsgálatot alátámasztó bizonyítékokkal együtt.

Magyarázat

Az EIR vagy rendszerelemek archiválásához a fejlesztőnek meg kell őriznie a kulcsfontosságú fejlesztési melléktermékeket, beleértve a hardverspecifikációkat, a forráskódot, az objektumkódot és a fejlesztési folyamat vonatkozó dokumentációit, amelyek könnyen elérhető konfigurációs kiindulási alapot biztosítanak a rendszer- és rendszerelem frissítésekhez vagy módosításokhoz.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie az EIR vagy rendszerelem fejlesztőjétől, hogy archiválja a kiadásra vagy szállításra kerülő EIR-t vagy rendszerelemet.
2. A szervezetnek biztosítania kell, hogy a fejlesztő a végső biztonsági felülvizsgálatot alátámasztó bizonyítékokkal együtt archiválja az EIR-t vagy rendszerelemet.
3. A szervezetnek ellenőriznie kell, hogy a fejlesztő megőrizte-e a kulcsfontosságú fejlesztési elemeket, beleértve a hardver specifikációkat, forráskódot, objektumkódot és a fejlesztési folyamatból származó releváns dokumentációt.
4. A szervezetnek ellenőriznie kell, hogy a fejlesztő a naplóban rögzítette-e a végső biztonsági felülvizsgálatot alátámasztó bizonyítékokat.
5. A szervezetnek rendszeresen ellenőriznie kell, hogy a fejlesztő betartja-e az archiválási követelményeket, és szükség esetén intézkedéseket kell hoznia a fejlesztő kötelezettségeinek betartásának biztosítása érdekében.

Kapcsolódó intézkedések

6.2. Alapkonfiguráció

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

SA-15(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.86. SZOFTVERFEJLESZTŐK OKTATÁSA

16.86. A szervezet kötelezi a rendszerfejlesztőt, hogy biztosítson képzést a szoftverfejlesztőknek a megvalósított biztonsági funkciók, szabályozások és mechanizmusok helyes használatáról és működéséről.

MAGYARÁZAT

Ez a követelmény a külső és belső fejlesztőkre is vonatkozik. A személyek képzése alapvető fontosságú a szervezeti EIR-eken belül végrehajtott biztonsági intézkedések hatékonyságának biztosításához. A képzési lehetőségek közé tartozik például az osztálytermi képzés, a webalapú/számítógép-alapú képzés és a gyakorlati képzés. A szervezetek megfelelő képzési anyagokat is kérhetnek a fejlesztőktől, hogy vállalati képzést végezzenek, vagy szervezeti munkavállalók számára akár önképzést nyújtsanak. A szervezetek meghatározzák a szükséges képzés típusát, és különböző típusú képzéseket igényelhetnek különböző biztonsági funkciókkal, követelményekkel vagy mechanizmusokkal kapcsolatban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először köteleznie kell a rendszerfejlesztőt, hogy biztosítson képzést a szoftverfejlesztők számára. Ez a képzési kötelezettség vonatkozik a külső és belső fejlesztőkre is.
2. A képzéssel is foglalkozó személyzet elengedhetetlen az EIR-en belül megvalósított intézkedések hatékonyságának biztosításához. A képzési formák közé tartozik a web-alapú és számítógép-alapú képzés, az osztálytermi stílusú képzés, és a gyakorlati képzés (beleértve a mikro-képzést is).
3. A szervezetnek lehetőséget kell bitztosítania, hogy képzési anyagokat kérjen be a fejlesztőktől, hogy házon belüli képzést végezzen, vagy önképzést kínáljon a szervezeti személyzet számára.
4. A szervezetnek meg kell határoznia a szükséges képzés típusát, és különböző típusú képzést igényelhet a különböző biztonsági és adatvédelmi funkciók, követelmények és mechanizmusok számára.
5. A szervezetnek dokumentálnia kell a képzési folyamatot és annak hatékonyságát, hogy biztosítsa a képzési követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.2. Biztonságtudatossági képzés

3.9. Szerepkör alapú biztonsági képzés

12.6. A fizikai belépés ellenőrzése

16.7. Beszerzések

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

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

3.3.3.7. Fejlesztői oktatás: Az érintett szervezet oktatásikötelezettséget ír elő az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára, hogy az érintett szervezet által kijelölt személyek - elsősorban adminisztrátorok - és biztonsági felelősök a megvalósított biztonsági funkciók, intézkedések és mechanizmusok helyes használatát és működését megismerhessék és elsajátíthassák.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SA-16

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakorlatok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

16.87. FEJLESZTŐI BIZTONSÁGI ARCHITEKTÚRA ÉS TERVEZÉS

16.87. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan tervezési specifikációt és biztonsági architektúrát hozzon létre, amely:

16.87.1. Illeszkedik a szervezet biztonsági architektúrájához és támogatja azt.

16.87.2. Leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között.

16.87.3. Bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.

MAGYARÁZAT

Ez a követelmény elsősorban külsős fejlesztőkre vonatkozik, bár belsős fejlesztésre is használható, amennyiben alkalmaznak külsős fejlesztőt. Ezzel ellentétben az információbiztonsági architektúra leírásáról szóló biztonsági követelménnyel, elsősorban a belső fejlesztőkre irányul, hogy biztosítsa, hogy a szervezet egységes információbiztonsági architektúrát alakít ki, és az ilyen biztonsági architektúra összhangban áll a vállalati architektúrával. Ez a megkülönböztetés fontos, abban az esetben, amelyben a szervezetek kiszervezik az EIR-ek, rendszerelemek vagy a rendszerszolgáltatások fejlesztését külső szervezetekhez, és szükség van a szervezet vállalati architektúrájával és az információbiztonsági architektúrával való összhang biztosítására.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie a rendszerfejlesztőjétől, hogy hozzon létre egy olyan tervezési specifikációt és biztonsági architektúrát, amely illeszkedik a szervezet saját biztonsági architektúrájához és támogatja azt.

2. A fejlesztőnek a tervezési specifikációban le kell írnia a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását az EIR fizikai és logikai összetevői között.

3. A fejlesztőnek be kell mutatnia, hogy az egyes biztonsági funkciók, mechanizmusok és szolgáltatások hogyan működnek együtt az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.
4. A szervezetnek ellenőriznie kell, hogy a fejlesztő által létrehozott tervezési specifikáció és biztonsági architektúra megfelel-e a szervezet saját biztonsági architektúrájának és támogatja-e azt.
5. A szervezetnek dokumentálnia kell a fejlesztő által végzett munkát, hogy biztosítsa a folyamat átláthatóságát és ellenőrizhetőségét.
6. A szervezetnek rendszeresen felül kell vizsgálnia a fejlesztő által létrehozott tervezési specifikációt és biztonsági architektúrát, hogy biztosítsa, hogy azok továbbra is megfelelnek a szervezet biztonsági követelményeinek és támogatják a szervezet biztonsági architektúráját.

Kapcsolódó intézkedések

13.2. Rendszerbiztonsági terv
13.6. Információbiztonsági architektúra leírás
1.7. Szervezeti architektúra
16.3.1. A rendszer fejlesztési életciklusa
16.7. Beszerzések
16.16. Biztonságtervezési elvek
17.17. A határok védelme

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

3.3.3.8. Fejlesztői biztonsági architektúra és tervezés

ISO/IEC 27001:2023 referencia

A.8.25; A.8.27

NIST SP 800-53 rev.5 referencia

SA-17

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

16.88. FEJLESZTŐI BIZTONSÁGI ARCHITEKTÚRA ÉS TERVEZÉS – FORMÁLIS SZABÁLYZATI MODELL

16.88. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.88.1. a fejlesztési folyamat szerves részeként hozzon létre egy formális szabályzati modellt, amely tartalmazza az érvényesítendő szervezeti biztonsági elemeket; és

16.88.2. gondoskodjon a formális szabályzati modell belső konzisztenciájának biztosításáról olyan módon, hogy az megfeleljen az előírt szervezeti biztonsági szabályoknak.

MAGYARÁZAT

A formális modellek bizonyos viselkedéseket vagy biztonsági szabályzatokat írnak le formális nyelvek segítségével, lehetővé téve ezáltal, hogy e viselkedések és szabályzatok helyessége formálisan bizonyítható legyen. Az EIR-ek nem minden eleme modellezhető. A formális specifikációk általában a viselkedésekre vagy szabályzatokra korlátozódnak, például a nem diszkrecionális hozzáférés-szabályokra. Az érintett szervezetek a formális modellezési nyelvet és megközelítést a leírandó viselkedések és irányelvek jellege és a rendelkezésre álló eszközök alapján választják ki.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie a rendszerfejlesztőjétől, hogy a fejlesztési folyamat szerves részeként hozzon létre egy formális szabályzati modellt. Ez a modell tartalmazza az érvényesítendő szervezeti biztonsági elemeket.
2. A formális szabályzati modell létrehozásakor a fejlesztőnek figyelembe kell vennie a specifikus viselkedéseket és biztonsági szabályzatokat, és formális nyelveket kell használnia ezek leírásához. Így a viselkedések és szabályzatok helyességét formálisan lehet igazolni.
3. Nem minden rendszerelemet lehet modellezni. Általában a formális specifikációk a fontos viselkedésekre vagy szabályzatokra koncentrálnak, mint például a nem diszkrecionális hozzáférési szabályok.
4. A szervezetnek ki kell választania a formális modellezési nyelvet és megközelítést a leírandó viselkedések és szabályok jellegétől, valamint az elérhető eszközöktől függően.

5. A szervezetnek gondoskodnia kell a formális szabályzati modell belső konzisztenciájáról, miután az elkészült. Ez azt jelenti, hogy a modellnek meg kell felelnie az előírt szervezeti biztonsági szabályoknak.
6. A szervezetnek dokumentálnia kell a formális szabályzati modell fejlesztését és annak belső konzisztenciáját, hogy biztosítsa a folyamat átláthatóságát és ellenőrizhetőségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.129. Referenciának való megfelelőség vizsgálata

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

SA-17(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.89. Fejlesztői biztonsági architektúra és tervezés – Biztonsági szempontból kiemelt rendszerelemek

16.89. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.89.1. határozza meg a biztonsági szempontból releváns hardvert, szoftvert és firmware-t; és

16.89.2. szolgáltasson indoklást arra vonatkozóan, hogy a biztonsági szempontból releváns hardver, szoftver és firmware meghatározás miért tekinthető teljesnek.

Magyarázat

A biztonság szempontjából releváns hardver, szoftver és firmware az EIR, rendszerelem vagy rendszerszolgáltatás azon részét képviseli, amely megbízhatóan működik az előírt biztonsági tulajdonságok fenntartása érdekében.

A követelmény alkalmazásának lépései

1. A szervezetnek fel kell vennie a kapcsolatot az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjével, és utasítania kell, hogy határozza meg a biztonsági szempontból releváns hardvert, szoftvert és firmware-t.
2. A szervezetnek biztosítania kell a fejlesztővel való egyeztetést a releváns hardver, szoftver és firmware meghatározásának folyamatáról és időkeretéről.
3. Miután a fejlesztő meghatározta a biztonsági szempontból releváns hardvert, szoftvert és firmware-t, a szervezetnek át kell tekintenie és értékelnie kell a fejlesztő által szolgáltatott információkat.
4. A szervezetnek meg kell kérnie a fejlesztőt, hogy indolkolja meg akár evidenciákkal alátámasztva, hogy a biztonsági szempontból releváns hardver, szoftver és firmware meghatározás miért tekinthető teljesnek.
5. A szervezetnek értékelnie kell a fejlesztőtől kapott indoklást, és meg kell győződnie arról, hogy az megfelelő és kielégítő.

6. Amennyiben a szervezet úgy ítéli meg, hogy a meghatározás és az indoklás nem teljes vagy nem megfelelő, akkor fejlesztőtől további információkat kell kérnie vagy a meghatározások módosítását.

7. A szervezetnek dokumentálnia kell a folyamatot, beleértve a fejlesztővel folytatott kommunikációt, a meghatározásokat és az indoklásokat, hogy bizonyítékot szolgáltasson a kiberbiztonsági követelményeknek való megfelelésről.

Kapcsolódó intézkedések

2.129. Referenciának való megfelelőség vizsgálata

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

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

SA-17(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.90. Fejlesztői biztonsági architektúra és tervezés – Formalizált specifikáció

16.90. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.90.1. Hozzon létre a fejlesztési folyamat szerves részeként egy formális, magasszintű specifikációt, amely meghatározza a biztonsági szempontból releváns hardver, szoftver és firmware interfészeket, kivételeket, hibaüzeneteket és hatásokat.

16.90.2. Mutassa be és szükség esetén bizonyítékokkal támassza alá, hogy a formális magasszintű specifikáció megfelel a szabályzati modellben meghatározott követelményeknek és elvárásoknak.

16.90.3. Mutassa be és bizonyítékokkal támassza alá, hogy a formális magasszintű specifikáció megfelel a szabályzati modellben meghatározott követelményeknek és elvárásoknak.

16.90.4. Mutassa be, hogy a formális magasszintű specifikáció teljesen lefedi a biztonsági szempontból releváns hardver, szoftver és firmware interfészeket.

16.90.5. Írja le azokat a biztonsági szempontból releváns hardver, szoftver és firmware mechanizmusokat, amelyeket a formális magasszintű specifikáció nem kezel, de a biztonsági szempontból releváns hardveren, szoftveren vagy firmware-en belül működnek.

Magyarázat

Az összhang fontos része annak a biztosítéknak, amit a modellezésen keresztül nyerünk. Azt bizonyítja, hogy a megvalósítás a modell pontos átmentése, és hogy a jelenlévő további kód vagy megvalósítási részletek nem befolyásolják a modellezett viselkedést vagy szabályokat. Formális módszerekkel kimutatható, hogy a magas szintű biztonsági tulajdonságokat a formális rendszerleírás kielégíti, és hogy a formális rendszerleírást valamilyen alacsonyabb szintű leírás, beleértve a hardverleírást is, helyesen valósítja meg. A formális felső szintű specifikáció és a formális irányelvmodellek közötti konzisztencia általában nem bizonyítható teljes mértékben. Ezért a konzisztencia bizonyításához a formális és informális módszerek kombinációjára lehet szükség. A formális felső szintű specifikáció és a tényleges megvalósítás közötti konzisztencia informális bizonyítást igényelhet, mivel a formális módszerek alkalmazhatóságának korlátai miatt a specifikációnak a megvalósítást pontosan tükröző voltát csak korlátozottan lehet

bizonyítani. A biztonsági szempontból releváns elemek belső hardver, szoftver és firmware mechanizmusai közé tartoznak a leképező regiszterek és a közvetlen memória bemenet és kimenet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell követelnie az EIR fejlesztőjétől, hogy hozzon létre egy formális, magasszintű specifikációt, amely meghatározza a biztonsági szempontból releváns hardver, szoftver és firmware interfészeket, kivételeket, hibaüzeneteket és hatásokat.
2. A szervezetnek meg kell követelnie a fejlesztőtől, hogy mutassa be és szükség esetén bizonyítékokkal támassza alá, hogy a formális magasszintű specifikáció megfelel a szabályzati modellben meghatározott követelményeknek és elvárásoknak.
3. A szervezetnek továbbá meg kell követelnie a fejlesztőtől, hogy mutassa be, hogy a formális magasszintű specifikáció teljesen lefedi a biztonsági szempontból releváns hardver, szoftver és firmware interfészeket.
4. A szervezetnek meg kell követelnie a fejlesztőtől, hogy írja le azokat a biztonsági szempontból releváns hardver, szoftver és firmware mechanizmusokat, amelyeket a formális magasszintű specifikáció nem kezel, de az EIR-en belül működnek.
5. A szervezetnek dokumentálnia kell a folyamatot, hogy bizonyítani tudja a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
2.28. Információáramlási szabályok érvényesítése
2.129. Referenciának való megfelelőség vizsgálata
16.7. Beszerzések
16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

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

SA-17(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.91. Fejlesztői biztonsági architektúra és tervezés – Nem formalizált specifikáció

16.91. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.91.1. A fejlesztési folyamat szerves részeként hozzon létre egy informális, leíró jellegű magasszintű specifikációt, amely meghatározza a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek interfészeit, kivételeket, hibajelzéseket és hatásokat.

16.91.2. Mutassa be és megfelelő érvekkel támassza alá, hogy a leíró jellegű magasszintű specifikáció megfelel a szervezet szoftverfejlesztésre vonatkozó elvárásainak.

16.91.3. Mutassa be informális bemutatóval, hogy a leíró jellegű magasszintű specifikáció teljeskörűen lefedi a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek interfészeit.

16.91.4. Bizonyítsa, hogy a leíró jellegű magasszintű specifikáció pontosan leírja a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek interfészeit; és

16.91.5. írja le azokat a mechanizmusokat, amelyeket nem vesz figyelembe a leíró jellegű magasszintű specifikáció, de a biztonsági szempontból releváns hardveren, szoftveren vagy firmware-en belül működnek.

Magyarázat

Az összhang fontos része annak a biztosítéknak, amit a modellezésen keresztül nyerünk. Azt bizonyítja, hogy a megvalósítás a modell pontos átalakítása, és hogy a jelenlévő további kód vagy megvalósítási részletek nem befolyásolják a modellezett viselkedést vagy szabályokat. Formális módszerekkel kimutatható, hogy a magas szintű biztonsági tulajdonságokat a formális rendszerleírás kielégíti, és hogy a formális rendszerleírást valamilyen alacsonyabb szintű leírás, beleértve a hardverleírást is, helyesen valósítja meg. A formális felső szintű specifikáció és a formális irányelvmodellek közötti konzisztencia általában nem bizonyítható teljes mértékben. Ezért a konzisztencia bizonyításához a formális és informális módszerek kombinációjára lehet szükség. A biztonsági szempontból releváns hardverek, szoftverek és firmware-ek belső mechanizmusai közé tartoznak a leképező regiszterek és a közvetlen memória bemenet és kimenet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie a fejlesztőtől, hogy mutassa be és megfelelő érvekkel támassza alá, hogy a leíró jellegű magasszintű specifikáció megfelel a szervezet szoftverfejlesztésre vonatkozó elvárásainak.
2. A szervezetnek meg kell követelnie a fejlesztőtől, hogy informális bemutatóval mutassa be, hogy a leíró jellegű magasszintű specifikáció teljeskörűen lefedi a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek interfészeit.
3. A szervezet követelje meg a fejlesztőtől, hogy bizonyítsa, hogy a leíró jellegű magasszintű specifikáció pontosan leírja a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek interfészeit.
4. A szervezetnek meg kell követelnie a fejlesztőtől, hogy írja le azokat a mechanizmusokat, amelyeket nem vesz figyelembe az informális, leíró jellegű magasszintű specifikáció, de a biztonsági szempontból releváns hardveren, szoftveren vagy firmware-en belül működnek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.129. Referenciának való megfelelőség vizsgálata

16.7. Beszerzések

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

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

SA-17(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.92. Fejlesztői biztonsági architektúra és tervezés – Egyszerű tervezési koncepció

16.92. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.92.1. úgy tervezze és strukturálja a biztonsági szempontból releváns hardvereket, szoftvereket és firmware-eket, hogy azok teljes, koncepcionálisan egyszerű védelmi mechanizmusokat alkalmazzanak, és amelyeknek a szemantikája pontosan meghatározott; és

16.92.2. a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek belső struktúráját ezen védelmi mechanizmus figyelembevételével alakítsa ki.

Magyarázat

A csökkentett komplexitás elve azt mondja ki, hogy az EIR tervezése a lehető legegyszerűbb és legkisebb legyen (lásd: Minimalizált komplexitás biztonságtervezési elve). A kicsi és egyszerű terv könnyebben érthető és elemezhető, valamint kevésbé hibaérzékeny (lásd: Biztonsági elemek minimalizálása biztonságtervezési elve; Referenciának való megfelelőség vizsgálata). A csökkentett komplexitás elve az EIR bármely aspektusára vonatkozik, de a biztonság szempontjából különös jelentőséggel bír az EIR kialakuló biztonsági tulajdonságára vonatkozó bizonyítékok megszerzése érdekében végzett különböző elemzések miatt. Ahhoz, hogy ezek az elemzések sikeresek legyenek, elengedhetetlen a kis és egyszerű tervezés. A csökkentett komplexitás elvének alkalmazása hozzájárul ahhoz, hogy a rendszerfejlesztők megértsék az EIR biztonsági funkcióinak helyességét és teljességét, és megkönnyíti a potenciális sebezhetőségek azonosítását. A csökkentett komplexitás következménye azt állítja, hogy az EIR egyszerűsége közvetlen kapcsolatban áll a benne található sebezhetőségek számával. Azaz az egyszerűbb EIR-ek kevesebb sebezhetőséget tartalmaznak. A csökkentett összetettség fontos előnye, hogy könnyebb megérteni, hogy az EIR tervezése során a biztonsági szabály érvényesül-e, és hogy a műszaki fejlesztés során valószínűleg kevesebb sebezhetőség kerül bevezetésre. További előny, hogy a helyességre, teljességre és a sebezhetőségek meglétére vonatkozó következtetések nagyobb bizonyossággal vonhatók le, szemben azokkal a következtetésekkel, amelyek olyan helyzetekben születnek, amikor a rendszertervezés eleve összetettebb.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a biztonsági szempontból releváns hardvereket, szoftvereket és firmware-eket úgy tervezze és strukturálja, hogy azok teljes, koncepcionálisan egyszerű védelmi mechanizmusokat alkalmazzanak. Ez azt jelenti, hogy a tervezésnek egyszerűnek és kis méretűnek kell lennie, hogy könnyen érthető és elemezhető legyen, valamint kevésbé hajlamos legyen a hibákra.
2. A szervezetnek biztosítania kell, hogy a fejlesztő a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek belső struktúráját a védelmi mechanizmus figyelembevételével alakítsa ki. Ez azt jelenti, hogy a fejlesztőnek meg kell értenie a védelmi funkciók helyességét és teljességét, és fel kell ismernie a potenciális sebezhetőségeket.
3. A szervezetnek biztosítania kell, hogy a fejlesztő a védelmi mechanizmusokat az EIR minden aspektusában alkalmazza, különösen a biztonság szempontjából, mivel ezeket az elemzéseket végezzük a rendszer biztonsági tulajdonságainak bizonyítása érdekében.
4. A szervezetnek biztosítania kell, hogy a fejlesztő könnyen megértse, hogy a biztonsági szabályzat megfelelően van-e beépítve az EIR tervezésébe, és hogy kevesebb sebezhetőség kerül bevezetésre a fejlesztés során. Ezenkívül a szervezetnek biztosítania kell, hogy a fejlesztő magasabb bizonyossággal jusson el a helyesség, teljesség és a sebezhetőségek következtetéséhez, mint abban helyzetekben, ahol az EIR tervezése alapvetően bonyolultabb.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.129. Referenciának való megfelelőség vizsgálata

16.16. Biztonságtervezési elvek

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

SA-17(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.93. Fejlesztői biztonsági architektúra és tervezés – Tesztelési struktúra

16.93. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan módon strukturálja a rendszereket és rendszerelemeket, hogy azok könnyen tesztelhetők legyenek a biztonsági hibák és sérülékenységek szempontjából.

Magyarázat

A biztonsági tervezési elvek alkalmazása elősegíti az EIR-ek, rendszerelemek és szolgáltatások teljes, következetes és átfogó tesztelését és értékelését. Az ilyen tesztelés alaposság hozzájárul az EIR, rendszerelem vagy szolgáltatás megbízhatóságára vonatkozó hatékony megbízhatósági eset vagy érv létrehozásához szükséges bizonyítékokhoz.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy alkalmazza az SP 800-160-1 biztonsági tervezési elveit.
2. A szervezetnek biztosítania kell, hogy az EIR-ek, rendszerelemek és rendszerszolgáltatások teljes, következetes, átfogó tesztelését és értékelését végezzék el.
3. A szervezetnek elő kell állítania a tesztelés eredményeiből származó bizonyítékokat, amelyek alátámasztják az EIR, rendszerelem vagy rendszerszolgáltatás megbízhatóságát.
4. A szervezetnek dokumentálnia kell a tesztelési és értékelési folyamatot, beleértve a tesztelési eredményeket és a megtett intézkedéseket.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a tesztelési és értékelési folyamatot, hogy biztosítsa az EIR, rendszerelemek és rendszerszolgáltatások folyamatos biztonságát.

Kapcsolódó intézkedések

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció
16.66. Fejlesztői biztonsági tesztelés

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

SA-17(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.94. Fejlesztői biztonsági architektúra és tervezés – Struktúra a legkisebb jogosultság elvéhez

16.94. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy úgy strukturálja a biztonsági szempontból releváns hardvert, szoftvert és firmware-t, hogy könnyen megvalósítható legyen a legkisebb jogosultság elvén alapuló hozzáférési szabályozás.

Magyarázat

A legkisebb jogosultság elve szerint minden elemnek elegendő jogosultságot biztosítanak a meghatározott funkcióinak ellátásához, de nem többet. A legkisebb jogosultság elvének alkalmazása korlátozza az elemek műveleteinek hatókörét, aminek két kívánatos hatása van. Először is, a rendszerelem meghibásodásának, sérülésének vagy visszaélésének biztonsági hatása minimálisra csökken. Másodszor, a rendszerelem biztonsági elemzése egyszerűsödik. A legkisebb jogosultság egy mindenre kiterjedő elv, amely a biztonságos rendszertervezés minden aspektusában visszaköszön. A rendszerelem képességének lehívására használt interfészek csak a felhasználók bizonyos részhalmazai számára állnak rendelkezésre, és az elemek tervezése támogatja a jogosultságok kellő finomságú dekompozícióját. Például egy naplózási mechanizmus esetében lehet egy interfész a naplózásért felelős részére, aki a naplózási beállításokat konfigurálja; egy interfész a naplózási operátor számára, aki biztosítja a naplózási adatok biztonságos összegyűjtését és tárolását; és végül egy másik interfész a naplózási ellenőr számára, akinek csak az összegyűjtött naplózási adatokat kell felülvizsgálnia, de nem kell műveleteket végrehajtania az adatokon.

Az EIR interfészén való megjelenésén túlmenően a legkisebb jogosultság az EIR belső felépítésének vezérelveként is használható. A belső legkisebb jogosultság egyik szempontja a modulok olyan felépítése, hogy a modulon belüli függvények csak a modul által lezárt elemeket kezelik közvetlenül. A modulon kívüli elemekhez, amelyeket a modul működése befolyásolhat, közvetett módon, az ezeket az elemeket tartalmazó modullal való kölcsönhatáson keresztül lehet hozzáférni. A belső legkisebb jogosultság másik aspektusa az, hogy egy adott modul vagy elem hatóköre csak azokat a rendszerelemeket tartalmazza, amelyek a funkcionalitásához szükségesek, és az elemekhez való hozzáférési módok (pl. olvasás, írás) minimálisak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a biztonsági szempontból releváns hardvert, szoftvert és firmware-t úgy strukturálja, hogy könnyen megvalósítható legyen a legkisebb jogosultság elvén alapuló hozzáférési szabályozás.
2. A szervezetnek biztosítania kell, hogy minden elem csak a szükséges jogosultságokkal rendelkezzen a meghatározott funkciók elvégzéséhez, de ne többel.
3. A szervezetnek biztosítania kell, hogy a legkisebb jogosultság elve minden EIR tervezési aspektusában jelen legyen. A rendszerelem képességének meghívására szolgáló interfészek csak bizonyos felhasználói csoportok számára érhetők el, és a rendszerelem tervezése támogatja a jogosultságok elegendően finomságú dekompozícióját.
4. A szervezetnek biztosítania kell, hogy a legkisebb jogosultság elve az EIR belső struktúrájára is alkalmazva legyen. Az egyik aspektusa ennek, hogy a modulokat úgy kell felépíteni, hogy csak a modul által kapszulázott elemeken működjenek közvetlenül a modulon belüli funkciók. A modulon kívüli elemeket, amelyeket a modul működése érinthet, közvetetten kell elérni azokat tartalmazó modullal való interakció révén.
5. A szervezetnek biztosítania kell, hogy egy adott modul vagy elem hatóköre csak azokat a rendszerelemeket tartalmazza, amelyek szükségesek a funkcionalitásához, és az elemekhez való hozzáférési módok (pl. olvasás, írás) minimálisak legyenek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.59. Felelősségek szétválasztása
2.60. Legkisebb jogosultság elve
16.16. Biztonságtervezési elvek

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

SA-17(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.95. Fejlesztői biztonsági architektúra és tervezés – Összehangolás

16.95. A szervezet meghatározza és megtervezi azokat a szervezet működése szempontjából kritikus EIR-eket, vagy rendszerelemeket, amelyek összehangoltan működnek a szervezet által meghatározott képességek végrehajtása érdekében.

Magyarázat

Az elosztott, különböző rétegekben vagy rendszerelemekben elhelyezkedő, vagy a megbízhatóság különböző szempontjait támogató biztonsági erőforrások előre nem látható vagy helytelen módon léphetnek kölcsönhatásba egymással. A kedvezőtlen következmények közé tartozhatnak a kaszkádszerű hibák, az interferencia vagy a lefedettségi hiányosságok. A biztonsági erőforrások viselkedésének összehangolása elkerülheti az ilyen negatív kölcsönhatásokat.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania és listáznia kell azokat az rendszerelemeket, amelyek kritikusak a szervezet működése szempontjából.
2. A szervezetnek meg kell terveznie, hogyan működnek összehangoltan ezek a rendszerelemek a szervezet által meghatározott képességek végrehajtása érdekében.
3. A szervezetnek figyelembe kell vennie, hogy a biztonsági erőforrások elosztottak, különböző rétegekben vagy különböző rendszerelemekben találhatók, vagy különböző megbízhatósági aspektusok támogatására vannak implementálva, és ezek nem várt vagy hibás módon működhetnek együtt.
4. A szervezetnek meg kell terveznie, hogyan koordinálja a biztonsági erőforrások viselkedését, hogy elkerülje az ilyen negatív kölcsönhatásokat.
5. A szervezetnek dokumentálja a biztonsági erőforrások viselkedését és a változásokat a rendszerelemekben, hogy nyomon követhesse azokat.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kritikus rendszerelemek listáját és a hozzájuk kapcsolódó koordinációs terveket, hogy biztosítsa a szervezet által meghatározott képességek folyamatos 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

SA-17(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kritikus rendszerek vagy rendszerelemek illetve a képességek (rendszer vagy rendszerelemek szerint) meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.96. Fejlesztői biztonsági architektúra és tervezés – Tervezési modellek diverzifikálása

16.96. A szervezet különböző tervezési modelleket alkalmaz az általa meghatározott és a szervezet működése szempontjából kritikus EIR-ek, vagy rendszerelemek esetében, hogy kielégítsen egy közös követelménykészletet vagy, hogy egyenértékű funkcionalitást biztosítson.

Magyarázat

A tervezési változatosságot úgy érik el, hogy ugyanazt a követelményspecifikációt több fejlesztőnek adják meg, akik mindegyike az EIR vagy a rendszerelem egy olyan változatának kifejlesztéséért felelős, amely megfelel a követelményeknek. A változatok lehetnek a szoftvertervezésben, a hardvertervezésben, vagy mind a hardver-, mind a szoftvertervezésben. A változatok tervezése közötti különbségek adódhatnak a fejlesztők tapasztalataiból, a tervezési stílusból (pl. egy szükséges funkció kisebb feladatokra bontásakor annak meghatározása, hogy mi számít különálló feladatnak, és hogy a feladatokat milyen mértékben kell részfeladatokra bontani), a változatba beépítendő könyvtárak kiválasztásából és a fejlesztőkörnyezetből (pl. a különböző tervezési eszközök egyes tervezési mintákat könnyebben megjeleníthetővé tesznek). A hardvertervezés sokfélesége magában foglalja a különböző döntések meghozatalát arra vonatkozóan, hogy milyen információt tartsunk meg analóg formában, és milyen információt alakítsunk át digitális formába, ugyanazt az információt különböző időpontokban továbbítsuk, és késleltetést vezessünk be a mintavételezésben (időbeli sokféleség). A tervezési diverzitást általában a hibatűrés támogatására használják.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, mely EIR-ek kritikusak a működése szempontjából.
2. A szervezetnek különböző tervezési modelleket kell alkalmaznia ezekre az EIR-ekre. A tervezési modellek lehetnek szoftver alapúak, hardver alapúak, vagy mindkettőt magukban foglalhatják.
3. A tervezési modellek különbözősége lehet a fejlesztők tapasztalatán, a tervezési stíluson, a beépített könyvtárak kiválasztásán, és a fejlesztési környezeten alapuló.

4. A hardver tervezési diverzitás magában foglalhatja az analóg és digitális információ kezelésének különbözőségét, az információ különböző időpontokban történő továbbítását, és a mintavételi késleltetések bevezetését.
5. A szervezetnek biztosítania kell, hogy a különböző tervezési modellek kielégítik a közös követelménykészletet, vagy egyenértékű funkcionalitást biztosítanak.
6. A tervezési diverzitás gyakran használt módszer a hibatűrés támogatására, ezért a szervezetnek dokumentálnia kell a nyomon követhetőség érdekében az EIR működését és az esetleges hibákat.
7. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a tervezési modelleket, hogy biztosítsa az EIR-ek biztonságát és hatékonyságát.

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

SA-17(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

16.97. KRITIKUS RENDSZERELEMEK EGYEDI FEJLESZTÉSE

16.97. A szervezet újratervezi vagy egyedileg továbbfejleszti az általa meghatározott és a szervezet működése szempontjából kritikus rendszerelemeket.

MAGYARÁZAT

Az érintett szervezetek megállapítják, hogy bizonyos rendszerelemek valószínűleg nem megbízhatóak, mivel azok olyan konkrét fenyegetéseknek és sebezhetőségeknek vannak kitéve, amelyekre nem léteznek megfelelő, kockázat csökkentésre alkalmas biztonsági intézkedések. Az ilyen elemek újbóli megvalósítása vagy egyedi fejlesztése megfelelhet a magasabb szintű megbízhatósági követelményeknek, és a rendszerelemek olyan változtatásainak kezdeményezésével történik, amelyek révén a támadók által elkövetett standard támadások sikere kevésbé lesz valószínű. Azokban az esetekben, amikor nem áll rendelkezésre alternatív beszerzési forrás, és a szervezetek úgy döntenek, hogy nem implementálják újra vagy fejlesztik ki a kritikus rendszerelemeket, további intézkedéseket kell alkalmazni. Az intézkedések közé tartozik a fokozott naplózás, a forráskódhoz és az EIR segédprogramjaihoz való hozzáférés korlátozása, valamint a rendszer- és alkalmazásfájlok törlése elleni védelem.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell állapítania, hogy bizonyos rendszerelemek valószínűleg nem megbízhatóak, mivel ezekben az elemekben specifikus fenyegetések és sebezhetőségek vannak, és a kockázatok mérséklésére nincsenek megfelelő biztonsági intézkedés.
2. A szervezetnek biztosítania lehet az ilyen elemek újratervezését vagy egyedi fejlesztését, ami kielégítheti a magasabb biztonsági követelményeket, és a rendszerelemekben változásokat kezdeményezhet, hogy a sikeres támadások bekövetkezése kevésbé legyen valószínű.
3. Amennyiben nem létezik megfelelő alternatív forrás a szervezetnek úgy lehet döntenie, hogy nem tervezi újra vagy nem fejleszti tovább a kritikus rendszerelemeket és helyette más intézkedéseket vezet be. Az intézkedések közé tartozik a naplózás fokozása, a forráskódhoz és az EIR segédprogramokhoz való hozzáférés korlátozása, valamint a rendszer- és alkalmazásfájlok törlésének védelme.

Kapcsolódó intézkedések

7.2. Üzletmenet-folytonossági terv

15.21. Rendszerelemek kritikusságának elemzése

16.16. Biztonságtervezési elvek

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

SA-20

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a kritikus rendszerelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

16.98. KÜLSŐ FEJLESZTŐK HÁTTÉRELLENŐRZÉSE

16.98. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

16.98.1. rendelkezzen a hivatalos feladatok alapján meghatározott megfelelő hozzáférési jogosultságokkal; és

16.98.2. teljesítse a szervezet által meghatározott további átvilágítási kritériumokat.

MAGYARÁZAT

A fejlesztői átvilágítás a külső fejlesztőkre irányul. A belső fejlesztői átvilágítással a személyek háttérellenőrzése című biztonsági követelmény foglalkozik. Mivel lehetséges, hogy az EIR, rendszerelem vagy rendszerszolgáltatás alapvető fontosságú kritikus tevékenységekben használható, az érintett szervezeteknek komoly érdeke fűződik ahhoz, hogy a fejlesztők megbízhatóak legyenek. A fejlesztőktől megkövetelt bizalom mértékének összhangban kell lennie az EIR-ekhez, rendszerelemekhez vagy rendszer-szolgáltatásokhoz a telepítést követően hozzáférő személyek bizalmával. Az engedélyezési és személyzeti átvilágítási kritériumok közé tartoznak a biztonsági átvilágítások, a háttérellenőrzések, az állampolgárság és a nemzetiség ellenőrzése. A fejlesztők megbízhatósága magában foglalhatja a szervezeti tulajdonviszonyok és a szervezetnek az olyan jogalanyokkal fennálló kapcsolatainak felülvizsgálatát és elemzését is, amelyek potenciálisan befolyásolhatják a fejlesztendő EIR-ek, elemek vagy szolgáltatások minőségét és megbízhatóságát. Az előírt hozzáférési jogosultságok és a személyzeti átvilágítási kritériumok teljesítése magában foglalja a kiválasztott EIR-en, rendszerelemen vagy rendszerszolgáltatáson fejlesztési tevékenységet végezni jogosult összes személy listájának rendelkezésre bocsátását, hogy a szervezetek ellenőrizhessék, hogy valamennyi külsős fejlesztő teljesítette-e az engedélyezési és átvilágítási követelményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a fejlesztők számára szükséges hozzáférési jogosultságokat és átvilágítási kritériumokat. Ezek a kritériumok tartalmazhatják a biztonsági engedélyeket, háttér ellenőrzéseket, állampolgárság és nemzetiség ellenőrzését.

2. A szervezetnek meg kell követelnie az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy rendelkezzen a hivatalos feladatok alapján meghatározott megfelelő hozzáférési jogosultságokkal.
3. A szervezetnek meg kell követelnie a fejlesztőtől, hogy teljesítse a szervezet által meghatározott további átvilágítási kritériumokat. Ez magában foglalhatja a cég tulajdonosi szerkezetének és kapcsolatainak áttekintését és elemzését, amelyek potenciálisan befolyásolhatják az EIR, rendszerelemek vagy rendszerszolgáltatások minőségét és megbízhatóságát.
4. A szervezetnek biztosítania kell, hogy a fejlesztők megbízhatóak. A fejlesztőkben való bizalom mértékének összhangban kell lennie azoknak az egyéneknek a bizalmával, akik hozzáférnek az EIR-hez, rendszerelemekhez vagy rendszerszolgáltatásokhoz, amint azok telepítésre kerülnek.
5. A szervezetnek ellenőriznie kell, hogy a fejlesztő teljesítette-e a hozzáférési jogosultságokat és az átvilágítási kritériumokat. Ez magában foglalja az összes olyan személy listájának biztosítását, akik jogosultak a kiválasztott EIR, rendszerelem vagy rendszerszolgáltatás fejlesztési tevékenységeinek végrehajtására, így az érintett szervezet ellenőrizheti, hogy valamennyi külsős fejlesztő teljesítette-e a hozzáférési és átvilágítási követelményeket.
6. A szervezetnek dokumentálnia kell a fejlesztők hozzáférési jogosultságait és átvilágítási kritériumait, azok felülvizsgálatainak eredményeit, hogy biztosítsa a folyamat átláthatóságát és nyomon követhetőségét.

Kapcsolódó intézkedések

14.2. Munkakörök biztonsági szempontú besorolása
14.3. Személyek háttérellenőrzése
14.9. Hozzáférési megállapodások
14.11. Külső személyekhez kapcsolódó biztonsági követelmények
16.7. Beszerzések
19.16. Beszállítók értékelése és felülvizsgálata

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.6.1

NIST SP 800-53 REV.5 REFERENCIA

SA-21

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az EIR, rendszerelem vagy rendszerszolgáltatás meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

16.99. TÁMOGATÁSSAL NEM RENDELKEZŐ RENDSZERELEMEK

16.99. A szervezet:

16.99.1. lecseréli a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetve

16.99.2. a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg.

MAGYARÁZAT

A rendszerelemek támogatása magában foglalja a szoftverjavításokat, a firmware-frissítéseket, a cserealkatrészeket és a karbantartási szerződéseket. A nem támogatott elemekre példa, amikor a gyártók már nem biztosítanak kritikus szoftverjavításokat vagy termékfrissítéseket, ami lehetőséget adhat a támadóknak a telepített elemek gyengeségeinek kihasználására. A nem támogatott rendszerelemek cseréje alóli kivételek közé tartoznak a kritikus ügymeneti vagy üzleti képességeket biztosító rendszerek, ahol nem állnak rendelkezésre újabb technológiák, vagy ahol az EIR-ek annyira elszigeteltek, hogy a csereelemek telepítése nem lehetséges.

Az alternatív támogatási források arra az igényre vonatkoznak, hogy folyamatos támogatást nyújtsanak az eredeti gyártók, fejlesztők vagy szállítók által már nem támogatott rendszerelemekhez, amennyiben ezek az elemek továbbra is alapvető fontosságúak a szervezeti ügymeneti és az üzleti funkciók szempontjából. Szükség esetén a szervezetek a kritikus szoftverelemekhez testreszabott javítások kifejlesztésével házon belüli támogatást hozhatnak létre, vagy alternatívaként külső szolgáltatók szolgáltatásait vehetik igénybe, akik szerződéses kapcsolatok révén folyamatos támogatást nyújtanak a kijelölt, nem támogatott elemekhez. Az ilyen szerződéses kapcsolatok közé tartozhatnak a nyílt forráskódú szoftverek értéknövelő szállítói. A nem támogatott rendszerelemek használatának megnövekedett kockázata csökkenthető például az ilyen elemek nyilvános vagy nem ellenőrzött hálózatokhoz való csatlakoztatásának megtiltásával, vagy az elszigetelés más formáinak megvalósításával.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek le kell cserélnie a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól. Ez magában foglalja a szoftverfrissítéseket, firmware frissítéseket, alkatrész cseréket és karbantartási szerződéseket.
2. Ha a rendszerelemek támogatása már nem elérhető, és ezek az elemek továbbra is létfontosságúak a szervezet ügymeneti és üzleti funkcióihoz, akkor a szervezetnek alternatív támogatást kell biztosítania.
3. Az alternatív támogatás biztosítása magában foglalhatja a belső erőforrások használatát, például a kritikus szoftverelemekhez szükséges egyedi javítások kifejlesztését.
4. Alternatív megoldásként a szervezetnek lehetősége van bevonnia külső szolgáltatókat, akik szerződéses kapcsolatok révén folyamatos támogatást nyújtanak a támogatás nélküli rendszerelemekhez.
5. A szervezetnek csökkentenie kell a rendszerelemek használatának kockázatát, például azzal, hogy megtiltja ezeknek az elemeknek a nyilvános vagy ellenőrizetlen hálózatokhoz való csatlakozását, vagy más izolációs formákat alkalmaz.
6. A szervezetnek dokumentálnia kell az összes lépést, hogy bizonyíthassa a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

13.2. Rendszerbiztonsági terv

16.3.1. A rendszer fejlesztési életciklusa

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

SA-22

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

16.100. SPECIÁLIS KÖVETELMÉNYEK

16.100. A szervezet tervezési, módosítási, bővítési vagy újrakonfigurálási eljárásokat alkalmaz azon rendszereken vagy rendszerelemeken, amelyek a szervezet számára nélkülözhetetlen szolgáltatásokat vagy funkciókat támogatnak.

MAGYARÁZAT

Az erőforrás megbízhatóságának maximalizálása érdekében gyakran szükséges, hogy az ügymenet szempontjából létfontosságú szolgáltatásokat vagy funkciókat támogató EIR-t vagy rendszerelemet továbbfejlesszék. Néha ez a fejlesztés a tervezés szintjén történik. Más esetekben a tervezést követően, vagy a szóban forgó rendszer módosításával, vagy az EIR további elemekkel történő bővítésével. Például kiegészítő hitelesítési vagy letagadhatatlansági funkciókkal egészíthető ki az EIR, hogy a kritikus erőforrások azonosságát a szervezet által meghatározott erőforrástól függő más erőforrásokkal szemben javítsák.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a rendszerelemeket, amelyek létfontosságú szolgáltatásokat vagy funkciókat támogatnak.
2. A szervezetnek tervezési eljárásokat kell alkalmaznia a rendszerelemeken, hogy maximalizálja az erőforrások megbízhatóságát. Ez magában foglalhatja a rendszerelemek új tervezését vagy a meglévők módosítását.
3. A szervezetnek módosítási eljárásokat kell alkalmaznia a létfontosságú rendszerelemeken, ha szükséges. Ez magában foglalhatja a meglévő rendszerelemek módosítását vagy újrakonfigurálását, hogy jobban megfeleljenek a kiberbiztonsági követelményeknek.
4. A szervezetnek bővítési eljárásokat kell alkalmaznia a rendszerelemeken, ha szükséges. Ez magában foglalhatja új rendszerelemek hozzáadását a meglévőkhöz, hogy növeljék a rendszer kiberbiztonsági védelmét.
5. A szervezetnek újrakonfigurálási eljárásokat kell alkalmaznia a rendszerelemeken, ha szükséges. Ez magában foglalhatja a meglévő rendszerelemek újrakonfigurálását, hogy jobban megfeleljenek a kiberbiztonsági követelményeknek.

6. A szervezetnek dokumentálnia kell a rendszerelemek tervezési, módosítási, bővítési és újrakonfigurálási eljárásait, hogy nyomon követhesse azokat. Ez segít az érintett szervezetnek bizonyítani, hogy megfelel a kiberbiztonsági követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.21. Rendszerelemek kritikusságának elemzése

16.16. Biztonságtervezési elvek

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

SA-23

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024