Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Konfigurációkezelés

Verzió 1.0

2024

Tartalomjegyzék

6.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

6.1. A szervezet:

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

6.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó konfigurációkezelési szabályzatot, amely

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

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

6.1.1.2. A konfigurációkezelési eljárásrendet, amely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

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

MAGYARÁZAT

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

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

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

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

Kapcsolódó intézkedések

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

16.16. Biztonságtervezési elvek

18.67. Információ kezelése és megőrzése

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

3.3.6.1. Konfigurációkezelési eljárásrend

ISO/IEC 27001:2023 referencia

5.2; 5.3; 7.5.1; 7.5.2; 7.5.3; A.5.1; A.5.2; A.5.4; A.5.31; A.5.36; A.5.37; A.8.9

NIST SP 800-53 rev.5 referencia

CM-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

6.2. ALAPKONFIGURÁCIÓ

6.2. A szervezet:

6.2.1. Kifejleszti, dokumentálja és karbantartja az EIR alapkonfigurációját.

6.2.2. Elvégzi az EIR alapkonfigurációjának felülvizsgálatát és frissítését:

6.2.2.1. meghatározott időközönként;

6.2.2.2. ha azt a meghatározott körülmények indokolják, vagy

6.2.2.3. az EIR vagy rendszerelemek telepítésekor vagy frissítésekor.

MAGYARÁZAT

Az EIR-ek és a rendszerelemek alapkonfigurációi a rendszerek csatlakoztathatósági, üzemeltetési és kommunikációs szempontjait foglalják magukban. Az alapkonfigurációk a rendszerek vagy a rendszereken belüli konfigurációs elemek dokumentált, hivatalosan felülvizsgált és elfogadott specifikációi. Az alapkonfigurációk szolgálnak a rendszerek jövőbeni felépítésének, kiadásának vagy módosításának alapjául, és tartalmazzák a biztonsági követelmények végrehajtását, az üzemeltetési eljárásokat, a rendszerelemekre vonatkozó információkat, a hálózati topológiát és az összetevők logikai elhelyezését a rendszerarchitektúrában. Az alapkonfigurációk fenntartása új alapkonfigurációk létrehozását teszi szükségessé, ahogy a szervezeti rendszerek idővel változnak. A rendszerek alapkonfigurációi az aktuális szervezeti architektúrát tükrözik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell fejlesztenie az EIR alapkonfigurációját, amely magában foglalja az EIR és a rendszerelemeinek csatlakoztathatósági, üzemeltetési és kommunikációs aspektusait.
2. A szervezetnek dokumentálnia kell az EIR alapkonfigurációját, melyet a szervezetnek felül kell vizsgálnia és el kell fogadnia. Ez a dokumentáció tartalmazza a biztonsági elvárások implementációját, az üzemeltetési eljárásokat, a rendszerelemekre vonatkozó információkat, a hálózati topológiát és az az összetevők logikai elhelyezését a rendszerarchitektúrában.
3. A szervezetnek karban kell tartania az EIR alapkonfigurációját, ami azt jelenti, hogy a szervezetnek idővel új alapkonfigurációt kell létrehoznia, ahogy a szervezeti rendszerek változnak.

4. A szervezetnek meghatározott időközönként felül kell vizsgálnia és frissítenie kell az EIR és a rendszerelemek alapkonfigurációját.
5. Az EIR vagy az EIR rendszerelemeinek telepítésekor vagy frissítésekor a szervezetnek felül kell vizsgálnia és frissítenie kell az EIR alapkonfigurációját.
6. A szervezetnek nyilvántartást kell vezetnie az EIR alapkonfigurációjának felülvizsgálatáról és frissítéséről.

Kapcsolódó intézkedések

2.113. Mobil eszközök hozzáférés-ellenőrzése
4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
5.24. Belső rendszerkapcsolatok
6.1. Szabályzat és eljárásrendek
6.7. A konfigurációváltozások felügyelete (változáskezelés)
6.18. A változtatásokra vonatkozó hozzáférés korlátozások
6.23. Konfigurációs beállítások
6.36. Rendszerelem leltár
6.45. Konfigurációkezelési terv
7.35. Az elektronikus információs rendszer mentései

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

3.3.6.2. Alapkonfiguráció

ISO/IEC 27001:2023 referencia

A.8.9

NIST SP 800-53 rev.5 referencia

CM-2

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

6.3. ALAPKONFIGURÁCIÓ – AUTOMATIKUS TÁMOGATÁS A PONTOSSÁG ÉS A NAPRA KÉSZSÉGÉRDEKÉBEN

6.3. A szervezet automatizált mechanizmusokat alkalmaz az EIR naprakész, teljes, pontos és állandóan rendelkezésre álló alapkonfigurációjának karbantartására.

MAGYARÁZAT

Az automatizált mechanizmusok, amelyek segítenek a szervezethez köthető EIR-ek konzisztens alapkonfigurációinak fenntartásában, magukban foglalják a konfigurációkezelő eszközöket, a hardver-, szoftver- és firmware leltárkészítő eszközöket, valamint a hálózatkezelési eszközöket. Az automatizált eszközök használhatók az érintett szervezet szintjén, a szervezeti célok és az üzleti folyamatok szintjén vagy rendszerszinten munkaállomásokon, szervereken, notebook számítógépeken, hálózati elemeken vagy mobil eszközökön. Az eszközökkel nyomon követhetők az operációs rendszerek, alkalmazások verziószámai, a telepített szoftverek típusai és az aktuálisan telepített javítások (patch). A pontosság és naprakészség automatizálási támogatása "Rendszerelem leltár – Automatizált karbantartás" pontban megfogalmazott biztonsági elvárások teljesítésével elégíthető ki azon szervezetek esetében, amelyek a rendszerelemek leltározását és az alapkonfigurációs tevékenységeket kombinálják.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy milyen automatizált mechanizmusokra van szüksége az EIR naprakész, teljes, pontos és állandóan rendelkezésre álló alapkonfigurációjának karbantartására.
2. A szervezetnek be kell szereznie és alkalmaznia kell a meghatározott automatizált mechanizmusokat, melyek lehetnek konfigurációkezelő eszközök, hardver-, szoftver- és firmware leltárkészítő eszközök, valamint hálózatkezelési eszközök.
3. A szervezet az automatizált eszközöket alkalmazhatja szervezeti szinten, a szervezeti célok és az üzleti folyamatok szintjén vagy rendszerszinten (munkaállomásokon, szervereken, notebook számítógépeken, hálózati elemeken vagy mobil eszközökön).

4. A szervezetnek nyomon kell követnie az operációs rendszerek, alkalmazások verziószámait, a telepített szoftverek típusait és az aktuálisan telepített javításokat (patch).

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.26. Legszűkebb funkcionalitás

8.10. Eszközök azonosítása és hitelesítése

15.10. Sérülékenységmonitorozás és szkennelés

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

3.3.6.2. Alapkonfiguráció

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-2(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

6.4. ALAPKONFIGURÁCIÓ – KORÁBBI KONFIGURÁCIÓK MEGŐRZÉSE

6.4. A szervezet megőrzi az EIR alapkonfigurációjának a szervezet által meghatározott számú korábbi verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.

MAGYARÁZAT

Az alapkonfigurációk korábbi verzióinak megőrzése a visszaállítás támogatása érdekében magában foglalja a hardvert, a szoftvert, a firmware-t, a konfigurációs fájlokat, a konfigurációs nyilvántartásokat és a kapcsolódó dokumentációt.

Az alapkonfiguráció adatai fontosak az EIR működésének megértéséhez és a hibaelhárításhoz. Az érintett szervezet által meghatározott számú korábbi verzió megőrzése lehetővé teszi, hogy a szervezet visszatérjen az EIR korábbi állapotához, ha szükséges. Ez különösen hasznos lehet, ha a jelenlegi konfiguráció problémákat okoz, vagy ha a szervezetnek vissza kell térnie egy korábbi konfigurációhoz biztonsági vagy működési okokból.

A korábbi verziók megőrzése azt is lehetővé teszi az érintett szervezet számára, hogy naplózza és nyomon kövesse az EIR konfigurációs változásait. Ez segíthet azonosítani a konfigurációs változásokat, amelyek problémákat okozhatnak, és segíthet a jövőbeni konfigurációs változások tervezésében és végrehajtásában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy hány korábbi verziót szeretne megőrizni az EIR alapkonfigurációjából. Ez a szám függ a szervezet belső szabályaitól, a rendelkezésre álló tárhelytől és a visszaállítási igényektől.

2. A szervezetnek meg kell őriznie az EIR alapkonfigurációjának meghatározott számú korábbi verzióit. Ez magában foglalja a hardver, szoftver, firmware, konfigurációs fájlok, konfigurációs adatok és a hozzájuk kapcsolódó dokumentáció mentését.

3. A szervezetnek a folyamat során szem előtt kell tartania a mentésre vonatkozó követelményeket (biztonságos tárolás, mentések tesztelése, visszaállítási folyamat meghatározása és rendszeres időközönkénti gyakorlása stb.).

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.3.6.2. Alapkonfiguráció

ISO/IEC 27001:2023 referencia

A.8.9

NIST SP 800-53 rev.5 referencia

CM-2(3)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a szám meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

6.5. ALAPKONFIGURÁCIÓ – FEJLESZTÉSI ÉS TESZTKÖRNYEZETEK

6.5. A szervezet egy-egy alapkonfigurációt tart fenn a rendszerfejlesztési és tesztkörnyezetekhez, amelyeket külön kezel az élesüzemi alapkonfigurációtól.

MAGYARÁZAT

Külön alapkonfigurációk létrehozása a fejlesztési, tesztelési és üzemeltetési környezetekhez megvédi az EIR-eket a fejlesztési és tesztelési tevékenységekhez kapcsolódó nem tervezett vagy váratlan eseményektől. A különálló alapkonfigurációk lehetővé teszik a szervezetek számára, hogy az egyes konfigurációtípusokhoz legmegfelelőbb konfigurációkezelést alkalmazzák. Például az üzemeltetési konfigurációk kezelése jellemzően a stabilitás szükségességét tartja szem előtt, míg a fejlesztési vagy tesztkonfigurációk kezelése nagyobb rugalmasságot igényel. A tesztkörnyezetben lévő konfigurációk az üzemeltetési környezetben lévő konfigurációkat tükrözik (amennyire ez kivitelezhető), hogy a tesztelés eredményei reprezentatívak legyenek az élesüzemi EIR-ekben javasolt változtatásokra vonatkozóan. A külön alapkonfigurációk nem feltétlenül igényelnek külön fizikai környezetet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia külön alapkonfigurációkat a fejlesztési, tesztelési és élesüzemi környezetek számára.
2. A szervezetnek biztosítania kell, hogy a különböző alapkonfigurációkat külön kezelje, és a legmegfelelőbb konfigurációkezelést alkalmazza minden egyes konfiguráció típusára.
3. A szervezetnek gondoskodnia kell arról, hogy a tesztelési környezetben lévő konfigurációk a lehető leginkább tükrözzék az élesüzemi környezetben lévő konfigurációkat, hogy a tesztelés eredményei reprezentatívak legyenek az élesüzemi EIR-ekben javasolt változtatásokra vonatkozóan.
4. A szervezetnek nem feltétlenül kell külön fizikai környezeteket létrehoznia a különböző alapkonfigurációk számára.

Kapcsolódó intézkedések

6.15. Biztonsági hatásvizsgálatok

17.4. Biztonsági funkciók elkülönítése

17.17. A határok védelme

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CM-2(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

6.6. Alapkonfiguráció – Rendszerek és rendszerelemek konfigurálása magas kockázatú területekre

6.6. A szervezet:

6.6.1. Meghatározott konfigurációs beállításokkal ellátott meghatározott EIR-eket vagy rendszerelemeket biztosít a szervezet által jelentős kockázatúnak ítélt helyszínen történő felhasználáshoz.

6.6.2. Meghatározott védelmi intézkedéseket alkalmaz a rendszerekre vagy rendszerelemekre a jelentős kockázatú helyszínekről történő visszatérést követően.

Magyarázat

Ha ismert, hogy az EIR-ek vagy rendszerelemek a szervezeten kívüli, magas kockázati besorolás alá eső területeken lesznek használva, akkor további védelmi intézkedéseket lehet bevezetni az ilyen területeken jelentkező fokozott fenyegetés elhárítására. A szervezet például védelmi intézkedéseket vezethet be a rendszeresen utazó személyek által használt hordozható számítógépek (pl.: notebook, mobil) esetében. Az intézkedések magukban foglalják kockázatos helyek meghatározását, a rendszerelemek szükséges konfigurációinak meghatározását, illetve annak biztosítását, hogy az utazás megkezdése előtt a rendszerelemek rendeltetésszerűen legyenek konfigurálva, valamint az utazás befejezését követően a rendszerelemekre vonatkozó intézkedések alkalmazását. A speciálisan konfigurált notebookok közé tartoznak a megtisztított merevlemezzel, korlátozott alkalmazásokkal és szigorúbb konfigurációs beállításokkal rendelkező számítógépek. A hordozható eszközökre az utazásból való visszatérés után alkalmazott intézkedések közé tartozik a hordozható eszköz vizsgálata a fizikai manipuláció jeleinek feltárására, valamint a lemezmeghajtók biztonságos törlése és újbóli telepítése. A hordozható eszközökön tárolt információkkal kapcsolatban az adathordozók védelmére vonatkozó védelmi intézkedések nyújtanak iránymutatást.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, hogy mely a szervezeten kívül eső területek minősülnek kockázatosnak az EIR vagy rendszerelemek használata szempontjából.

2. A szervezetnek meg kell határoznia azokat a szükséges konfigurációs beállításokat az EIR-ek vagy a rendszerelemek vonatkozásában, amelyeket a kockázatosnak ítélt helyszíneken használni kell pl.: a hordozható eszközök vonatkozásában milyen biztonsági előírásokat kell betartani, amennyiben azt a szervezeten kívül használja egy szervezethez köthető személy.
3. A szervezetnek biztosítania kell, hogy az EIR-ek vagy rendszerelemek a szükséges konfigurációs beállításokkal rendelkezzenek, mielőtt a kockázatosnak ítélt helyszínen használatra kerülnek.
4. A szervezetnek meg kell határoznia, hogy milyen védelmi megoldásokat kell alkalmazni, az EIR-ekre vagy rendszerelemekre a kockázatosnak ítélt helyszínekről történő visszatérést követően pl.: hordozható eszköz vizsgálata fizikai manipuláció jeleinek feltárására, lemezmeghajtók biztonságos törlése és újbóli telepítése.

Kapcsolódó intézkedések

11.4. Adathordozók tárolása
11.6. Adathordozók szállítása

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

3.3.6.2. Alapkonfiguráció

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CM-2(7)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

6.7. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE (VÁLTOZÁSKEZELÉS)

6.7. A szervezet:

6.7.1. Meghatározza és dokumentálja a változáskezelési felügyelet ellenőrzés hatálya alá eső rendszermódosításokat.

6.7.2. Megvizsgálja, valamint biztonsági szempontokat érvényesítve jóváhagyja vagy elutasítja a konfigurációra vonatkozó módosítási javaslatokat.

6.7.3. Dokumentálja az EIR-ben történt változtatásokra vonatkozó döntéseket.

6.7.4. Megvalósítja a jóváhagyott változtatásokat az EIR-ben.

6.7.5. Meghatározott időtartamig nyilvántartja és visszakereshetően megőrzi az EIR-ben megvalósított változtatások dokumentumait.

6.7.6. Ellenőrzi és felülvizsgálja a konfiguráció ellenőrzés hatálya alá eső változtatásokkal kapcsolatos tevékenységeket.

6.7.7. Koordinálja és felügyeli a konfigurációváltoztatásokat egy erre a célra kijelölt egység (például személy, testület, szoftver, folyamat stb.) által, amelyet meghatározott gyakorisággal vagy a konfigurációmódosítási feltételek fennállása esetén alkalmaznak.

MAGYARÁZAT

Az EIR konfigurációváltozásainak felügyelete alatt a szervezethez köthető EIR-ekre vonatkozó változási javaslatokat, azok indoklását, megvalósítását, tesztelését, felülvizsgálatát, illetve az ezek alapján elrendelt EIR-ben végrehajtott változásokat (pl.: frissítések és módosítások) értjük. A konfigurációváltozás felügyelete magában foglalja az alapkonfigurációk, az EIR konfigurációs elemeinek, a működési eljárások, valamint a rendszerelemek konfigurációs beállításainak változásait, illetve a sérülékenységek javítását, a nem tervezett vagy engedély nélküli változásokat. Az EIR-ek konfigurációs módosításainak kezelésére szolgáló folyamatok közé tartoznak a konfiguráció ellenőrzésére létrehozot testületek vagy a változtatásokkal kapcsolatos tanácsadó testületek, amelyek felülvizsgálják és jóváhagyják a javasolt változtatásokat. Új rendszer- vagy egyéb nagyobb frissítések esetén a szervezet fontolóra veszi, hogy a konfiguráció ellenőrzésére vagy a változtatásokkal kapcsolatos tanácsadó testületekbe bevonja a fejlesztői terület képviselőit is. A változtatások ellenőrzése magában foglalja az EIR-

ekben végrehajtott változtatások előtti és utáni tevékenységeket, valamint az ilyen változtatások végrehajtásához szükséges ellenőrzési tevékenységeket. A konfigurációváltozások felügyeletével kapcsolatos egyéb elvárások a "fejlesztői változáskövetés" kontrollnál kerültek kifejtésre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell azokat az rendszermódosításokat, amelyek a változáskezelési felügyelet hatálya alá esnek.
2. A szervezetnek gondoskodnia kell a konfigurációváltozások felügyeletének menedzseléséről, mely magában foglalja a szervezethez köthető EIR-ekre vonatkozó változási javaslatokat, azok indoklását, megvalósítását, tesztelését, felülvizsgálatát, illetve az ezek alapján elrendelt EIR-ben végrehajtott változásokat (pl.: frissítések és módosítások).
3. A szervezet szükség esetén létrehozhat olyan testületeket, melyek a konfigurációkat ellenőrzik, illetve amelyek felülvizsgálják és jóváhagyják a javasolt változtatásokat.
4. A szervezetnek meg kell vizsgálnia és biztonsági szempontokat érvényesítve jóvá kell hagynia vagy el kell utasítania az EIR konfigurációjára vonatkozó módosítási javaslatokat.
5. A szervezetnek dokumentálnia kell az EIR konfigurációjában történt változtatásokra vonatkozó döntéseket.
6. A szervezetnek meg kell valósítania a jóváhagyott változtatásokat az EIR-ben.
7. A szervezetnek meghatározott időtartamig visszakereshetően meg kell őriznie az EIR-ben megvalósított változtatások dokumentumait.
8. A szervezetnek meghatározott időszakonként felül kell vizsgálnia az EIR konfigurációellenőrzés hatálya alá eső változtatásokkal kapcsolatos tevékenységeket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.14. Folyamatos felügyelet
6.2. Alapkonfiguráció
6.15. Biztonsági hatásvizsgálatok
6.18. A változtatásokra vonatkozó hozzáférés korlátozások
6.23. Konfigurációs beállítások
6.45. Konfigurációkezelési terv
6.49. Felhasználó által telepített szoftver

8.10. Eszközök azonosítása és hitelesítése

10.2. Szabályozott karbantartás

12.42. Be- és kiszállítás

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

3.3.6.3. A konfigurációváltozások felügyelete (változáskezelés)

ISO/IEC 27001:2023 REFERENCIA

8.1; 9.3.3; A.8.9; A.8.32

NIST SP 800-53 REV.5 REFERENCIA

CM-3

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

6.8. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE – AUTOMATIZÁLT DOKUMENTÁCIÓ, ÉRTESÍTÉS ÉS VÁLTOZTATÁSI TILALOM

6.8. A szervezet meghatározott automatizált mechanizmusokat alkalmaz:

6.8.1. az EIR-ben javasolt változtatások dokumentálására;

6.8.2. a jóváhagyásra jogosultak értesítése a javasolt változtatási igényekről;

6.8.3. azon változások kiemelésére, amelyeket még nem hagytak jóvá vagy késedelmesen hagytak jóvá;

6.8.4. a még nem jóváhagyott változások végrehajtásának megakadályozására;

6.8.5. az EIR-ben végrehajtott változások teljes dokumentálására;

6.8.6. a jóváhagyásra jogosultak értesítésére a jóváhagyott változtatások végrehajtásáról.

MAGYARÁZAT

Az automatizált mechanizmusok használata segít koordinálni és felügyelni a konfigurációváltozások felügyeletének folyamatát. Az automatizált mechanizmusok segíthetnek az EIR-ben javasolt változtatások dokumentálásában; a jóváhagyásra jogosultak értesítésében a javasolt változtatási igényekről; azon változások kiemelésében, amelyeket még nem hagytak jóvá vagy késedelmesen hagytak jóvá; a még nem jóváhagyott változások végrehajtásának megakadályozásában; az EIR-ben végrehajtott változások teljes dokumentálásában; a jóváhagyásra jogosultak értesítésében a jóváhagyott változtatások végrehajtásáról.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek az 6.7-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat az automatizált eszközöket, amelyeket a konfigurációváltozások felügyeletében használni kíván.

2. A szervezetnek biztosítania kell, hogy ezek az automatizált eszközök képesek legyenek segítséget nyújtani a konfigurációváltozások felügyeletében pl.: automatizált dokumentáció, értesítés és igényelt változtatások kezelése.

3. A szervezetnek biztosítania kell, hogy az automatizált eszközök által szolgáltatott információk mindig rendelkezésre álljanak a szervezet számára. Ez magában foglalhatja az információk tárolását és archiválását, valamint a hozzáférés biztosítását a szükséges személyek számára.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.6.3. A konfigurációváltozások felügyelete (változáskezelés)

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.9. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE – VÁLTOZÁSOK TESZTELÉSE, JÓVÁHAGYÁSA ÉS DOKUMENTÁLÁSA

6.9. A szervezet teszteli, jóváhagyja és dokumentálja az EIR változtatásait azok bevezetése előtt.

MAGYARÁZAT

Az EIR változások magukban foglalják a hardver, szoftver vagy firmware elemek és a "konfigurációs beállításokra" vonatkozó követelményekben meghatározott konfigurációs beállítások módosításait. Az érintett szervezet biztosítja, hogy a tesztelés ne zavarja a szervezeti célokat és üzleti funkciókat támogató rendszerüzemeltetést. A teszteket végző személyek vagy csoportok tudomásul veszik a biztonsági szabályzatokat és eljárásokat, az EIR biztonsági szabályait és eljárásait, valamint a specifikus létesítményekkel vagy folyamatokkal kapcsolatos egészségügyi, biztonsági és környezeti kockázatokat. Előfordulhat, hogy a tesztelés elvégzése előtt az üzemi EIR-eket le kell kapcsolni, vagy a lehetőségekhez mérten replikálni kell azokat. Ha az EIR-eket a teszteléshez le kell kapcsolni, a teszteket lehetőség szerint a tervezett rendszerleállások idejére kell ütemezni. Ha a tesztelés nem végezhető el az üzemi EIR-eken, a szervezetnek kompenzációs intézkedéseket kell alkalmaznia.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell az EIR potenciális változtatásait, amelyek magukban foglalhatják a hardver, szoftver vagy firmware elemek és a "konfigurációs beállításokra" vonatkozó követelményekben meghatározott konfigurációs beállítások módosításait.
2. A szervezetnek biztosítania kell, hogy a tesztelés ne zavarja a szervezeti célokat és üzleti funkciókat támogató rendszerüzemeltetést.
3. A szervezetnek gondoskodnia kell arról, hogy a teszteket végző személyek vagy csoportok tudomásul veszik a biztonsági szabályzatokat és eljárásokat, az EIR biztonsági szabályait és eljárásait, valamint a specifikus létesítményekkel vagy folyamatokkal kapcsolatos egészségügyi, biztonsági és környezeti kockázatokat.

4. A szervezetnek el kell döntenie, hogy az üzemi EIR-eket a tesztelés elvégzése előtt le kell-e kapcsolni, vagy replikálni kell azokat. Ha az üzemi EIR-eket le kell kapcsolni a teszteléshez, a teszteket a tervezett leállás idején kell végrehajtani, amennyiben az lehetséges.
5. Ha a tesztelést nem lehet az üzemi EIR-en elvégezni, a szervezetnek kompenzációs kontrollokat kell alkalmaznia.
6. A szervezetnek jóvá kell hagynia az EIR változtatásait a tesztelés után.
7. A szervezetnek dokumentálnia kell az EIR változtatásait, beleértve a változtatások leírását, a tesztelési eredményeket és a jóváhagyás részleteit. A dokumentáció segíti a szervezetet abban, hogy nyomon tudja követni az EIR-ben bekövetkezett változásokat.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.3.6.3. A konfigurációváltozások felügyelete (változáskezelés)

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CM-3(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

6.10. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE – AUTOMATIZÁLT VÁLTOZÁSBEVEZETÉS

6.10. A szervezet meghatározott automatizált mechanizmusok segítségével hajtja végre az alapkonfiguráció módosítását és a frissített alapkonfiguráció telepítését az EIR-ben.

MAGYARÁZAT

Az automatizált eszközök javíthatják az alapkonfigurációval kapcsolatos információk pontosságát, következetességét és elérhetőségét. Az automatizáció továbbá adatösszegzési és adatösszefüggési képességeket, riasztási mechanizmusokat és irányítópultokat (dashboard) is biztosíthat, amelyek támogatják a kockázatalapú döntéshozatalt az érintett szervezetben.
Az automatizált eszközök segítségével a szervezet képes lehet gyorsan és hatékonyan reagálni a biztonsági fenyegetésekre, mivel az automatizált mechanizmusok segíthetnek gyorsabban módosítani és frissíteni az EIR alapkonfigurációját.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek az 6.7-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:
1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a automatizált konfigurációkezelést támogató eszközöket, amelyek segítségével képes lesz módosítani az alapkonfigurációt és telepíteni a frissített alapkonfigurációt az EIR-ben.
2. A szervezetnek biztosítania kell, hogy ezek az automatizált eszközök képesek legyenek segítséget nyújtani az automatizált változásbevezetésben pl.: biztonsági frissítések automatikus telepítése.
3. A szervezetnek biztosítania kell, hogy az automatizált eszközök által szolgáltatott információk mindig rendelkezésre álljanak a szervezet számára. Ez magában foglalhatja az információk tárolását és archiválását, valamint a hozzáférés biztosítását a szükséges személyek számára.

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

CM-3(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.11. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE – AUTOMATIZÁLT BIZTONSÁGI VÁLASZLÉPÉSEK

6.11. A szervezet automatikusan végrehajtja a meghatározott biztonsági válaszlépéseket, amennyiben az alapkonfigurációt jogosulatlanul megváltoztatják.

MAGYARÁZAT

Az automatizált biztonsági válaszlépések magukban foglalják bizonyos rendszerfunkciók leállítását, a rendszer feldolgozási folyamatainak leállítását, valamint riasztások vagy értesítések küldését a felelős szervezeti személyeknek, amennyiben jogosulatlan módosítást hajtanak végre egy konfigurációs elemen. Ez azt jelenti, hogy amennyiben az EIR alapkonfigurációját jogosulatlanul megváltoztatják, a szervezet automatikusan végrehajtja a meghatározott biztonsági válaszlépéseket. Az automatizált biztonsági válaszlépések segítenek minimalizálni az alapkonfiguráció jogosulatlan megváltoztatásával járó kockázatot, mivel lehetőséget biztosítanak az azonnali reagálásra.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek az 6.7-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a automatizált biztonsági válaszlépéseket támogató eszközöket, amelyek segítségével képes lehet a szervezet az azonnali reagálásra, amennyiben az EIR alapkonfigurációját jogosulatlanul megváltoztatják.
2. A szervezetnek biztosítania kell, hogy az automatizált eszközök képesek legyenek segítséget nyújtani az automatizált biztonsági válaszlépések megtételében pl.: rendszerfunkciók leállítása, riasztások és értesítések küldése.
3. A szervezetnek biztosítania kell, hogy az automatizált eszközök által szolgáltatott információk mindig rendelkezésre álljanak a szervezet számára. Ez magában foglalhatja az információk tárolását és archiválását, valamint a hozzáférés biztosítását a szükséges személyek számára.

4. A szervezetnek biztosítania kell a naplózást, annak érdekében, hogy képes legyen rögzíteni az összes konfigurációval kapcsolatos módosítást, beleértve a jogosulatlan módosításokat is. A naplózás segíthet a jogosulatlan módosítások forrásának azonosításában.
5. A szervezetnek be kell állítania azokat a biztonsági válaszlépéseket, amelyek automatikusan végrehajtódnak, ha jogosulatlan módosítás történik pl.: rendszerfunkciók leállítása, riasztások és értesítések küldése.

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

CM-3(5)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági válaszok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

6.12. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE – KRIPTOGRÁFIA KEZELÉSE

6.12. A szervezet az általa meghatározott védelmi intézkedésekhez használt kriptográfiai mechanizmusokat a konfigurációkezelés hatálya alá vonja.

MAGYARÁZAT

Függetlenül attól, hogy az érintett szervezet milyen kriptográfiai mechanizmusokat alkalmaz, rendelkeznie kell olyan folyamatokkal és eljárásokkal, amelyek kezelik ezeket a mechanizmusokat. Például, ha a rendszerelemek tanúsítványokat használnak azonosításra és hitelesítésre, akkor szükséges, hogy legyen egy folyamat, amely figyeli a tanúsítványok lejáratát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a védelmi intézkedéseket, amelyekhez kriptográfiai mechanizmusokat használ. Ezek a mechanizmusok lehetnek például titkosítási algoritmusok, digitális aláírások vagy tanúsítványok.
2. A szervezetnek be kell vonnia ezeket a kriptográfiai mechanizmusokat az EIR konfigurációkezelésének hatálya alá. Ez azt jelenti, hogy a szervezetnek nyomon kell követnie és dokumentálnia kell a mechanizmusok beállításait, változásait és frissítéseit.
3. A szervezetnek biztosítania kell, hogy a kriptográfiai mechanizmusokat megfelelően kezelik. Például, ha a rendszerelemek tanúsítványokat használnak azonosításra és hitelesítésre, akkor a szervezetnek be kell vezetnie egy folyamatot, amely figyeli a tanúsítványok lejáratát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.49. Kriptográfiai kulcs előállítása és 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

CM-3(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.13. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE – RENDSZER VÁLTOZÁSAINAK FELÜLVIZSGÁLATA

6.13. A szervezet meghatározott gyakorisággal, vagy a szervezet által meghatározott körülmények esetén megvizsgálja a rendszerben történt változásokat annak megállapítása érdekében, hogy történtek-e jogosulatlan változtatások.

MAGYARÁZAT

Az érintett szervezetnek folyamatosan nyomon kell követnie és ellenőriznie kell az EIR-ben történt változásokat. Az EIR változásainak felülvizsgálatát indukálhatják a szervezet által végrehajtott konfigurációváltozási folyamatokból és a folyamatos felügyeletből származó információk is. Például, ha a szervezet észleli, hogy az EIR-ben olyan változások történtek, amelyek nem felelnek meg a szervezet által meghatározott szabályoknak vagy előírásoknak, akkor a szervezetnek meg kell vizsgálnia az EIR-t, hogy megállapítsa, történtek-e jogosulatlan változtatások.

Ez a folyamat magában foglalhatja a naplók ellenőrzését is, amelyek részletes információkat tartalmaznak az EIR-ben történt változásokról.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a felülvizsgálat gyakoriságát, illetve azokat a körülményeket, amelyek indokolják az EIR-ben történt változások vizsgálatát.
2. A szervezetnek létre kell hoznia egy folyamatot, amely lehetővé teszi a változások nyomon követését az EIR-ben. Ez magában foglalhatja a változáskezelési folyamatot vagy a folyamatos felügyelet kialakítását is.
3. A szervezetnek biztosítania kell a naplózást, annak érdekében, hogy képes legyen rögzíteni az összes konfigurációval kapcsolatos módosítást, beleértve a jogosulatlan módosításokat is. A naplózás segíthet a jogosulatlan módosítások forrásának azonosításában.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

6.7. A konfigurációváltozások felügyelete (változáskezelés)

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.9

NIST SP 800-53 REV.5 REFERENCIA

CM-3(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság illetve a körülmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.14. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE – KONFIGURÁCIÓ MEGVÁLTOZTATÁSÁNAK MEGAKADÁLYOZÁSA VAGY KORLÁTOZÁSA

6.14. A szervezet meghatározott körülmények esetén megakadályozza vagy korlátozza az EIR konfigurációjának módosítását.

MAGYARÁZAT

Az EIR konfigurációjának módosulásai negatívan befolyásolhatják a kritikus rendszerbiztonsági funkciókat. A változások korlátozását automatizált mechanizmusokon keresztül lehet érvényesíteni. Az érintett szervezetnek biztosítania kell, hogy az EIR konfigurációjának módosítását csak meghatározott körülmények között lehessen végrehajtani. Ez azt jelenti, hogy az érintett szervezetnek olyan szabályokat és eljárásrendeket kell bevezetnie, amelyek meghatározzák, hogy milyen esetekben, kik és milyen módon módosíthatják az EIR konfigurációját. Ez magában foglalhatja például azt, hogy csak bizonyos felhasználók, csak bizonyos időpontokban, csak bizonyos módosításokat hajthatnak végre, és csak a megfelelő engedélyezés után.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a körülményeket, amelyek esetén megakadályozza vagy korlátozza az EIR konfigurációjának módosítását.
2. A szervezetnek olyan automatizált mechanizmust kell implementálnia, amely képes érzékelni és kezelni a konfigurációs változásokat.
3. A szervezetnek úgy kell beállítania a mechanizmust, hogy az megakadályozza vagy korlátozza a konfigurációs változásokat a meghatározott körülmények között. Ez azt jelenti, hogy a mechanizmus blokkolja a változásokat, vagy csak korlátozott számú változást engedélyez egy adott időszakban.
4. A szervezetnek biztosítania kell a naplózást, annak érdekében, hogy képes legyen rögzíteni az összes konfigurációval kapcsolatos módosítást, beleértve a jogosulatlan módosításokat is. A naplózás segíthet a jogosulatlan módosítások forrásának azonosításában.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.8.9

NIST SP 800-53 rev.5 referencia

CM-3(8)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a körülmények meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

6.15. BIZTONSÁGI HATÁSVIZSGÁLATOK

6.15. A szervezet még a változtatások bevezetése előtt megvizsgálja az EIR-ben tervezett változtatásoknak az információbiztonsági hatásait.

MAGYARÁZAT

A biztonsági hatásvizsgálatokat végző felelősöknek rendelkezniük kell a szükséges készségekkel és technikai szaktudással az EIR-ben tervezett változások, valamint a biztonsági következmények elemzéséhez. A biztonsági hatásvizsgálatok magukban foglalják a biztonsági tervek, szabályzatok és eljárásrendek áttekintését a szabályozási követelmények megértése érdekében; az EIR tervezési dokumentációjának és működési eljárásainak áttekintését a szabályozási megvalósítás megértése és a specifikus EIR változások hatásának megértése érdekében; a változások hatásának áttekintését a szervezet ellátási láncában érintett partnereivel és az egyéb érdekelt felekkel. A hatásvizsgálatok magukban foglalják a kockázatok értékelését, mely által világossá válik a változások hatása és hogy szükség van-e további védelmi intézkedésekre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek a megfelelően képzett felelősök bevonásával el kell végeznie a hatásvizsgálatot.
2. A hatásvizsgálatoknak magukban kell foglalniuk a biztonsági tervek, szabályzatok és eljárások áttekintését a követelmények tisztázása végett, valamint az EIR tervezési dokumentációjának és üzemeltetési eljárásainak áttekintését.
3. A szervezetnek meg kell határoznia, hogy a változások milyen hatással lesznek az érintett szervezet ellátási lánc partnereire és az egyéb érdekelt felekre, illetve, hogy a változások az EIR-ben hogyan teremtenek új kockázatokat a megvalósított védelmi képességek vonatkozásában.
4. A változások bevezetése előtt a szervezet felülvizsgálja a tervezett változásokat és elemzi azok kockázatait, illetve információbiztonsági hatásait. Ez segít abban, hogy a szervezet megfeleljen a kiberbiztonsági követelményeknek, és biztosítsa, hogy az EIR-ben tervezett változások ne jelentsenek kockázatot az információbiztonságra. Emellett segít a szervezetnek

meghatározni, hogy a tervezett változások miatt szükséges-e további védelmi intézkedések bevezetése.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.14. Folyamatos felügyelet

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.36. Rendszerelem leltár

6.45. Konfigurációkezelési terv

10.2. Szabályozott karbantartás

15.4. Kockázatértékelés

15.10. Sérülékenységmonitorozás és szkennelés

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

16.16. Biztonságtervezési elvek

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

3.3.6.4. Biztonsági hatásvizsgálat

ISO/IEC 27001:2023 REFERENCIA

A.8.9

NIST SP 800-53 REV.5 REFERENCIA

CM-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

6.16. BIZTONSÁGI HATÁSVIZSGÁLATOK – KÜLÖNÁLLÓ TESZTKÖRNYEZETEK

6.16. A szervezet elkülönített tesztkörnyezetben vizsgálja a változtatásokat, mielőtt azokat éles rendszerben alkalmazná, keresve a biztonsági hatásokat, amelyek hiányosságokból, sérülékenységekből, kompatibilitási problémákból vagy szándékos rosszindulatból adódhatnak.

MAGYARÁZAT

Az elkülönített tesztkörnyezethez olyan környezetre van szükség, amely fizikailag vagy logikailag elkülönül az éles üzemi környezettől. Az elkülönítés elegendő annak biztosítására, hogy a tesztkörnyezetben végzett tevékenységek ne befolyásolják az éles üzemi környezetben végzett tevékenységeket, és hogy az éles üzemi környezetben lévő információk ne kerüljenek véletlenül a tesztkörnyezetbe. Az elkülönített környezetek fizikai vagy logikai eszközökkel valósíthatók meg. Ha fizikailag elkülönített tesztkörnyezetek nem kerülnek megvalósításra, az érintett szervezet meghatározza a logikai elkülönítés megvalósításához szükséges mechanizmus erősségét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy elkülönített tesztkörnyezetet, amely fizikailag vagy logikailag elkülönül az éles környezettől. Ez a szeparáció biztosítja, hogy a tesztkörnyezetben végzett tevékenységek ne befolyásolják az éles környezetben folyó munkát, és hogy az éles környezetben található információk ne kerüljenek véletlenül át a tesztkörnyezetbe.
2. Ha a szervezet nem tud fizikailag elkülönített tesztkörnyezetet létrehozni, akkor meg kell határoznia a logikai szeparáció erősségét.
3. A szervezetnek a tervezett változtatásokat először a tesztkörnyezetben kell vizsgálnia, mielőtt azokat az EIR-ben alkalmazná.
4. A tesztelés során a szervezetnek fel kell tárnia azokat a biztonsági hatásokat, amelyek hiányosságokból, sérülékenységekből, kompatibilitási problémákból vagy szándékos rosszindulatból adódhatnak.

5. A szervezetnek dokumentálnia kell a tesztelési folyamatot, beleértve az összes feltárt hibát és sérülékenységet, valamint azokat a lépéseket, amelyeket a problémák megoldására tett.
6. Mielőtt a változtatásokat az EIR-ben alkalmazná, a szervezetnek ellenőriznie kell, hogy a tesztkörnyezetben feltárt összes hibát és sérülékenységet megfelelően kezelte-e.

KAPCSOLÓDÓ INTÉZKEDÉSEK

16.66. Fejlesztői biztonsági tesztelés

17.17. A határok védelme

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

3.3.6.4. Biztonsági hatásvizsgálat

ISO/IEC 27001:2023 REFERENCIA

A.8.31

NIST SP 800-53 REV.5 REFERENCIA

CM-4(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.17. BIZTONSÁGI HATÁSVIZSGÁLATOK – KÖVETELMÉNYEK ELLENŐRZÉSE

6.17. A szervezet a rendszermódosítások után ellenőrzi, hogy a védelmi intézkedések helyesen lettek-e bevezetve, megfelelően működnek-e, és biztosítják-e a kívánt eredményeket, figyelembe véve az EIR biztonsági követelményeit.

MAGYARÁZAT

Az érintett szervezetnek gondoskodnia kell arról, hogy a rendszermódosítások után ellenőrizze, hogy a védelmi intézkedések helyesen lettek-e bevezetve. Ez azt jelenti, hogy a szervezetnek meg kell győződnie arról, hogy az új vagy módosított biztonsági intézkedések megfelelően működnek-e, és hogy ezek az intézkedések biztosítják-e a kívánt eredményeket.

Az ellenőrzés során az érintett szervezetnek figyelembe kell vennie az EIR biztonsági követelményeit. Ez azt jelenti, hogy a szervezetnek meg kell győződnie arról, hogy az új vagy módosított biztonsági intézkedések összhangban vannak-e az EIR biztonsági követelményeivel, és hogy ezek az intézkedések ténylegesen hozzájárulnak-e az EIR biztonságának javításához.

A szervezet dokumentálja az ellenőrzési folyamatot, annak érdekében, hogy dokumentálja az ellenőrzés eredményeit és bizonyítékot szolgáltasson arról, hogy a védelmi intézkedések helyesen lettek bevezetve és megfelelően működnek. A dokumentációban a szervezet rögzíti az ellenőrzés időpontját, a védelmi intézkedések állapotát, az ellenőrzés eredményeit és az esetleges problémákat vagy hiányosságokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A rendszermódosítások bevezetése után a szervezetnek ellenőriznie kell, hogy a védelmi intézkedések helyesen lettek-e bevezetve és megfelelően működnek-e. Ez magában foglalhatja a módosított funkciók tesztelését, a biztonsági beállítások ellenőrzését, és a rendszer sérülékenységvizsgálatát.
2. A szervezetnek meg kell győződnie arról, hogy a védelmi intézkedések biztosítják-e a kívánt eredményeket. A folyamat során a szervezetnek figyelembe kell vennie az EIR biztonsági követelményeit. Ez magában foglalhatja a biztonsági célok elérésének értékelését, a rendszer

stabilitásának és megbízhatóságának ellenőrzését, és a felhasználói visszajelzések figyelembevételét.

3. A szervezetnek dokumentálnia kell az ellenőrzés eredményeit és bizonyítékot kell szolgáltatnia arról, hogy a védelmi intézkedések helyesen lettek bevezetve és megfelelően működnek. A dokumentációban a szervezet rögzíti az ellenőrzés időpontját, a védelmi intézkedések állapotát, az ellenőrzés eredményeit és az esetleges problémákat vagy hiányosságokat.

Kapcsolódó intézkedések

16.66. Fejlesztői biztonsági tesztelés

17.4. Biztonsági funkciók elkülönítése

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

CM-4(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

6.18. A VÁLTOZTATÁSOKRA VONATKOZÓ HOZZÁFÉRÉS KORLÁTOZÁSOK

6.18. A szervezet meghatározza, dokumentálja, jóváhagyja és érvényesíti azokat a fizikai és logikai hozzáférési korlátozásokat, amelyek az EIR változtatásaihoz kapcsolódnak.

MAGYARÁZAT

Az EIR-ek hardver-, szoftver- vagy firmware-elemeinek vagy az EIR-hez kapcsolódó üzemeltetési eljárásoknak a megváltoztatása jelentős hatással lehet az EIR-ek biztonságára. Ezért az érintett szervezet csak a meghatározott személyeknek engedélyezi az EIR-ekhez való hozzáférést a változtatások kezdeményezése céljából. A hozzáférési korlátozások közé tartoznak a fizikai és logikai hozzáférés-felügyeletek (az ezekre vonatkozó biztonsági követelmények a "Hozzáférés-ellenőrzés érvényesítése" és "A fizikai belépés ellenőrzése" kontrolloknál kerültek bővebben kifejtésre), a szoftverkönyvtárak, a munkafolyamatok automatizálása, az adathordozón található könyvtárak, az absztrakt rétegek (azaz a külső interfészekbe, nem pedig közvetlenül az EIR-ekbe implementált változtatások) és a változtatási időablakok (azaz a változtatások csak meghatározott időpontokban történnek).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet meghatározza azokat a fizikai és logikai hozzáférési korlátozásokat, amelyek az EIR változásaihoz kapcsolódnak. Ez magában foglalhatja a fizikai és logikai hozzáférési kontrollokat, szoftverkönyvtárakat, munkafolyamat-automatizálást, az adathordozókon található könyvtárakat, absztrakt rétegeket, és változtatási időablakokat (amikor a változások csak meghatározott időpontokban történnek).
2. A szervezetnek dokumentálnia kell a korlátozásokat. A szervezetnek írásban kell rögzítenie az összes fizikai és logikai hozzáférési korlátozást, beleértve a hozzáférési szabályokat, a hozzáférési jogosultságokat és a hozzáférési eljárásokat.
3. A szervezetnek jóvá kell hagynia a dokumentált korlátozásokat. Ez azt jelenti, hogy a jóváhagyásra jogosult felelősnek el kell fogadnia és jóvá kell hagynia a korlátozásokat, mielőtt azokat érvényesítenék.

4. A szervezetnek érvényesítenie kell a jóváhagyott korlátozásokat. Ez azt jelenti, hogy a szervezetnek be kell vezetnie és alkalmaznia kell a korlátozásokat az EIR-ben, és naplóznia kell minden hozzáférési kísérletet, hogy nyomon követhető legyen, ki próbált hozzáférni az EIR-hez, mikor és milyen célból.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hozzáférési korlátozásokat, hogy biztosítsa azok relevanciáját és hatékonyságát. A naplókat is rendszeresen át kell nézni, hogy azonosítsák a szabálytalanságokat és a potenciális biztonsági réseket.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.59. Felelősségek szétválasztása

2.60. Legkisebb jogosultság elve

6.45. Konfigurációkezelési terv

12.6. A fizikai belépés ellenőrzése

17.81. Tárolt (at rest) adatok védelme

17.98. Végrehajtható, de nem módosítható programok

17.105. Sávon kívüli csatornák

18.2. Hibajavítás

18.59. Bemeneti információ ellenőrzés

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

3.3.6.5. A változtatásokra vonatkozó hozzáférés korlátozások

ISO/IEC 27001:2023 referencia

A.8.2; A.8.4; A.8.9; A.8.19; A.8.31; A.8.32

NIST SP 800-53 rev.5 referencia

CM-5

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

6.19. A VÁLTOZTATÁSOKRA VONATKOZÓ HOZZÁFÉRÉS KORLÁTOZÁSOK – AUTOMATIZÁLT HOZZÁFÉRÉS-ÉRVÉNYESÍTÉS ÉS NAPLÓBEJEGYZÉSEK

6.19. Az EIR:

6.19.1. automatizált mechanizmusok segítségével érvényesíti a hozzáférési korlátozásokat, és

6.19.2. automatikusan előállítja a naplóbejegyzéseket az érvényesítési műveletekről.

MAGYARÁZAT

Az érintett szervezet naplózza a konfigurációváltozások alkalmazásához kapcsolódó rendszer-hozzáféréseket, hogy biztosítsa a konfigurációváltozások felügyeletének végrehajtását, és hogy támogassa az utólagos intézkedéseket, ha a szervezet jogosulatlan változtatásokat fedez fel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy milyen automatizált hozzáférési korlátozásokat kíván alkalmazni a konfigurációváltozások alkalmazásához kapcsolódó rendszer-hozzáférésekre.

2. A szervezetnek biztosítania kell a naplózást, annak érdekében, hogy képes legyen rögzíteni az összes konfigurációval kapcsolatos módosítást, beleértve a jogosulatlan módosításokat is. A naplózás segíthet a jogosulatlan módosítások forrásának azonosításában.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

4.40. Naplóbejegyzések létrehozása

6.23. Konfigurációs beállítások

6.49. Felhasználó által telepített szoftver

18.67. Információ kezelése és megőrzése

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

3.3.6.5. A változtatásokra vonatkozó hozzáférés korlátozások

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-5(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.20. A VÁLTOZTATÁSOKRA VONATKOZÓ HOZZÁFÉRÉS KORLÁTOZÁSOK – KETTŐS JÓVÁHAGYÁS

6.20. A szervezet kettős jóváhagyást alkalmaz a változások végrehajtásához, a szervezet által meghatározott rendszerelemek és rendszerszintű információk esetében.

MAGYARÁZAT

Az érintett szervezet kettős jóváhagyást alkalmaz annak biztosítása érdekében, hogy a kiválasztott rendszerelemek és információk változásai csak akkor következhessenek be, ha két feljogosított személy hagyja jóvá és hajtja végre az ilyen változtatásokat. A két személynek rendelkeznie kell azzal a képességgel és szakértelemmel, hogy megállapítsa, a javasolt változások megfelelő implementációi-e az elfogadott változásoknak. A kettős jóváhagyást négy szem elvnek is nevezik. A összejátszás vagy csalás kockázatának csökkentése érdekében az érintett szervezet fontolóra veheti a kettős jóváhagyási feladatok több személy közötti rotációját.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet határozza meg, mely rendszerelemek és rendszerszintű információk esetében szükséges a kettős jóváhagyás.
2. A szervezet válasszon ki két személyt, akik felelősek lesznek a változások jóváhagyásáért és végrehajtásáért.
3. A kiválasztott személyeknek meg kell tudniuk határozni, hogy a javasolt változtatások megfelelő implementációi-e az elfogadott változtatásoknak.
4. A szervezetnek fontolóra kell vennie a kettős jóváhagyási feladatok más személyek közötti rotációját, hogy csökkentse az összejátszás vagy csalás kockázatát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.59. Felelősségek szétválasztása

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

CM-5(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek és rendszerszintű információk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.21. A VÁLTOZTATÁSOKRA VONATKOZÓ HOZZÁFÉRÉS KORLÁTOZÁSOK – JOGOSULTSÁGOK KORLÁTOZÁSA ÉLESÜZEMI RENDSZEREK ESETÉN

6.21. A szervezet:

6.21.1. Korlátozza a rendszerelemek és a rendszerrel kapcsolatos információk módosítására vonatkozó jogosultságokat az élesüzemi környezetben.

6.21.2. Meghatározott időközönként felülvizsgálja és újraértékeli a jogosultságokat.

MAGYARÁZAT

Egy rendszer több szervezeti célt és üzleti funkciót is támogathat. A rendszerelemek módosítására vonatkozó jogosultságok korlátozása az élesüzemi környezet tekintetében azért szükséges, mert egy rendszerelem módosítása negatív hatással lehet a rendszer által támogatott szervezeti célokra és üzleti folyamatokra. A rendszerek és a szervezeti célok/üzleti folyamatok közötti kapcsolatokkal általában nincsenek tisztában a fejlesztők. A rendszerszintű információk magukban foglalnak üzemeltetési eljárásrendeket is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek korlátoznia kell a jogosultságokat a rendszer elemeinek módosítására az élesüzemi környezetben. Ez azt jelenti, hogy csak a megfelelően képzett és jogosult személyeknek szabad módosítaniuk a rendszerelemeket.

2. A szervezetnek meghatározott időközönként felül kell vizsgálnia és újra kell értékelnie a jogosultságokat. Ez azt jelenti, hogy rendszeresen ellenőrizni kell, hogy a jogosultságok még mindig megfelelőek-e, és szükség esetén módosítani kell őket.

3. A szervezetnek biztosítania kell, hogy a jogosultságok korlátozása ne befolyásolja negatívan a rendszer által támogatott szervezeti célokat és üzleti folyamatokat. Ez azt jelenti, hogy a korlátozásoknak rugalmasnak kell lenniük, hogy szükség esetén módosíthatók legyenek az üzleti igényekhez igazodva.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-5(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.22. A VÁLTOZTATÁSOKRA VONATKOZÓ HOZZÁFÉRÉS KORLÁTOZÁSOK – SZOFTVERKÖNYVTÁRI JOGOSULTSÁGOK KORLÁTOZÁSA

6.22. A szervezet korlátozza a szoftverkönyvtárakban lévő szoftverek módosítására vonatkozó jogosultságokat.

MAGYARÁZAT

Az EIR-ben található szoftverkönyvtárakban lévő szoftverek módosításának korlátozása kritikus fontosságú a kiberbiztonság szempontjából. Ha a szoftverkönyvtárakban lévő szoftverek módosítására vonatkozó jogosultságokat nem korlátozzák megfelelően, az EIR sérülékennyé válhat az esetleges rosszindulatú szoftvermódosítások következtében.

Az érintett szervezetnek rendszeresen naplóznia kell a szoftverkönyvtárakban lévő szoftverek módosítását, hogy nyomon követhető legyen, ki, mikor és milyen módosításokat hajtott végre. Ez lehetővé teszi a szervezet számára, hogy gyorsan észlelje és kezelje a jogosulatlan módosításokat, és minimalizálja az ezzel együtt járó esetleges káros hatásokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie, hogy mely személyeknek van jelenleg hozzáférésük a szoftverkönyvtárakban lévő szoftverek módosításához.
2. A szervezetnek meg kell határoznia, hogy mely személyeknek van ténylegesen szükségük arra, hogy módosíthassák a szoftvereket a szoftverkönyvtárakban.
3. A szervezetnek be kell állítania a hozzáférési jogosultságokat az EIR-ben, hogy csak a szükséges személyek módosíthassák a szoftverkönyvtárakban lévő szoftvereket. Ez magában foglalja a hozzáférési jogosultságok felülvizsgálatát és a nem szükséges jogosultságok eltávolítását.
4. A szervezetnek be kell vezetnie egy naplózási rendszert, amely nyomon követi és rögzíti az összes módosítást, amelyet a szoftverkönyvtárakban lévő szoftvereken végeznek. Ez lehetővé teszi a szervezet számára, hogy gyorsan észlelje és reagáljon a nem engedélyezett módosításokra.

5. A szervezetnek rendszeresen felül kell vizsgálnia a naplókat, hogy biztosítsa a jogosultságok megfelelő használatát és az EIR biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-5(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.23. KONFIGURÁCIÓS BEÁLLÍTÁSOK

6.23. A szervezet

6.23.1. Kialakítja és dokumentálja a rendszerelemekben alkalmazott egységes biztonsági konfigurációs beállításokat, amelyek az üzemeltetési követelményekkel összhangban lévő legkorlátozottabb üzemmódot képviselik.

6.23.2. Elvégzi a konfigurációs beállításokat az EIR valamennyi elemében.

6.23.3. Azonosítja, dokumentálja és elfogadja a meghatározott rendszerelemek konfigurációs beállításaiban a működési követelmények által meghatározott konfigurációs beállításoktól való eltéréseket.

6.23.4. Figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait a szervezeti szabályzatokkal és eljárásokkal összhangban.

MAGYARÁZAT

A konfigurációs beállítások olyan paraméterek, amelyeket a hardver, szoftver vagy firmware rendszerelemekben lehet módosítani, és amelyek befolyásolják az EIR biztonsági állapotát vagy funkcionalitását. Azon eszközök, amelyekhez konfigurációs beállításokat lehet meghatározni, lehetnek nagy teljesítményű számítógépek, szerverek, munkaállomások, operációs rendszerek, mobil eszközök, bemeneti/kimeneti eszközök, protokollok és alkalmazások. A következő paraméterek fejthetnek ki hatást az EIR biztonsági állapotára: rendszerleíró adatbázis (registry) beállításai; felhasználói fiók, fájl vagy könyvtár jogosultságok beállításai; a funkciókhoz, protokollokhoz, portokhoz, szolgálatásokhoz és távoli kapcsolatokhoz tartozó beállítások.

A szervezet feladata, hogy meghatározza a szervezeti szintű konfigurációs elvárásokat, majd ezekből származtassa az EIR specifikus konfigurációs beállításokat. Az így meghatározott beállítások az EIR alapkonfigurációját képezik. A központilag előírt biztonsági konfigurációs beállítások (common secure configuration) (biztonsági konfigurációra vonatkozó ellenőrző lista, biztonsági útmutatók (hardening guide/security reference guide)) elismert, sztenderdizált és jól bevált referenciák, amelyek útmutatásul szolgálnak az EIR biztonságos konfigurálásához. Ezáltal az EIR-ek megfelelhetnek a működéssel kapcsolatos előírásoknak. Központilag előírt biztonsági konfigurációs beállításokat (common secure configurations) több szervezet is kidolgozhat, beleértve az EIR-ek fejlesztőit, gyártóit, viszonteladóit, állami szerveket,

tudományos intézeteket, iparági szereplőket és egyéb köz- és versenyszférában tevékenykedő szervezeteket. A központilag előírt biztonsági konfigurációs beállítások (common secure configuration) implementációjával kapcsolatos elvárás megjelenhet szervezeti szinten, a szervezeti célok és üzleti folyamatok szintjén, az EIR szintjén vagy akár magasabb szinten is, egy hatóság által.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a szervezeti szintű, egységes konfigurációs elvárásokat, melyeket dokumentálnia is kell. Ezeknek a beállításoknak a szükséges minimum elvét kell képviselniük, összhangban az üzemeltetési követelményekkel.
2. A szervezetnek a szervezeti szinten meghatározott konfigurációs elvárásokból kell származtatnia az elektronikus információs rendszerelemekben alkalmazott biztonsági konfigurációs beállításokat. Ezeknek a beállításoknak a szükséges minimum elvét kell képviselniük, összhangban az üzemeltetési követelményekkel.
3. A szervezet a konfigurációs beállítások meghatározásához felhasználhatja a központilag előírt biztonsági konfigurációs beállításokat (common secure configuration), melyek elismert, sztenderdizált és jól bevált referenciák, illetve amelyek útmutatásul szolgálhatnak az EIR biztonságos konfigurálásához pl.: biztonsági útmutatók (hardening guide/security reference guide).
4. A szervezetnek el kell végeznie a konfigurációs beállításokat az EIR összes elemében. Ez magában foglalja a hardver, szoftver és firmware rendszerelemek beállításait, amelyek befolyásolhatják az EIR biztonsági állapotát vagy funkcionalitását pl.: rendszerleíró adatbázis (registry) beállításokat, a fiók-, fájl- vagy könyvtár beállítások, valamint a funkciók, protokollok, portok, szolgáltatások és távoli kapcsolatok beállításai.
5. A szervezetnek szükséges azonosítania, dokumentálnia, illetve el kell fogadnia a meghatározott rendszerelemek konfigurációs beállításaiban a működési követelmények által meghatározott konfigurációs beállításoktól való eltéréseket.
4. A szervezet figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változásait a szervezeti szabályzatokkal és eljárásokkal összhangban.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.113. Mobil eszközök hozzáférés-ellenőrzése

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

5.24. Belső rendszerkapcsolatok

6.2. Alapkonfiguráció

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.26. Legszűkebb funkcionalitás

6.49. Felhasználó által telepített szoftver

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

3.3.6.6. Konfigurációs beállítások

ISO/IEC 27001:2023 referencia

A.8.9

NIST SP 800-53 rev.5 referencia

CM-6

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

6.24. KONFIGURÁCIÓS BEÁLLÍTÁSOK – AUTOMATIZÁLT KEZELÉS, ALKALMAZÁS ÉS ELLENŐRZÉS

6.24. A szervezet az által meghatározott automatizált mechanizmusok segítségével irányítja, alkalmazza és ellenőrzi a szervezet által meghatározott rendszerelemek konfigurációs beállításait.

MAGYARÁZAT

Az automatizált eszközök (pl.: védelmi intézkedések bevezetésére (hardening) alkalmas eszközök, alapkonfigurációt kezelő eszközök) javíthatják a konfigurációs beállítások információinak pontosságát, következetességét és elérhetőségét. Az automatizáció továbbá adatösszegzési és adatösszefüggési képességeket, riasztási mechanizmusokat és irányítópultokat (dashboard) is biztosíthat, amelyek támogatják a kockázatalapú döntéshozatalt az érintett szervezetben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek az 6.23-as pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a automatizált konfigurációbeállítást támogató eszközöket, amelyek segítségével képes lesz irányítani, alkalmazni és ellenőrizni a szervezet által meghatározott rendszerelemek konfigurációs beállításait.
2. A szervezetnek biztosítania kell, hogy ezek az automatizált eszközök képesek legyenek segítséget nyújtani a szervezet által meghatározott rendszerelemek konfigurációs beállításainak irányításában, alkalmazásában és ellenőrzésében.
3. A szervezetnek biztosítania kell, hogy az automatizált eszközök által szolgáltatott információk mindig rendelkezésre álljanak a szervezet számára. Ez magában foglalhatja az információk tárolását és archiválását, valamint a hozzáférés biztosítását a szükséges személyek számára.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.14. Folyamatos felügyelet

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

3.3.6.6. Konfigurációs beállítások

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-6(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.25. KONFIGURÁCIÓS BEÁLLÍTÁSOK – REAGÁLÁS A JOGOSULATLAN VÁLTOZTATÁSOKRA

6.25. A szervezet meghatározott lépéseket tesz a szervezet által meghatározott konfigurációs beállítások jogosulatlan módosításaira válaszul.

MAGYARÁZAT

A konfigurációs beállítások jogosulatlan megváltoztatására adott válaszok közé tartozik a felelős szervezeti személyzet figyelmeztetése, a meghatározott konfigurációs beállítások visszaállítása vagy - szélsőséges esetekben - az érintett rendszerfeldolgozás leállítása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a felelős személyeket, akiket értesíteni kell a konfigurációs beállítások jogosulatlan módosításának észlelése esetén.
2. A szervezetnek dokumentáltan vezetnie kell az EIR konfigurációs beállításait, hogy könnyen visszaállítható legyen az eredeti állapot, ha jogosulatlan módosítás történik.
3. A szervezetnek be kell állítania egy figyelmeztető rendszert, amely értesíti a felelős személyeket, ha a konfigurációs beállításokban jogosulatlan módosítás történik.
4. A szervezetnek fel kell készülnie arra, hogy szükség esetén leállítsa az érintett EIR feldolgozási folyamatait, ha a jogosulatlan módosítások veszélyeztetik a rendszer biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

9.9.1. Biztonsági események kezelése

9.27. A biztonsági események jelentése

18.42. Szoftver- és információsértetlenség

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

3.3.6.6. Konfigurációs beállítások

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-6(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a konfigurációs beállítások, illetve a tevékenységek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.26. LEGSZŰKEBB FUNKCIONALITÁS

6.26. A szervezet:

6.26.1. Az EIR-t úgy konfigurálja, hogy az csak az ügy- és üzletmenet szempontjából szükséges szolgáltatásokat nyújtsa.

6.26.2. Meghatározza a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat.

MAGYARÁZAT

Egy EIR számos funkciót és szolgáltatást nyújthat. Néhány, alapértelmezés szerint rendszeresen nyújtott funkció és szolgáltatás nem feltétlenül szükséges az érintett szervezet ügy- és üzletmenetének támogatásához. Ugyan kényelmes lehet egyetlen rendszerelemből több szolgáltatást nyújtani, de ez növeli a kockázatot. Amennyiben lehetséges, a szervezet a rendszerelemek funkcióit egyetlen funkcióra korlátozza rendszerelemenként. A szervezet megfontolhatja a nem használt vagy felesleges szoftverek eltávolítását, valamint a nem használt vagy felesleges fizikai és logikai portok és protokollok letiltását, hogy megakadályozzák a rendszerelemek jogosulatlan csatlakoztatását és az információ kiszivárgását. A szervezet hálózati szkennelő eszközöket, behatolásjelző (intrusion detection system (IDS)) és behatolásmegelőző (intrusion prevention system (IPS)) rendszereket, valamint végpontvédelmi technológiákat alkalmazhatnak, mint például tűzfalakat és hoszt alapú behatolásjelző rendszereket (host-based intrusion detection system), hogy azonosítsák és megakadályozzák a tiltott funkciók, protokollok, portok és szolgáltatások használatát. A legszűkebb funkcionalitás elvét figyelembe kell venni az EIR tervezése és teljes fejlesztési életciklusa során (az ezzel kapcsolatos információk bővebben kifejtésre kerültek a "Biztonságtervezési elvek", a "Rendszer és felhasználói funkciók szétválasztása", valamint a "Biztonsági funkciók elkülönítése" kontrolloknál).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek úgy kell konfigurálnia az EIR-t, hogy az csak az ügy- és üzletmenet szempontjából létfontosságú szolgáltatásokat nyújtsa.

2. A szervezet határozza meg a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat. Ez azt jelenti, hogy az EIR-ben le kell tiltani vagy korlátozni

kell azokat a funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat, amelyek nem szükségesek az ügy- és üzletmenet szempontjából, vagy amelyek kockázatot jelenthetnek a szervezet számára.

3. A szervezet alkalmazzon olyan megoldásokat, melyek képesek azonosítani és megakadályozni a a tiltott funkciók, protokollok, portok és szolgáltatások használatát pl.: hálózati szkennelő eszközök, behatolásjelző (intrusion detection system (IDS)) és behatolásmegelőző (intrusion prevention system (IPS)) rendszerek, végpontvédelmi technológiák, mint például tűzfalak és hoszt alapú behatolásjelző rendszerek (host-based intrusion detection system).

4. A szervezet vegye figyelembe a legszűkebb funkcionalitás elvét az EIR tervezése és teljes fejlesztési életciklusa során.

5. A szervezetnek dokumentálnia kell az EIR konfigurációját és ebben szerepeltetnie kell a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

6.2. Alapkonfiguráció

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.23. Konfigurációs beállítások

6.49. Felhasználó által telepített szoftver

15.10. Sérülékenységmonitorozás és szkennelés

16.7. Beszerzések

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

16.16. Biztonságtervezési elvek

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

3.3.6.7. Legszűkebb funkcionalitás

ISO/IEC 27001:2023 referencia

A.8.19

NIST SP 800-53 REV.5 REFERENCIA

CM-7

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

6.27. LEGSZŰKEBB FUNKCIONALITÁS – RENDSZERES FELÜLVIZSGÁLAT

6.27. A szervezet:

6.27.1. Meghatározott gyakorisággal átvizsgálja az EIR-t, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.

6.27.2. Kikapcsolja vagy eltávolítja azokat a funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat, amelyeket szükségtelennek vagy nem biztonságosnak ítél.

MAGYARÁZAT

A szervezet felülvizsgálja az EIR-ek vagy rendszerelemek által nyújtott funkciókat, portokat, protokollokat és szolgáltatásokat, hogy meghatározza azokat a funkciókat és szolgáltatásokat melyeket meg kíván szüntetni. Az ilyen felülvizsgálatok különösen fontosak a régebbi technológiákról az újabb technológiákra történő átállás időszakában. Ezek a technológiai átmenetek szükségessé tehetik a régebbi és az újabb technológiák egyidejű bevezetését az átmeneti időszak alatt, és a lehető leghamarabb történő visszaállítást a szükséges funkciókhoz, portokhoz, protokollokhoz és szolgáltatásokhoz. A szervezet eldöntheti, hogy mely funkciót, portot, protokollt és/vagy szolgáltatást tartja relatíve biztonságosnak, vagy a biztonsággal kapcsolatos döntést más szervezetek értékelésére alapozhatják. A nem biztonságos protokollok közé tartoznak a Bluetooth, az FTP és a peer-to-peer hálózatok.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet meghatározott gyakorisággal átvizsgálja az EIR-ek vagy rendszerelemek által nyújtott funkciókat, portokat, protokollokat és szolgáltatásokat.
2. Az átvizsgálás során a szervezet meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat. Az ilyen technológiai átmenetek során lehet, hogy a régebbi és az újabb technológiákat egyszerre kell alkalmazni, és a lehető legkorábban vissza kell térni a minimálisan szükséges funkciókhoz, portokhoz, protokollokhoz és szolgáltatásokhoz.
3. A szervezet eldöntheti, hogy mely funkciót, portot, protokollt és/vagy szolgáltatást tartja relatíve biztonságosnak, vagy a biztonsággal kapcsolatos döntést más szervezetek értékelése

alapján hozhatja meg. A nem biztonságos protokollok közé tartozik például a Bluetooth, az FTP és a peer-to-peer hálózatok.

4. Az érintett szervezet kikapcsolja vagy eltávolítja azokat a funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat, amelyeket szükségtelennek vagy nem biztonságosnak ítél.

Kapcsolódó intézkedések

2.108. Vezeték nélküli hozzáférés

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

3.3.6.7. Legszűkebb funkcionalitás

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CM-7(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

6.28. Legszűkebb funkcionalitás – Program futtatásának megakadályozása

6.28. A szervezet megakadályozza a program futtatását, amennyiben az nem a meghatározott szabályzatok és eljárásrendek szerint történik.

Magyarázat

A szervezet megakadályozza a program futtatását amennyiben az nem az érintett szervezet szabályzatai, viselkedési szabályai és/vagy a szoftverhasználatot tiltó hozzáférési megállapodások és a fejlesztő vagy gyártó előírásai (beleértve a szoftverlicencelést és a szerző jogokat) szerint történik. A korlátozások közé tartozik az automatikus futtatás funkció tiltása, a program futtatásának jóváhagyására jogosult szerepkörök korlátozása, bizonyos szoftverprogramok engedélyezése vagy tiltása, vagy az egyszerre futtatott programok számának korlátozása, valamint a hordozható (portable) programok futtatásának tiltása.

A követelmény alkalmazásának lépései

1. Az érintett szervezetnek létre kell hoznia és a gyakorlatban is alkalmaznia kell egy olyan szabályzatot, amely meghatározza, milyen szoftverek futtatása engedélyezett és azok milyen feltételek teljesülése esetén futhatnak.
2. A szervezetnek meg kell akadályoznia azoknak a programoknak a futtatását, melyek nem engedélyezettek. Ezt többek között megteheti az automatikus futtatás funkció tiltásával, a program futtatásának jóváhagyására jogosult szerepkörök korlátozásával, bizonyos szoftverprogramok engedélyezésével vagy tiltásával, vagy az egyszerre futtatott programok számának korlátozásával, valamint a hordozható (portable) programok futtatásának tiltásával.

Kapcsolódó intézkedések

6.36. Rendszerelem leltár

13.3.1. Viselkedési szabályok

13.9. Központi kezelés

1.5. Elektronikus információs rendszerek nyilvántartása

14.9. Hozzáférési megállapodások

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-7(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a program futtatásának korlátozására és használatára vonatkozó szabályzatok, eljárásrendek és hozzáférési megállapodások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

6.29. LEGSZŰKEBB FUNKCIONALITÁS – REGISZTRÁCIÓS KÖVETELMÉNYEKNEK VALÓ MEGFELELÉS

6.29. A szervezet biztosítja, hogy a funkciók, portok, protokollok és szolgáltatások regisztrációja megfeleljen a meghatározott követelményeknek.

MAGYARÁZAT

Az érintett szervezet a regisztrációs folyamatot használja az EIR-ek, funkciók, portok, protokollok és szolgáltatások kezelésére, nyomon követésére és felügyeletére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a funkciókat, portokat, protokollokat és szolgáltatásokat, amelyeket az EIR-ben használ.
2. A szervezetnek létre kell hoznia egy regisztrációs folyamatot, amely lehetővé teszi a funkciók, portok, protokollok és szolgáltatások regisztrálását és ezáltal azok nyomon követését és felügyeletét.
3. A szervezetnek biztosítania kell, hogy a regisztrációs folyamat megfelel a meghatározott követelményeknek.
4. A szervezetnek biztosítania kell, hogy a regisztrációs folyamat eredményei dokumentálva legyenek, és rendelkezésre álljanak.

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

CM-7(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a funkciók, portok, protokollok és szolgáltatások regisztrációjára vonatkozó követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.30. Legszűkebb funkcionalitás – Engedély nélküli szoftverek — Kivételes letiltás

6.30. A szervezet:

6.30.1. Azonosítja az EIR-ben a nem engedélyezett szoftvereket.

6.30.2. Alkalmazza az alapértelmezett engedélyezés és a kivétel alapú tiltás szabályt, amely megtiltja a nem engedélyezett szoftverek futtatását.

6.30.3. Rendszeresen felülvizsgálja és frissíti az EIR-ben nem engedélyezett szoftverek listáját.

Magyarázat

A szervezet a nem engedélyezett szoftvereket tilthatja specifikus verziók vagy specifikus források alapján. A nem engedélyezett szoftverek futtatásának tiltása vonatkozhat a felhasználók által végrehajtott műveletekre, az EIR-hez köthető portokra és protokollokra, IP címekre és tartományokra, weboldalakra és MAC címekre.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania kell az EIR-ben a nem engedélyezett szoftvereket. Ez azt jelenti, hogy az EIR-ben futó összes szoftvert át kell vizsgálni, és meg kell határozni, hogy melyek azok, amelyek nem rendelkeznek megfelelő engedélyezéssel.
2. A szervezetnek az alapértelmezett engedélyezést és a kivétel alapú tiltás szabályát kell alkalmaznia, mely által megtiltja a nem engedélyezett szoftverek futtatását.
3. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az EIR-ben nem engedélyezett szoftverek listáját. Ez azt jelenti, hogy a szervezetnek folyamatosan nyomon kell követnie az EIR-ben futó szoftvereket, és frissítenie kell a nem engedélyezett szoftverek listáját, ha új szoftverek kerülnek bevezetésre, vagy ha a már engedélyezett szoftverek engedélye lejár vagy visszavonásra kerül.

Kapcsolódó intézkedések

6.23. Konfigurációs beállítások

6.36. Rendszerelem leltár

6.47. A szoftverhasználat korlátozásai

13.9. Központi kezelés

1.5. Elektronikus információs rendszerek nyilvántartása

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

3.3.6.7. Legszűkebb funkcionalitás

ISO/IEC 27001:2023 REFERENCIA

A.8.19

NIST SP 800-53 REV.5 REFERENCIA

CM-7(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.31. Legszűkebb funkcionalitás – Engedélyezett szoftverek — Kivételes engedélyezés

6.31. A szervezet:

6.31.1. Azonosítja az EIR-en vagy EIR által futtatható szoftvereket.

6.31.2. Alkalmazza az alapértelmezett tiltás és a kivétel alapú engedélyezés szabályt a rendszeren futtatható szoftverek esetében.

6.31.3. Meghatározott gyakorisággal felülvizsgálja és frissíti az engedélyezett szoftverek listáját.

Magyarázat

A szervezet az engedélyezett szoftvereket korlátozhatja specifikus verziók vagy specifikus források alapján. A teljes körű engedélyezett szoftverfolyamat elősegítésének és az alkalmazásszinten engedélyezett szoftver átjátszása elleni védelem erősítésének érdekében, a szoftverprogramokat különböző szintekre lehet bontani és elemenként monitorozni. Ezek a szintek magukban foglalják az alkalmazásokat, az alkalmazásprogramozási felületeket (application programing interface (API)), alkalmazásmodulokat, scripteket, rendszerfolyamatokat, rendszerszolgáltatásokat, kernel funkciókat, rendszerleíró adatbázisokat (registry), illesztőprogramokat és dinamikus linkkönyvtárakat. Az engedélyezett szoftverek futtatatásának engedélyezése vonatkozhat a felhasználók által végrehajtott műveletekre, az EIR-hez köthető portokra és protokollokra, IP címekre és tartományokra, weboldalakra és MAC címekre.

A szervezet fontolóra veheti az engedélyezett szoftverprogramok sértetlenségének ellenőrzését digitális aláírások, kriptográfiai ellenőrzőösszegek vagy hash funkciók segítségével. Az engedélyezett szoftverek ellenőrzése történhet a végrehajtás előtt vagy az EIR indításakor. A weboldalakhoz köthető, engedélyezett URL-ek felismerésével kapcsolatos biztonsági követelmények "A határok védelme" kontrollnál kerültek bővebben kifejtésre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezet azonosítja az EIR-ben futtatható szoftvereket.
2. Az érintett szervezet alkalmazza az alapértelmezett tiltás és a kivétel alapú engedélyezés szabályát az EIR-en futtatható szoftverek esetében. Ez azt jelenti, hogy csak azok a szoftverek futtathatók, amelyeket kifejezetten engedélyeztek.
3. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az EIR-ben engedélyezett szoftverek listáját. Ez azt jelenti, hogy a szervezetnek folyamatosan nyomon kell követnie az EIR-ben futó szoftvereket, és frissítenie kell az engedélyezett szoftverek listáját, ha új szoftverek kerülnek bevezetésre, vagy ha a már engedélyezett szoftverek engedélye lejár vagy visszavonásra kerül.
4. Az érintett szervezet megfontolhatja az engedélyezett szoftverprogramok sértetlenségének ellenőrzését digitális aláírások, kriptográfiai ellenőrzőösszegek vagy hash funkciók segítségével. Az engedélyezett szoftverek ellenőrzése történhet a végrehajtás előtt vagy az EIR indításakor.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció
6.23. Konfigurációs beállítások
6.36. Rendszerelem leltár
6.47. A szoftverhasználat korlátozásai
13.9. Központi kezelés
1.5. Elektronikus információs rendszerek nyilvántartása
16.58. Fejlesztői változáskövetés
17.98. Végrehajtható, de nem módosítható programok
18.42. Szoftver- és információsértetlenség

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.19

NIST SP 800-53 REV.5 REFERENCIA

CM-7(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

6.32. LEGSZŰKEBB FUNKCIONALITÁS – KORLÁTOZOTT JOGOSULTSÁGÚ ZÁRT KÖRNYEZETEK

6.32. A szervezet megköveteli, hogy a meghatározott felhasználók által telepített szoftvereket fizikai vagy virtuális gépi környezetben korlátozott jogosultságokkal futtassák.

MAGYARÁZAT

Az érintett szervezet azonosítja azokat a szoftvereket, amelyek eredete vagy potenciális kártékony kód tartalma miatt aggodalomra adhatnak okot. Az ilyen típusú szoftverek felhasználói telepítése korlátozott működési környezetben történik - fizikai vagy virtuális gépi környezetben -, hogy korlátozza vagy megakadályozza a kártékony kódok által okozott károkat. A szervezet megköveteli, hogy a meghatározott felhasználók által telepített szoftvereket korlátozott jogosultságokkal futtassák. Ez azt jelenti, hogy a felhasználóknak csak korlátozott hozzáférésük van az EIR-hez, és csak bizonyos műveleteket hajthatnak végre. Ez segít megelőzni a nem kívánt változásokat és a legtöbb olyan szoftver telepítését, mely nem engedélyezett (kivétel lehet azonban a hordozható (portable) szoftver mellyel kapcsolatban vélhetően egyéb biztonsági intézkedéseket kell foganatosítani).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először azonosítania kell azokat a szoftvereket, amelyek eredete vagy potenciális kártékony kódja miatt aggodalomra adhatnak okot.
2. Az azonosított szoftvereket a szervezetnek korlátozott jogosultságú zárt környezetben kell futtatniuk.
3. A korlátozott jogosultságokkal történő futtatásnak fizikai vagy virtuális gépi környezetben kell történnie. Ez azt jelenti, hogy a szoftver futtatása egy elkülönített környezetben történik, amely korlátozza a potenciális kártékony kód által okozható károkat.
4. A szervezet meg kell követelnie, hogy a meghatározott felhasználók által telepített szoftvereket korlátozott jogosultságokkal futtassák. Ez azt jelenti, hogy a felhasználóknak csak korlátozott hozzáférésük van az EIR-hez, és csak bizonyos műveleteket hajthatnak végre. Ez segít megelőzni a nem kívánt változásokat és a legtöbb olyan szoftver telepítését, mely nem

engedélyezett (kivétel lehet azonban a hordozható (portable) szoftver mellyel kapcsolatban vélhetően egyéb biztonsági intézkedéseket kell foganatosítani).

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.49. Felhasználó által telepített szoftver

17.122. Izolált futtatási környezetek

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-7(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a felhasználó által telepített szoftver meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.33. LEGSZŰKEBB FUNKCIONALITÁS – KÓDVÉGREHAJTÁS VÉDETT KÖRNYEZETEKBEN

6.33. A szervezet a bináris vagy gépi kód futtatását csak korlátozott fizikai vagy virtuális környezetben és a meghatározott személyek vagy szerepkörök külön jóváhagyásával engedélyezi, ha az ilyen kód:

6.33.1. korlátozott garanciájú vagy garancia nélküli forrásból származik;

6.33.2. forráskódját nem bocsátották rendelkezésre.

MAGYARÁZAT

Az érintett szervezet információbiztonsági követelményei szerint a bináris vagy gépi kód futtatása csak korlátozott fizikai vagy virtuális környezetben engedélyezett, és csak a meghatározott személyek vagy szerepkörök külön jóváhagyásával. Ez a követelmény minden bináris vagy gépi kódra vonatkozik, beleértve a kereskedelmi szoftvereket és firmware-eket, valamint a nyílt forráskódú (open-source) szoftvereket.

Ez a követelmény különösen fontos, ha a kód korlátozott garanciájú vagy garancia nélküli forrásból származik, vagy ha a forráskódját nem bocsátották rendelkezésre. Ilyen esetekben fokozott a kockázata annak, hogy a kód tartalmazhat biztonsági réseket vagy rosszindulatú funkciókat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy korlátozott fizikai vagy virtuális környezetet, amelyben a bináris vagy gépi kód futtatása lehetséges.

2. A szervezetnek be kell vezetnie egy jóváhagyási folyamatot, amelyben a meghatározott személyek vagy szerepkörök jóváhagyják a bináris vagy gépi kód futtatását. Erre akkor van szükség, ha a kód korlátozott garanciájú vagy garancia nélküli forrásból származik, és a forráskódját nem bocsátották rendelkezésre.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.47. A szoftverhasználat korlátozásai

17.122. Izolált futtatási környezetek

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-7(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.34. LEGSZŰKEBB FUNKCIONALITÁS – BINÁRIS VAGY GÉPI FUTTATHATÓ KÓD

6.34. A szervezet:

6.34.1. megtiltja az olyan forrásból származó bináris vagy gépi futtatható kódok használatát, amelynek nincs vagy korlátozott a garanciája, vagy amelynek a forráskódját nem bocsátották rendelkezésre;

6.34.2. kivételeket csak nyomós szervezeti érdek vagy működési követelmények esetén engedélyez a felelős engedélyező tisztviselő jóváhagyásával.

MAGYARÁZAT

Az érintett szervezet megtiltja a bináris vagy gépi futtatható kódok használatát olyan forrásból, amelynek nincs vagy korlátozott a garanciája, vagy amelynek a forráskódját nem bocsátották rendelkezésre. Ez minden bináris vagy gépi futtatható kód forrására vonatkozik, beleértve a kereskedelmi szoftvereket és firmware-eket, valamint az nyílt forráskódú (open-source) szoftvereket. A szervezet értékeli a forráskód nélküli szoftvertermékeket, vagy a korlátozott vagy nem létező garanciával rendelkező forrásokból származó szoftvereket a potenciális biztonsági hatások szempontjából. Az értékelések figyelembe veszik, hogy a forráskód nélküli szoftvertermékek felülvizsgálata, javítása vagy bővítése nehézkes lehet. Ezenkívül előfordulhat, hogy nincsenek tulajdonosok, akik az érintett szervezet nevében a javításokat elvégeznék. A nyílt forráskódú (open-source) szoftverek használata esetén figyelembe kell venni, hogy nincs garancia és a nyílt forráskódú (open-source) szoftver tartalmazhat hátsó ajtókat (backdoor) vagy kártékony szoftvereket, és előfordulhat, hogy nincs szoftvertámogatás. Kivételeket csak nyomós szervezeti érdek vagy működési követelmények esetén engedélyez az érintett szervezet felelős engedélyező tisztviselőjének jóváhagyásával. Ez azt jelenti, hogy csak akkor használhatók a korlátozott garanciájú vagy forráskód nélküli szoftverek, ha a szervezet működéséhez elengedhetetlenül szükségesek, és ezt az engedélyezésért felelős személy jóváhagyta.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell tiltania az olyan forrásból származó bináris vagy gépi futtatható kódok használatát, amelynek nincs vagy korlátozott a garanciája, vagy amelynek a forráskódját nem bocsátották rendelkezésre. Ez magában foglalja a kereskedelmi szoftvereket és firmware-eket, valamint a nyílt forráskódú (open-source) szoftvereket.
2. A szervezetnek értékelnie kell a forráskód nélküli szoftvertermékeket, vagy a korlátozott vagy nem létező garanciával rendelkező forrásokból származó szoftvereket a potenciális biztonsági hatások szempontjából. Az értékeléseknek figyelembe kell venniük, hogy a forráskód nélküli szoftvertermékek felülvizsgálata, javítása vagy bővítése nehézkes lehet. Ezenkívül előfordulhat, hogy nincsenek tulajdonosok, akik az érintett szervezet nevében a javításokat elvégeznék.
3. Ha a szervezet nyílt forráskódú (open-source) szoftvert használ, az értékeléseknek figyelembe kell venniük, hogy nincs garancia, a nyílt forráskódú (open-source szoftver) tartalmazhat hátsó ajtókat (backdoor) vagy rosszindulatú szoftvereket, és lehet, hogy nincs szoftvertámogatás.
4. Kivételeket csak nyomós szervezeti érdek vagy működési követelmények esetén engedélyez a szervezet az engedélyezésért felelős személy jóváhagyásával. Ez azt jelenti, hogy a szervezetnek egyértelműen meg kell határoznia, milyen körülmények között lehet kivételt tenni, és ki az engedélyezésért felelős személy, aki a kivételeket jóváhagyja. Emellett csak akkor használhatók a korlátozott garanciájú vagy forráskód nélküli szoftverek, ha a szervezet működéséhez elengedhetetlenül szükségesek, és ezt az engedélyezésért felelős személy jóváhagyta.

KAPCSOLÓDÓ INTÉZKEDÉSEK

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció
16.99. Támogatással nem rendelkező rendszerelemek

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-7(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.35. LEGSZŰKEBB FUNKCIONALITÁS – NEM ENGEDÉLYEZETT HARDVEREK HASZNÁLATÁNAK TILALMA

6.35. A szervezet:

6.35.1. Azonosítja azokat a hardverelemeket, amelyek használata az EIR-ben engedélyezett.

6.35.2. Megtiltja a nem engedélyezett hardverelemek használatát vagy csatlakoztatását.

6.35.3. Meghatározott gyakorisággal felülvizsgálja és frissíti az engedélyezett hardverelemek listáját.

MAGYARÁZAT

Az érintett szervezet számára a hardverelemek képezik az alapját az EIR-nek, és biztosítják a platformot az engedélyezett szoftverprogramok futtatásához. A hardverelemek leltárának kezelése és azon hardverelemek ellenőrzése, amelyek telepítése vagy csatlakoztatása az EIR-hez engedélyezett, elengedhetetlen a megfelelő biztonság fenntartása érdekében.

Az érintett szervezetnek azonosítania kell azokat a hardverelemeket, amelyek használata az EIR-ben engedélyezett. Ez magában foglalja a hardverelemek specifikációinak, helyének és állapotának nyomon követését. Az érintett szervezetnek szigorúan tiltnia kell a nem engedélyezett hardverelemek használatát vagy csatlakoztatását az EIR-hez. Ez magában foglalja a nem engedélyezett hardverelemek azonosítását és eltávolítását, valamint a megfelelő biztonsági intézkedések megtételét a nem engedélyezett hardverelemek használatának megakadályozása érdekében.

Az érintett szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és frissítenie az engedélyezett hardverelemek listáját. Ez magában foglalja a hardverelemek állapotának, biztonsági állapotának és teljesítményének rendszeres ellenőrzését, valamint az engedélyezett hardverelemek listájának frissítését a változások alapján. Az érintett szervezetnek naplót kell vezetnie a hardverelemek felülvizsgálatáról és frissítéséről, hogy bizonyítékot szolgáltasson a megfelelő hardverkezelési gyakorlatokról.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a hardverelemeket, amelyek használata az EIR-ben engedélyezett. Ez magában foglalhatja a számítógépeket, szervereket, hálózati eszközöket, nyomtatókat és egyéb perifériás eszközöket.
2. Miután a szervezet azonosította az engedélyezett hardverelemeket, meg kell tiltania a nem engedélyezett hardverelemek használatát vagy csatlakoztatását az EIR-hez. Ez azt jelenti, hogy a szervezetnek szabályokat és eljárásrendeket kell bevezetnie a hardverelemek használatának és csatlakoztatásának ellenőrzésére.
3. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és frissítenie az engedélyezett hardverelemek listáját. Ez magában foglalhatja a hardverelemek teljesítményének, biztonságának és megbízhatóságának értékelését, valamint az új technológiák és eszközök figyelemmel kísérését.

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

CM-7(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.36. RENDSZERELEM LELTÁR

6.36. A szervezet:

6.36.1. Leltárt készít az EIR elemeiről.

6.36.1.1. A leltár pontosan tükrözi az EIR-t.

6.36.1.2. A leltár tartalmazza a rendszeren belül található összes elemet.

6.36.1.3. Megakadályozza az elemek kettős elszámolását.

6.36.1.4. A leltár a nyomon követés és a jelentéstétel szempontjából a szükséges részletességet biztosítja.

6.36.1.5. A leltárban szereplő információk lehetővé teszik a rendszerelemekkel történő hatékony elszámolást.

6.36.2. Meghatározott gyakorisággal felülvizsgálja és frissíti a rendszerelemek leltárát.

MAGYARÁZAT

Az EIR elemei olyan azonosítható információs technológiai eszközök, amelyek hardvert, szoftvert és firmware-t tartalmaznak. Az érintett szervezet dönthetnek úgy, hogy központosított leltárt hoz létre, amely magában foglalja az összes szervezeti rendszerelemet. Ilyen helyzetekben a szervezet biztosítja, hogy a leltárak tartalmazzák a rendszerspecifikus információkat, amelyek az elemek elszámolásához szükségesek. A rendszerelemek hatékony elszámolásához szükséges információk közé tartozik az EIR neve, a szoftver tulajdonosai, a szoftver verziószámai, a hardver leltárspecifikációi, a szoftverlicensz információk, és a hálózatba kötött elemek esetében a gépnevek és hálózati címek az összes implementált protokollon (pl. IPv4, IPv6) keresztül. A leltárspecifikációk tartalmazzák a beérkezés dátumát, a költséget, a modellt, a sorozatszámot, a gyártót, a beszállítói információt, az elem típusát és a fizikai helyszínt.

A rendszerelemek kettős elszámolásának megakadályozása az elszámoltathatóság hiányát kezeli, amely akkor következik be, amikor az elem tulajdonjoga és az EIR-hez meglévő viszonya nem ismert. Ez különösen nagy vagy összetett hálózatot alkotó EIR-ek esetén fordulhat elő. A rendszerelemek kettős elszámolásának megakadályozására hatékony intézkedés lehet, ha a szervezet minden elemhez egyedi azonosító rendel. A szoftverleltár esetében a központilag kezelt szoftvert, amelyet más rendszereken keresztül érnek el, azon az EIR-en belüli elemként kezelik, amelyen telepítve és kezelve van. A szoftver, amelyet több

szervezeti EIR-re telepítettek és az EIR szintjén kezelnek, minden egyes EIR-re vonatkozóan kezelt, és többször is szerepelhet a központosított elemleltárban, ami szükségessé teszi az EIR kapcsolatot minden szoftverpéldányhoz a központosított leltárban, hogy elkerüljék az elemek kettős elszámolását. A több hálózati protokollt (pl. IPv4 és IPv6) implementáló rendszerek szkennelése kettős elem azonosítást eredményezhet különböző címtartományokban. A "Rendszerelem leltár – Automatizált karbantartás" kontroll esetén elvárt biztonsági követelmények implementálása segíthet kiküszöbölni az elemek kettős elszámolását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek leltárt kell készítenie a rendszerelemekről. A rendszerelemek diszkrét, azonosítható információs technológiai eszközök, amelyek hardvert, szoftvert és firmware-t tartalmaznak.
2. A szervezetnek biztosítania kell, hogy a leltár pontosan tükrözi az EIR-t és tartalmazza az EIR-en belül található összes elemet.
3. A szervezet létrehozhat központosított leltárt, amely magában foglalja az összes szervezeti rendszerelemet. A szervezetnek biztosítania kell, hogy a leltár tartalmazza a rendszerspecifikus információkat, amelyek az elemek elszámolásához szükségesek. A rendszerelemek hatékony elszámolásához szükséges információk közé tartozik az EIR neve, a szoftver tulajdonosai, a szoftver verziószámai, a hardver leltárspecifikációi, a szoftverlicensz információk, és a hálózatba kötött elemek esetében a gépnevek és hálózati címek az összes implementált protokollon (pl. IPv4, IPv6) keresztül. A leltárspecifikációk tartalmazzák a beérkezés dátumát, a költséget, a modellt, a sorozatszámot, a gyártót, a beszállítói információt, az elem típusát és a fizikai helyszínt.
4. A szervezetnek törekednie kell a rendszerelemek kettős elszámolásának kiküszöbölésére. Ennek megakadályozására hatékony intézkedés lehet, ha a szervezet minden elemhez egyedi azonosító rendel.
5. Megakadályozza az elemek kettős elszámolását. Az érintett szervezet hatékonyan megakadályozza a rendszerelemek kettős elszámolását egyedi azonosítók használatával minden komponens számára.
6. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és frissítenie kell az elektronikus információs rendszerelemek leltárát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció

6.26. Legszűkebb funkcionalitás

6.45. Konfigurációkezelési terv

6.47. A szoftverhasználat korlátozásai

6.49. Felhasználó által telepített szoftver

7.2. Üzletmenet-folytonossági terv

7.35. Az elektronikus információs rendszer mentései

10.2. Szabályozott karbantartás

10.21. Kellő időben történő karbantartás

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

3.3.6.8. Elektronikus információs rendszerelem leltár

ISO/IEC 27001:2023 REFERENCIA

A.5.9; A.8.9

NIST SP 800-53 REV.5 REFERENCIA

CM-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

6.37. RENDSZERELEM LELTÁR – FRISSÍTÉSEK A TELEPÍTÉS ÉS ELTÁVOLÍTÁS SORÁN

6.37. A szervezet a rendszerelemek leltárát frissíti minden egyes rendszerelem telepítése, eltávolítása és frissítése alkalmával.

MAGYARÁZAT

A szervezet javíthatja a rendszerelemek leltárának pontosságát, teljességét és egységességét, ha a leltárt frissíti minden egyes rendszerelem telepítése, eltávolítása és frissítése alkalmával. Ha a leltárt nem frissíti a szervezet az említett kulcsfontosságú lépéseknél, akkor megnő a valószínűsége annak, hogy az információkat nem rögzítik és dokumentálják megfelelően. A rendszerfrissítések magukban foglalják a hardver-, szoftver- és firmware elemeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy eljárást, amelynek keretében minden egyes rendszerelem telepítése, eltávolítása és frissítése során frissíti a rendszerelemek leltárát.
2. A szervezet rendszeresen ellenőriznie kell a leltárt, hogy biztosítsa annak pontosságát, teljességét és következetességét.
3. A szervezetnek biztosítania kell, hogy a rendszerelem leltár frissítésénél az információkat megfelelően rögzítsék és dokumentálják.

KAPCSOLÓDÓ INTÉZKEDÉSEK

1.17. Fenyegetettség tudatosító program

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

3.3.6.8. Elektronikus információs rendszerelem leltár

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-8(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

6.38. RENDSZERELEM LELTÁR – AUTOMATIZÁLT KARBANTARTÁS

6.38. A szervezet meghatározott automatizált mechanizmusokat alkalmaz a rendszerelem leltár naprakészségének, teljességének, pontosságának és hozzáférhetőségének a fenntartására.

MAGYARÁZAT

Az érintett szervezet a képességeinek és lehetőségeinek megfelelő mélységű és részletességű leltárt készít és tart fenn az rendszerelemekről. Például a virtuális gépek felügyelete nehézkes lehet, mert ezek a gépek csak akkor láthatók a hálózaton, ha használják őket. Ilyen esetekben a szervezet olyan naprakész, teljes és pontos leltárt tartanak fenn, amelyet ezen sajátosságok figyelembevételével észszerűnek tart. A szervezet az automatizált karbantartást megvalósíthatja az "Alapkonfiguráció – Automatikus támogatás a pontosság és a napra készségérdekében" kontrollban elvárt követelmények implementálásával, akkor, ha a szervezet kombinálja az rendszerelem leltárral és az alapkonfigurációval kapcsolatos tevékenységeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek a 6.36-os és 6.37-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a automatizált karbantartást támogató eszközöket, amelyek segítségével képes lesz megfelelően naprakész, teljes, pontos és hozzáférhető leltárt készíteni és fenntartani a rendszerelemekről.
2. A szervezetnek biztosítania kell, hogy ezek az automatizált eszközök képesek legyenek segítséget nyújtani a szervezet számára a rendszerelemek leltározásában.
3. A szervezetnek biztosítania kell, hogy az automatizált mechanizmusok megfelelően működnek, és képesek fenntartani az rendszerelemek leltárának naprakészségét, teljességét, pontosságát és hozzáférhetőségét. Ez magában foglalhatja az automatizált mechanizmusok rendszeres tesztelését és karbantartását is.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.6.8. Elektronikus információs rendszerelem leltár

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-8(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.39. RENDSZERELEM LELTÁR – JOGOSULATLAN ELEMEK AUTOMATIKUS ÉSZLELÉSE

6.39. A szervezet:

6.39.1. Meghatározott gyakorisággal, automatizált mechanizmusok segítségével vizsgálja a rendszerben található jogosulatlan hardver-, szoftver-, és firmware-elemek jelenlétét.

6.39.2. A jogosulatlan elemek észlelése esetén letiltja az ilyen elemek hálózati hozzáférését, izolálja a rendszerelemeket és értesíti a szervezet által meghatározott személyeket vagy szerepköröket.

MAGYARÁZAT

A jogosulatlan távoli kapcsolatok és mobil eszközök monitorozása mellett az érintett szervezet automatikusan detektálja a jogosulatlan rendszerelemeket is. A jogosulatlan rendszerelemek figyelése folyamatosan, vagy rendszeres időközönkénti vizsgálatokkal/szkennelésekkel is történhet. Az automatizált mechanizmusokat arra is használhatja a szervezet, hogy megakadályozza a jogosulatlan rendszerelemek kapcsolódását (az ezzel kapcsolatos információk bővebben kifejtésre kerültek a "Legszűkebb funkcionalitás – Nem engedélyezett hardverek használatának tilalma" kontrollnál). Az automatizált mechanizmusok a teljes EIR szintjén, vagy különálló rendszerelemekben is alkalmazhatóak. A szervezetnek az automatizált mechanizmusok beszerzésénél és implementációjánál figyelembe kell vennie, hogy az adott típusú rendszerelemek támogatják-e az említett mechanizmusokat, ugyanis lehetnek olyan rendszerelemek, melyek nem képesek erre (pl.: IoT eszközök, szenzorok). Jogosulatlan rendszerelemek izolációja többféle módon elérhető, például a jogosulatlan rendszerelemek külön tartományokba (domain), alhálózatokba, vagy karanténba helyezésével. Ezeket az izolációs technikákat általában homokozónak (sandboxing) nevezik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek a 6.36-os és 6.37-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a automatizált mechanizmusokat, amelyek segítségével képes lesz észlelni a jogosulatlan rendszerelemeket.

2. A szervezetnek biztosítania kell, hogy az automatizált mechanizmusok képesek legyenek segítséget nyújtani a szervezet számára a jogosulatlan rendszerelemek észlelésében. Emellett arról is meg kell bizonyosodnia a szervezetnek, hogy az automatizált mechanizmusok jogosulatlan elemek észlelése esetén képesek letiltani az ilyen elemek hálózati hozzáférését, képesek izolálni a rendszerelemeket és képesek értesíteni a szervezet által meghatározott személyeket vagy szerepköröket.

3. A szervezetnek biztosítania kell, hogy az automatizált mechanizmusok megfelelően működnek. Ez magában foglalhatja az automatizált mechanizmusok rendszeres tesztelését és karbantartását is.

4. A szervezetnek az automatizált mechanizmusok felhasználásával figyelemmel kell kísérnie az esetleges jogosulatlan rendszerelemeket. Ez történhet folyamatos felügyelet vagy rendszeres időközönkénti vizsgálatokkal/szkennelésekkel.

Kapcsolódó intézkedések

2.113. Mobil eszközök hozzáférés-ellenőrzése

5.14. Folyamatos felügyelet

15.10. Sérülékenységmonitorozás és szkennelés

17.4. Biztonsági funkciók elkülönítése

17.108. A folyamatok elkülönítése

17.122. Izolált futtatási környezetek

18.8. Kártékony kódok elleni védelem

18.13. Az EIR monitorozása

18.42. Szoftver- és információsértetlenség

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

3.3.6.8. Elektronikus információs rendszerelem leltár

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CM-8(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.40. Rendszerelem leltár – Elszámoltathatósággal kapcsolatos információk

6.40. A szervezet a rendszerelem leltárt olyan módon alakítja ki, amely lehetővé teszi a rendszerelemek kezeléséért felelős és számon kérhető személyek azonosítását név, munkakör és szerepkör alapján.

Magyarázat

Az érintett szervezetben a a rendszerelem leltár oly módon történő kialakítása, amely lehetővé teszi a rendszerelemek kezeléséért felelős és számonkérhető személyek azonosítását név, munkakör és szerepkör alapján biztosítja, hogy a hozzájuk rendelt elemek megfelelően kerüljenek kezelésre, és hogy a szervezet kapcsolatba léphessen ezekkel a személyekkel, ha valamilyen intézkedésre van szükség (pl.: ha a szervezet beazonosítja, hogy mely rendszerelem felelős egy adatszivárgásért, akkor szükséges lehet annak kivonása, helyettesítése vagy áthelyezése).

A követelmény alkalmazásának lépései

1. A szervezetnek úgy kell kialakítania a rendszerelem leltárt, hogy azonosítani lehessen a rendszerelemek kezeléséért felelős és számonkérhető személyeket név, munkakör és szerepkör alapján.
2. A szervezetnek gondoskodnia kell a rendszerelemek kezeléséért felelős feladatok ellátásáról és arról is, hogy az említett feladatot ellátó személy számonkérhető legyen.
3. A szervezetnek biztosítania kell, hogy amennyiben szükséges, kapcsolatba lehessen lépni a rendszerelemek kezeléséért felelős személyekkel, annak érdekében, hogy szükség esetén meg tudják tenni a megfelelő lépéseket.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

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

3.3.6.8. Elektronikus információs rendszerelem leltár

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-8(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

6.41. RENDSZERELEM LELTÁR – ÉRTÉKELÉS ALATT ÁLLÓ KONFIGURÁCIÓK ÉS JÓVÁHAGYOTT ELTÉRÉSEK

6.41. Az értékelés alatt álló rendszerelem konfigurációknak, valamint az aktuálisan telepített konfigurációktól való minden jóváhagyott eltérésnek szerepelnie kell a rendszerelem leltárában.

MAGYARÁZAT

Az értékelés alatt álló konfigurációk és jóváhagyott eltérésekkel kapcsolatban figyelembe kell venni a rendszerelemekben a szervezet által megvalósított konfigurációs beállításokat; az egyes, a szükséges konfigurációs beállításokhoz mérten, megfelelőségi szempontból értékelt rendszerelemeket; és minden jóváhagyott, a kialakított konfigurációs beállításoktól meglévő eltérést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell az egyes rendszerelemek szervezet által jóváhagyott konfigurációs beállításait.
2. A szervezetnek értékelnie kell a rendszerelemek konfigurációit, hogy megállapítsa, megfelelnek-e a szervezet által jóváhagyott beállításoknak.
3. A szervezetnek jóvá kell hagynia és dokumentálnia kell minden eltérést az aktuálisan jóváhagyott konfigurációs beállításoktól.

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

CM-8(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.42. RENDSZERELEM LELTÁR – KÖZPONTI ADATTÁR

6.42. A szervezet egy központi adattárat biztosít a rendszerelem leltárának.

MAGYARÁZAT

Az érintett szervezet megvalósíthat központi rendszerelem leltárat, amely magában foglalja az összes szervezethez köthető rendszerelemet. A központosított adattárak lehetőséget biztosítanak a hardver-, szoftver- és firmware eszközök hatékony elszámolására. Az ilyen típusú adattárak segíthetnek a szervezetnek gyorsan azonosítani a problémás rendszerelemek helyét, illetve az azokért felelős személyeket. A szervezet biztosítja, hogy a létrejövő központi rendszerelem leltár tartalmazza azokat a rendszerspecifikus információkat, amelyek szükségesek az elemek megfelelő elszámolásához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet létre kell hoznia egy központi rendszerelem leltárat, amely tartalmazza az összes szervezethez köthető rendszerelemet.
2. A szervezetnek biztosítania kell, hogy a létrejövő központi rendszerelem leltár tartalmazza azokat a rendszerspecifikus információkat, amelyek szükségesek az elemek megfelelő elszámolásához.

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

CM-8(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.43. RENDSZERELEM LELTÁR – AUTOMATIZÁLT HELYMEGHATÁROZÁS

6.43. A szervezet automatizált mechanizmusokat alkalmaz a rendszerelemek földrajzi hely szerinti nyomon követésének támogatására.

MAGYARÁZAT

Az automatizált mechanizmusok alkalmazása a rendszerelemek földrajzi hely szerinti nyomon követésére növelheti a rendszerelemek leltárának pontosságát. Ez a képesség segíthet az érintett szervezetnek gyorsan azonosítani a problémás rendszerelemek földrajzi helyét, illetve az azokért felelős személyeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a automatizált helymeghatározást támogató eszközöket, amelyek segítségével képes lesz azonosítani azoknak a rendszerelemeknek a földrajzi helyét és a felelső személyek.
2. A szervezetnek biztosítania kell, hogy ezek az automatizált eszközök képesek legyenek segítséget nyújtani a szervezet számára a rendszerelemek földrajzi helyének meghatározásában.
3. A szervezetnek biztosítania kell, hogy az automatizált mechanizmusok megfelelően működnek, és képesek fenntartani az rendszerelemek leltárának naprakészségét, teljességét, pontosságát és hozzáférhetőségét. Ez magában foglalhatja az automatizált mechanizmusok rendszeres tesztelését és karbantartását is.

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

CM-8(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.44. RENDSZERELEM LELTÁR – RENDSZERELEMEK RENDSZERHEZ RENDELÉSE

6.44. A szervezet:

6.44.1. Minden rendszerelemet legalább egy EIR-hez rendel.

6.44.2. A hozzárendelésről visszaigazolást kap a szervezet által meghatározott személyektől vagy szerepköröktől.

MAGYARÁZAT

Azon rendszerelemek, amelyek nincsenek hozzárendelve egy EIR-hez, elképzelhető, hogy nincsenek rendszeresen karbantartva, nem rendelkeznek a szervezet által elvárt védelemmel, és sérülékenységet jelenthetnek az érintett szervezet számára.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek minden rendszerelemét hozzá kell rendelnie legalább egy EIR-hez.
2. A szervezetnek biztosítania kell, hogy a hozzárendelési folyamatot dokumentálják annak érdekében, hogy nyomon követhető legyen.
3. A meghatározott személyeknek vagy szerepköröknek visszaigazolást kell adniuk a hozzárendelésről a szervezet számára.

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

CM-8(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.45. KONFIGURÁCIÓKEZELÉSI TERV

6.45. A szervezet kialakít, dokumentál és végrehajt egy, az EIR-re vonatkozó konfigurációkezelési tervet, amely:

6.45.1. figyelembe veszi a szerepköröket, a felelősségeket, és a konfigurációkezelési folyamatokat és eljárásokat;

6.45.2. bevezet egy folyamatot a rendszerfejlesztési életciklus folyamán a konfigurációs elemek azonosítására a konfigurációs elemek konfigurációjának kezelése céljából;

6.45.3. meghatározza az EIR konfigurációs elemeit, és a konfigurációs elemeket a konfigurációkezelés hatálya alá helyezi;

6.45.4. a meghatározott személyek vagy szerepkörök által kerül felülvizsgálatra és jóváhagyásra;

6.45.5. védi a konfigurációkezelési tervet a jogosulatlan közzététellel és módosítással szemben.

MAGYARÁZAT

Az EIR-rel kapcsolatos konfigurációkezelési tevékenységek az egész rendszerfejlesztési életciklus során előfordulnak. Ennek megfelelően vannak fejlesztéssel kapcsolatos konfigurációkezelési tevékenységek (pl.: a kód és a szoftverkönyvtárak ellenőrzése) és működéssel kapcsolatos konfigurációkezelési tevékenységek (pl.: az telepített elemek ellenőrzése és azok konfigurációjának beállítása). A konfigurációkezelési tervek teljesítik a konfigurációkezelési szabályokat, miközben az egyes EIR-ekhez igazodnak. A konfigurációkezelési tervek meghatározzák azokat folyamatokat és eljárásokat, melyek megszabják, hogy a konfigurációkezelést hogyan kell használni a rendszerfejlesztési életciklus tevékenységeinek támogatására.

A konfigurációkezelési terveket az EIR fejlesztési és beszerzési szakaszában hozzák létre. A tervek leírják, hogyan lehet megtenni a változásokat a változáskezelési folyamatokon keresztül; frissíteni a konfigurációs beállításokat és alapkonfigurációkat; fenntartani az elemleltárakat; ellenőrizni a fejlesztési, tesztelési és működési környezeteket; és kidolgozni, kiadni és frissíteni a legfontosabb dokumentumokat.

A szervezet kész sablonokat alkalmazhat annak biztosítása érdekében, hogy a konfigurációkezelési tervek következetesen és időben kifejlesztésre, illetve végrehajtásra kerüljenek. A sablonok megjeleníthetik az érintett szervezet konfigurációkezelési tervét, a terv

egyes részeit pedig EIR-enként hajtják végre. A konfigurációkezeléssel kapcsolatos jóváhagyási folyamatok magukban foglalják azon kulcsfontosságú felelős személyek meghatározását, akik felelősek az EIR-ekben javasolt változások felülvizsgálatáért és jóváhagyásáért, valamint azokat a személyeket, akik biztonsági vizsgálatokat végeznek a változások végrehajtása előtt. A konfigurációs elemek olyan rendszerelemek (pl.: hardver, szoftver, firmware, dokumentáció), amelyeket konfigurációs szempontból kezelni kell. Ahogy az EIR halad előre a rendszerfejlesztési életciklusban, új konfigurációs elemek kerülhetnek azonosításra, illetve kiderülhet, hogy néhány meglévő konfigurációs elemet már nem szükséges konfigurációs szempontból tovább kezelni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell alakítania egy konfigurációkezelési tervet az EIR-re vonatkozóan, amely figyelembe veszi a szerepköröket, a felelősségeket, és a konfigurációkezelési folyamatokat és eljárásokat. Ez a terv a fejlesztési és beszerzési szakaszban készül el, és leírja, hogyan lehet változtatásokat végrehajtani a változáskezelési folyamatokon keresztül, frissíteni a konfigurációs beállításokat és az alapkonfigurációkat, fenntartani az elemleltárakat, ellenőrizni a fejlesztési, tesztelési és működési környezeteket, valamint kidolgozni, kiadni és frissíteni a kulcsdokumentumokat.
2. A szervezetnek be kell vezetnie egy folyamatot a rendszerfejlesztési életciklus folyamán a konfigurációs elemek azonosítására a konfigurációs elemek konfigurációjának kezelése céljából. Ez magában foglalja olyan hardver, szoftver, firmware és dokumentáció azonosítását, amelyeket konfigurációs szempontból kezelni kell.
3. A szervezetnek meg kell határoznia az EIR konfigurációs elemeit, és a konfigurációs elemeket a konfigurációkezelés hatálya alá kell helyeznie. Ahogy az EIR halad előre a fejlesztési életciklusban, új konfigurációs elemek kerülhetnek azonosításra, illetve kiderülhet, hogy néhány meglévő konfigurációs elemet már nem szükséges konfigurációs szempontból tovább kezelni.
4. A szervezetnek gondoskodnia kell arról, hogy a konfigurációkezelési tervet a felelős személyek vagy szerepkörök által felülvizsgálják és jóváhagyják. Ehhez a szervezetnek meg kell határoznia azokat a személyeket, akik felelősek a rendszerekhez javasolt változások felülvizsgálatáért és jóváhagyásáért, valamint azokat a személyeket, akik biztonsági vizsgálatot

végeznek az EIR-ekben javasolt változásokkal kapcsolatban mielőtt azokat ténylegesen végrehajtanák.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.15. Biztonsági hatásvizsgálatok

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.36. Rendszerelem leltár

13.2. Rendszerbiztonsági terv

16.58. Fejlesztői változáskövetés

18.67. Információ kezelése és megőrzése

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

3.3.6.9. Konfigurációkezelési terv

ISO/IEC 27001:2023 REFERENCIA

A.5.2; A.8.9

NIST SP 800-53 REV.5 REFERENCIA

CM-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

6.46. KONFIGURÁCIÓKEZELÉSI TERV – FELELŐSSÉG HOZZÁRENDELÉSE

6.46. A szervezet a konfigurációkezelési folyamat fejlesztésének felelősségét olyan személyre bízza, aki közvetlenül nem vesz részt a rendszerfejlesztésben.

MAGYARÁZAT

Az érintett szervezetben, ha nincsenek kifejezetten konfigurációkezelési feladatokra kijelölt csapatok, a rendszerfejlesztők feladata lehet a konfigurációkezelési folyamatok kialakítása olyan személyek segítségével, akik közvetlenül nem vesznek részt az EIR fejlesztésben vagy integrációjában. A felelősségek szétválasztása biztosítja, hogy a szervezet megfelelő függetlenséget alakít ki és tart fenn az EIR fejlesztési és integrációs folyamatai, valamint a konfigurációkezelési folyamatok között, így elősegítve a minőségellenőrzést és a hatékonyabb felügyeletet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek a konfigurációkezelési folyamat fejlesztését olyan személyre kell bíznia, aki közvetlenül nem vesz részt a rendszerfejlesztésben. Ha nincsenek kifejezetten konfigurációkezelési feladatokra kijelölt csapatok a szervezetben, a rendszerfejlesztők feladata lehet a konfigurációkezelési folyamatok kialakítása olyan személyek segítségével, akik közvetlenül nem vesznek részt az EIR fejlesztésben vagy integrációjában.

3. A szervezetnek a felelősségek szétválasztásával kell biztosítania, hogy a szervezet megfelelő függetlenséget alakít ki és tart fenn az EIR fejlesztési és integrációs folyamatai, valamint a konfigurációkezelési folyamatok között, így elősegítve a minőségellenőrzést és a hatékonyabb felügyeletet.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.9

NIST SP 800-53 REV.5 REFERENCIA

CM-9(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.47. A SZOFTVERHASZNÁLAT KORLÁTOZÁSAI

6.47. A szervezet:

6.47.1. Kizárólag olyan szoftvereket és olyan kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, valamint a szerzői jogi vagy más jogszabályi előírásoknak.

6.47.2. A másolatok és megosztások ellenőrzésére nyomon követi a mennyiségi licenc alá eső szoftverek és a kapcsolódó dokumentációk használatát.

6.47.3. Ellenőrzi és dokumentálja az állománymegosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett művek jogosulatlan terjesztésére, megjelenítésére, előadására vagy sokszorosítására.

MAGYARÁZAT

Az érintett szervezetnek gondoskodnia kell arról, hogy minden használt szoftver és dokumentáció megfeleljen a szerződésben meghatározott követelményeknek, beleértve a szerzői jogi és egyéb jogszabályi előírásokat is. Nyomon kell követni a mennyiségi licenc alá eső szoftverek és a kapcsolódó dokumentációk használatát, hogy ellenőrizze a szervezet a másolatok és megosztások számát. Ez a nyomon követés lehet manuális vagy automatizált, a szervezet igényeitől függően. A szerződési megállapodások például szoftverlicenc-megállapodásokat is tartalmazhatnak, melyeket központilag szükséges kezelni és periodikusan felül kell vizsgálni. A szervezetnek ellenőrzni és dokumentálni szükséges a megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett művek, szoftverek jogosulatlan terjesztésére, megjelenítésére vagy sokszorosítására. Ez azt jelenti, hogy a szervezetnek naplót kell vezetnie minden EIR megosztásról, és rendszeresen ellenőriznie kell, hogy a megosztások megfelelnek-e a szerzői jogi és egyéb jogszabályi előírásoknak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy csak olyan szoftvereket és kapcsolódó dokumentációkat használjon, amelyek megfelelnek a szerződéses elvárásoknak és a szerzői jogi vagy más jogszabályi előírásoknak. Ez azt jelenti, hogy az érintett szervezetnek át kell néznie

a szoftverek licencszerződéseit és a kapcsolódó dokumentációkat, hogy meggyőződjön arról, hogy megfelelnek-e a szerződéses követelményeknek.

2. A szervezetnek nyomon kell követnie a mennyiségi licenc alá eső szoftverek és a kapcsolódó dokumentációk használatát. Ez azt jelenti, hogy a szervezetnek rendszeresen ellenőriznie kell hogy, mely szoftvereket használják, és milyen kihasználtsággal használják őket. Ezt meg lehet tenni manuálisan, de automatizált eszközök is léteznek, amelyek segíthetnek ebben a folyamatban.

3. A szervezetnek ellenőriznie és dokumentálnia kell az állománymegosztásokat. Ez azt jelenti, hogy a szervezetnek naplót kell vezetnie arról, hogy mely fájlok vannak megosztva, és kikkel vannak megosztva. Ez segít meggyőződni arról, hogy a szerzői joggal védett műveket, szoftvereket nem terjesztik, jelenítik meg, vagy nem sokszorosítanak jogosulatlanul.

4. A szervezetnek rendszeresen felül kell vizsgálnia ezeket a folyamatokat, hogy biztosítsa, hogy továbbra is megfelelnek a követelményeknek. Ez magában foglalja a szoftverlicenc-nyomon követési folyamatok, az állománymegosztás-ellenőrzési folyamatok és a naplózás felülvizsgálatát.

Kapcsolódó intézkedések

2.100. Távoli hozzáférés

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

6.26. Legszűkebb funkcionalitás

6.36. Rendszerelem leltár

1.21. Ellátási lánc kockázatkezelési stratégiája

17.17. A határok védelme

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

3.3.6.10. A szoftverhasználat korlátozásai

ISO/IEC 27001:2023 referencia

A.5.32

NIST SP 800-53 rev.5 referencia

CM-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

6.48. A SZOFTVERHASZNÁLAT KORLÁTOZÁSAI – NYÍLT-FORRÁSKÓDÚ SZOFTVER

6.48. A szervezet meghatározott korlátozásokat alkalmaz a nyílt forráskódú szoftverek használatára vonatkozóan.

MAGYARÁZAT

Az nyílt forráskódú szoftverek olyan szoftverek, amelyek forráskód formájában érhetők el. Bizonyos szoftverjogok, amelyek normál esetben a szerzői jogok tulajdonosait illetik meg, rendszerint szoftverlicensz szerződések alapján biztosítottak, amelyek lehetővé teszik az egyének számára a szoftver tanulmányozását, módosítását és továbbfejlesztését. Biztonsági szempontból a nyílt forráskódú szoftverek fő előnye, hogy lehetőséget biztosítanak az érintett szervezet számára, hogy a forráskódot megvizsgálhassa. Néhány esetben a szoftverhez online közösség is köthető, amely folyamatosan ellenőrzi, teszteli, frissíti azt, emellett jelenti a szoftverben található problémákat. Ugyanakkor a nyílt forráskódú szoftverekben található sérülékenységek kijavítása problémás lehet. A nyílt forráskódú szoftverekkel kapcsolatban licencelési problémák is felmerülhetnek, beleértve az ilyen szoftverek felhasználására vonatkozó korlátozásokat. A kizárólag bináris formában elérhető nyílt forráskódú szoftverek növelhetik az ilyen szoftverek használatának kockázatát.

Az érintett szervezet meghatározott korlátozásokat alkalmaz a nyílt forráskódú szoftverek használatára. Ez azt jelenti, hogy az érintett szervezet csak bizonyos feltételek mellett használhatja ezeket a szoftvereket. Ezek a korlátozások általában a szoftverek biztonságával, a licencelési feltételekkel és a szoftverek használatának kockázataival kapcsolatosak. Az érintett szervezetnek gondosan meg kell vizsgálnia a nyílt forráskódú szoftverek használatának előnyeit és kockázatait, mielőtt döntést hozna a használatukról. A nyílt forráskódú szoftverek használatának korlátozása segíthet az érintett szervezetnek az EIR biztonságának megőrzésében, a licencelési problémák elkerülésében és a kockázatok csökkentésében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondosan meg kell vizsgálnia a nyílt forráskódú szoftverek használatának előnyeit és kockázatait, mielőtt döntést hozna a használatukról.

2. A szervezetnek fel kell mérnie, mely nyílt forráskódú szoftvereket használja jelenleg.

3. A szervezetnek meg kell határoznia a nyílt forráskódú szoftverek használatának szabályait. Ez magában foglalhatja a nyílt forráskódú szoftverek használatának korlátozásait, a licenceléssel kapcsolatos előírásokat, a forráskód ellenőrzését és a hibajavítások kezelését.

4. A szervezetnek implementálnia kell a nyílt forráskódú szoftverek használatának szabályait.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a nyílt forráskódú szoftverek használatának szabályait, hogy biztosítsa azok naprakészségét.

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

CM-10(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a korlátozások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.49. FELHASZNÁLÓ ÁLTAL TELEPÍTETT SZOFTVER

6.49. A szervezet:

6.49.1. Megfogalmazza az EIR vonatkozásában a szervezetre érvényes követelményeket, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségeit.

6.49.2. Érvényesíti a szoftvertelepítésre vonatkozó szabályokat a szervezet által meghatározott módszerek szerint.

6.49.3. Meghatározott gyakorisággal ellenőrzi a szabályok betartását.

MAGYARÁZAT

Az érintett szervezetben a felhasználók, ha megfelelő jogosultságokkal rendelkeznek, telepíthetnek szoftvereket az EIR-ben. A telepített szoftverek felett tartott ellenőrzés érdekében az érintett szervezet meghatározza a szoftvertelepítéssel kapcsolatos engedélyezett és tiltott tevékenységeket. Az engedélyezett szoftvertelepítések közé tartozhatnak a meglévő szoftverek frissítései és biztonsági javításai, valamint az új alkalmazások letöltése az érintett szervezet által jóváhagyott alkalmazásboltokból. A tiltott szoftvertelepítések közé tartoznak az ismeretlen vagy gyanús eredetű szoftverek, vagy azok a szoftverek, amelyeket az érintett szervezet potenciálisan károsnak tart. A felhasználó által telepített szoftverekre vonatkozó szabályokat az érintett szervezet által kidolgozott vagy valamilyen külső entitás által biztosított szabályzat tartalmazza. A szabályok érvényesítési módszerei közé tartozhatnak az ellenőrző eljárások, valamint az automatizált eszközök.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a szoftvertelepítéssel kapcsolatos szervezetre érvényes követelményeket, melyeknek tartalmaznia kell a felhasználók lehetőségeit a szoftvertelepítéssel kapcsolatban, valamint a szoftvertelepítéssel kapcsolatos engedélyezett és tiltott tevékenységeket.

2. A szervezetnek figyelembe kell vennie a szoftvertelepítéssel kapcsolatos szervezetre érvényes követelmények kidolgozásakor, hogy a felhasználók privilegizált jogosultság nélkül is képesek lehetnek telepíteni hordozható (portable) programokat. A szervezetnek a hordozható (portable) programok futtatásának megakadályozására védelmi követelményeket kell kidolgoznia.

3. A szervezetnek érvényesítenie kell a szoftvertelepítésre vonatkozó szabályokat az általa meghatározott módszerek szerint.

4. A szervezetnek meghatározott gyakorisággal ellenőriznie kell a szabályok betartását.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

6.2. Alapkonfiguráció

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.23. Konfigurációs beállítások

6.26. Legszűkebb funkcionalitás

6.36. Rendszerelem leltár

13.3.1. Viselkedési szabályok

18.13. Az EIR monitorozása

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

3.3.6.11. A felhasználó által telepített szoftverek

ISO/IEC 27001:2023 referencia

A.8.19

NIST SP 800-53 rev.5 referencia

CM-11

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

6.50. Felhasználó által telepített szoftverek – Szoftvertelepítés privilegizált státusszal

6.50. A szervezet csak a kifejezetten privilegizált jogosultsággal rendelkező felhasználóknak engedélyezi a szoftverek telepítését.

Magyarázat

A szervezet elvárja, hogy csak privilegizált jogosultsággal rendelkező felhasználók legyenek képesek szoftvereket telepíteni. A követelmény célja, hogy megvédje az EIR-t a nem kívánt vagy káros szoftverek telepítésétől, amelyek veszélyeztethetik az EIR biztonságát. A privilegizált felhasználók általában olyan személyek (pl.: rendszer adminisztrátorok), akiknek emelt jogosultságú hozzáférésük van az EIR-hez, és képesek olyan műveleteket végrehajtani, amelyeket a normál felhasználók nem (pl.: szoftverek telepítése, rendszerbeállítások módosítása, naplók ellenőrzése stb.).

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, kik azok a felhasználók, akik privilegizált jogosultsággal rendelkeznek. Általában a rendszer adminisztrátorok rendelkeznek ilyen jogosultsággal.
2. A szervezetnek úgy kell beállítania jogosultságokat, hogy csak a privilegizált felhasználók telepíthessenek szoftvereket.
3. A szervezetnek be kell vezetnie egy szabályt, amely meghatározza, hogy milyen körülmények között adható meg a privilegizált jogosultság, és ehhez milyen feltételeknek kell megfelelniük a privilegizált felhasználóknak.

Kapcsolódó intézkedések

2.59. Felelősségek szétválasztása

2.60. Legkisebb jogosultság elve

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-11(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.51. A FELHASZNÁLÓ ÁLTAL TELEPÍTETT SZOFTVEREK – AUTOMATIZÁLT KIKÉNYSZERÍTÉS ÉS FELÜGYELET

6.51. A szervezet automatizált mechanizmusokat alkalmaz a szoftvertelepítési szabályok kikényszerítésére és ellenőrzésére.

MAGYARÁZAT

Az érintett szervezet automatizált mechanizmusokat alkalmaz a szoftvertelepítési szabályok kikényszerítésére és ellenőrzésére, így képes gyorsabban észlelni és reagálni a jogosulatlan szoftvertelepítésekre, amelyek belső vagy külső támadás jelei lehetnek. Az automatizált mechanizmusok lehetővé teszik az érintett szervezet számára, hogy proaktívan kezelje az EIR-ekben található szoftvereket, és biztosítsa, hogy csak a megfelelően engedélyezett és ellenőrzött szoftverek legyenek telepítve.

Ezek az automatizált mechanizmusok gyakran tartalmaznak olyan funkciókat, amelyek képesek blokkolni vagy figyelmeztetni a felhasználókat, ha olyan szoftvert próbálnak telepíteni, amely nem felel meg a szervezet szoftvertelepítési szabályainak. Ezen kívül képesek naplózni és jelentést készíteni minden olyan eseményről, amikor a szoftvertelepítési szabályokat megsértették, lehetővé téve az érintett szervezet számára, hogy gyorsan reagáljon és megtegye a szükséges lépéseket a probléma orvoslására.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek a 6.49-es és 6.50-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a automatizált mechanizmusokat, amelyek segítségével képes lesz a szoftvertelepítési szabályok kikényszerítésére és ellenőrzésére.

2. A szervezetnek biztosítania kell, hogy az automatizált mechanizmusok képesek legyenek segítséget nyújtani a szervezet számára a szoftvertelepítési szabályok kikényszerítésében és ellenőrzésében. Emellett arról is meg kell bizonyosodnia a szervezetnek, hogy az automatizált mechanizmusok képesek gyorsan észlelni és reagálni a jogosulatlan szoftvertelepítésekre.

3. A szervezetnek úgy kell beállítania az automatizált mechanizmusokat, hogy azok automatikusan értesítést küldjenek, ha nem megfelelő szoftvert telepítenek az EIR-en, illetve képesek legyenek megakadályozni a nem kívánt szoftverek telepítését.
4. A szervezetnek biztosítania kell, hogy az automatizált mechanizmusok megfelelően működnek. Ez magában foglalhatja az automatizált mechanizmusok rendszeres tesztelését és karbantartását is.

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

CM-11(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

6.52. INFORMÁCIÓ HELYÉNEK AZONOSÍTÁSA ÉS DOKUMENTÁLÁSA

6.52. A szervezet:

6.52.1. azonosítja és dokumentálja a meghatározott információk, valamint azon konkrét rendszerelemeket helyét, amelyeken az információfeldolgozásra és tárolásra kerül;

6.52.2. azonosítja és dokumentálja azokat a felhasználókat, akik hozzáféréssel rendelkeznek a rendszerhez és a rendszerelemekhez, ahol az információ feldolgozásra és tárolásra kerül; és

6.52.3. dokumentálja azokat a változásokat, amelyek az információ feldolgozásának és tárolásának helyét érintik.

MAGYARÁZAT

Az információ helyének azonosítása magában foglalja a meghatározott információk és a rendszerelemek helyének azonosítását, valamint azt, hogy hogyan kerül feldolgozásra az információ, így megérthető az információáramlás, és megfelelő védelmet és szabályozást biztosíthatunk az ilyen információk és rendszerelemek számára. Az információ biztonsági kategóriája is tényező a szükséges követelmények meghatározásában, hogy megvédjük az információt és az rendszerkomponenst, ahol az információ található. Az információ és az rendszerelemek helye is meghatározó tényező a rendszer architektúrájának és tervezésének meghatározásában (az ezekre vonatkozó biztonsági követelmények a "Beszerzések", "A biztonságtervezési elvek", valamint a "Fejlesztői biztonsági architektúra és tervezés" kontrolloknál kerültek bővebben kifejtésre)).

A felhasználók azonosítása és dokumentálása kritikus aspektusa a kiberbiztonságnak. Ez magában foglalja azoknak a felhasználóknak az azonosítását és dokumentálását, akik hozzáférnek rendszerhez és a rendszerelemekhez, ahol az információ feldolgozásra és tárolásra kerül. Ez létfontosságú az EIR sértetlenségének és biztonságának fenntartásához, mivel lehetővé teszi a felhasználói tevékenység nyomon követését és a felhasználók felelősségre vonását rendszeren belüli cselekményeikért.

Azoknak a változásoknak a dokumentálása, amelyek érintik az információ feldolgozásának és tárolásának helyét, szintén kulcsfontosságú követelmény. Ez magában foglalja minden olyan változás dokumentálását, amelyet a rendszerben végeztek, és amely potenciálisan

befolyásolhatja, hogy hol és hogyan kerül feldolgozásra és tárolásra az információ. Ez fontos a rendszer sértetlenségének és biztonságának fenntartásához, mivel lehetővé teszi a változások nyomon követését és szükség esetén a korábbi konfigurációkhoz való visszatérést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania és dokumentálnia kell a meghatározott információk helyét, valamint azon konkrét rendszerelemek helyét, ahol az információfeldolgozás és tárolás történik. Ez magában foglalja a specifikus információ típusok és az információ helyének azonosítását a rendszerelemekben, valamint azt, hogy hogyan történik az információfeldolgozás, hogy megérthető legyen az információáramlás és megfelelő védelmet lehessen biztosítani az információ és a rendszerelemek számára.
2. A szervezetnek azonosítania és dokumentálnia kell azokat a felhasználókat, akik hozzáféréssel rendelkeznek az EIR-hez és a rendszerelemekhez, ahol az információ feldolgozásra és tárolásra kerül. Ez segít a hozzáférési jogosultságok kezelésében és a potenciális biztonsági kockázatok csökkentésében.
3. A szervezetnek dokumentálnia kell azokat a változásokat, amelyek az információ feldolgozásának és tárolásának helyét érintik. Ez magában foglalja az EIR architektúrájának és tervezésének változásait is. A változások naplózása segít a szervezetnek nyomon követni az EIR állapotát és biztosítani, annak érdekében, hogy a változások ne befolyásolják negatívan az információ biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.60. Legkisebb jogosultság elve

2.125. Adatbányászat elleni védelem

6.36. Rendszerelem leltár

1.5. Elektronikus információs rendszerek nyilvántartása

15.2. Biztonsági osztályba sorolás

16.7. Beszerzések

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

CM-12

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

6.53. ALÁÍRT RENDSZERELEMEK

6.53. A szervezet megakadályozza a meghatározott szoftver- és firmware-összetevők telepítését még annak ellenőrzését megelőzően, hogy az összetevő digitális aláírása a szervezet által jóváhagyott tanúsítvánnyal megtörtént.

MAGYARÁZAT

A szoftver- és firmware-összetevők - amelyek telepítése csak elismert és jóváhagyott tanúsítványokkal történő aláírás után lehetséges - a szoftver- és firmware-verziófrissítések, javítások, szervízcsomagok, eszközillesztők és alapvető beviteli/kimeneti rendszerfrissítések közé tartoznak. A szervezetek az alkalmazandó szoftver- és firmware-összetevőket típus, konkrét elemek vagy a kettő kombinációja alapján azonosíthatják. A digitális aláírások és az ilyen aláírások szervezeti ellenőrzése a kódhitelesítés egyik módszere.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a szoftver- és firmware-összetevőket, amelyek telepítését meg szeretné akadályozni, amíg azok digitális aláírása nem történt meg a szervezet által jóváhagyott tanúsítvánnyal. Ez magában foglalhatja a szoftver- és firmware-verzió frissítéseket, javításokat, szolgáltatási csomagokat, eszközmeghajtókat és az alapvető bemeneti/kimeneti rendszer frissítéseket.
2. A szervezetnek létre kell hoznia egy olyan rendszert, amely képes azonosítani a megfelelő szoftver- és firmware-összetevőket, akár típus szerint, akár konkrét elemek szerint, vagy mindkettő kombinációjával.
3. A szervezetnek be kell vezetnie egy digitális aláírásokat használó módszert, amelyet az EIR hitelesít. Ez magában foglalhatja a digitális aláírások létrehozását, ellenőrzését és kezelését.
4. A szervezetnek biztosítania kell, hogy az EIR képes legyen ellenőrizni a digitális aláírásokat, és csak akkor engedélyezze a szoftver- és firmware-összetevők telepítését, ha azok digitális aláírása megegyezik a szervezet által jóváhagyott tanúsítvánnyal.
5. A szervezetnek dokumentálnia kell minden olyan eseményt, amikor a szoftver- vagy firmware-összetevő telepítését megakadályozták, mert annak digitális aláírása nem egyezett meg a szervezet által jóváhagyott tanúsítvánnyal.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.26. Legszűkebb funkcionalitás

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

18.42. Szoftver- és információsértetlenség

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CM-14

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szoftver és firmware összetevők meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024