Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Ellátási lánc kockázatkezelése

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

19.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

19.1. A szervezet:

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

19.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó ellátási láncra vonatkozó kockázatmenedzsment szabályzatot, amely

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

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

19.1.1.2. az ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásrendet, amely az ellátási láncra vonatkozó kockázatkezeléséhez kapcsolódó szabályok és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

19.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki az ellátási láncra vonatkozó kockázatmenedzsment szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

19.1.3. Felülvizsgálja és frissíti az aktuális ellátási láncra vonatkozó kockázatmenedzsment szabályzatot és az ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

Az ellátási láncra vonatkozó kockázatkezelési szabályzat és eljárások az ellátási lánc kockázatkezelése követelménycsoportba tartozó védelmi intézkedésekkel foglalkoznak, amelyek az EIR-ekben, illetve a szervezetekben bevezetésre kerülnek.

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

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

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell az ellátási láncra vonatkozó kockázatkezelési szabályzat és eljárásrendek kidolgozásával, dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatok ellátásáról.
2. A szervezetnek meg kell bizonyosodnia arról, hogy az ellátási láncra vonatkozó kockázatkezelési 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 az ellátási láncra vonatkozó kockázatkezelési 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 ellátási láncra vonatkozó kockázatkezelési 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
1.21. Ellátási lánc kockázatkezelési stratégiája
14.12. Fegyelmi intézkedések
18.67. Információ kezelése és megőrzése

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

Nincs vonatkozó referencia.

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.5.19; A.5.31; A.5.36; A.5.37

NIST SP 800-53 rev.5 referencia

SR-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

19.2. ELLÁTÁSI LÁNCRA VONATKOZÓ KOCKÁZATMENEDZSMENT SZABÁLYZAT

19.2. A szervezet:

19.2.1. A meghatározott EIR-ek, rendszerelemek vagy rendszerszolgáltatások tekintetében szabályzatot dolgoz ki a kutatás-fejlesztés, tervezés, gyártás, beszerzés, szállítás, integráció, üzemeltetés és karbantartás, kivezetés, valamint a selejtezés során felmerülő ellátási lánccal kapcsolatos kockázatok kezelésére.

19.2.2. Meghatározott gyakorisággal felülvizsgálja és frissíti az ellátási lánc kockázatmenedzsment szabályzatát, illetve szükség szerint annak érdekében, hogy kezelje a fenyegetéseket, valamint a szervezeti és környezeti változásokat.

19.2.3. Védi az ellátási lánc kockázatmenedzsment szabályzatát a jogosulatlan közzétételtől és módosítástól.

MAGYARÁZAT

Az érintett szervezet függősége a külső szolgáltatóktól származó termékektől, rendszerektől és szolgáltatásoktól, valamint a szolgáltatókkal való kapcsolatok jellege, növekvő kockázatot jelent. A tevékenységek, amelyek növelhetik a biztonsági vagy adatvédelmi kockázatokat, magukban foglalják a jogosulatlan gyártást, a hamisítványokra való cserét, vagy azok használatát, a módosításokat, a lopást, a rosszindulatú szoftverek és hardverek beillesztését, valamint a nem megfelelő gyártási és fejlesztési gyakorlatot az ellátási láncban. Az ellátási lánc kockázatai endémiásak vagy rendszerszintűek lehetnek egy rendszerelemben, egy EIR-en, egy szervezeten, egy ágazaton vagy a nemzeten belül. Az ellátási lánc kockázatkezelése összetett, többoldalú feladat, amely koordinált erőfeszítést igényel a szervezeten belül a bizalmi kapcsolatok kiépítéséhez és a belső és külső érdekeltekkel való kommunikációhoz. Az ellátási lánc kockázatkezelési tevékenységek (SCRM) magukban foglalják a kockázatok azonosítását és értékelését, a megfelelő kockázat válaszintézkedések meghatározását, a kockázatkezelési tervek kidolgozását a válaszintézkedések dokumentálására, és a teljesítmény ellenőrzését a tervekkel szemben. Az ellátási lánc kockázatkezelési (SCRM) terv (a rendszer szintjén) implementáció specifikus, biztosítja a szabályzatok végrehajtását, követelményeket, korlátozásokat és következményeket. Ez lehet önálló vagy beépíthető a rendszer biztonsági és

adatvédelmi terveibe. Az ellátási lánc kockázatkezelési terv kezeli a kockázatkezelési követelmények végrehajtását és nyomon követését, valamint a rendszerek fejlesztését/fenntartását a rendszerfejlesztési életcikluson (SDLC) keresztül az ügymeneti és üzleti funkciók támogatása érdekében.

Mivel az ellátási láncok jelentősen eltérhetnek a szervezeten belül és között, az ellátási lánc kockázatkezelési (SCRM) tervek az egyéni programokhoz, szervezeti és működési kontextusokhoz igazodnak. A testre szabott kockázatkezelési tervek azon meghatározás alapját képezik, hogy egy technológia, szolgáltatás, rendszerelem, vagy rendszer alkalmas-e a célra, és ennek megfelelően szükséges a követelmények testre szabása. A testre szabott kockázatkezelési tervek segítenek a szervezeteknek a legkritikusabb ügymeneti és üzleti funkciókra összpontosítani erőforrásaikat az ügymeneti és üzleti követelmények, valamint a kockázati környezet alapján.

A kockázatkezelési tervek tartalmazzák a szervezet ellátási lánc kockázattűrésének értékeit, az elfogadható ellátási lánc kockázatcsökkentő stratégiákat vagy követelményeket, egy folyamatot az elfogadható kockázat kiértékelésére és nyomon követésére, a tervek alkalmazásáról, illetve az arról való tájékoztatás folyamatát, valamint egy összefoglalót a megtett intézkedések szükségességéről és az érintett személyekről és szerepkörökről.

Ezek mellett az ellátási lánc kockázatkezelési tervei a megbízható, biztonságos, személyes adatokat védő és rugalmas rendszerelemek és -rendszerek fejlesztésére vonatkozó követelményekkel is foglalkoznak, beleértve az életciklus-alapú rendszerek biztonságtechnikai folyamatainak részeként megvalósított biztonsági tervezési elvek alkalmazását (lásd Rendszer- és szolgáltatásbeszerzés kontrollcsaládot).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azon rendszereket, rendszerelemeket vagy rendszerszolgáltatásokat, melyek ellátási láncával kapcsolatos kockázatokat kezelni kell.
2. A szervezetnek meg kell határoznia egy szabályzatot a szükséges kockázatkezelési intézkedések elvégzésére a meghatározott rendszerek, rendszerelemek vagy rendszerszolgáltatások ellátási láncával kapcsolatosan.
3. A szervezetnek meg kell határoznia a gyakoriságot, mellyel a meghatározott kockázatkezelési szabályzatot felülvizsgálja.

4. A szervezetnek alkalmaznia kell a meghatározott szabályzatot az érintett rendszerek, rendszerelemek vagy rendszerszolgáltatások ellátási láncának kockázatkezelésére.

5. A szervezetnek biztosítania kell, hogy az ellátási lánc kockázatkezelési szabályzata tartalmazza a rendszerfejlesztési életciklus során fennálló kockázatok meghatározását és kezelését is.

6. A szervezetnek felül kell vizsgálnia az ellátási lánc kockázatkezelési szabályzatot a meghatározott gyakorisággal.

Kapcsolódó intézkedések

5.2. Biztonsági értékelések

7.13. Üzletmenet-folytonossági terv tesztelése

9.9.1. Biztonsági események kezelése

10.2. Szabályozott karbantartás

10.21. Kellő időben történő karbantartás

12.42. Be- és kiszállítás

13.2. Rendszerbiztonsági terv

1.10. Kockázatkezelési stratégia

1.21. Ellátási lánc kockázatkezelési stratégiája

15.4. Kockázatértékelés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.19; A.5.20; A.5.21; A.8.30

NIST SP 800-53 rev.5 referencia

SR-2

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.3. ELLÁTÁSI LÁNCRA VONATKOZÓ KOCKÁZATMENEDZSMENT SZABÁLYZAT – ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSÉÉRT FELELŐS CSOPORT LÉTREHOZÁSA

19.3. A szervezet létrehoz egy, az ellátási lánc kockázatait kezelő csapatot, amely a meghatározott személyekből, szerepkörökből és felelősségi körökből áll.

MAGYARÁZAT

Az ellátási lánc kockázatkezelési tervek végrehajtása érdekében az érintett szervezetek koordinált, csapat alapú megközelítést alkalmaznak az ellátási lánc kockázatainak azonosítására és értékelésére, valamint a kockázatok kezelésére programozási és technikai enyhítési módszerek alkalmazásával. A csapat megközelítés lehetővé teszi a szervezetek számára, hogy elemzést végezzenek az ellátási láncukról, kommunikáljanak belső és külső partnerekkel vagy érdekelt felekkel, és széles körű konszenzust érjenek el az ellátási lánc kockázatkezeléséhez (SCRM) szükséges erőforrásokkal kapcsolatban. Az ellátási lánc kockázatkezelési (SCRM) csapat a szervezet különböző szerepkörű és felelősségi körű személyzetéből áll, akik vezetői és támogatói szerepet töltenek be a tevékenységekben, beleértve a kockázati menedzsment feladatokat, az információs technológiát, a szerződéskötést, az információbiztonságot, az adatvédelmet, ügymeneti, vagy üzleti tevékenységet, a jogi, az ellátási lánc és logisztikai, a beszerzési, az üzletmenet-folytonossági és más releváns funkciókat. Az ellátási lánc kockázatkezelési (SCRM) csapat tagjai különböző aspektusokban vesznek részt a szoftverfejlesztési életciklusban (SDLC), és mind ismerik és szakértelmet nyújtanak a beszerzési folyamatokban, jogi gyakorlatokban, sérülékenységek kezelésében, fenyegetések és támadási vektorok kezelésében, valamint megértik a rendszer technikai aspektusait és függőségeit. Az ellátási lánc kockázatkezelési (SCRM) csapat kiterjesztése lehet a biztonsági és adatvédelmi kockázatkezelési folyamatoknak, vagy bevonható a szervezet kockázatkezelési csapatába.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az ellátási lánc kockázatainak kezelése szempontjából érintett személyeket, szerepköröket és felelősségi köröket.
2. A szervezetnek létre kell hoznia egy csapatot, mely az ellátási lánc kockázatainak kezeléséért felelős és a meghatározott személyekből, szerepkörökből és felelősségi körökből áll.
3. A szervezet által meghatározott csapatnak teljesítenie kell az ellátási lánc kockázatainak kezelése szempontjából fontos feladatokat.
4. A szervezetnek biztosítania kell, hogy az ellátási lánc kockázatkezelési csapata részt vegyen a szoftverfejlesztési életciklusban és szükséges szakértelmet biztosítson.
5. A szervezetnek dokumentálnia kell az ellátási lánc kockázatkezelési csapata személyzetét és az általuk elvégzett elemzéseket és intézkedéseket.

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

SR-2(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek, szerepkörök és felelősségi körök, illetve az ellátási lánc kockázatkezelési tevékenységek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

19.4. ELLÁTÁSI LÁNCRA VONATKOZÓ KÖVETELMÉNYEK ÉS FOLYAMATOK

19.4. A szervezet:

19.4.1. Folyamatot vagy folyamatokat alakít ki annak érdekében, hogy azonosítsa és kezelje a gyengeségeket vagy hiányosságokat a meghatározott EIR ellátási láncának elemeiben és folyamataiban, a szervezet által meghatározott ellátási láncért felelős személyekkel együttműködve.

19.4.2. Alkalmazza a szervezet által meghatározott ellátási lánccal kapcsolatos kontrollokat annak érdekében, hogy védje az EIR-t, rendszerelemet vagy rendszer szolgáltatást az ellátási lánccal kapcsolatos kockázatokkal szemben és csökkentse az ellátási lánccal kapcsolatos eseményekből eredő károkat és következményeket.

19.4.3. Dokumentálja a meghatározott és bevezetett ellátási láncot érintő folyamatokat és kontrollokat a biztonsági szabályzatokban, az ellátási lánc kockázatmenedzsment szabályzatában és egyéb, a szervezet által meghatározott dokumentumban.

MAGYARÁZAT

Az ellátási lánc elemei magukban foglalják azokat a szervezeteket, szereplőket vagy eszközöket, amelyeket az EIR és a rendszerelemeinek kutatására és fejlesztésére, tervezésére, gyártására, beszerzésére, szállítására, integrációjára, üzemeltetésére és karbantartására, valamint selejtezésére használnak. Az ellátási lánc folyamatai magukban foglalják a hardver-, szoftver- és firmware-fejlesztési folyamatokat; a szállítási és kezelési eljárásokat; a személyi és fizikai biztonsági programokat; a konfigurációs menedzsment eszközeit, technikáit és intézkedéseit az eredetiség biztosítására; vagy más programokat, folyamatokat vagy eljárásokat, amelyek az EIR és a rendszerelemeinek fejlesztésével, beszerzésével, karbantartásával és selejtezésével kapcsolatosak. Az ellátási lánc elemeit és folyamatait a szervezet, az rendszerintegrátorok vagy külső szolgáltatók biztosíthatják. Az ellátási lánc elemeiben vagy folyamataiban lévő gyengeségek vagy hiányosságok potenciális sérülékenységeket jelentenek, amelyeket a támadók kihasználhatnak a szervezet károsítására és annak képességének befolyásolására, hogy végrehajtsa ügymeneti feladatait vagy üzleti funkcióit.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azon EIR-hez kötődő ellátási láncot és ellátási láncelemeket, melyek gyengeségeit azonosítani és kezelni kell.
2. A szervezetnek meg kell határoznia az ellátási láncért felelős személyeket.
3. A szervezetnek meg kell határoznia az ellátási lánccal kapcsolatos események naplózására használt dokumentumokat.
4. A szervezetnek ki kell dolgoznia egy stratégiát, mely alapján a meghatározott ellátási lánc gyengeségeit, vagy hiányosságait azonosítja és kezeli. Ez magában foglalja az ellátási láncért felelős személyekkel való együttműködést is.
5. A szervezetnek naplóznia kell a meghatározott ellátási lánccal kapcsolatos eseményeket a meghatározott dokumentumokba.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.2. Biztonsági értékelések
10.2. Szabályozott karbantartás
10.21. Kellő időben történő karbantartás
12.6. A fizikai belépés ellenőrzése
12.42. Be- és kiszállítás
13.6. Információbiztonsági architektúra leírás
1.21. Ellátási lánc kockázatkezelési stratégiája
16.2. Erőforrások rendelkezésre állása
16.3.1. A rendszer fejlesztési életciklusa
16.7. Beszerzések

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.5.20; A.5.21

NIST SP 800-53 REV.5 REFERENCIA

SR-3

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.5. ELLÁTÁSI LÁNC ELLENŐRZÉSEK ÉS FOLYAMATOK – DIVERZIFIKÁLT BESZÁLLÍTÓI BÁZIS

19.5. A szervezet többféle beszállítót vesz igénybe a meghatározott rendszerelemek és szolgáltatások vonatkozásában.

MAGYARÁZAT

Többféle beszállító igénybevétele a rendszerelemek és rendszerszolgáltatások vonatkozásában csökkenti a valószínűségét annak, hogy rosszindulatú támadók sikeresen azonosítsák és célba vegyék az ellátási láncot, valamint csökkenti az ellátási lánc kompromittálódásának hatását. Több beszállító azonosítása a cserélhető rendszerelemekhez csökkentheti annak a valószínűségét, hogy a cserélhető rendszerelem elérhetetlenné válik. A különböző fejlesztők vagy logisztikai szolgáltatók alkalmazása csökkentheti egy természeti katasztrófa vagy más ellátási láncbeli esemény hatását. A szervezetek fontolóra vehetik az EIR tervezését olyan szempontok figyelembevételével, hogy az különböző anyagokat és elemeket tartalmazzon.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely rendszerelemeket szerezzen be különböző beszállítóktól.
2. A szervezetnek ki kell dolgoznia egy stratégiát a beszállítói kör sokoldalúbbá tételére, hogy a meghatározott rendszerelemeket több beszállítótól is beszerezhesse.
3. A szervezetnek alkalmaznia kell a meghatározott rendszerelemek több beszállítótól való beszerzését biztosítani hivatott stratégiát.
4. A szervezetnek dokumentálnia kell és rendszeresen felül kell vizsgálnia a beszállítóinak listáját és ha szükséges frissítenie kell azt.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az rendszerelemek és szolgáltatások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

19.6. Ellátási lánc ellenőrzések és folyamatok – károk csökkentése

19.6. A szervezet meghatározott ellenintézkedéseket alkalmaz a szervezeti ellátási láncot azonosító és célba vevő potenciális ellenérdekű felek által okozott kár csökkentése érdekében.

Magyarázat

Az érintett szervezet által alkalmazható biztonsági intézkedések, amelyek csökkentik annak valószínűségét, hogy rosszindulatú támadók sikeresen azonosítsák és célba vegyék az ellátási láncot lehetnek például: a személyre szabott vagy nem szabványos konfigurációk beszerzésének kerülése, jó hírnévvel rendelkező, jóváhagyott beszállítói listák alkalmazása, az előre meghatározott karbantartási ütemtervek, továbbá a frissítési és javítási mechanizmusok követése, vészhelyzeti terv fenntartása az ellátási lánc kompromittálódásának esetére, beszerzési kivételeket használata, amelyek kizárásokat biztosítanak a kötelezettségek alól, változatos szállítási útvonalak használata, a vásárlási döntések és a szállítás közötti idő minimalizálása.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania kell a lehetséges rosszindulatú támadások által okozhatott potenciális károkat.
2. A szervezetnek biztonsági intézkedéseket kell alkalmaznia a rosszindulatú támadók által okozhatott potenciális károk ellen, például a szervezetnek kerülnie kell a személyre szabott vagy nem szabványos konfigurációk beszerzését, jóváhagyott beszállítói listákat kell alkalmaznia stb...
3. A szervezetnek folyamatosan monitoroznia kell az általa alkalmazott ellátási lánc ellenintézkedések hatékonyságát és dokumentálnia kell az eredményeket.
4. A szervezetnek rendszeresen felül kell vizsgálnia az ellátási lánc biztonsága érdekében alkalmazott védelmi intézkedések hatékonyságát és ha szükséges a legújabb iparági gyakorlatokat kell implementálnia a meglévő biztonsági követelmények kielégítésére.

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

SR-3(2)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

19.7. Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók

19.7. A szervezet gondoskodik arról, hogy az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.

Magyarázat

Az ellátási lánc kockázatának hatékony és átfogó kezelése érdekében fontos, hogy az érintett szervezetek biztosítsák az ellátási lánc kockázatkezelési szabályainak beépítését az ellátási lánc összes szintjén. Ez magában foglalja azt is, hogy az 1. szintű vállalkozók megvalósították-e azokat a folyamatokat, amelyek lehetővé teszik az ellátási lánc kockázatkezelési szabályainak és intézkedéseinek továbbítását az alacsonyabb szintű alvállalkozók felé. Erről bővebb információt az Ellátási láncra vonatkozó követelmények és folyamatok című biztonsági követelményél találhat.

A követelmény alkalmazásának lépései

1. A szervezetnek fel kell mérnie a kiberbiztonsági kockázatokat, amelyek az EIR-rel összefüggő szerződésekben szerepelnek.
2. A szervezetnek biztosítania kell, hogy a fővállalkozók tisztában vannak az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményekkel.
3. A szervezetnek meg kell követelnie, hogy a fővállalkozók biztosítsák, hogy az alvállalkozók szerződései is tartalmazzák az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket.
4. A szervezetnek rendszeresen felül kell vizsgálnia a fővállalkozóktól elvárt az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelmények relevanciáját és ha szükséges módosítania kell azokat.

Kapcsolódó intézkedések

19.13. Beszerzési stratégiák, eszközök és módszerek

19.19. Értesítési 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

SR-3(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.8. RENDSZERELEMEK ÉS KAPCSOLÓDÓ ADATOK EREDETISÉGE

19.8. A szervezet dokumentálja, monitorozza és megőrzi a meghatározott EIR-ekhez, rendszerelemekhez kapcsolódó, azok eredetiségét igazoló adatokat.

MAGYARÁZAT

Minden EIR és rendszerelem rendelkezik egy eredeti állapottal, és változhat az életciklusa során. Az eredetiség az EIR vagy rendszerelem és a hozzá kapcsolódó adatok eredetének, fejlődésének, tulajdonjogának, helyének és változásainak időrendje. Tartalmazhatja a személyzetet és a folyamatokat is, amelyeket az EIR-rel, rendszerelemmel vagy a hozzá kapcsolódó adatokkal való interakcióhoz vagy módosításához használnak. A szervezetek fontolóra veszik eljárások kialakítását a rendszer és rendszerelemek eredetiségéért felelős személyek kijelölésére; az eredetiség dokumentációjának és felelősségének átadására más szervezetek között; és az eredetiség nyilvántartásokhoz történő jogosulatlan változtatások megelőzésére és monitorozására. A szervezeteknek vannak módszereik az EIR-ek, rendszerelemek és kapcsolódó adatok érvényes eredetiség-alapjainak dokumentálására, monitorozására és fenntartására. Ezek a tevékenységek segítenek nyomon követni, értékelni és dokumentálni az eredetiségben bekövetkező változásokat, beleértve az ellátási lánc elemek vagy a konfiguráció változásait, és segítenek biztosítani az eredetiség információinak és az eredetiség változásai naplójának megmásíthatatlanságát. Az eredetiség szempontjait figyelembe veszik az EIR fejlesztési életciklusa során, és szükség szerint beépítik a szerződésekbe és egyéb megállapodásokba.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia minden EIR és rendszerelem eredetiségét igazoló adatokat.
2. A szervezetnek eljárásokat kell meghatároznia az EIR és rendszerelemek eredetiségéért felelős személyek kijelölésére, az eredetiség dokumentálásának, karbantartásának és monitorozásának; az eredetiség dokumentációjának és felelősségének átadására más

szervezetek között; és az eredetiség nyilvántartásokhoz történő jogosulatlan változtatások megelőzésére és monitorozására.

3. A szervezetnek alkalmaznia kell a meghatározott eljárásokat az EIR-ek, rendszerelemek és a hozzájuk kapcsolódó adatok érvényes eredetiségének kezelésére.

4. A szervezetnek az EIR-en vagy rendszerelemeken végrehajtott változtatásokat is dokumentálnia kell, biztosítva az eredetiség naplóinak megmásíthatatlanságát.

Kapcsolódó intézkedések

6.36. Rendszerelem leltár

10.2. Szabályozott karbantartás

10.21. Kellő időben történő karbantartás

15.21. Rendszerelemek kritikusságának elemzése

16.3.1. A rendszer fejlesztési életciklusa

16.16. Biztonságtervezési elvek

18.13. Az EIR monitorozása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.21; A.8.30

NIST SP 800-53 rev.5 referencia

SR-4

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az EIR-ekhez, rendszerelemekhez kapcsolódó, azok eredetiségét igazoló adatok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

19.9. RENDSZERELEMEK ÉS KAPCSOLÓDÓ ADATOK EREDETISÉGE - AZONOSÍTÁS

19.9. A szervezet az EIR, valamint a szervezet működése szempontjából kritikus rendszerelemek ellátási láncának meghatározott elemeire folyamataira és a hozzájuk köthető személyzetre azonosítási folyamatot alakít ki és tart fenn.

MAGYARÁZAT

Az érintett szervezet számára létfontosságú, hogy tisztában legyen azzal, kik és mik vannak az EIR és a szervezet működése szempontjából kritikus rendszerelemek ellátási láncában, hogy betekintést nyerjen az ellátási lánc tevékenységeibe. Az ellátási lánc tevékenységeinek átláthatósága szintén fontos a magas kockázatú események és tevékenységek figyeléséhez és azonosításához. Az ellátási lánc elemeinek, folyamatainak és személyzetének átláthatósága nélkül a szervezetek számára nagyon nehéz megérteni és kezelni a kockázatot, és csökkenteni a kedvezőtlen eseményekre való hajlamukat. Az ellátási lánc elemei közé tartoznak azok a szervezetek, szereplők vagy eszközök, amelyeket az EIR és annak rendszerelemeinek kutatás-fejlesztésére, tervezésére, gyártására, beszerzésére, szállítására, integrációjára, működtetésére, karbantartására és selejtezésére használnak. Az ellátási lánc folyamatai közé tartoznak a hardver, szoftver és firmware fejlesztési folyamatai; a szállítási és kezelési eljárások; a konfigurációs menedzsment eszközei, technikái és intézkedései az eredetiség biztosítására; a személyzet és a fizikai biztonsági programok; vagy más programok, folyamatok vagy eljárások, amelyek az ellátási lánc elemeinek előállításával és terjesztésével kapcsolatosak. Az ellátási lánc személyzete olyan személyek, akiknek specifikus szerepük és felelősségük van az EIR és annak rendszerelemeinek kutatás-fejlesztésével, tervezésével, gyártásával, beszerzésével, szállításával, integrációjával, működtetésével és karbantartásával, valamint selejtezésével kapcsolatban. Az azonosítási módszerek elegendőek ahhoz, hogy támogassák a vizsgálatot egy ellátási lánc változás esetén, kompromittálódás esetén, vagy esemény bekövetkeztekor.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell az EIR és a szervezet működése szempontjából kritikus rendszerelemek ellátási láncának elemeit, folyamatait és az azokhoz köthető személyzetet.

2. A szervezetnek ki kell dolgoznia és fenn kell tartania egy azonosítási folyamatot, amely elegendő támogatást nyújt egy vizsgálat számára, ha az ellátási láncban változás történik, vagy kompromittálódik.
3. A szervezetnek alkalmaznia kell az azonosítási folyamatot minden, korábban meghatározott, a szervezet működése szempontjából kritikus rendszerelemek ellátási láncának elemeire, folyamataira és az azokhoz köthető személyzetre.
4. A szervezetnek dokumentálnia kell a kritikus fontosságú EIR-jeinek ellátási láncának folyamatait, szereplőit és változás esetén frissítenie kell a dokumentumot.

KAPCSOLÓDÓ INTÉZKEDÉSEK

8.2. Azonosítás és hitelesítés
8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)
12.42. Be- és kiszállítás

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-4(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az EIR, valamint a szervezet működése szempontjából kritikus rendszerelemek ellátási láncának meghatározott elemei, folyamatai és a hozzájuk köthető személyzet meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

19.10. Rendszerelemek és kapcsolódó adatok eredetisége – Ellátási láncon keresztül történő nyomon követés

19.10. A szervezet az EIR-eket, valamint a szervezet működése szempontjából kritikus rendszerelemeket egyedileg azonosítja az ellátási láncon keresztül történő nyomon követés céljából.

Magyarázat

Az EIR-ek és a rendszerelemek egyedi azonosításának nyomon követése a fejlesztési és szállítási tevékenységek során alapvető azonosítási struktúrát biztosít az eredetiség vizsgálatának segítéséhez és fenntartásához. Például a rendszerelemeket címkézni lehet sorozatszámokkal vagy meg lehet jelölni rádiófrekvenciás azonosító címkékkel. A címkék és jelzések jobb láthatóságot biztosíthatnak egy EIR vagy rendszerelem eredetiségvizsgálatába. Egy EIR vagy rendszerelem több egyedi azonosítóval is rendelkezhet. Az azonosítási módszerek elegendőek ahhoz, hogy támogassák a vizsgálatot egy ellátási lánc kompromittálása vagy esemény után.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania kell az EIR és a szervezet működése szempontjából kritikus rendszerelemeket.
2. A szervezetnek egyedi azonosításra alkalmas címkéket vagy jelöléseket használ a rendszerelemek ellátási láncon keresztül történő nyomon követés céljából.
3. A szervezet gondoskodik arról, hogy az ellátási láncban bekövetkező esemény vagy kompromittációt követően a rendszerelemek esetén használt azonosítási módszerek segítség a vizsgálatot.

Kapcsolódó intézkedések

8.2. Azonosítás és hitelesítés

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

12.42. Be- és kiszállítás

13.2. Rendszerbiztonsági terv

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-4(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

19.11. EREDET – VALÓDISÁG ÉS MÓDOSÍTATLANSÁG HITELESÍTÉSE

19.11. A szervezet meghatározott védelmi intézkedéseket alkalmaz annak ellenőrzésére, hogy az EIR vagy rendszerelem eredeti és nem módosított.

MAGYARÁZAT

Számos EIR és rendszerelem tekintetében, különösen a hardverek esetében, léteznek technikai eszközök annak megállapítására, hogy az elemek eredetiek-e vagy módosították-e őket, ilyenek az optikai és nanotechnológiai címkézést, a fizikailag nem klónozható funkciókat, az oldalsó csatorna elemzést, a kriptográfiai hash ellenőrzéseket vagy digitális aláírásokat, valamint a látható manipuláció elleni címkéket vagy matricákat. Az ellenőrzések magukban foglalhatják a specifikáción kívüli teljesítmény monitorozását is, ami a hamisítás vagy a manipuláció jele lehet. A szervezetek kihasználhatják a beszállítók és szerződéses partnerek folyamatait annak ellenőrzésére, hogy egy EIR, vagy rendszerelem eredeti-e és nem módosították-e, valamint a gyanús EIR, vagy rendszerelem cseréjére. A manipuláció bizonyos jelei láthatóak és kezelhetőek lehetnek a szállítás elfogadása előtt, mint például az össze nem illő csomagolás, a megtört pecsétek és a helytelen címkék. Amikor egy EIR-t, vagy rendszerelemet módosítottnak, vagy hamisítottnak gyanítanak, a beszállító, a szerződéses partner, vagy az eredeti berendezés gyártója cserélheti az elemet, vagy olyan vizsgálati képességeket biztosíthat, amely meghatározza a hamisított, vagy módosított elem eredetét. A szervezetek képzést biztosíthatnak a személyzetnek arra vonatkozóan, hogyan ismerjék fel a gyanúsnak tűnő, leszállított EIR-eket, vagy rendszerelemeket. .

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy milyen technikai eszközöket és intézkedéseket alkalmazzon az EIR és rendszerelemek hitelességének és módosítatlanságának ellenőrzésére.
2. A szervezetnek alkalmaznia kell az EIR és rendszerelemek hitelességének és módosítatlanságának ellenőrzésére meghatározott technikai eszközöket és intézkedéseket.
3. Amennyiben a szervezet gyanús EIR, vagy rendszerelem jelét fedezi fel, támaszkodhat a beszállítói és szerződéses fél folyamataira annak ellenőrzésére, hogy az EIR, vagy rendszerelem

eredeti és nem módosított, valamint a gyanús EIR, vagy rendszerelem cseréjére. A berendezés eredeti gyártója képes lehet az elem cseréjére, vagy olyan vizsgálati képesség biztosítására, amely meghatározza a hamisítvány vagy a módosított elem eredetét.

4. A szervezetnek lehetősége van képzést biztosítania a személyzet számára a gyanús EIR, vagy rendszerelemek szállításának azonosítására.

5. A szervezetnek dokumentálnia kell az ilyen jellegű képzést, a későbbi kiberbiztonsági követelménynek való megfelelés alátámasztása érdekében.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

19.20. Hamisítás elleni védelem

19.22. Rendszerek vagy rendszerelemek vizsgálata

19.23. Rendszerelem hitelessége

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SR-4(3)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

19.12. EREDET – ELLÁTÁSI LÁNC SÉRTETLENSÉGE – JÓHÍRNÉV

19.12. A szervezet meghatározott védelmi intézkedéseket alkalmaz, és meghatározott elemzéseket végez az EIR és rendszerelemek sértetlenségének biztosítása érdekében, a szervezet működése szempontjából kritikus technológiák, termékek és szolgáltatások belső összetételének és eredetének ellenőrzésével.

MAGYARÁZAT

Az érintett szervezet számára az EIR és rendszerelemek, szolgáltatások belső összetételének és eredetének megbízható információi erős alapot nyújtanak a bizalomhoz. A technológiák, termékek és szolgáltatások belső összetételének és eredetének ellenőrzését jóhírnévnek nevezzük. A mikroelektronikában ez magában foglalja az alkatrészek anyagi összetételét is. A szoftverek esetében ez magában foglalja az nyílt forrású és saját kódok összetételét, beleértve az elem verzióját az adott időpontban. A jóhírnév növeli a bizalmat abban, hogy a szállítók által a termékeik, szolgáltatásaik és technológiáik belső összetételéről és eredetéről tett állításaik érvényesek. A belső összetétel és eredet ellenőrzését különböző bizonyítékok vagy nyilvántartások segítségével lehet elérni, amelyeket a gyártók és szállítók a technológia, termékek és szolgáltatások kutatás-fejlesztés, tervezés, gyártás, beszerzés, szállítás, integráció, üzemeltetés és karbantartás, valamint selejtezés során állítanak elő. A bizonyítékok közé tartoznak, de nem korlátozódnak a szoftverazonosító (SWID) címkékre, a szoftverelemek-leltárára, a gyártók platform attribútumokra vonatkozó nyilatkozataira (pl. sorozatszámok, hardverelem-leltár) és olyan mérésekre (pl. firmware hash-ek), amelyek szorosan kötődnek a hardverhez magához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a kritikus technológiákat, termékeket és szolgáltatásokat, amelyek a működés szempontjából fontosak.
2. A szervezetnek meg kell határoznia és alkalmaznia kell a védelmi intézkedéseket és elemzéseket, amelyek biztosítják a rendszer és rendszerelemek sértetlenségét.

3. A szervezetnek ellenőriznie kell az általa igénybe vett EIR, rendszerelem vagy szolgálatás belső összetételét és eredetét, melyre a szállítók állításait veszi alapul összevetve más bizonyítékokkal.
4. A szervet gondoskodik róla, hogy a szállítók kiválasztásakor figyelembe vegye az adott szervezetek jóhírnevét is, melyről a fenti folyamatok elvégzésével tud megbizonyosodni.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.4. Kockázatértékelés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-4(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

19.13. BESZERZÉSI STRATÉGIÁK, ESZKÖZÖK ÉS MÓDSZEREK

19.13. A szervezet meghatározott beszerzési stratégiákat, szerződéses eszközöket és beszerzési módszereket alkalmaz annak érdekében, hogy kivédje, azonosítsa és csökkentse az ellátási láncból eredő kockázatokat.

MAGYARÁZAT

A beszerzési folyamat fontos eszköz lehet az ellátási lánc védelmében. Sok hasznos eszköz és technika áll rendelkezésre, beleértve az EIR és rendszerelemek végső felhasználásának elrejtését, vak vagy szűrt vásárlásokat, módosításoknak ellenálló csomagolás megkövetelését vagy megbízható vagy ellenőrzött forgalmazás használatát. Az ellátási lánc kockázatértékeléséből származó eredmények szabhatják meg a leginkább alkalmazható stratégiákat, eszközöket és módszereket. Az eszközök és technikák védelmet nyújthatnak a jogosulatlan gyártás, lopás, manipuláció, hamisítványokra való csere, kártékony szoftverek vagy hátsó ajtók beállítása, valamint a rossz fejlesztési gyakorlatok ellen a fejlesztési életciklus során. Az érintett szervezetek azt is mérlegelhetik, hogy ösztönözzék azon szállítókat, amelyek ellenőrzéseket hajtanak végre, átláthatóságot biztosítanak folyamataikba és biztonsági és adatvédelmi gyakorlataikba, szerződést biztosítanak, amely megtiltja a hamisított elemek használatát, és korlátozzák a vásárlásokat megbízhatatlan szállítóktól. A szervezetek mérlegelik a személyzet számára a beszállítói lánccal kapcsolatos kockázatokról, a rendelkezésre álló védelmi stratégiákról és a programok alkalmazásának időpontjáról szóló képzési, oktatási és tudatosságnövelő programok biztosítását. A fejlesztési tervek, dokumentációk és bizonyítékok áttekintésére és védelmére szolgáló módszerek összemérhetőek az érintett szervezet biztonsági és adatvédelmi követelményeivel. A szerződések meghatározhatják a dokumentáció védelmi követelményeit.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell az ellátási láncból eredő kockázatokat.
2. A szervezetnek meg kell határoznia a beszerzési stratégiáit, amelyek segítenek kivédeni, azonosítani és csökkenteni az ellátási láncból eredő kockázatokat.
3. A szervezetnek alkalmaznia kell az ellátási láncból eredő kockázatok kivédésére, azonosítására és csökkentésére szolgáló beszerzési stratégiát.

4. A szervezetnek lehetősége van beszállítói lánccal kapcsolatos kockázatokról, a rendelkezésre álló védelmi stratégiákról biztonságtudatosságot növelő képzést biztosíthat a személyzet számára.

5. A szervezetnek dokumentálnia kell a beszerzési startégiát, az alkalmazott eszközöket és technikákat, melyeket rendszeresen felül kell vizsgálnia a változó fenyegetési környezet elleni eredményes védekezés érdekében.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

16.2. Erőforrások rendelkezésre állása

16.3.1. A rendszer fejlesztési életciklusa

16.7. Beszerzések

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

16.16. Biztonságtervezési elvek

16.49. Külső elektronikus információs rendszerek szolgáltatásai

16.58. Fejlesztői változáskövetés

16.76.1. Fejlesztési folyamat, szabványok és eszközök

19.16. Beszállítók értékelése és felülvizsgálata

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.20; A.5.21; A.5.23

NIST SP 800-53 rev.5 referencia

SR-5

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a beszerzési stratégia, szerződéses eszközök és beszerzési módszerek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.14. Beszerzési stratégiák, eszközök és módszerek – Megfelelő utánpótlás

19.14. A szervezet meghatározott követelményeket alkalmaz annak érdekében, hogy a meghatározott és a szervezet működése szempontjából kritikus rendszerelemek ellátása és utánpótlása megfelelő legyen.

Magyarázat

A támadók megpróbálhatják akadályozni az érintett szervezet működését azzal, hogy megszakítják a kritikus rendszerelemek ellátását vagy megzavarják a beszállítói műveleteket. A szervezetek nyomon követhetik az EIR-ek és az alkatrészek átlagos meghibásodási idejét, hogy enyhítsék az ideiglenes vagy végleges rendszerfunkció elvesztését. A kritikus rendszerelemek megfelelő ellátását biztosító védelmi intézkedések kiterjednek a több beszállító használatára az ellátási láncban az azonosított kritikus elemek számára, a tartalék elemek vagy alkatrészek felhalmozására, hogy biztosítsák a működést a szervezeti alapfeladatok szempontjából kritikus időszakokban, és a funkcionálisan azonos vagy hasonló elemek azonosítására, amelyeket szükség esetén fel lehet használni.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania kell a szervezet működése szempontjából kritikus rendszerelemeket.
2. A szervezetnek meg kell határoznia a követelményeket annak érdekében, hogy a szervezet működése szempontjából kritikus rendszerelemek ellátása és utánpótlása megfelelő legyen. Ez magában foglalhatja például a több beszállító használatát az ellátási láncban az azonosított kritikus elemek számára, a tartalék elemek felhalmozását, és a funkcionálisan azonos vagy hasonló elemek azonosítását.
3. A szervezetnek szükség esetén alkalmaznia kell a szervezet működése szempontjából kritikus rendszerelemek ellátására és utánpótlására szolgáló intézkedéseket, amennyiben szükséges.
4. A szervezetnek dokumentálnia kell a kritikus rendszerek vagy rendszerelemek ellátása és utánpótlása érdekében hozott intézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.21. Rendszerelemek kritikusságának elemzése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-5(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kritikus rendszerelemek, illetve a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

19.15. Beszerzési stratégiák, eszközök és módszerek – Kiválasztás, elfogadás, módosítás vagy frissítés előtti értékelések

19.15. A szervezet értékeli az EIR-t, rendszerelemet vagy rendszerszolgáltatást a kiválasztást, az elfogadást, a módosítást vagy a frissítést megelőzően.

Magyarázat

Az érintett szervezet személyzete vagy független, külső szereplők értékelik az EIR-t, rendszerelemeket, termékeket, eszközöket és szolgáltatásokat, annak érdekében, hogy azonosítsanak egy esetleges hamisítást, szándékosan és nem szándékosan bevezetett sérülékenységet, vagy a beszállítói lánc ellenőrzésével kapcsolatos hiányosságokat. Ezek lehetnek kártékony kódok, kártékony folyamatok, hibás szoftverek, hátsó ajtók és hamisítványok. Az értékelések magukban foglalhatnak egyéb értékeléseket; tervezési javaslatok felülvizsgálatát; vizuális vagy fizikai ellenőrzést; statikus és dinamikus elemzések; vizuális, röntgen vagy mágneses részecskét alkalmazó ellenőrzéseket; szimulációkat; white, gray vagy blackbox alapú tesztelést; fuzz alapú tesztelést; stressz tesztelést; és sérülékenységvizsgálatot. Az értékelések során keletkező bizonyítékokat dokumentálják, melyek szükségesek lehetnek a szervezet későbbi intézkedéseinek megtételéhez. Az ellátási lánc elemekről elvégzett értékelések során keletkezett bizonyítékokat fel lehet használni az ellátási lánc folyamatainak és kockázatmenedzsment folyamatainak támogatására. A bizonyítékokat fel lehet használni a további értékelésekben. A bizonyítékokat és az egyéb dokumentumokat meg is lehet osztani más szervezetekkel, amennyiben ezt a szervezet megállapodásai lehetővé teszik.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell bíznia a személyzetet vagy független, külső szereplőket az EIR, rendszerelem vagy rendszerszolgáltatás értékelésével a kiválasztást, az elfogadást, a módosítást vagy a frissítést megelőzően.

2. A szervezetnek dokumentálnia kell az értékelés során keletkezett bizonyítékokat, hogy azok felhasználhatóak legyenek a későbbi lépésekben pl. a kockázatmenedzsment folyamatainak támogatására.

3. A szervezetnek lehetősége van a bizonyítékok és dokumentumok megosztására más szervezetekkel. amennyiben erre lehetősége van.

4. A szervezetnek rendszeresen el kell végeznie az EIR, rendszerelemek és rendszerszolgálatások értékelését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.20. Behatolásvizsgálat (penetration testing)

15.10. Sérülékenységmonitorozás és szkennelés

16.66. Fejlesztői biztonsági tesztelés

18.42. Szoftver- és információsértetlenség

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.29

NIST SP 800-53 REV.5 REFERENCIA

SR-5(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

19.16. BESZÁLLÍTÓK ÉRTÉKELÉSE ÉS FELÜLVIZSGÁLATA

19.16. A szervezet meghatározott gyakorisággal értékeli és felülvizsgálja a beszállítókkal vagy szerződéses partnerekkel, illetve az általuk biztosított EIR-rel, rendszerelemmel vagy rendszerszolgáltatással kapcsolatos ellátási láncból eredő kockázatokat.

MAGYARÁZAT

Az érintett szervezet által elvégzett beszállítói kockázatértékelés és -felülvizsgálat magában foglalja a biztonsági és ellátási lánc kockázatkezelési folyamatait, a külföldi tulajdonlást, az irányítást vagy befolyást, valamint az ellátó képességét arra, hogy hatékonyan értékelje az alárendelt második és harmadik szintű beszállítókat és szerződéses partnereket. A felülvizsgálatokat a szervezet vagy egy független, harmadik fél végezheti. A felülvizsgálatok figyelembe veszik a dokumentált folyamatokat, a dokumentált követelményeket, az összes forrásból származó információt, és a beszállítóval vagy szerződéses partnerrel kapcsolatos, nyilvánosan elérhető információkat. A szervezetek nyílt forrású információkat is használhatnak arra, hogy figyelemmel kísérjék a lopott információkat, a gyenge fejlesztési és minőségellenőrzési gyakorlatokat, illetve az információszivárgás vagy a hamisítványokra utaló jeleket. Egyes esetekben érdemes vagy szükséges lehet az értékelések és felülvizsgálatok eredményeit megosztani más szervezetekkel. Ennek során figyelembe kell venni az erre vonatkozó szabályokat, szabályzatokat, vagy a szervezetek közötti megállapodásokat vagy szerződéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-hez kapcsolódó ellátási lánc-elemeket, folyamatokat és szereplőket.
2. A szervezetnek ki kell dolgoznia a kockázatkezelési programot, stratégiákat és végrehajtási terveket a meghatározott ellátási lánc-elemekhez, folyamatokhoz és szereplőkhöz. Ez magában foglalhatja a szervezeti és független harmadik fél által végzett elemzéseket és teszteket.
3. A szervezetnek alkalmaznia kell a meghatározott stratégiákat és végrehajtási terveket az érintett ellátási lánc-elemek, folyamatok és szereplők vizsgálatára.

4. A szervezetnek lehetősége van más szervezetekkel megosztani a beszállítók értékelésének és felülvizsgálatának eredményeit összhangban az alkalmazandó szabályokkal, irányelvekkel és szerződésekkel összhangban.

KAPCSOLÓDÓ INTÉZKEDÉSEK

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

19.13. Beszerzési stratégiák, eszközök és módszerek

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.5.22

NIST SP 800-53 REV.5 REFERENCIA

SR-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

19.17. BESZÁLLÍTÓ ÉRTÉKELÉSEK ÉS FELÜLVIZSGÁLATOK – TESZTELÉS ÉS ELEMZÉS

19.17. A szervezet az EIR-hez, rendszerelemhez vagy rendszerszolgáltatáshoz kapcsolódó, szervezet által meghatározott ellátási lánc-elemekkel, folyamatokkal és szereplőkkel kapcsolatosan szervezeti és független harmadik fél által végzett elemzéseket és teszteket alkalmaz.

MAGYARÁZAT

Az ellátási lánc-elemek magukban foglalják azokat a szervezeteket, szereplőket vagy eszközöket, amelyeket az EIR kutatására és fejlesztésére, tervezésére, gyártására, beszerzésére, szállítására, integrációjára, üzemeltetésére, karbantartására és selejtezésére használnak. Az ellátási lánc folyamatok közé tartoznak az ellátási lánc kockázatkezelési programok; személyi és fizikai biztonsági programok; hardver-, szoftver- és firmware-fejlesztési folyamatok; konfigurációs menedzsment eszközök, technikák és intézkedések az eredetiség biztosítására; szállítási és kezelési eljárások; valamint az ellátási lánc-elemek előállításával és terjesztésével kapcsolatos programok, folyamatok vagy eljárások. Az ellátási lánc szereplői olyan személyek, akiknek specifikus szerepük és felelősségük van az ellátási láncban. Az ellátási lánc-elemek, folyamatok és szereplők elemzése és tesztelése során előállított és gyűjtött bizonyítékokat dokumentálják, és ezeket felhasználják a szervezet kockázatkezelési tevékenységeinek és döntéseinek megalapozására.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-hez, rendszerelemhez, vagy rendszerszolgáltatáshoz kapcsolódó, ellátási lánc-elemeket, folyamatokat és szereplőket, melyeket vizsgálni szükséges.
2. A szervezetnek a meghatározott ellátási lánc-elemekre, folyamatokra és szereplőkre szervezeti és független harmadik fél által végzett elemzéseket és teszteket kell alkalmaznia.
3. A szervezetnek gondoskodnia kell róla, hogy az ellátási lánc-elemek, folyamatok és szereplők elemzése és tesztelése során előállított és gyűjtött bizonyítékokat dokumentálják.

4. A szervezetnek fel kell használnia a bizonyítékokat kockázatkezelési tevékenységeinek és döntéseinek megalapozására.

Kapcsolódó intézkedések

5.20. Behatolásvizsgálat (penetration testing)

18.13. Az EIR monitorozása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SR-6(1)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az ellátási lánc-elemek, folyamatok és szereplők meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

19.18. ELLÁTÁSI LÁNC MŰKÖDÉSBIZTONSÁGA (OPSEC)

19.18. A szervezet meghatározott működésbiztonsági (OPSEC) kontrollokat alkalmaz annak érdekében, hogy védje az EIR-hez, rendszerelemhez vagy rendszerszolgáltatáshoz köthető, ellátási lánchoz kapcsolódó információkat.

MAGYARÁZAT

Az ellátási lánc működésbiztonsága kiterjeszti a működésbiztonsága (OPSEC) hatókörét a beszállítókra és potenciális beszállítókra is. A működésbiztonság egy folyamat, amely magában foglalja a kritikus információk azonosítását, az ismert szereplők műveleteivel kapcsolatos tevékenységek elemzését azon a cselekvések azonosításához, amelyeket a potenciális támadók megfigyelhetnek, azon indikátorok meghatározását, amelyeket rosszindulatú támadók megszerezhetnek, és amelyeket össze lehetne illeszteni, vagy értelmezni annak érdekében, hogy kárt okozzanak a szervezeteknek, védelmi intézkedések vagy ellenintézkedések alkalmazását a kihasználható sebezhetőségek és a kockázat elfogadható szintre csökkentése érdekében, és annak figyelembe vételét, hogy az összegyűjtött információk hogyan tehetik ki veszélynek a felhasználókat vagy az ellátási lánc specifikus részeit. Az ellátási lánc információi közé tartoznak a felhasználói azonosítók; az EIR, a rendszerelemek és a rendszerszolgáltatások felhasználása; a beszállítók azonosítói; biztonsági és adatvédelmi követelmények; az EIR-ek és az rendszerelemek konfigurációi; a beszállítói folyamatok; a tervezési specifikációk; és a tesztelési és értékelési eredmények. Az ellátási lánc működésbiztonsága megkövetelheti az érintett szervezetektől, hogy tartsák vissza a küldetési vagy üzleti információkat a beszállítóktól, és magában foglalhatja a közvetítők használatát annak érdekében, hogy elrejtsék az EIR-ek, a rendszerelemek, vagy a rendszerszolgáltatások végső felhasználását vagy felhasználóit. .

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-hez, rendszerelemhez vagy rendszerszolgáltatáshoz köthető, ellátási lánchoz kapcsolódó információkat, melyeket védeni szükséges.

2. A szervezetnek meg kell határoznia olyan működésbiztonsági intézkedéseket, melyekkel megvédheti az érintett EIR-hez, rendszerelemhez vagy rendszerszolgáltatáshoz köthető, ellátási lánchoz kapcsolódó információkat.
3. A szervezetnek alkalmaznia kell a meghatározott működésbiztonsági intézkedéseket az érintett EIR-hez, rendszerelemhez vagy rendszerszolgáltatáshoz köthető, ellátási lánchoz kapcsolódó információkra.
4. A szervezetnek rendszeres időnként felül kell vizsgálnia a működésbiztonsági követelményeket és azok megvalósítását, a változó fenyegetési környezet elleni folyamatos, hatékony védelem biztosítása érdekében.

Kapcsolódó intézkedések

17.107. Működésbiztonság

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.22

NIST SP 800-53 rev.5 referencia

SR-7

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a működésbiztonsági (OPSEC) kontrollok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

19.19. ÉRTESÍTÉSI MEGÁLLAPODÁSOK

19.19. A szervezet megállapodásokat köt és eljárásokat hoz létre a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezetekkel.

MAGYARÁZAT

Az egyezmények és eljárások létrehozása elősegíti a beszállítói láncban részt vevő szervezetek közötti kommunikációt. Az EIR, rendszerelemek vagy rendszerszolgáltatásokat negatívan befolyásoló vagy befolyásolható támadások és potenciális támadásokra figyelmeztető korai értesítése elengedhetetlen, hogy a szervezet hatékonyan reagálhasson az ilyen eseményekre. A felmérések vagy naplók eredményei tartalmazhatnak nyílt forrású információkat, amelyek hozzájárultak egy döntéshez vagy eredményhez, és segíthetnek a beszállítói láncban részt vevő szervezetnek megoldani egy problémát vagy javítani a folyamatait.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a beszállítói láncában részt vevő szervezeteket.
2. A szervezetnek megállapodásokat kell kötnie a beszállítói láncában részt vevő szervezetekkel, amelyek meghatározzák a felelősségi köröket, a biztonsági követelményeket és a kommunikációs protokollokat.
3. A szervezetnek rendszeresen naplót kell vezetnie a beszállítói láncának értékeléséről vagy auditálásáról.
4. A szervezetnek biztosítania kell, hogy az EIR rendelkezik a rendszerelemeket vagy rendszerszolgálatásokat potenciálisan bekövetkező támadásokra való előrejelző figyelmeztetési képességgel.
5. A szervezetnek lehetősége van a fenti eljárások és technikák segítségével javítania a beszállítói láncot ért biztonsági eseményekre való szervezeti reagálást.

KAPCSOLÓDÓ INTÉZKEDÉSEK

9.9.1. Biztonsági események kezelése

9.27. A biztonsági események jelentése

9.34. Biztonsági eseménykezelési terv

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információ meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.20. HAMISÍTÁS ELLENI VÉDELEM

19.20. A szervezet hamisítás elleni védelmi programot vezet be a rendszer, rendszerelem vagy rendszerszolgáltatás védelmére.

MAGYARÁZAT

A hamisítás elleni technológiák, eszközök és technikák védelmet nyújtanak az EIR, rendszerelemek és rendszerszolgáltatások számára számos fenyegetéssel szemben, beleértve a visszafejtést, módosítást és helyettesítést. Az erős azonosítás kombinálva a hamisítás elleni védelemmel és/vagy a hamisítás észlelésével elengedhetetlen az EIR és a rendszerelemek védelmében a terjesztés során és használat közben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely rendszerelemeket és rendszerszolgáltatásokat kell védeni a hamisítás ellen.
2. A szervezetnek be kell vezetnie a hamisítás elleni technológiákat, eszközöket és technikákat.
3. A szervezetnek erős azonosítási rendszert kell bevezetnie, amely kombinálva a hamisítás elleni védelemmel és/vagy a hamisítás észlelésével hatékony védelmet jelenthet az érintett rendszerelemek és rendszerszolgáltatások védelmében.
4. A szervezetnek rendszeresen felül kell vizsgálnia az általa alkalmazott hamisítás elleni védelemi programot, annak érdekében, hogy naprakészek legyenek a benne meghatározott követelmények és intézkedések.

KAPCSOLÓDÓ INTÉZKEDÉSEK

12.6. A fizikai belépés ellenőrzése
1.21. Ellátási lánc kockázatkezelési stratégiája
16.76.1. Fejlesztési folyamat, szabványok és eszközök
18.13. Az EIR monitorozása
18.42. Szoftver- és információsértetlenség
19.4. Ellátási láncra vonatkozó követelmények és folyamatok
19.8. Rendszerelemek és kapcsolódó adatok eredetisége
19.13. Beszerzési stratégiák, eszközök és módszerek

19.22. Rendszerek vagy rendszerelemek vizsgálata

19.23. Rendszerelem hitelessége

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

19.21. HAMISÍTÁS ELLENI VÉDELEM - RENDSZERFEJLESZTÉSI ÉLETCIKLUS

19.21. A szervezet hamisítás elleni technológiákat, eszközöket és technikákat alkalmaz a teljes rendszerfejlesztési életciklus során.

MAGYARÁZAT

Az EIR fejlesztési életciklusa magában foglalja a kutatást és fejlesztést, a tervezést, a gyártást, a beszerzést, a szállítást, az integrációt, az üzemeltetést és karbantartást, valamint a selejtezést. Az érintett szervezetek hardver- és szoftvertechnikákat alkalmaznak a hamisítás elleni védelem és felderítés érdekében. A szervezetek obfuszkáció és önvizsgálatot használnak, hogy a visszafejtést és a módosításokat nehezebbé, időigényesebbé és költségesebbé tegyék a támadók számára. Az EIR és a rendszerelemek testreszabása megkönnyítheti a cserék észlelését, és így korlátozhatja a károkat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a hamisítás elleni technológiákat, eszközöket és technikákat, az EIR-ek, rendszerelemek és rendszerszolgáltatások védelmére.
2. A szervezetnek alkalmaznia kell a meghatározott technológiákat, eszközöket és technikákat a teljes rendszerfejlesztési életciklus során.
3. A szervezetnek lehetősége van hardver- és szoftvertechnikákat alkalmaznia a hamisítás felfedése és az az elleni védelem érdekében.
4. A szervezetnek biztosítania kell az EIR-ek és rendszerelemek testreszabását, annak érdekében, hogy a cserék észlelését megkönnyítse.

KAPCSOLÓDÓ INTÉZKEDÉSEK

16.3.1. A rendszer fejlesztési életciklusa

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-9(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

19.22. RENDSZEREK VAGY RENDSZERELEMEK VIZSGÁLATA

19.22. A szervezet eseti jelleggel vagy meghatározott gyakorisággal és meghatározott esetekben ellenőrzi A EIR-eket vagy rendszerelemeket az esetleges hamisítás felderítése érdekében.

MAGYARÁZAT

Az EIR-ek vagy rendszerelemek hamisítással kapcsolatos ellenállóképességének és felderítésének ellenőrzése a fizikai és logikai hamisítást érinti, mely az érintett szervezet által ellenőrzött területekről eltávolított EIR-ekre és rendszerelemekre vonatkozik. Az ellenőrzés szükségességére utaló jelek közé tartozik a csomagolás, a specifikációk, a gyár helyszínének vagy az alkatrész beszerzéséért felelős entitás változása, valamint amikor személyek magas kockázati besorolással rendelkező helyszínekről térnek vissza.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia mely rendszerelemeket szükséges ellenőrizni a hamisítás felderítésének érdekében.
2. A szervezetnek szükség esetén meg kell határoznia milyen gyakorisággal ellenőrzi a meghatározott rendszerelemeket a hamisítás felderítésének érdekében.
3. A szervezetnek alkalmaznia kell a meghatározott rendszerelemek vizsgálatát az általa meghatározott ellenőrzés szükségességére utaló jelek észlelése esetekben.
4. A szervezetnek dokumentálnia kell a meghatározott ellenőrzés szükségességére utaló jeleket, és valamennyi elvégzett ellenőrzést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.9. Szerepkör alapú biztonsági képzés
1.21. Ellátási lánc kockázatkezelési stratégiája
18.13. Az EIR monitorozása
18.42. Szoftver- és információsértetlenség
19.4. Ellátási láncra vonatkozó követelmények és folyamatok
19.8. Rendszerelemek és kapcsolódó adatok eredetisége
19.13. Beszerzési stratégiák, eszközök és módszerek
19.20. Hamisítás elleni védelem

19.23. Rendszerelem hitelessége

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság, illetve az átvizsgálás szükségességre utaló jelek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.23. RENDSZERELEM HITELESSÉGE

19.23. A szervezet:

19.23.1. kialakítja és bevezeti a hamisítás elleni szabályokat és eljárásokat, amelyek magukban foglalják a hamisított rendszerelemek észlelését és annak megelőzését, hogy ezek bejussanak az EIR-be; valamint

19.23.2. jelenti a hamisított rendszerelemeket és azok forrását a szervezet által meghatározott külső szervezeteknek, illetve a szervezet által meghatározott személyeknek vagy szerepköröknek.

MAGYARÁZAT

Hamisított alkatrészek érkezhetnek gyártóktól, fejlesztőktől, szállítóktól és szerződéses partnerektől. A hamisítás elleni szabályok és eljárások támogatják a hamisítás elleni védelmet, valamint további védelmet biztosítanak a kártékony kódok ellen is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell alakítania a hamisítás elleni szabályokat és eljárásokat.

2. A szervezetnek jelentenie kell a hamisított rendszerelemeket és azok forrását a szervezet által meghatározott személyeknek vagy szerepköröknek.

3. A szervezetnek dokumentálnia kell, amennyiben hamisított rendszerelemeket vagy alkatrészeket fedez fel és fel kel vennie a kapcsolatot a hamisított alkatrész forrásával, vagy az illetékes hatósággal.

KAPCSOLÓDÓ INTÉZKEDÉSEK

12.6. A fizikai belépés ellenőrzése

16.7. Beszerzések

18.42. Szoftver- és információsértetlenség

19.20. Hamisítás elleni védelem

19.22. Rendszerek vagy rendszerelemek vizsgálata

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-11

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.24. RENDSZERELEM HITELESSÉGE – HAMISÍTÁS ELLENI KÉPZÉS

19.24. A szervezet a meghatározott személyeknek vagy szerepköröknek képzést biztosít a hamisított rendszerelemek (beleértve a hardvert, szoftvert és firmware-t) felismerésére.

MAGYARÁZAT

Az érintett szervezetnek meg kell határozni a rendszerek felügyeletéért felelős szerepköröket, majd ezen szerepkörök részére olyan képzési programokat kell kialakítania és végrehajtania, amelyek segítenek megérteni és felismerni a hamisított rendszerelemeket. A képzésnek magában kell foglalnia a hamisított hardverek, szoftverek és firmware-ek felismerésének módszereit és technikáit. A képzésnek részletesnek kell lennie, és magában kell foglalnia a hamisított EIR-ekkel kapcsolatos legújabb trendeket és fenyegetéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely személyek vagy szerepkörök felelősek az rendszerek felügyeletéért és kezeléséért.
2. A szervezetnek ki kell dolgoznia egy képzési programot, amely részletesen bemutatja, hogyan lehet felismerni a hamisított hardvert, szoftvert és firmware-t.
3. A szervezetnek implementálnia kell a képzési programot, és biztosítania kell, hogy a meghatározott személyek vagy szerepkörök részt vesznek a képzésen.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.9. Szerepkör alapú biztonsági képzés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-11(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.25. Rendszerelem hitelessége – Konfigurációfelügyelet

19.25. A szervezet fenntartja a konfiguráció felügyeletét a meghatározott szervizelésre vagy javításra váró vagy olyan rendszerelemek esetén, amelyeket szervizeltek vagy javítottak, és arra várnak, hogy újból üzembe állítsák őket.

Magyarázat

A konfigurációfelügyelet magában foglalja a változások naplózását, amelyeket a rendszerelemen végeznek, beleértve a szervizelést és a javítást is. A naplózás lehetővé teszi az érintett szervezet számára, hogy nyomon követhesse a rendszerelem teljes élettartamát, és biztosítsa, hogy minden változást megfelelően dokumentálnak és ellenőriznek.

A követelmény alkalmazásának lépései

1. A szervezetnek nyilvántartást kell vezetnie a rendszerelemekről, amelyek szervizelésre vagy javításra várnak, vagy amelyeket már szervizeltek vagy javítottak, és arra várnak, hogy újból üzembe állítsák őket.
2. A szervezetnek ki kell dolgoznia egy konfiguráció felügyeleti rendszert, mely lehetővé teszi a konfiguráció felügyeletét a meghatározott rendszerelemekre.
3. A szervezetnek alkalmaznia kell a meghatározott felügyeleti rendszert a meghatározott rendszerelemekre.
4. A szervezetnek minden egyes rendszerelemen elvégzett módosítást naplóznia kell, hogy nyomon követhetőek legyenek a változások a rendszerelem teljes életciklusa alatt.

Kapcsolódó intézkedések

6.7. A konfigurációváltozások felügyelete (változáskezelés)

10.2. Szabályozott karbantartás

10.11. Távoli karbantartás

16.58. Fejlesztői változáskövetés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-11(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

19.26. RENDSZERELEM HITELESSÉGE – HAMISÍTÁS ELLENI INTÉZKEDÉSEK

19.26. A szervezet meghatározott gyakorisággal ellenőrzi rendszerét a hamisított rendszerelemek után kutatva.

MAGYARÁZAT

A rendszerelem típusától függ, hogy milyen ellenőrzést kell elvégezni rajta. Például, ha a rendszerelem egy webalkalmazás, akkor webalkalmazás-vizsgálatot kell végezni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a vizsgálandó rendszerelemeket és azok típusát.
2. A szervezetnek meg kell határoznia egy rendszeres ellenőrzési ütemtervet, amely meghatározza, hogy milyen gyakran kell ellenőrizni a rendszert hamisított rendszerelemek után kutatva.
3. A szervezetnek végre kell hajtania a szükséges vizsgálatokat a meghatározott gyakorisággal.
4. A szervezetnek dokumentálnia kell valamennyi elvégzett vizsgálatot és azok eredményét és amennyiben hamisítás jeleit fedezi fel meg kell határoznia a válaszintézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.10. Sérülékenységmonitorozás és szkennelés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-11(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

19.27. RENDSZERELEM SELEJTEZÉSE, MEGSEMMISÍTÉSE

19.27. A szervezet meghatározott technikákkal és módszerekkel selejtezi a meghatározott adatokat, dokumentációkat, eszközöket és rendszerelemeket.

MAGYARÁZAT

Az adatok, dokumentációk, eszközök vagy rendszerelemek bármikor selejtezhetők a rendszerfejlesztési életciklus során. Például a selejtezés megtörténhet a kutatás és fejlesztés, tervezés, prototípus készítés vagy üzemeltetés/karbantartás során és magában foglalhat olyan módszereket, mint a lemez tisztítása, a kriptográfiai kulcsok eltávolítása, az alkatrészek részleges újrafelhasználása. A selejtezés során bekövetkezett esetleges kompromittálódás érinti a fizikai és logikai adatokat, beleértve a papíralapú vagy digitális formában meglévő rendszerdokumentációt; a szállítással és kézbesítéssel kapcsolatos dokumentációt; a szoftverkóddal rendelkező memóriakártyákat; illetve routereket vagy szervereket, amelyek állandó adathordozóval rendelkeznek és bizalmas, vagy védett információkat tartalmazhatnak. Emellett az rendszerelemek megfelelő selejtezése segít megakadályozni, hogy az említett elemekkel kétes eredetű árukat forgalmazó piactereken kereskedjenek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely adatokat, dokumentációkat, eszközöket és rendszerelemeket kell selejteznie.
2. A szervezetnek ki kell dolgoznia egy módszertant és technikákat a selejtezésre.
3. A szervezetnek alkalmaznia kell a kidolgozott selejtezési módszertant a selejtezére szoruló rendszerelemekre.
4. A szervezetnek dokumentálnia kell a selejtezést és annak tárgyát képező rendszerelemet, alkatrészt vagy adatot, valamint gondoskodnia kell az érintett elemek kivezetéséről rendszerelem leltárból.

KAPCSOLÓDÓ INTÉZKEDÉSEK

11.8. Adathordozók törlése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SR-12

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az adatok, dokumentáció, eszközök vagy rendszerelemek, illetve a technikák és módszerek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024